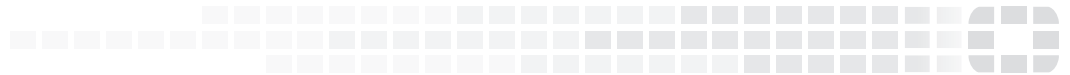


**FORTINET®**  
High Performance Network Security



# FortiWAN - Handbook

VERSION 4.5.5



## **FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

## **FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

## **FORTINET BLOG**

<https://blog.fortinet.com>

## **CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

## **FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

## **FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

## **FORTIGUARD CENTER**

<http://www.fortiguard.com>

## **END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

## **FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



September 25, 2018

FortiWAN 4.5.5 Handbook Revision 1

38-455-514922-20180925

# TABLE OF CONTENTS

|                                                               |           |
|---------------------------------------------------------------|-----------|
| <b>Introduction</b>                                           | <b>8</b>  |
| Product Benefits                                              | 8         |
| Key Concepts and Product Features                             | 10        |
| WAN load balancing (WLB)                                      | 10        |
| Installation                                                  | 10        |
| Bidirectional load balancing                                  | 10        |
| Auto Routing (Outbound Load Balancing)                        | 10        |
| Multihoming (Inbound Load Balancing)                          | 11        |
| Fall-back or Fail-over                                        | 11        |
| Virtual Private Services (Tunnel Routing)                     | 11        |
| Virtual Servers (Server Load Balancing and High Availability) | 11        |
| Optimum Routing                                               | 11        |
| Traffic Shaping (Bandwidth Management)                        | 11        |
| Firewall and Security                                         | 11        |
| Scope                                                         | 12        |
| Installation                                                  | 12        |
| Functions                                                     | 12        |
| Monitoring                                                    | 12        |
| <b>What's new</b>                                             | <b>13</b> |
| <b>Document enhancements</b>                                  | <b>23</b> |
| <b>How to set up your FortiWAN</b>                            | <b>29</b> |
| Registering your FortiWAN                                     | 29        |
| Planning the network topology                                 | 29        |
| Glossary for FortiWAN network setting                         | 29        |
| WAN, LAN and DMZ                                              | 30        |
| Network interfaces and port mapping                           | 31        |
| WAN link and WAN port                                         | 33        |
| WAN types: Routing mode and Bridge mode                       | 34        |
| Near WAN                                                      | 37        |
| Public IP Pass-through (DMZ Transparent Mode)                 | 38        |
| Scenarios to deploy subnets                                   | 39        |
| VLAN and port mapping                                         | 40        |
| IPv6/IPv4 Dual Stack                                          | 40        |
| FortiWAN in HA (High Availability) Mode                       | 41        |

|                                                             |            |
|-------------------------------------------------------------|------------|
| Web UI and CLI Overview.....                                | 45         |
| Connecting to the Web UI and the CLI.....                   | 45         |
| Using the Web UI.....                                       | 49         |
| Console Mode Commands.....                                  | 53         |
| Automated Local Configuration.....                          | 68         |
| <b>Configuring Network Interface (Network Setting).....</b> | <b>73</b>  |
| Set DNS server to FortiWAN.....                             | 73         |
| Aggregated, Redundant, VLAN Ports and Port Mapping.....     | 75         |
| Configuring networks to FortiWAN.....                       | 87         |
| Configuring your WAN and DMZ.....                           | 88         |
| Routing-mode WAN link.....                                  | 94         |
| Bridge-mode (multiple static IP) WAN link.....              | 109        |
| Bridge-mode (one static IP) WAN link.....                   | 114        |
| Configurations for a WAN link in Bridge Mode: PPPoE.....    | 117        |
| Configurations for a WAN link in Bridge Mode: DHCP.....     | 118        |
| LAN Private Subnet.....                                     | 119        |
| WAN/DMZ Private Subnet.....                                 | 124        |
| Automatic addressing within a basic subnet.....             | 129        |
| Deployment Scenarios for Various WAN Types.....             | 139        |
| MIB fields for WAN links and VLANs.....                     | 147        |
| <b>System Configurations.....</b>                           | <b>152</b> |
| Dashboard.....                                              | 152        |
| Optimum Route Detection.....                                | 161        |
| Port Speed/Duplex Settings.....                             | 166        |
| Backup Line Settings.....                                   | 167        |
| IP Grouping.....                                            | 168        |
| Service Grouping.....                                       | 170        |
| Busyhour Settings.....                                      | 170        |
| Diagnostic Tools.....                                       | 171        |
| Setting the system time & date.....                         | 174        |
| Remote Assistance.....                                      | 174        |
| Administration.....                                         | 175        |
| Administrator and Monitor Password.....                     | 175        |
| RADIUS Authentication.....                                  | 176        |
| Firmware Update (via Web UI).....                           | 177        |
| Firmware Upgrade/Downgrade via CLI.....                     | 178        |
| Configuration File.....                                     | 180        |
| Maintenance.....                                            | 182        |
| Web UI Port.....                                            | 182        |
| License Control.....                                        | 184        |
| Login Session Management.....                               | 184        |
| <b>Load Balancing &amp; Fault Tolerance.....</b>            | <b>186</b> |

|                                                          |            |
|----------------------------------------------------------|------------|
| Load Balancing Algorithms.....                           | 186        |
| Round Robin (weighted).....                              | 187        |
| By Connection.....                                       | 187        |
| By Downstream Traffic.....                               | 189        |
| By Upstream Traffic.....                                 | 189        |
| By Total Traffic.....                                    | 190        |
| By Optimum Route.....                                    | 191        |
| By Response Time.....                                    | 191        |
| By Static.....                                           | 191        |
| By Fixed.....                                            | 191        |
| Fail-Over.....                                           | 192        |
| Hash.....                                                | 192        |
| Outbound Load Balancing and Failover (Auto Routing)..... | 193        |
| Auto Routing Mechanism.....                              | 193        |
| Fault Tolerance Mechanism.....                           | 193        |
| Configurations.....                                      | 195        |
| Inbound Load Balancing and Failover (Multihoming).....   | 201        |
| Multihoming.....                                         | 201        |
| Introduction to DNS.....                                 | 201        |
| SwiftDNS.....                                            | 202        |
| How does SwiftDNS work?.....                             | 202        |
| Prerequisites for Multihoming.....                       | 203        |
| DNSSEC Support.....                                      | 203        |
| Relay Mode.....                                          | 204        |
| Enable Backup.....                                       | 204        |
| Configurations.....                                      | 204        |
| Scenarios.....                                           | 222        |
| Tunnel Routing.....                                      | 226        |
| How the Tunnel Routing Works.....                        | 227        |
| Tunnel Routing - Setting.....                            | 234        |
| How to set up routing rules for Tunnel Routing.....      | 241        |
| Tunnel Routing - Benchmark.....                          | 247        |
| Scenarios.....                                           | 249        |
| Virtual Server & Server Load Balancing.....              | 260        |
| WAN Link Health Detection.....                           | 267        |
| <b>IPSec.....</b>                                        | <b>270</b> |
| IPSec VPN Concepts.....                                  | 270        |
| IPSec VPN overview.....                                  | 271        |
| IPSec key exchange.....                                  | 272        |
| How IPSec VPN Works.....                                 | 276        |
| IPSec set up.....                                        | 277        |
| About FortiWAN IPSec VPN.....                            | 277        |

|                                                      |            |
|------------------------------------------------------|------------|
|                                                      | 279        |
| Limitation in the IPsec deployment .....             | 279        |
| Planning your VPN.....                               | 282        |
| IPsec VPN in the Web UI.....                         | 283        |
| Define routing policies for an IPsec VPN.....        | 298        |
| Establish IPsec VPN with FortiGate.....              | 307        |
| <b>Optional Services.....</b>                        | <b>315</b> |
| Firewall.....                                        | 315        |
| NAT.....                                             | 318        |
| Persistent Routing.....                              | 324        |
| Bandwidth Management.....                            | 327        |
| Inbound BM and Outbound BM.....                      | 327        |
| Managing Bandwidth for Tunnel Routing and IPsec..... | 329        |
| Scenarios.....                                       | 331        |
| Connection Limit.....                                | 336        |
| Cache Redirect.....                                  | 337        |
| Internal DNS.....                                    | 340        |
| DNS Proxy.....                                       | 343        |
| SNMP.....                                            | 350        |
| IP MAC Mapping.....                                  | 352        |
| <b>Statistics.....</b>                               | <b>353</b> |
| Traffic.....                                         | 353        |
| Bandwidth management statistics.....                 | 353        |
| Persistent Routing.....                              | 355        |
| WAN Link Health Detection.....                       | 356        |
| Dynamic IP WAN Link.....                             | 356        |
| DHCP Lease Information.....                          | 357        |
| RIP & OSPF Status.....                               | 358        |
| Connection Limit.....                                | 358        |
| Virtual Server Status.....                           | 358        |
| FQDN.....                                            | 359        |
| Tunnel Status.....                                   | 359        |
| Tunnel Traffic.....                                  | 361        |
| IPsec.....                                           | 361        |
| Traffic Statistics for Tunnel Routing and IPsec..... | 363        |
| <b>Logs.....</b>                                     | <b>366</b> |
| Log View.....                                        | 366        |
| Log format.....                                      | 367        |
| Log Control.....                                     | 374        |
| Notification.....                                    | 375        |
| Enable Reports.....                                  | 378        |
| <b>Reports.....</b>                                  | <b>379</b> |

|                                                                 |            |
|-----------------------------------------------------------------|------------|
| Create a Report .....                                           | 380        |
| Export and Email .....                                          | 381        |
| Device Status .....                                             | 381        |
| Bandwidth .....                                                 | 381        |
| CPU .....                                                       | 382        |
| Session .....                                                   | 383        |
| WAN Traffic .....                                               | 383        |
| WAN Reliability .....                                           | 384        |
| WAN Status .....                                                | 384        |
| TR Reliability .....                                            | 384        |
| TR Status .....                                                 | 385        |
| Bandwidth Usage .....                                           | 385        |
| Inclass .....                                                   | 386        |
| Outclass .....                                                  | 387        |
| WAN .....                                                       | 388        |
| Services .....                                                  | 389        |
| Internal IP .....                                               | 390        |
| Traffic Rate .....                                              | 391        |
| Function Status .....                                           | 392        |
| Connection Limit .....                                          | 392        |
| Firewall .....                                                  | 392        |
| Virtual Server .....                                            | 393        |
| Multihoming .....                                               | 393        |
| Advanced Functions of Reports .....                             | 394        |
| Drill In .....                                                  | 394        |
| Custom Filter .....                                             | 398        |
| Export .....                                                    | 401        |
| Report Email .....                                              | 401        |
| Reports Database Tool .....                                     | 403        |
| Reports Settings .....                                          | 411        |
| Reports .....                                                   | 412        |
| IP Annotation .....                                             | 412        |
| Email Server .....                                              | 413        |
| Scheduled Emails .....                                          | 414        |
| Disk Space Control .....                                        | 414        |
| Database Data Utility .....                                     | 415        |
| Filter the negligible traffic off .....                         | 416        |
| <b>Appendix A: Default Values .....</b>                         | <b>418</b> |
| <b>Appendix B: Suggested Maximum Configuration Values .....</b> | <b>421</b> |
| <b>Appendix C: What if your password is lost? .....</b>         | <b>426</b> |

# Introduction

Enterprises are increasingly relying on the internet for delivery of critical components for everyday business operations. Any delays or interruptions in connectivity can easily result in reduced productivity, lost business opportunities and a damaged reputation. Maintaining a reliable and efficient internet connection to ensure the operation of critical applications is therefore key to the success of the enterprise.

FortiWAN is a separate and discrete hardware appliance with exclusive operating system, specifically designed to intelligently balance internet and intranet traffic across multiple WAN connections, providing additional low-cost incoming and outgoing bandwidth for the enterprise and substantially increased connection reliability. FortiWAN is supported by a user-friendly UI and a flexible policy-based performance management system.

FortiWAN provides a unique solution that offers comprehensive multi-WAN management that keeps costs down as well as keeping customers and users connected.

## Product Benefits

### **FortiWAN is the most robust, cost-effective way to:**

- Increase the performance of your:
  - Internet access
  - Public-to-Enterprise access
  - Site-to-site private intranet
- Lower Operating Costs
- Increase your network reliability
- Enable Cloud / Web 2.0 Applications
- Monitor Network Performance

### **Increase Network Performance**

FortiWAN increases network performance in three key areas:

- Access to Internet resources from the Enterprise
- Access to Enterprise resources from the Internet
- Creation of Enterprise Intranet connections between sites

FortiWAN intelligently aggregates multiple broadband and/or leased access lines to significantly increase Internet access performance. FortiWAN makes reacting to network demands fast, flexible and inexpensive. FortiWAN transforms underperforming networks into responsive, cost-effective and easy-to-manage business assets.

FortiWAN load balances Internet service requests from Enterprise users, optimally distributing traffic across all available access links. FortiWAN's 7 different Load Balancing algorithms provide the flexibility to maximize productivity from any network scenario.

FortiWAN gives you high-performance inter-site connectivity without the need to lease expensive links such as T1 and T3. FortiWAN aggregates multiple low-cost Internet access links to create site-to-site Virtual Private Line



(VPL) Tunnels for LAN-like performance between company locations. By using multiple carriers and media, reliability of these VPL Tunnels can exceed that of traditional engineered carrier links.

## Substantially Lower Operating Costs

Once bandwidth requirements exceed traditional asymmetrical Internet access services (like ADSL) there is a very high jump in bandwidth cost to engineered, dedicated access facilities like DS-1/DS-3. Even Metro Ethernet is a large cost increment where it is available. Adding shared Internet access links is substantially less expensive and delivery is substantially faster.

Traditional point-to-point private lines for company intranets are still priced by distance and capacity. Replacing or augmenting dedicated point-to-point services with Virtual Private Line Tunnels reduces costs substantially while increasing available bandwidth and reliability.

FortiWAN makes low-cost network access links behave and perform like specially-engineered carrier services at a fraction of the cost.

- Deploy DSL services and get DS-3/STM-1-like speed and reliability while waiting for the carrier to pull fiber.
- Add and remove bandwidth for seasonal requirements quickly and easily.
- Increase bandwidth to web servers and use multiple ISPs without BGP4 management issues.

## Increase Network Reliability

Businesses can no longer afford Internet downtime. FortiWAN provides fault tolerance for both inbound and outbound IP traffic to ensure a stable and dependable network. Even multiple link failures, while reducing available bandwidth, will not stop traffic. By using diverse media (fiber, copper, wireless) and multiple ISPs (Telco, Cableco, 4G), FortiWAN can deliver better than carrier-class “5-9’s” reliability.

FortiWAN can be deployed in High Availability mode with fully redundant hardware for increased reliability. Larger FortiWAN models also feature redundant power supplies for further protection from hardware failures.

## Enable Cloud / Web 2.0 Applications

Traditional WAN Optimization products expect that all users connect only to Headquarters servers and Internet gateways over dedicated, symmetric leased lines, but that is already “yesterday’s” architecture. Today users want to mix HQ connectivity with direct Cloud access to Web 2.0 applications like email, collaborative documentation, ERP, CRM and online backup.

FortiWAN gives you the flexibility to customize your network, giving you complete control. Direct cloud-based applications to links optimized for them and reduce the bandwidth demand on expensive dedicated circuits. Combine access links and/or dedicated circuits into Virtual Private Line Tunnels that will support the fastest video streaming or video conferencing servers that Headquarters can offer.

FortiWAN is designed for easy deployment and rapid integration into any existing network topology.

## Monitor Network Performance

FortiWAN provides comprehensive monitoring and reporting tools to ensure your network is running at peak efficiency. With the built-in storage and database, FortiWAN's Reports function provides historical detail and reporting over longer periods of time, so that it not only allows management to react to network problems, but to plan network capacity, avoiding unnecessary expense while improving network performance.

FortiWAN is managed via a powerful Web User Interface. Configuration changes are instantly stored without the need to re-start the system. Configuration files can be backed-up and restored remotely. Traffic measurements, alarms, logs and other management data are stored for trend analysis and management overview.

## Key Concepts and Product Features

### WAN load balancing (WLB)

General speaking, load balancing are mechanisms (methods) for managing (distributing) workload across available resources, such as servers, computers, network links, CPU or disk storage. The FortiWAN's WAN load balancing aims to distribute (route) WAN traffic across multiple network links. The major purposes are optimizing bandwidth usage, maximizing transmission throughput and avoiding overload of any single network link. When we talk about WAN load balancing, it always implies automatic traffic distribution across multiple network links. Different from general routing, WAN load balancing involves algorithms, calculations and monitoring to dynamically determine the availability of network links for network traffic distribution.

### Installation

FortiWAN is an edge device that typically connects an internal local area network (LAN) with an external wide area network (WAN) or the Internet. The physical network ports on FortiWAN are divided into WAN ports, LAN ports and DMZ (Demilitarized Zone) ports, which are used to connect to the WAN or the Internet, subnets in LAN, and subnets in DMZ respectively. Please refer to FortiWAN QuickStart Guides for the ports mapping for various models.

### Bidirectional load balancing

Network data transmission passing through FortiWAN is bidirectional that are inbound and outbound. Network data transmission contains session establish and packet transmission. An inbound session refers to the session which is established from elsewhere (external) to the FortiWAN (internal), while an outbound session refers to the session which is established from the FortiWAN (internal) to elsewhere (external). For example, a request from the internal network to a HTTP server on the Internet means the first asking packet is outgoing to the external server, which is an outbound session established. Inversely, a request from the external area to a HTTP server behind FortiWAN means the first asking packet is incoming to the internal server, which is an inbound session established. No matter which direction a session is established in, packets transmission might be bidirectional (depends on the transmission protocol employed). FortiWAN is capable of balancing not only outbound but also inbound sessions and packets across multiple network links.

### Auto Routing (Outbound Load Balancing)

FortiWAN distributes traffic across as many as 50 WAN links, under control of load balancing algorithms. FortiWAN's many advanced load balancing algorithms let you easily fine-tune how traffic is distributed across the available links. Each deployment can be fully customized with the most flexible assignment of application traffic in the industry.

## Multihoming (Inbound Load Balancing)

Many enterprises host servers for email, and other public access services. FortiWAN load balances incoming requests and responses across multiple WAN Links to improve user response and network reliability. Load balancing algorithms assure the enterprise that priority services are maintained and given appropriate upstream bandwidth.

## Fall-back or Fail-over

FortiWAN detects local access link failures and end-to-end failures in the network and can either fall-back to remaining WAN links or fail-over to redundant WAN links, if needed. Fall-back and Fail-over behavior is under complete control of the administrator, with flexible rule definitions to meet any situation likely to occur. Links and routes are automatically recovered when performance returns to acceptable levels. Notifications will be sent automatically to administrators when link or route problems occur.

## Virtual Private Services (Tunnel Routing)

FortiWAN offers the most powerful and flexible multi-link VPN functionality in the industry. Inter-site Tunnels can be created from fractional, full, multiple and fractions of multiple WAN links. Applications requiring large single-session bandwidth such as VPN load balancing, video conferencing or WAN Optimization can use multiple links to build the bandwidth needed. Multi-session traffic can share an appropriately-sized Tunnel. Tunnels have the same functionality as single links, supporting Load Balancing, Fall-back, Failover and Health Detection within and between Tunnels. Dynamic IP addresses and NAT pass through are supported for the VPL services deployments.

## Virtual Servers (Server Load Balancing and High Availability)

FortiWAN supports simple server load balancing and server health detection for multiple servers offering the same application. When service requests are distributed between servers, the servers that are slow or have failed are avoided and/or recovered automatically. Performance parameters are controlled by the administrator.

## Optimum Routing

FortiWAN continuously monitors the public Internet to select the shortest and fastest route for mission-critical applications. Non-critical traffic can be routed away from the best links when prioritized traffic is present on the links or traffic can be assigned permanently to different groups of WAN links.

## Traffic Shaping (Bandwidth Management)

FortiWAN optimizes, guarantees performance or increase usable bandwidth for specified traffic by traffic classification and rate limiting.

## Firewall and Security

FortiWAN provides the stateful firewall, access control list and connection limit to protect FortiWAN unit, internal network and services from malicious attacks.

## Scope

This document describes how to set up your FortiWAN appliance. For first-time system deployment, the suggested processes are:

## Installation

- Register your FortiWAN appliance before you start the installation. Please refer to the topic: [[Register your FortiWAN](#)] for further information.
- Planning the network topology to introduce FortiWAN to current network. It requires a clear picture of your WAN link types the ISP provides and how to use the available public IP addresses of a WAN link. The topic [[Planning the Network Topology](#)] provides the sub-topics that are necessary concepts for planning your network topology.
- Topic [Web UI Overview] and its sub-topics provide the instructions to connect and log into the Web management interface. System time and account/password resetting might be performed for FortiWAN while the first-time login, please refer to topics [[Setting the System Time & Date](#)] and [[Administrator](#)] for further information.
- For implementation of the network topology you planned, topic [[Configuring Network Interface \(Network Setting\)](#)] and its sub-topics give the necessary information about the configurations of network deployments on Web UI. FortiWAN's diagnostic tools is helpful for trouble shooting when configuring network, please refer to topic [[Diagnostic Tools](#)] .
- Besides configuring Network Setting of individual FortiWAN for installation. Automated local configuration is another way to install batches of FortiWAN devices over sites. See [Automated Local Configuration](#) for details.

## Functions

- After installing FortiWAN into your network, the next step is to configure the major features, load balancing and fail-over, on FortiWAN. Topic [[Load Balancing & Fault Tolerance](#)] and its sub-topics contain the information about performing FortiWAN's load balancing and failover mechanisms for incoming and outgoing traffic, virtual servers and single-session services.
- Topic [[Optional Services](#)] gives the information about configurations of FortiWAN's optional services, such as Bandwidth Management, Firewall, Connection Limit, NAT, SNMP, Cache Redirect, and etc.

## Monitoring

- After FortiWAN works a while, related traffic logs, statistics and report analysis might be required for monitor or trouble shooting purposes. Topics [[Logs](#)], [[Statistics](#)] and [[Reports](#)] provide the information how to use those logs, statistics and reports to improve management policies on FortiWAN.

The following topics are covered elsewhere:

- Appliance installation—Refer to the quick start guide for your appliance model.
- Virtual appliance installation—Refer to the FortiWAN-VM Install Guide.

# What's new

The following features are new or changed since FortiWAN 4.0.0:

## FortiWAN 4.5.5

- **CLI** -
  - `sysctl enable-database-port` - A new command is added to allow/block PostgreSQL's TCP 5432 on FortiWAN. By default, TCP 5432 is blocked. See [Allow/block Reports database port](#).
  - `exec config save tftp` - A new command is added to save the FortiWAN configuration as a file and download the configuration file. See [exec config save tftp](#).

## FortiWAN 4.5.4

- **Mail client** - FortiWAN's mail client (Notification and Reports) supports command STARTTLS to upgrade a plain text connection to an encrypted connection. See [Notification](#) and [Reports Email Server Setting](#).
- **Notification** - Add the corresponding hostname and serial number to the subject of a FortiWAN's notification mails for recognition.

## FortiWAN 4.5.3

- **CLI** -
  - `exec optpath cache list` - A newly added command used to display Optimum Route's cache information. See [exec optpath](#).
  - `exec conntrack delete` - A newly added command used to clear conntrack entries (ICMP, TCP, UDP, GRE, ESP). See [exec conntrack](#).

## FortiWAN 4.5.2

Bug fixes only. Please refer to FortiWAN 4.5.2 Release Notes.

## FortiWAN 4.5.1

Bug fixes only. Please refer to FortiWAN 4.5.1 Release Notes.

## FortiWAN 4.5.0

- **Default WAN Type** - By default, WAN1 is now configured as a DHCP client port. This is to allow local configuration features as described below. WAN1 can be reconfigured via GUI/CLI at any time.
- **Automated Local Configuration** - Through FortiWAN Manager 4.5.0, network administrator can predefine configurations for batches of FortiWAN devices on the Fortinet call-home server in advance. As long as local installer equips a FortiWAN with Internet access by connecting it to a DHCP-based network, FortiWAN's call-home process can automatically connect and authenticate itself to the call-home server, then download and apply the correct configuration to itself. This is an efficient way for cross-regional FortiWAN deployment over many sites, even countries.
- **Password Management** - There is a new process to recover lost passwords. Please contact your nearest TAC.
- **Bandwidth Management** - Priority levels of bandwidth management class are expanded to 8 levels: Highest (0), Higher (1), High (2), Normal (3), Normal-low (4), Low (5), Lower (6) and Lowest (7).

- **Virtual Server** - You can enable/disable individual backend server in server pools for virtual servers. A virtual server only distributes received requests to enabled backend servers of the associated server pool.
- **Login Session Management** - The administration login sessions to Web UI and CLI can be managed individually by configuring the inactivity timeout duration. A login session will be expired and logged off after the given time of inactivity.
- **Reports** - For statistics of FortiWAN's bandwidth usage, you can set a lower bound to ignore certain traffic if it is less than the bound. Reports might be in high CPU usage (highly frequented database update) when suffering a network scanning, which is characterized by tiny traffic but large number of IP pairs. Filtering the negligible traffic off can protect Reports from this.
- **CLI** -
  - `date` - A newly added command used to display and set system software/hardware time.
  - `callhome` - A newly added command used to display logs of the call-home process.
  - `resetconfig` - This command is updated as:
    - Whether parameters are specified or not, following two default values are reset:
      - Default DNS server that FortiWAN uses is 8.8.8.8.
      - Default status of call-home is enabled.
    - A new parameter `[wan WANSPEC]` is added:
      - This is used to set WAN link type and necessary information to the default WAN link of a specified WAN port.
      - Without this parameter being specified, the default WAN link on WAN1 port will be set to a DHCP WAN link.
    - All the other default values are as usual.

### FortiWAN 4.4.1

Bug fixes only. Please refer to FortiWAN 4.4.1 Release Notes.

### FortiWAN 4.4.0

- **Tunnel Routing** -
  - Tunnel Routing dynamically determines whether to distribute traffic to a tunnel according to quality of the tunnel, which is evaluated with the values of RTT and Jitter between two endpoints of the tunnel. See [Monitoring quality of a tunnel](#).
  - You can configure the settings of detection period, number of retries and number of successful detections for tunnel health detection. See [Configuring the parameters for tunnel health detection](#).
  - CLI can display tunnel quality and health detection status of tunnels. See [showtrstat](#).
- **Geo IP Database** - A built-in Geo IP database is supported. This database is the mapping between geographical regions or countries and the public IP addresses that are known to originate from them. FortiWAN can recognize the countries that connections originate from or destined to, and take the corresponding actions to the traffic according to the policies. See [Geo IP database](#).
- **Network Setting** - Applying network settings will restart a network interface if this interface is using PPPoE or DHCP, or the applying involves changes related to MAC address or MTU of this network interface. A warning is added in the original pop-up confirmation for notifying users that applying network settings might restart network interfaces and disrupt established connections. Applying network settings will no longer cause static-IP-based network interfaces to restart.

- **New Dashboard** - The original Web UI pages, System > Summary and Reports > Dashboard, are integrated as System > Dashboard with new look and feel. Page Reports > Dashboard is removed. See [Dashboard](#).
  - **Bandwidth Management** -
    - A warning is added for notifying users that applying bandwidth management settings causes traffic loss for a short period. See [Bandwidth Management](#).
    - A limit line is displayed in BM traffic statistics charts (Statistics > BM) to indicate the maximum allowed bandwidth that the default BM class defines to the WAN link when the real traffic is very close to the limitation. See [Bandwidth management statistics](#).
    - Moving the mouse over the BM statistics chart displays the corresponding traffic distribution. See [Bandwidth management statistics](#).
  - **Multihoming** -
    - Add a new inbound traffic distribution algorithm called Fail-Over. When this algorithm is enabled, Multihoming evaluates the WAN link candidates of an A/AAAA policy from top to bottom and responses the first-available WAN link for DNS queries. See [Policy Settings: A/AAAA Record Policy](#).
    - Allow configuring CNAME records with wildcard characters. See [Support wildcard in CName records](#).
    - You can enable/disable the WAN links defined in a A/AAAA policy. See [Policy Settings: A/AAAA Record Policy](#).
  - **Reports** - Supports visibility of individual application in a Tunnel Routing transmission. Although the entire Tunnel Routing traffic in each tunnel consists of various applications and originates from internal network behind the FortiWAN appliance, these applications and source IPs of traffic in the tunnel were identified as GRE and the WAN port IP in Reports. From this release, Reports can recognize individual application and its internal IP of a tunnel traffic. See [Managing Bandwidth for Tunnel Routing and IPsec](#) and [Traffic Statistics for Tunnel Routing and IPsec](#).
- Annotation: Bandwidth Management and Traffic Statistics support visibility to Tunnel Routing traffic since FWN 4.2.0.
- **Virtual Server** - Process of configuring virtual servers on the Web UI is improved by separating the original configuration into two different configurations, Server Pool and Virtual Server. A server pool can be easily associated with a virtual server without lots of config modifications when it requires to change the mapping between the backend servers and the virtual server. See [Virtual Server & Server Load Balancing](#).
  - **Log** - Logs displayed on Log > View are now stored in FortiWAN's hard disk. These logs are no longer cleared because of system reboot. It supports pushing logs through syslog, FTP and SMTP. See [Logs](#).

#### FortiWAN 4.3.1

- **Tunnel Routing** - From this release, the Generic Receive Offload (GRO) mechanism on each of FortiWAN's network interfaces is disabled by default for better Tunnel Routing transmission performance. The parameter "generic-receive-offload" of CLI command sysctl added in release 4.2.3 to enable/disable GRO is removed; it is unable to enable GRO on FortiWAN. Related descriptions were removed from [Console Mode Commands](#), [How the Tunnel Routing Works](#) and [How to set up routing rules for Tunnel Routing](#)

#### FortiWAN 4.3.0

- **Tunnel Routing** -

- Supports large-scale Tunnel Routing network deployment with allowing a maximum of
  - FWN-200B: **100** tunnel groups
  - FWN-1000B: **400** tunnel groups
  - FWN-3000B: **1000** tunnel groups

For all FortiWAN models, each tunnel group supports up to **16** enabled GRE tunnels, and a maximum total of **2500** enabled GRE tunnels is supported. See [Tunnel Routing Scale](#), [Tunnel Routing - Setting](#) and [How to set up routing rules for Tunnel Routing](#).

- A new measurement case is added to benchmark to evaluate transmission performance of a tunnel group. Packets of a measurement session will be distributed and sent over all the tunnels of the tunnel group, just like how Tunnel Routing generally works in real practice. This is a more accurate way to evaluate your Tunnel Routing network. See [Tunnel Routing - Benchmark](#).
- **IPSec** - Supports Internet Key Exchange Protocol Version 2 (IKEv2) for the establishments of Security Association. Please note that a specific procedure will be required when you switch IKE version to an existing IPSec VPN connectivity. See [Specifications of FortiWAN's IPsec VPN](#) and [IKE Phase 1 Web UI fields - Internet Key Exchange](#).
- **DHCP Relay** - Supports up to two DHCP servers for a relay agent. Once two DHCP servers are configured, the relay agent will forward a DHCP request to both of the DHCP servers. The first response received by the relay agent will be first apply to the DHCP client, and the subsequent responses will be ignored. See [DHCP Relay](#).
- **Reports** - Supports scheduled report email. According to the scheduling, system performs automatic report email sending periodically (daily, weekly or monthly). See [Report Email](#) and [Scheduled Emails](#).
- **CLI command** - A new parameter `PORT` is added to command `resetconfig` for specifying port mapping to LAN port while resetting configurations to factory default. See [CLI Command - resetconfig](#).
- **DNS Proxy** - It is acceptable to configure the Intranet Source field of a DNS Proxy policy with an IPv4 range or subnet. See [DNS Proxy Setting Fields](#).
- **WAN link health detection** - A new parameter that is used to indicate the number of continuously successful detections for declaring a WAN link indeed available is added to WAN link health detection policies. See [WAN Link Health Detection](#).
- **Web UI account** - The ability for Monitor accounts to reset their own password is removed. From this release, Web UI page System > Administration is not available to Monitor accounts and only Administrator accounts have the permission to reset passwords. Also the Apply button is greyed-out and inactive for Monitor users. See [Administrator and Monitor Password](#).
- **Multihoming** - Supports SOA and NS records for the reverse lookup zones. See [Global Settings: IPv4/IPv6 PTR Record](#).
- **Web UI** - New look and feel.

### FortiWAN 4.2.7

Bug fixes only. Please refer to FortiWAN 4.2.7 Release Notes.

### FortiWAN 4.2.6

Bug fixes only. Please refer to FortiWAN 4.2.6 Release Notes.

### FortiWAN 4.2.5



Bug fixes only. Please refer to FortiWAN 4.2.5 Release Notes.

#### FortiWAN 4.2.4

Bug fixes only. Please refer to FortiWAN 4.2.4 Release Notes.

#### FortiWAN 4.2.3

- **Tunnel Routing** - Performance of transmission in a tunnel group can be greatly enhanced (increased) by disabling Generic Receive Offload (GRO) mechanism on each of participated network interfaces on both the participated FortiWAN units. A new parameter "generic-receive-offload" is added to CLI command `sysctl` to enable/disable the GRO module. See [How the Tunnel Routing Works](#), [Tunnel Routing - Setting](#) and [Console Mode Commands](#).
- **DHCP** - Supports Vender Specific Information (Vender Encapsulated Options, option code: 43) and TFTP Server Name (option code: 66). The two DHCP options are used by DHCP clients to request vender specific information and TFTP server IP addresses from the DHCP server for device configuration purposes. FortiWAN's DHCP server delivers the specified information to clients according to the two option codes. See [Automatic addressing within a basic subnet](#).
- **Bandwidth Management** - A new field Input Port is added to Bandwidth Managment's outbound IPv4/IPv6 filters to evaluate outbound traffic by the physical ports where it comes from. Corresponding network ports (VLAN ports, redundant ports, aggregated ports and etc.) will be the options for setting the field, if they are configured in Network Setting. See [Bandwidth Management](#).
- **Port Mapping** - The original configuration panels "Aggregated LAN Port" and "Aggregated DMZ Port" are merged into one panel "Aggregated Port". Instead of mapping the member-ports to LAN/DMZ before aggregating them, it requires creating the logical aggregated port with two non-mapping member ports first, and then mapping LAN/DMZ or defining VLANs to the aggregated port. See [Configurations for VLAN and Port Mapping](#).
- **Multihoming** -
  - Supports wildcard characters for configuring the Host Name field of A/AAAA records. A single wildcard character matches the DNS queries for any hostname that does not appear in any NS record, primary name server, external subdomains and other A/AAAA records of a domain, and so that the specified A/AAAA policy matches. Note that wildcard characters are not acceptable to records (NS, MX, TXT and etc.) except A/AAAA. See [Inbound Load Balancing and Failover \(Multihoming\)](#).
  - Supports configuring CName records for DKIM signing. It is acceptable to configure the Name Server, Alias, Target, Host Name and Mail Server fields of NS, CName, DName, MX and TXT records within dot characters. A dot character is still not acceptable to A/AAAA records. See [Inbound Load Balancing and Failover \(Multihoming\)](#).
- **Auto Routing** - All the WAN links (WAN parameters) of an Auto Routing policy were set to checked by default when you create it on the Web UI for configuring. To programe it for the real networks, you might to uncheck the unused WAN links one at a time. From this release, the WAN parameters of an AR policy are checked by default only if the corresponding WAN links have been enabled via Network Setting. See [Outbound Load Balancing and Failover \(Auto Routing\)](#).
- **Statistics** - Measurement of Round Trip Time (RTT) is added to Statistics > Tunnel Status for each GRE tunnel of configured tunnel groups. See [Tunnel Status](#).

#### FortiWAN 4.2.2

Bug fixes only. Please refer to FortiWAN 4.2.2 Release Notes.

## FortiWAN 4.2.1

Bug fixes only. Please refer to FortiWAN 4.2.1 Release Notes.

## FortiWAN 4.2.0

- **IPSec VPN** - Supports standard IPSec VPN which is based on the two-phase Internet Key Exchange (IKE) protocol. FortiWAN's IPSec VPN provides two communication modes, tunnel mode and transport mode. Tunnel mode is a common method used to establish IPSec VPN between two network sites. FortiWAN IPSec tunnel mode transfers data traffic within single connection (single WAN link), therefore bandwidth aggregation and fault tolerance are not available to the VPN. On the other hand, FortiWAN's transport mode is designed to provide protections to Tunnel Routing transmission on each of the TR tunnels, so that the IPSec VPN with ability of bandwidth aggregation and fault tolerance can be implemented.  
FortiWAN's IPSEC tunnel mode supports single-link connectivity between FortiWAN devices, FortiWAN and FortiGate and FortiWAN and any appliance supporting standard IPSEC. FortiWAN's IPSEC transport mode supports multi-link Tunnel Routing between FortiWAN devices. IPSEC Aggressive Mode is not supported in this release. See "[IPSec VPN](#)".
- **Tunnel Routing** - Supports IPSec encryption. With cooperation with FortiWAN's IPSec tunnel mode, the Tunnel Routing communication can be protected by IPSec Security Association (IPSec SA), which provides strict security negotiations, data privacy and authenticity. The VPN network implemented by Tunnel Routing and IPSec transport mode has the advantages of high security level, bandwidth aggregation and fault tolerance. See "[Tunnel Routing](#)".
- **Basic subnet** - Supports DHCP Relay on every LAN port and DMZ port. FortiWAN forwards the DHCP requests and responses between a LAN or DMZ subnet and the specified DHCP server (standalone), so that centralized DHCP management can be implemented. With appropriate deployments of Tunnel Routing (or Tunnel Routing over IPSec Transport mode), the DHCP server of headquarters is capable to manage IP allocation to regional sites through DHCP relay. FortiWAN's DHCP relay is for not only a local network but also a Tunnel Routing VPN network. See "[Automatic addressing within a basic subnet](#)".
- **DHCP** - Supports static IP allocation by Client Identifier (Options code: 61). According to the client identifier, FortiWAN's DHCP recognizes the user who asks for an IP lease, and assigns the specified IP address to him. See "[Automatic addressing within a basic subnet](#)".
- **Bandwidth Management** - Supports the visibility to Tunnel Routing traffic. In the previous version, individual application encapsulated by Tunnel Routing was invisible to FortiWAN's Bandwidth Management. Bandwidth Management is only capable of shaping the overall tunnel (GRE) traffic. From this release, Bandwidth Management evaluates traffic before/after Tunnel Routing encapsulation/decapsulation, so that traffic of individual application in a Tunnel Routing transmission can be controlled. See "[Bandwidth Management](#)".
- **Administration** - Ability of changing their own password for Monitor accounts is added. In the previous version, password of accounts belonging to Monitor group can be changed by only administrators. From this release, Monitor accounts can change their own password. See "[Administration](#)".
- **HA synchronization** - After system configuration file is restored (System > Administration > Configuration File), the master unit automatically synchronizes the configurations to slave unit. See "[Administration](#)".
- **DNS Proxy** - Supports wildcard character for configuration of Proxy Domains on Web UI. See "[DNS Proxy](#)".

- **Account** - The default account `maintainer` was removed from FortiWAN's authentication.

### FortiWAN 4.1.3

Bug fixes only. Please refer to FortiWAN 4.1.3 Release Notes.

### FortiWAN 4.1.2

Bug fixes only. Please refer to FortiWAN 4.1.2 Release Notes.

### FortiWAN 4.1.1

- **New CLI command** `shutdown` - Use this command to shut FortiWAN system down. All the system processes and services will be terminated normally. This command might not power the appliance off, please turn on/off the power switch or plug/unplug the power adapter to power on/off the appliance. See "[Console Mode Commands](#)".
- **Firmware upgrade** - A License Key will no longer be required for upgrading system firmware to any release.

### FortiWAN 4.1.0

- **The timezone of FortiWAN's hardware clock (RTC) is switched to UTC from localtime. The system time might be incorrect after updating firmware from previous version to this version due to mismatched timezone. Please reset system time and synchronize it to FortiWAN's hardware clock (executing Synchronize Time in System > Date/Time via Web UI), so that the hardware clock is kept in UTC.**
- **New models** - FortiWAN introduces two models, FortiWAN-VM02 and FortiWAN-VM04, for deployment on VMware. FortiWAN V4.1.0 is the initial version of the two models. FortiWAN-VM02 supports the maximum of 2 virtual CPUs, and FortiWAN-VM04 supports the maximum of 4 virtual CPUs. Both of the two models support 9 virtual network adapters. Each port can be programmed as WAN, LAN or DMZ. Each of the two models. FortiWAN-VM supports the deployments on VMware vSphere ESXi. Refer to "FortiWAN-VM Install Guide".
- **Bandwidth capability changes** :
  - FortiWAN 200B - The basic bandwidth is upgraded to 200Mbps from 60Mbps. With a bandwidth license, system supports advanced bandwidth up to 400Mbps and 600Mbps.
  - FortiWAN 1000B - The basic bandwidth is upgraded to 1 Gbps from 500Mbps. With a bandwidth license, system supports advanced bandwidth up to 2 Gbps.
  - FortiWAN 3000B - The basic bandwidth is upgraded to 3 Gbps from 1 Gbps. With a bandwidth license, system supports advanced bandwidth up to 6 Gbps and 9 Gbps.
- **Notification** - Supports delivering event notifications via secure SMTP. See "[Notification](#)".
- **Connection Limit** - Customers can manually abort the connections listed in Connection Limit's Statistics. FortiWAN's Connection Limit stops subsequent connections from malicious IP addresses when system is under attacks with high volumes of connections. However, system takes time to normally terminate the existing malicious connections (connection time out). Connection Limit's Statistics lists the existing connections; aborting these connections recovers system immediately from memory occupied. See "[Statistics > Connection Limit](#)".
- **Multihoming** - Supports specifying an IPv6 address in an A record and an IPv4 address in an AAAA record to evaluate the source of a DNS request. See "[Inbound Load Balancing and Failover \(Multihoming\)](#)".

- **Automatic default NAT rules** - Supports for all the types of IPv6 WAN link. Previously, system generates automatically the default NAT rules for any type of IPv4 WAN link and PPPoE IPv6 WAN link after the WAN links are applied. From this release, all the types of IPv6 WAN links are supported. See ["NAT"](#).
- **Firmware update under HA deployment** - Simple one-instruction update to both master and slave units. The master unit triggers firmware update to slave unit first, and then runs update itself. See ["FortiWAN in HA \(High Availability\) Mode"](#).
- **New Reports pages:**
  - Dashboard - This is a chart-based summary of FortiWAN's system information and hardware states. See ["Reports > Device Status > Dashboard"](#).
  - Settings - This is used to manage FortiWAN Reports. See ["Reports Settings"](#).
- **Auto Routing** - A new field Input Port is added to Auto Routing's rules to evaluate outbound traffic by the physical ports where it comes from. Correspondent VLAN ports, redundant LAN ports, redundant DMZ ports, aggregated LAN ports and aggregated DMZ ports are the options for setting the field, if they are allocated. See ["Using the Web UI"](#).
- **New and enhanced CLI commands** (See ["Console Mode Commands"](#)):
  - New command `arp` - Use this command to manipulate (add and delete entries) or display the IPv4 network neighbor cache.
  - Enhanced command `resetconfig` - A new parameter is added to the CLI command `resetconfig` to specify a static routing subnet to the default LAN port. With specifying a proper private LAN subnet and static routing rule, users can connect to Web UI via the default LAN port without modifications of their current network after system reboots from resetting system to factory default.
  - Pagination - Paginate the output of a command if it is longer than screen can display.
- **Changes on FortiWAN Logins** -
  - Fortinet default account/password (admin/null) is supported for FortiWAN's Web UI and CLI. The old default accounts/passwords will be still accessible. See ["Connecting to the Web UI and the CLI"](#).
  - FortiWAN CLI accepts logins of any customized account belongs to group Administrator. A special account maintainer is provided to reset admin password to factory default via CLI for case that no one with the password is available to login to the WEB UI and CLI. See ["Administration"](#).
  - All the accounts belong to group Administrator are acceptable to login to FortiWAN over SSH.
  - Web UI Supports multiple sign-in. System accept the maximum of 20 concurrent logins. Note that system does not provide concurrent executions of Tunnel Routing Benchmark for multiple logins. See ["Using the Web UI"](#).

## FortiWAN 4.0.6

Bug fixes only. Please refer to FortiWAN 4.0.6 Release Notes.

## FortiWAN 4.0.5

Bug fixes only. Please refer to FortiWAN 4.0.5 Release Notes.

## FortiWAN 4.0.4

Bug fixes only. Please refer to FortiWAN 4.0.4 Release Notes.

### FortiWAN 4.0.3

FortiWAN 4.0.3 is the initial release for FortiWAN 3000B. For bug fixes, please refer to FortiWAN 4.0.3 Release Notes.

### FortiWAN 4.0.2

Bug fixes only. Please refer to FortiWAN 4.0.2 Release Notes.

### FortiWAN 4.0.1

FortiWAN introduces new hardware platforms FortiWAN 1000B and FortiWAN 3000B, and new FortiWAN 4.0.1 firmware based on the AscenLink series of Link Load Balancing appliances already in the market. FortiWAN 4.0.1 is substantially similar to AscenLink V7.2.3 with the additions noted below.

To assess the impact of deploying FortiWAN 4.0.1 on your network and processes, review the following new and enhanced features.

- **Data Port Changes -**

- FortiWAN 1000B supports 3 GE RJ45 ports and 4 GE SFP ports. Each port can be programmed as WAN, LAN or DMZ. Redundant LAN and DMZ ports can be configured. 2-link LACP/LAG LAN or DMZ ports can be configured. Default LAN port is Port 6 and default DMZ port is Port 7.
- FortiWAN 3000B supports 8 GE RJ45 ports, 8 GE SFP ports and 8 10GE SFP+ ports. Each port can be programmed as WAN, LAN or DMZ. Redundant LAN and DMZ ports can be configured. 2-link LACP/LAG LAN or DMZ ports can be configured. Default LAN port is Port 11 and default DMZ port is Port 12.

- **HA Configuration Synchronization** - Two FortiWAN appliances can be connected in active-passive High Availability mode via an Ethernet cable between the systems' HA RJ-45 ports. HA will not interoperate between AscenLink and FortiWAN and will not interoperate between different FortiWAN models or the same model with different Throughput licenses. Model and Throughput must match.

- **HDD** - FWN 1000B and FWN 3000B add internal 1TB HDDs for Reports data storage.

- **Hardware Support** - FortiWAN 4.0.1 for FortiWAN supports FortiWAN 200B and FortiWAN 1000B. AscenLink series models are not supported. Note that FortiWAN 4.0.1 does not support FortiWAN 3000B, please look forward to the sequential releases.

### FortiWAN 4.0.0

FortiWAN introduces new hardware platform FortiWAN 200B and new FortiWAN 4.0.0 firmware based on the AscenLink series of Link Load Balancing appliances already in the market. FortiWAN 4.0.0 is substantially similar to AscenLink V7.2.2 with the additions noted below.

To assess the impact of deploying FortiWAN 4.0.0 on your network and processes, review the following new and enhanced features.

- **Data Port Changes** - FortiWAN 200B supports 5 GE RJ45 ports. Each port can be programmed as WAN, LAN or DMZ. Redundant LAN and DMZ ports can be configured. 2-link LACP/LAG LAN or DMZ ports can be configured. Default LAN port is Port4 and default DMZ port is Port 5.
- **HA Port Change** - FortiWAN supports one GE RJ45 HA Port. This port must be direct-cabled via Ethernet cable, to a second FWN unit HA port for HA operation. HA will not interoperate between AscenLink and FortiWAN and will not interoperate between different FortiWAN models.

- **HDD** - FWN 200B adds an internal 500BG HDD for Reports data storage. See below for more information on Reports.
- **HA Configuration Synchronization** - Two FWN 200B appliances can be connected in active-passive High Availability mode via an Ethernet cable between the systems' HA RJ-45 ports.
- **New Functionality** - FortiWAN 4.0.0 has the same functionality as AscenLink V7.2.2 PLUS the addition of built-in Reports which is the equivalent functionality to the external LinkReport for AscenLink.
- **Reports** - Reports captures and stores data on traffic and applications across all WAN links in the system. Reports include connections, link and aggregate bandwidth, link and VPN reliability, and data on Multi-Homing requests, Virtual Server (SLB) requests, and more. Reports can be viewed on-screen, exported to PDF or CSV files or emailed immediately in PDF or CSV format.
- **GUI** - FWN 4.0.0 adopts the Fortinet "look and feel".
- **Hardware Support** - FortiWAN 4.0.0 for FortiWAN supports FortiWAN 200B. AscenLink series models are not supported.

# Document enhancements

The following document content is enhanced or changed since FortiWAN 4.0.1:

## FortiWAN 4.5.5

- Description of newly-added CLI commands `sysctl enable-database-port` and `exec config save tftp` are added. See [Allow/block Reports database port](#) and [exec config save tftp](#).

## FortiWAN 4.5.4

- Description of setting port for SMTP server is changed for supporting STARTTLS. See [Notification and Reports Email Server Setting](#).

## FortiWAN 4.5.3

- Description of newly-added CLI commands `exec conntrack` and `exec optpath` are added. See [exec conntrack](#) and [exec optpath](#).
- Description about how packets are matched to TR's persistent rules, routing rules and default rules was corrected. See [Configuring persistent rules for tunnel routing](#).

## FortiWAN 4.5.2

- None

## FortiWAN 4.5.1

- Content of the Enable checkbox of Policy Advanced Setting was updated. See [Policy Settings: A/AAAA Record Policy](#).
- Content of Tunnel Routing's persistent rule was updated. See [Configuring persistent rules for tunnel routing](#).

## FortiWAN 4.5.0

- A new topic about Automated Local Configuration was added. See [Automated Local Configuration](#).
- Content of [Scope](#), [How to set up your FortiWAN](#) and [Appendix A: Default Values](#) was updated for the new feature Automated Local Configuration.
- A new appendix about processes to recover lost password was added. See [Appendix C: What if your password is lost?](#).
- Content of Bandwidth Management was updated for the expanded priority levels. See [Bandwidth Management](#).
- Content of [Virtual Server & Server Load Balancing](#) and [Virtual Server Status](#) was updated for the ability of enabling/disabling backend servers in a server pool.
- Content of [Login Session Management](#) was added for the new login session management mechanism.
- A new topic about filtering bandwidth logs off for Reports was added. See [Filter the negligible traffic off](#).
- Content of [Console Mode Commands](#) was updated for the new commands `callhome` and `date`, and an updated command `resetconfig`. See [callhome](#), [date](#) and [resetconfig](#).

## FortiWAN 4.4.1

- Content of Connection Limit was updated. See [Connection Limit](#).
- Content of upgrading firmware via TFTP was added. See [Firmware Update via CLI](#).

## FortiWAN 4.4.0

- Content of tunnel quality policy was added. See [Monitoring quality of a tunnel](#), [Configuring tunnel quality policies](#), [Configuring a routing rule](#) and [Example for using quality policies](#).
- Content of Tunnel Routing health detection was updated. See [Configuring the parameters for tunnel health detection](#).
- Content of the CLI command `showtrstat` was added. See [showtrstat](#).
- Content of Geo IP was added. See [Geo IP database](#).
- Content of the updated dashboard was added. See [Dashboard](#).
- Content of Bandwidth Management statistics was updated for the updated statistics chart. See [Bandwidth management statistics](#).
- Content of Multihoming was updated for the new algorithm, wildcard support for CName record and the ability to enable/disable individual A/AAAA record policy. See [Policy Settings: A/AAAA Record Policy](#).
- Content of Load Balancing Algorithms was updated for the new Multihoming algorithm. See [Load Balancing Algorithms](#).
- Content of Bandwidth Management and Statistics was updated for the support that individual application of a Tunnel Routing transmission is visible in Reports. See [Managing Bandwidth for Tunnel Routing and IPsec](#) and [Traffic Statistics for Tunnel Routing and IPsec](#).
- Content of Virtual Server was updated for the updated configuration interface. See [Virtual Server & Server Load Balancing](#).
- Content of Log and Log View was updated for the support storing log files in hard disk. See [Logs](#) and [Log View](#).

### FortiWAN 4.3.1

- Parameter generic-receive-offload of command `sysctl` was removed from [Console Mode Commands](#). Related descriptions about disabling GRO were removed as well from [How the Tunnel Routing Works](#) and [How to set up routing rules for Tunnel Routing](#).
- An appendix was added for suggested maximum configuration values, see [Appendix B: Suggested Maximum Configuration Values](#)
- A topic about possible query loop was added in [DNS Proxy](#).
- A description was added for suggested IPsec encryption algorithms, see [IPsec VPN in the Web UI](#).

### FortiWAN 4.3.0

- Content of Tunnel Routing was updated for large-scale TR network support and the updated benchmark. See [Tunnel Routing Scale](#), [Tunnel Routing - Setting](#), [How to set up routing rules for Tunnel Routing](#) and [Tunnel Routing - Benchmark](#).
- Content of IPsec was updated for IKEv2 support. See [Specifications of FortiWAN's IPsec VPN and IKE Phase 1 Web UI fields](#).
- Content of automatic IP addressing was updated for dual DHCP servers support in a DHCP relay. See [DHCP Relay](#).
- Content of [Report Email](#) and [Reports Settings](#) was updated, and a new page [Scheduled Emails](#) was added for the new Reports feature - scheduled report email.
- Content of [Reports Settings](#) and [Reports Database Tool](#) was updated, and a new page [Database Data Utility](#) was added for the new Reports feature - Web-based Reports database management tool.
- Content of CLI commands was updated for the new parameter `PORT` of `resetconfig` and the change to `init_reports_db`. See [CLI Command - resetconfig](#).
- Content of DNS Proxy was updated for the changes to the Source configuration. See [DNS Proxy Setting Fields](#).
- Content of WAN link health detection was updated for the new condition "Number of successful detection" to declare a WAN link available. See [WAN Link Health Detection](#).



- Content of Administrator was updated for the changes to Monitor account. See [Administrator and Monitor Password](#).
- Content of Multihoming was updated for the new configurations to support SOA and NS records for the reverse lookup zones. See [Global Settings: IPv4/IPv6 PTR Record](#).
- Diagrams related to Web UI were updated for the new look and feel.
- A glossary for FortiWAN network setting was added. See [Glossary for FortiWAN network setting](#).
- Content about network deployment was enhanced: [Configuring networks to FortiWAN](#), [Configuring Network Interface \(Network Setting\)](#), [Configuring your WAN and DMZ](#), [Network interfaces and port mapping](#), [WAN, LAN and DMZ](#), [WAN link and WAN port](#), [WAN types: Routing mode and Bridge mode](#), [Public IP Pass-through \(DMZ Transparent Mode\)](#), [Aggregated, Redundant, VLAN Ports and Port Mapping](#), [Bridge-mode \(one static IP\) WAN link](#), [Routing-mode WAN link and Bridge-mode \(multiple static IP\) WAN link](#).
- Description about default rule was added to Firewall section. See [Firewall](#).
- A note about accessing to WebUI through WAN ports was added, see [Connecting to the Web UI and the CLI](#).

#### FortiWAN 4.2.7

- None

#### FortiWAN 4.2.6

- None

#### FortiWAN 4.2.5

- Content of section *Performance* in [How the Tunnel Routing Works](#) was enhanced by adding two subsections, *Throughput of bidirectional TR transmission* and *Persistent Route in Tunnel Routing*. A description about configuring for better bidirectional TR transmission was added in [Tunnel Routing - Setting](#).

#### FortiWAN 4.2.4

- None

#### FortiWAN 4.2.3

- Content about how to enhance Tunnel Routing performance was added to section *Performance* in [How the Tunnel Routing Works](#) and section *Tunnel Group* in [Tunnel Routing - Setting](#).
- Content about a new system parameter `generic-receive-offload-<port>` of CLI command `sysctl` was added in [Console Mode Commands](#), and the other content of command `sysctl` was enhanced.
- Content about DHCP options 43 (Vender Specific Information) and 66 (TFTP Server Name) was added to section *DHCP* in [Automatic addressing within a basic subnet](#).
- Content about the new filter item Input Port was added to section *Inbound & Outbound IPv4/IPv6 Filter* in [Bandwidth Management](#).
- Content about aggregated port in [Configurations for VLAN and Port Mapping](#) was updated, and the other content was enhanced also.
- Content about supporting wildcard for A/AAAA records and dot characters for other resource records was added in [Inbound Load Balancing and Failover \(Multihoming\)](#), and the other content was enhanced also.
- Content of Parameter of section *Configurations* in [Outbound Load Balancing and Failover \(Auto Routing\)](#) was updated.

- Content about a new measure Round Trip Time (RTT) was added to section *Tunnel Health Status* in [Tunnel Status](#).
- Content of [Load Balancing Algorithms](#) was enhanced.
- Content of [Optimum Route Detection](#) was enhanced.

#### FortiWAN 4.2.2

- None

#### FortiWAN 4.2.1

- A garbage character *R* at the leftmost position of the topic line ["Define routing policies for an IPSec VPN"](#) in page 198 was removed.

#### FortiWAN 4.2.0

- New page ["Automatic addressing within a basic subnet"](#) was added for the new features DHCP Relay and static addressing by client identifier. Related pages ["LAN Private Subnet"](#), ["Configurations for a WAN link in Routing Mode"](#) and ["Configurations for a WAN link in Bridge Mode: Multiple Static IP"](#) were enhanced.
- New topic ["IPSec"](#) and new page ["Statistics > IPSec"](#) were added for new feature IPSec. Related pages ["Log > View"](#), ["Log > Log Control"](#), ["How the Tunnel Routing Works"](#) and ["Tunnel Routing - Setting"](#) were enhanced.
- Content of ["Bandwidth Management"](#) was updated for a behavior change - visibility to Tunnel Routing traffic. A new page ["Traffic Statistics for Tunnel Routing and IPSec"](#) was added for this.
- Content of ["Administration"](#) was updated in sections ["Administrator and Monitor Password"](#) and ["Configuration File"](#) for updated features - allowing change personal password by Monitor account and performing synchronization to slave unit after configurations are restored on master unit.
- The description of the account "maintainer" in ["Connecting to the Web UI and the CLI"](#) was removed.
- Content of ["Optimum Route Detection"](#), ["DNS Proxy"](#), ["Configurations for VLAN and Port Mapping"](#), ["Internal DNS"](#), ["Set DNS server for FortiWAN"](#), ["FortiWAN in HA \(High Availability\) Mode"](#) and ["Inbound Load Balancing and Failover \(Multihoming\)"](#) was enhanced.

#### FortiWAN 4.1.3

- A section describing log format was added in ["Log > View"](#).

#### FortiWAN 4.1.2

- Content of ["Global Settings: IPv4 / IPv6 PTR Record"](#) in ["Inbound Load Balancing and Failover \(Multihoming\)"](#) was changed.

#### FortiWAN 4.1.1

- Content was added to ["Console Mode Commands"](#) for the new CLI command `shutdown`.
- Requirement of License Key was removed from section Firmware Upgrade in ["FortiWAN in HA \(High Availability\) Mode"](#) and ["Administration"](#).
- Two deployment scenarios were added to ["Tunnel Routing > Scenarios"](#).
- Correspondent MIB fields and OIDs were added to ["FortiWAN in HA \(High Availability\) Mode"](#), ["Summary"](#), ["Administration"](#) and ["Network Setting > MIB fields for WAN links and VLANs"](#).
- Content of ["SNMP"](#) and ["Notification"](#) was enhanced.
- Content of ["Statistics > WAN Link Health Detection"](#) was enhanced.

#### FortiWAN 4.1.0

- Content was added to "Scope", "Default Port Mapping", "FortiWAN in HA (High Availability) Mode", "Connecting to the Web UI and the CLI", "Configurations for VLAN and Port Mapping" and "Summary" for the new model FortiWAN-VM.
- Content of "Administration > License Control" was updated for new bandwidth capabilities that FortiWAN supports.
- Content was added to "Notification" for the support to notify via secure SMTP.
- Content was added to "Statistics > Connection Limit" for the Abort function.
- Content was added to "Multihoming" for the support to evaluate an A record query by its IPv6 source and an AAAA record query by its IPv4 source.
- Content of "Configurations for a WAN link in Bridge Mode: One Static IP" and "Configurations for a WAN link in Bridge Mode: Multiple Static IP" was updated for supporting IPv6 default NAT rule.
- Content of "Administration > Firmware Update" and "FortiWAN in HA (High Availability) Mode" was updated for the new firmware update mechanism under HA deployment.
- For the new features that Reports supports, new topics "Dashboard", "Reports Settings", "Reports Settings > Reports", "Reports Settings > IP Annotation", "Reports Settings > Dashboard Page Refresh Time", "Reports Settings > Email Server" and "Reports Settings > Disk Space Control" were added , and content of "Reports" and "Create a Report" was updated.
- Content was added to "Using the Web UI" for the support to evaluate traffic by its Input Port.
- For the new CLI command `arp` and enhanced command `resetconfig`, correspondent content was added and updated to "Console Mode Commands".
- Content of "Connecting to the Web UI and the CLI", "Administration > Administrator and Monitor Password" and "Appendix A: Default Values" for the updated local authentication mechanism.
- Content was added to "Using the Web UI" for supporting concurrent multiple logins.
- The parameters of CLI command `sysctl` were fixed from "sip\_helper" and "h323\_helper" to "sip-helper" and "h323-helper" (See "Console Mode Commands").

#### FortiWAN 4.0.6

- None

#### FortiWAN 4.0.5

- None

#### FortiWAN 4.0.4

- Content was enhanced for Reports > Session (See "Reports > Session").
- Content was enhanced for Virtual Server (See "Load Balancing & Fault Tolerance" and "Virtual Server" ) and Persistent Routing (See "Persistent Routing").

#### FortiWAN 4.0.3

##### • Revision 2

- Topic "Web UI and CLI Overview" was reorganized and content was enhanced on connecting to Web UI and CLI (See "Connecting to the Web UI and the CLI"), Web UI operations (See "Using the web UI") and CLI commands (See "Console Mode Commands").
- Content was enhanced on account management, RADIUS, and firmware update (See "Administration").
- Content was enhanced for NAT, NAT default rule in pages "NAT", "Configurations for a WAN link in Routing Mode", "Configurations for a WAN link in Bridge Mode: Multiple Static IP" and "Configurations for a WAN link in Bridge Mode: One Static IP".

- Content was enhanced for the state of peer information in page "Summary".
- A new topic "Reports Database Tool" was added, and Reports related topics are enhanced (See ["Reports Database Tool"](#), ["Reports"](#), and ["Enable Reports"](#)).

#### • Revision 1

- Add a new page ["Default port mappings"](#) in section "How to set up your FortiWAN > Planning the network topology".
- Content was changed and enhanced for pages ["Configurations for VLAN and Port Mapping"](#), ["WAN, LAN and DMZ"](#), ["WAN link and WAN port"](#) and ["Configuring your WAN"](#).
- Content was changed and enhanced for [Tunnel Routing](#). New subsections were added "GRE Tunnel", "Routing", "How the Tunnel Routing Works". Subsections were enhanced "Tunnel Routing - Setting" and "Tunnel Routing - Benchmark".

#### FortiWAN 4.0.2

- A note about the restrictions on duplicate configurations of group tunnel was added in [Tunnel Routing](#).
- Content was enhanced for [Multihoming](#) in sections "Prerequisites for Multihoming", "DNSSEC Support", "Enable Backup", "Configurations", "Relay Mode" and "External Subdomain Record".
- Content was changed and enhanced for [WAN Link Health Detection](#) and [FortiWAN in HA \(High Availability\) Mode](#).
- A typographical error in [Introduction > Scope](#) was fixed.

#### FortiWAN 4.0.1

- The default username to login to Command Line Interface (Console Mode) was fixed from "administrator" to "Administrator" in Using the web UI and the CLI and [Appendix A: Default Values](#).
- The reference for information on console command in [Administration > Maintenance](#) was fixed from "Appendix A: Default Values" to "Console Mode Commands".

# How to set up your FortiWAN

These topics describe the tasks you perform to initially introduce a FortiWAN appliance to your network. These topics contain the necessary information and instructions to plan network topology, using Web UI and Configure network interfaces on FortiWAN. These topics introduce some key concepts for deploying FortiWAN, but you are assumed to have and be familiar with the fundamental concepts related networking knowledge.

If you have batches of FortiWAN need to be deployed over many site or even countries, spending lots of time to configure every appliances and quality of local installers might be the problems. Automated Local Configuration can automatically download and apply the predefined configurations from the Fortinet call-home server. See [Automated Local Configuration](#) for details.

## Registering your FortiWAN

Before you begin, take a moment to register your Fortinet product at the Fortinet Technical Support web site:

<https://support.fortinet.com>

***Many Fortinet customer services such as firmware updates, technical support, and FortiGuard services require product registration.***

For more information, see the Fortinet Knowledge Base article [Registration Frequently Asked Questions](#).

## Planning the network topology

FortiWAN is the appliance designed to perform load balancing and fault tolerance between different networks. The network environment that a FortiWAN is introducing into might be various, especially with multiple WAN links and various WAN type. A plan of network topology before adding FortiWAN recklessly into current network would be suggested to avoid damages.

## Glossary for FortiWAN network setting

This glossary gives definitions of the key terms and concepts that are frequently used in the following chapters. It will be a great help for making a deployment plan, configuring and using the FortiWAN if you are clearly understand the these terms and concepts.

The glossary contains the following terms and concepts:

[WAN, LAN and DMZ](#)

[Network interfaces and port mapping](#)

[WAN link and WAN port](#)

[WAN types: Routing mode and Bridge mode](#)

[Near WAN](#)

[Public IP pass through \(DMZ transparent mode\)](#)

[VLAN and port mapping](#)

[IPv6/IPv4 dual stack](#)

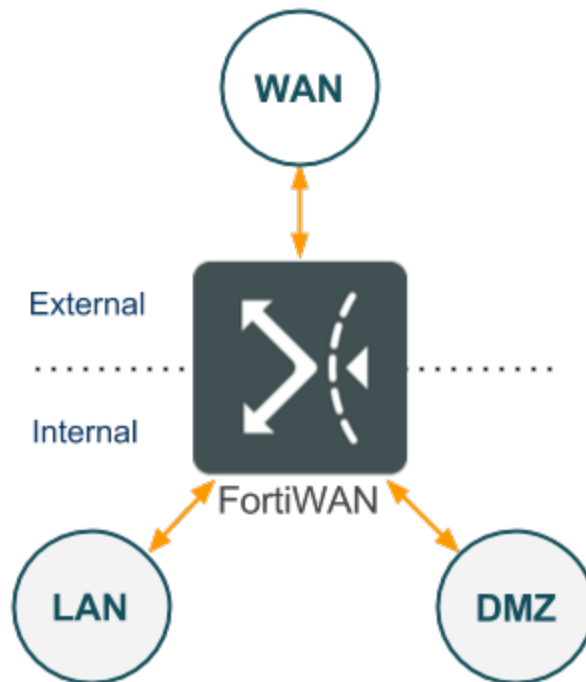
[FortiWAN in HA \(High Availability\) mode](#)

## WAN, LAN and DMZ

According to the scale and purpose, a network can be defined as a Wide Area Network (WAN), Local Area Network (LAN) and Demilitarized Zone (DMZ).

- **Wide Area Network:** WAN (Wide Area Network) is the network that geographically covers a large area which consists of telecommunications networks. It can be simply considered the Internet as well. An internal user can communicate with the Internet via a telecommunications (called Internet Service Provider as well) network connected to FortiWAN's WAN ports. The transmission lines can be classified as xDSL, leased line (T1, E1 and etc.), ISDN, frame relay, cable modem, FTTB, FTTH and etc.
- **Local Area Network:** LAN (Local Area Network) is the computer networks within a small geographical area without leased telecommunication lines involved. In this document, a LAN is considered as an internal private network which is a closed network to WAN.
- **Demilitarized Zone:** DMZ (Demilitarized Zone) is a local subnetwork that is separated from LAN for security issues. A DMZ is used to locate external-facing server farm which is accessible from an untrusted network (usually the Internet), but inaccessible to LAN. FortiWAN provides physical ports for the DMZ purpose.

A network site generally consists of the three basic components, WAN, LAN and DMZ. As an edge device of a network site, FortiWAN basically plays the role routing packets and provides services for communications among LAN, WAN and DMZ. The FortiWAN connects those networks (WAN, LAN and DMZ) to its network interfaces (called network ports as well) and so that the networks can communicate with each other appropriately. This involves two configurations, defining the purpose of a network port (see [Network interfaces and port mapping](#)) and correct network settings on the network port for the connected network (see [Configuring Network Interface](#)).



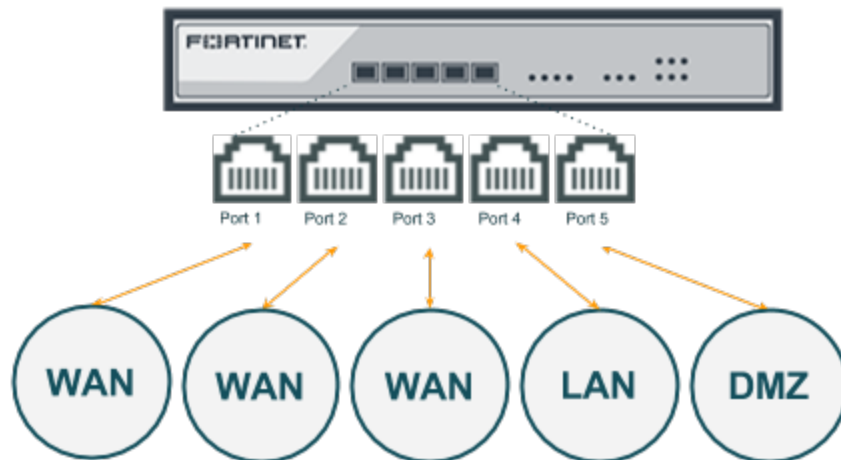
## Network interfaces and port mapping

### Physical network interfaces and the port mapping

The physical network ports (network interfaces) on the panel of a FortiWAN appliance are used to connect the FortiWAN with WAN, LAN and DMZ networks, so that the networks can communicate with each other. Each of the network ports can be mapped to one of the following types which differ in function:

- **WAN port:** is used to connect FortiWAN with a WAN network.
- **LAN port:** is used to connect FortiWAN with a LAN network.
- **DMZ port:** is used to connect FortiWAN with a DMZ network.
- **HA port:** is used to connect two FortiWAN units for HA deployment (See [FortiWAN in HA \(High Availability\) Mode](#)).

The network port type indicates the network type (WAN, LAN or DMZ) that a network port is supposed to connect to. Most of FortiWAN's functions, such as NAT, auto routing, firewall, bandwidth management, traffic statistics, public IP pass-through and etc., are relative to the direction of traffic flow passing through FortiWAN. It strongly requires correspondence between types of a network port and the connected network. FortiWAN might function incorrectly if a network is not corrected to a corresponding network port, for example connecting a WAN network (WAN link) to a LAN port. For the details of physical network interfaces, you can see [FortiWAN Quick Start Guide](#).



The diagram above shows the port mapping of a FortiWAN that ports 1~3 are WAN ports, port 4 and port 5 are a LAN port and a DMZ port respectively. Port mapping can be programmed from FortiWAN's Web UI, see [Configurations for VLAN and Port Mapping](#).

**Note:** To make a FortiWAN operate correctly with the connected networks, it requires not only the correspondence between types of network ports and the connected networks, but also corresponding configurations to the network port (see [Configuring Network Interface](#)).

### Default port mappings

Except the HA port, each of the physical network ports can be programmed as WAN, LAN or DMZ via Web UI. However, for the first time you access the Web UI (see [Connecting to the web UI and the CLI](#)), you probably need to know the default port mapping so that you can access the correct network port for Web UI. All the network ports on the panel of FortiWAN appliance are numbered, and the default mappings are as follows:

| Model     | Ports Supported                                       | WAN Ports        | LAN Port | DMZ Port |
|-----------|-------------------------------------------------------|------------------|----------|----------|
| FWN 200B  | 5 GE RJ45 ports                                       | Port 1 ~ Port 3  | Port 4   | Port 5   |
| FWN 1000B | 3 GE RJ45 ports and 4 GE SFP ports                    | Port 1 ~ Port 5  | Port 6   | Port 7   |
| FWN 3000B | 8 GE RJ45 ports, 8 GE SFP ports and 8 10GE SFP+ ports | Port 1 ~ Port 10 | Port 11  | Port 12  |
| FWN VM    | 10 vNICs                                              | vNIC 2           | vNIC 3   | vNIC 4   |

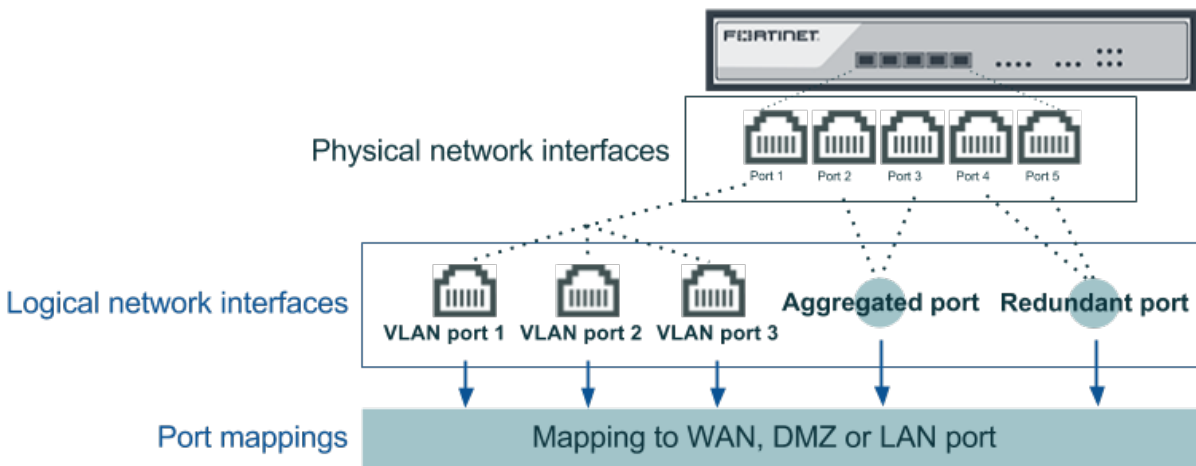
FortiWAN 3000B's Port 13 ~ Port 24 and FortiWAN VM's vNIC 5 ~ vNIC 10 are undefined by default, they can be defined via Web UI (see [VLAN and Port Mapping](#)). After logging onto the Web UI, you can also check and program the network port mapping on *System > Network Setting > VLAN and Port Mapping*.

### Logical network interfaces

For extension, aggregation and redundancy, you can create multiple VLAN ports on a physical network interface, and an aggregated or a redundant port on any pair of the physical network interfaces. Each of the created logical



network interfaces can be programmed as WAN, LAN or DMZ port (whether a physical or a logical port, the port type must be defined to connect the network port with a network). FortiWAN supports the IEEE 802.1Q for VLAN tagging and the IEEE 802.3ad for port aggregation (see [Configurations for VLAN and Port Mapping](#)).

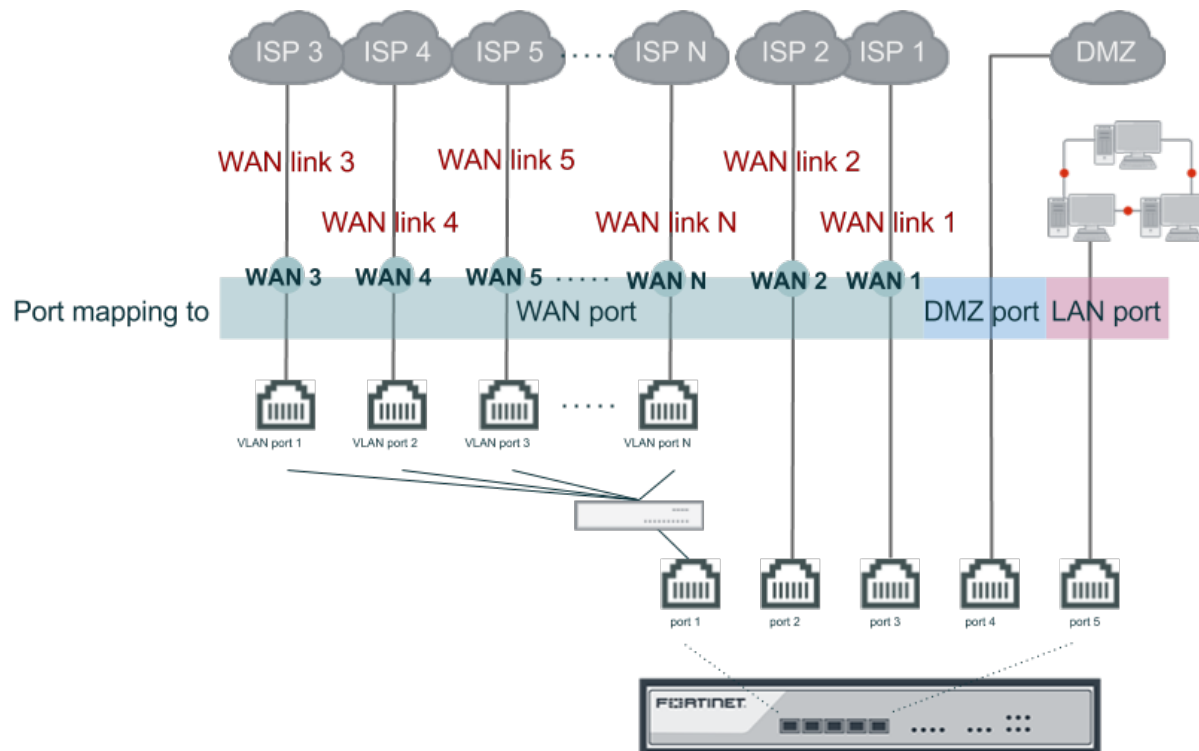


## WAN link and WAN port

A FortiWAN appliance has limited physical network interfaces (ports) depending on the models, but unlimited logical network interfaces (ports) can be created on the physical ports. With correct port mappings, FortiWAN can connect to more networks than the supported number of physical ports.

As previous description, whether a physical or a logical network interface, it requires the network interface mapped to a port type (WAN, DMZ or LAN) for connecting to corresponding network type. A WAN port is a physical or logical network port that is port mapped to the WAN type. A WAN link is a connectivity between a FortiWAN and an ISP network. Actually, a WAN link connects a WAN port of FortiWAN with the remote device (modem or ATU-R) of an ISP, so that the internal networks and the Internet can communicate to each other through the WAN link. A WAN link requires corresponding settings on the WAN port. Configuration of a WAN port contains the information provided by the ISP, such as the IP addresses, default gateway, network mask or username/password, it depends on the WAN link type you apply to the ISP (See "[WAN types: Routing mode and Bridge mode](#)"). You will see the two terms, WAN link and WAN port, frequently in this document.

For purposes of traffic load balancing and fault tolerance, you will need multiple WAN links to connect to the Internet. In case that the WAN links demanded are more than the physical network ports of a FortiWAN appliance in quantity, you can have enough WAN ports for the WAN links by creating multiple logical network ports (VLAN ports) on a physical port (See "[Configurations for VLAN and Port Mapping](#)"). Although you can create VLAN ports on a physical port without limitation in quantity, FortiWAN supports limited WAN links. **FortiWAN 200B** supports up to **25 WAN links**, **FortiWAN 1000B** and **3000B** support up to **50 WAN links**, even if you create more than 50 VLAN ports. These WAN links are named with numbers, such as WAN 1, WAN 2 and WAN 3. You will see this when you configure settings of a WAN port (See "[Configuring your WAN](#)").



The above diagram shows how to create N WAN ports (WAN 1 ~ WAN N) through the three physical network ports of a FortiWAN. Two of the WAN ports use two of the physical network ports and the rest of the WAN ports use the VLAN ports. The N WAN links connect the N WAN ports with N ISP networks. Traffic of WAN link 1 and 2 will be transferred through physical port 2 and port 3 respectively, and traffic of the remaining WAN link (WAN link 3 ~ WAN link N) will be transferred through physical port 1.

### See also

[Configurations for VLAN and Port Mapping](#)

## WAN types: Routing mode and Bridge mode

Before configuring the settings of a WAN port (see WAN link and WAN port) on FortiWAN for a WAN link, you need to know the connection type (we will call it WAN link type or WAN type in this document) that ISP provides you to connect to its network for accessing the Internet. An ISP provides the Internet access service for customers with various connection types, such as static/dynamic IP address, one/multiple IP address and routing/transparent mode. It depends on what you apply for. Different WAN types involve different mechanisms for ISP and FortiWAN to deliver network connections. When you configure a WAN port for a WAN link, you have to exactly indicate the type of the WAN link to FortiWAN so that it works in the correct way for the WAN link. FortiWAN supports the following WAN types:

- **Routing Mode** (See "[Configurations for a WAN link in Routing Mode](#)")
- **Bridge Mode: One Static IP** (See "[Configurations for a WAN link in Bridge Mode: One Static IP](#)")
- **Bridge Mode: Multiple Static IP** (See "[Configurations for a WAN link in Bridge Mode: Multiple Static IP](#)")
- **Bridge Mode: PPPoE** (See "[Configurations for a WAN link in Bridge Mode: PPPoE](#)")
- **Bridge Mode: DHCP Client** (See "[Configurations for a WAN link in Bridge Mode: DHCP](#)")

This section shows you the way to recognize the WAN type of a WAN link that you apply to ISP for.

### Dynamic-IP WAN link

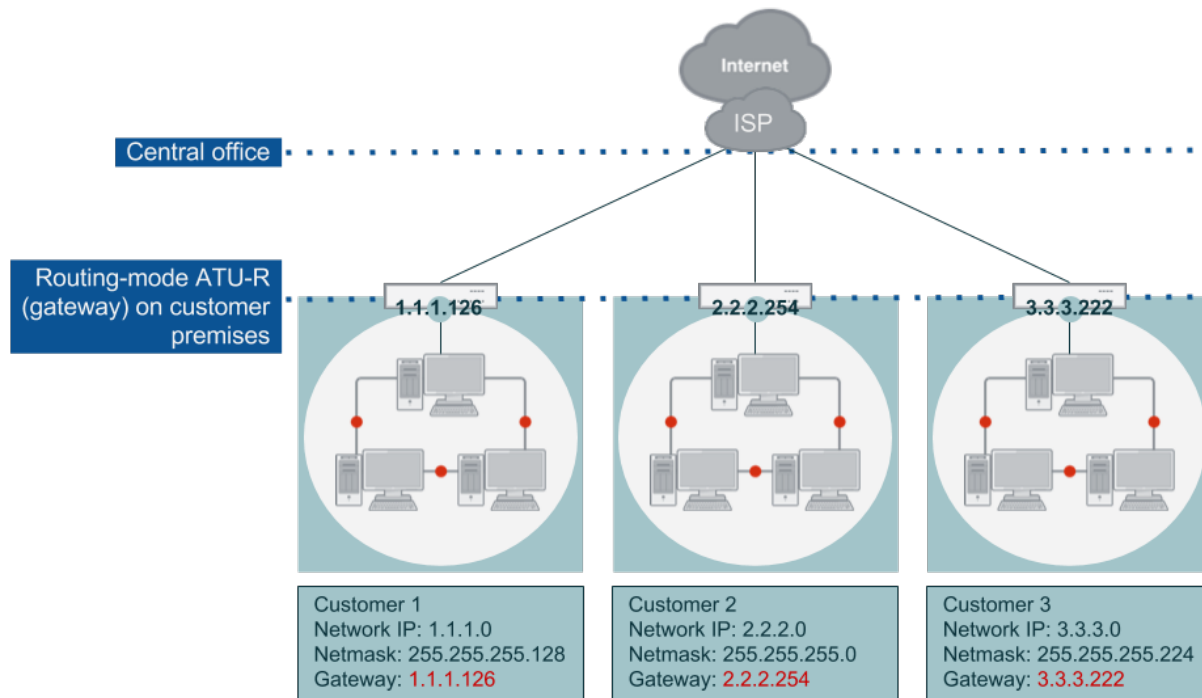
PPPoE and DHCP are the most common ways (protocols) for ISP to assign dynamic IP addresses and provide the Internet access service to customers. If you applied for a dynamic-IP WAN link, you can simply configure the WAN port as [Bridge Mode: PPPoE](#) or [Bridge Mode: DHCP Client](#) for the WAN link. For the two WAN types, you will not be aware of the IP address, netmask and gateway of the WAN link. ISP will provides the account and password for accessing if it is PPPoE.

### Static-IP WAN link

ISP will provides you one or multiple static public IP address if you apply for a static-IP WAN link. Generally, static-IP WAN links between ISP's central offices and customers premises could be divided into routing mode and bridge mode (transparent mode). Each involves different mechanisms. From general customer's viewpoint, it might be not such important to distinguish between the two modes because it is a kind of back-end stuff. They could access the Internet only if they have the correct IP addresses, netmask and gateway configured. However, for FortiWAN users, it is necessary to exactly indicate the mode of the static-IP WAN link to FortiWAN so that it can cooperate with ISP for the connectivity in the correct mechanism.

### Routing mode

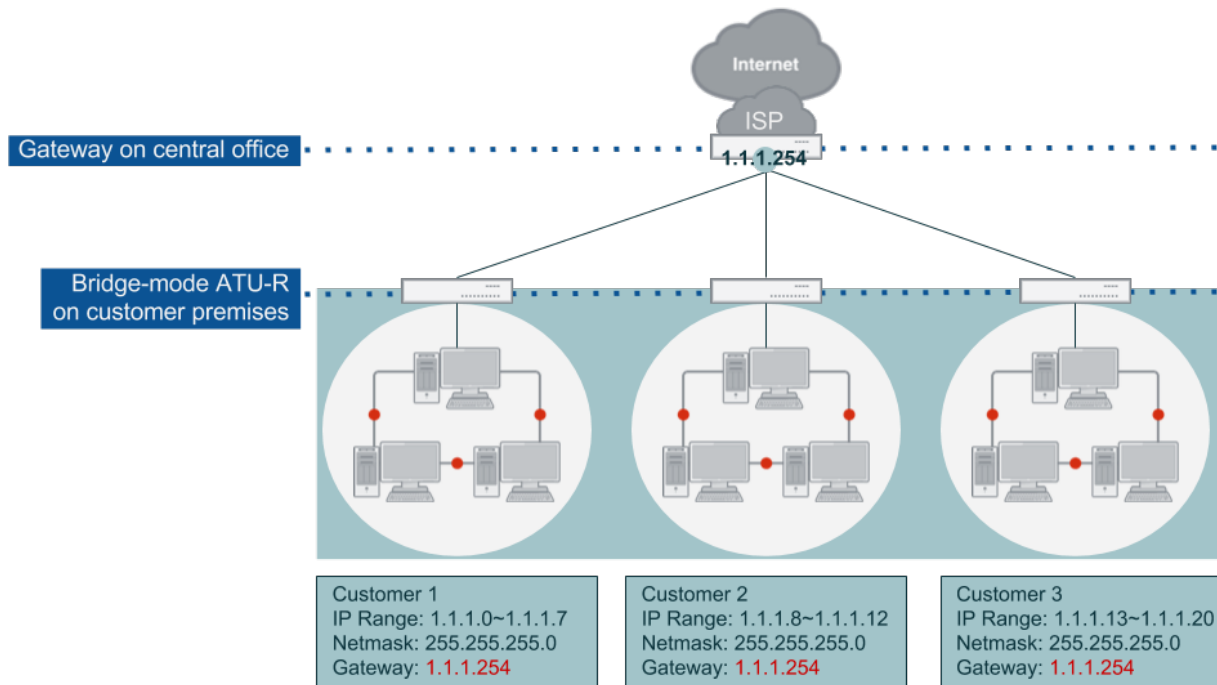
If you apply to ISP for a routing-mode WAN link, you will obtain an individual IP network (layer 3) which is separated from any other networks of the ISP. In that case, the ATU-R at a customer premises plays the role of a gateway to route packets between your network and the Internet. In the other words, the ATU-R connects your network with the ISP central office in routing mode. The IP addresses, default gateway and netmask that the ISP provides you can tell you whether a WAN link is routing mode or not. If the number of deducting 3 (network IP, gateway IP and broadcast IP) from the IP range that the netmask determines matches the number of usable IP addresses that ISP provides you, it means you are given a separate network, a routing-mode WAN link. For example, the ISP gives you five usable IP addresses 203.69.118.10 - 203.69.118.14, default gateway 203.69.118.9 and netmask 255.255.255.248. The netmask 255.255.255.248 divides eight IP addresses which contains five host addresses, one gateway address, one broadcast address and one address for the network ID. It just matches the number of the usable IP addresses the ISP provides. In that case you are strongly recommended to configure the WAN link on FortiWAN as [Routing Mode](#).



## Bridge mode

Opposite to the routing mode, the ATU-R will play the role of a bridge to combine network segments (data link layer, layer 2) of customer premises and the ISP central office, if the WAN link is in bridge-mode. In that case, ISP allocates a block of IP addresses (or a network segment) of an IP network (layer 3) for you rather than a separate IP network. It implies that you and other customers (other network segments) of the ISP that in the same IP network use the same gateway, which is located at the ISP's central office.

You can identify a bridge-mode WAN link by the IP addresses, default gateway and netmask that the ISP provides you. If the number of deducting 3 (network IP, gateway IP and broadcast IP) from the IP range that the netmask divides is larger than the number of usable IP addresses that ISP provides you, it means you are given a segment of a IP network, a bridge-mode WAN link. For example, the ISP gives you three usable IP addresses 61.88.100.1 - 61.88.100.3, default gateway 61.88.100.254 and netmask 255.255.255.0. The netmask 255.255.255.0 divides 256 IP addresses which contains 253 host addresses, one gateway address, one broadcast address and one address for the network ID. The number of host addresses that the netmask divides (253) is larger than number of IP addresses the ISP provides (3). You have to configure a WAN link to FortiWAN as **Bridge Mode: One Static IP** if the WAN link is in bridge-mode and ISP allocates only one IP address for you, or **Bridge Mode: Multiple Static IP** if the WAN link is in bridge-mode and ISP allocates multiple IP addresses for you.



Traffic going to or coming from the near WAN (see Near WAN) is treated by FortiWAN in two different ways for routing-mode WAN link and bridge-mode WAN link. Configuring WAN links to FortiWAN as mismatched WAN type results in unexpected behaviors to traffic.

### See also

- [Configurations for a WAN link in Routing Mode](#)
- [Configurations for a WAN link in Bridge Mode: One Static IP](#)
- [Configurations for a WAN link in Bridge Mode: Multiple Static IP](#)
- [Configurations for a WAN link in Bridge Mode: PPPoE](#)
- [Configurations for a WAN link in Bridge Mode: DHCP](#)

## Near WAN

FortiWAN defines an area in WAN as near WAN, which traffic transferred in/from/to the area would not be counted to the WAN links. That means traffic coming from or going to near WAN through a WAN port would not be controlled by FortiWAN.

FortiWAN defines a near WAN for a WAN link in different ways between routing mode and bridge mode.

- In routing mode, the default gateway of a subnet deployed in WAN or in WAN and DMZ is near to FortiWAN. Therefore, the area between the default gateway and FortiWAN is called near WAN. In the other words, FortiWAN treats directly the subnet deployed on the WAN port as near WAN. The near WAN contains the default gateway.

- In bridge mode, the default gateway is located at ISP's COT and the IP addresses allocated on FortiWAN are just a small part of a subnet shared with others. Therefore, only the IP addresses deployed in WAN are treated as near WAN (not include the remote gateway).

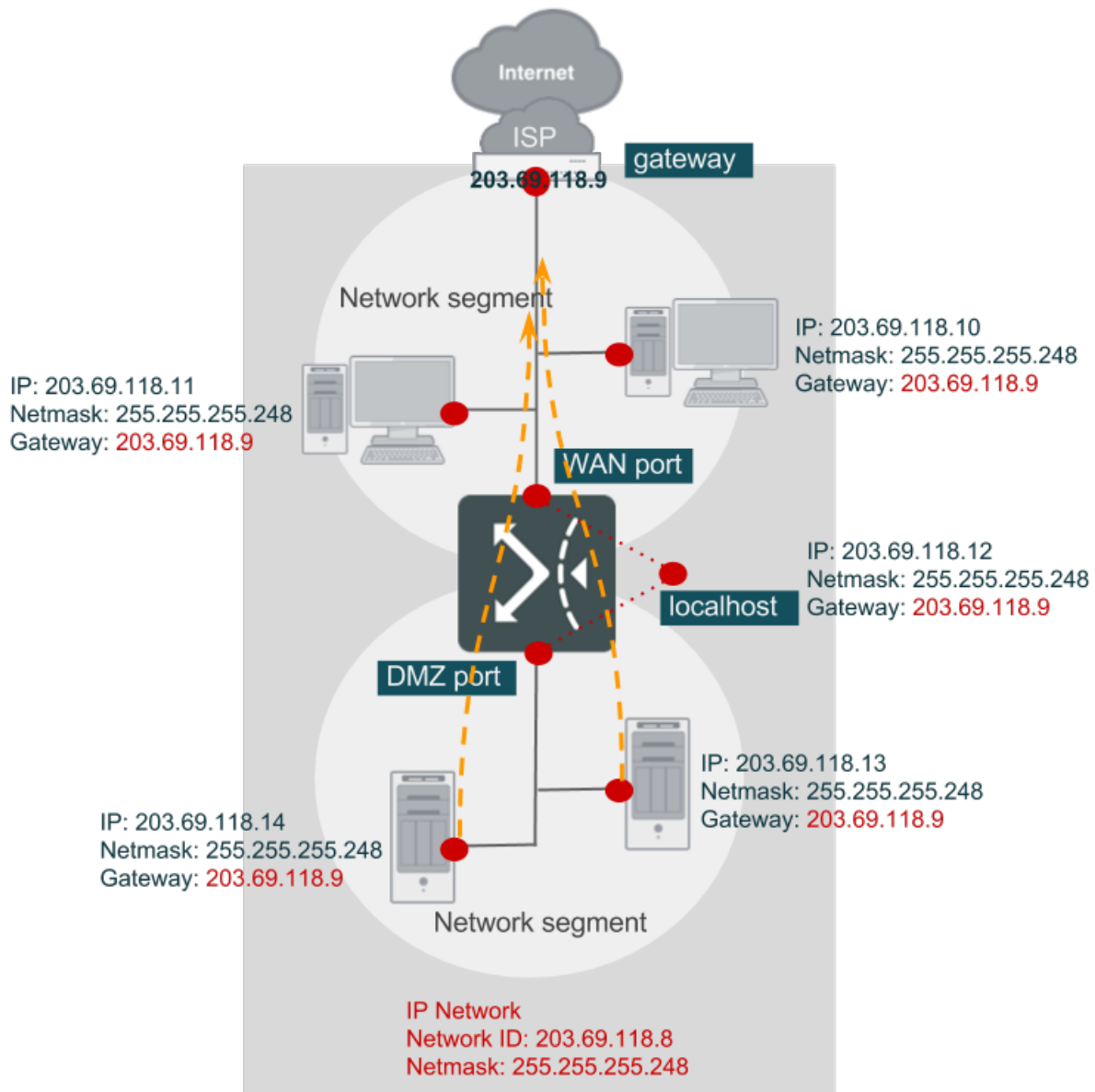
This is the reason FortiWAN separates WAN link configuration into different type: routing mode and bridge mode (See "[WAN types: Routing mode and Bridge mode](#)"). If you configure a bridge-mode WAN link that ISP provides on FortiWAN as Routing Mode and the bridge-mode WAN link might belong to a shared class C subnet, FortiWAN treats the whole class C network as near WAN, traffic goes to or comes from the class C network would be ignored for FortiWAN's balancing, management and statistics functions. That would be a big mistake.

#### See also

[WAN types: Routing mode and Bridge mode](#)

### Public IP Pass-through (DMZ Transparent Mode)

As an intelligent router, FortiWAN is generally supposed to forwards packets between networks connected to its network ports according to the specified IP routing table, and any IP broadcast packet, including the ARP request, would not be forwarded. So that each of the connected network segments should be a separate layer 3 IP network. However, this can be different for particular WAN link deployments - **routing-mode WAN links** and **multiple-static -IP bridge-mode WAN links**. FortiWAN's Public IP Pass-through logically combines a WAN port and a DMZ port to one localhost. By performing Proxy ARP (for IPv4) and ND Proxy (for IPv6) on the combined localhost, the connected layer 1 segments are combined to a common layer 2 segment. An IP network can be deployed and operate correctly over the two network segments. Public IP Pass-through minimizes the adaptation to current network topology and requires no changes to configurations on existing servers while introducing FortiWAN into the network. It is flexible to deploy some of the multiple public IPs that ISP provides for the WAN link to DMZ for external-facing services. Note that Public IP Pass-through will be activated automatically if a WAN link is configured as routing mode and deployed with "subnet in WAN and DMZ", or configured as multiple-static -IP bridge mode with IP addresses being deployed in both WAN and DMZ segments. The following diagram shows how an IP network 203.69.118.11/255.225.255.248 is deployed over a WAN port and a DMZ port.



### See also

- [WAN types: Routing mode and Bridge mode](#)
- [Scenarios to deploy subnets](#)
- [Configuring your WAN](#)

## Scenarios to deploy subnets

No matter an available subnet (routing mode) or an IP range of a shared subnet you obtain from ISP, you will need making a plan how to deploy the multiple IP addresses.

To deploy the available subnet that ISP provides (routing mode) on FortiWAN, there are four different scenarios (be called subnet types as well) for your options:

**Subnet in WAN** : Deploy the subnet in WAN.

**Subnet in DMZ** : Deploy the subnet in DMZ.

**Subnet in WAN and DMZ** : Deploy the subnet in both WAN and DMZ. FortiWAN's Public IP Pass-through function makes the two Ethernet segments in WAN and in DMZ one IP subnetwork (See "[Public IP Pass-through](#)").

**Subnet on Localhost** : Deploy the whole subnet on localhost.

For cases of obtaining an IP range (bridge mode), the IP addresses could be allocated to:

**IP(s) on Localhost** : Allocate the IP addresses on localhost.

**IP(s) in WAN** : Allocate the IP addresses in WAN.

**IP(s) in DMZ** : Allocate the IP addresses in DMZ.

## Static Routing Subnet

If there are subnets, which are called static routing subnets, connected to a basic subnet, it's necessary to configure the static routing for external accessing to the static routing subnets.

### See also

- [WAN types: Routing mode and Bridge mode](#)
- [Public IP Pass-through](#)
- [Configuring your WAN](#)
- [LAN Private Subnet](#)

## VLAN and port mapping

Customers can assign every physical port (except the HA port) to be a WAN port, LAN port or a DMZ port on demand, which is called Port Mapping as well. The WAN ports, LAN ports and DMZ ports are actually physical ports on FortiWAN, they are just not at the fixed positions. The port mapping will be reflected in related configurations. FortiWAN supports IEEE 802.1Q (also known as VLAN Tagging), but it does not support Cisco's ISL. Every physical port (except the HA port) can be divided into several VLAN with a VLAN switch, and those virtual ports can be mapped to WAN port, LAN port or DMZ port as well.

### See also

[Configurations for VLAN and Port Mapping](#)

## IPv6/IPv4 Dual Stack

FortiWAN supports deployment of IPv6/IPv4 Dual Stack in [[Routing Mode](#)], [[Bridge Mode: One Static IP](#)], [[Bridge Mode: Multiple Static IP](#)] and [[Bridge Mode: PPPoE](#)]. For configuration of IPv6/IPv4 Dual Stack, please select appropriate WAN Type (See "[WAN types: Routing mode and Bridge mode](#)") for the WAN link according to the IPv4 you are provided by ISP as mentioned previously, and configure for IPv4 and IPv6 at the WAN link together.



Except a WAN IPv6 subnet used to deploy for a WAN link, ISP might provide an extra LAN IPv6 subnet for deploying your LAN. Depending on the demand, the LAN IPv6 subnet can be deployed as basic subnet in DMZ as well for the WAN link.

## FortiWAN in HA (High Availability) Mode

### Installing FortiWAN in HA mode

When two FortiWAN units work together, they can be configured to HA (High Availability) double-device backup mode. This setup allows two FortiWAN units to server as backup for each other. The master is the main functioning unit, while the slave is the backup unit in standby. An FortiWAN unit alone already has built-in fault tolerance mechanism. All its OS and control applications are stored in Flash Memory, so sudden loss of electricity will not damage the system. But when the network must provide non-stop service for mission-critical applications, the HA mode becomes a must. With HA, FortiWAN serves a significant solution to accomplish network fault tolerance.

FortiWAN supports hot backup in HA by heartbeat mechanism. When both FortiWAN are on, one unit (the master) performs operations, with the other (the slave) in standby. If the master fails for power failure or hardware failure (including normal power off and system reboot), hot backup performs a switch-over to the slave (heartbeat detection fails). This function logically promotes the slave to activate HA and to resume the role of the master. The failed master unit will take the role of slave after it resumes from reboot. The HA hot-backup solution significantly limits the downtime, and secures uninterrupted operation for critical applications.

Hot backup also implies data synchronization. FortiWAN HA performs system configurations synchronization between the master and slave units. Applying configurations to the master unit from Web UI triggers a synchronization to the slave unit. Besides, as long as the peer unit resumes as slave mode from system rebooting, the master also synchronizes system configures with it. This mechanism guarantees the identical system configurations for the two units.

In case that two units are inconsistent with firmware version, FortiWAN model and throughput license, only one unit takes the role of master while the peer unit stay the booting status. A master unit cannot synchronize system configurations with the unit that is in booting status. A message "Incompatible" is displayed for Peer Information in the Summary page of the master's Web UI.

### Setting Up HA

FortiWAN's double-device backup setup is easy to use. Simply connect the HA RJ-45 ports on both FortiWAN units with a Ethernet cable. Note that HA deployment requires identical firmware version, model and throughput license on the two units.

#### Activating HA Mode

1. Install the master FortiWAN.
2. Connect the slave FortiWAN to the master with a Ethernet cable.
3. Switch on the slave.

FortiWAN-VM uses the vNIC1 as the HA port. To deploy FortiWAN-VM appliances as HA mode, allocate the vNIC1 of two appliances to the same virtual network (vSwitch). HA deployment is not supported for two FortiWAN-VM appliances that both are 15-day trails. It requires one 60-day trial or a permanent license for the two appliances (in DH mode) at least.

After HA mode has been activated, the Master emits 4 beeps, and the Slave does 3. The status of the Slave is displayed under [System] > [Summary] > [Peer Information] on the master's Web UI. Note that a slave's Web UI is not available.

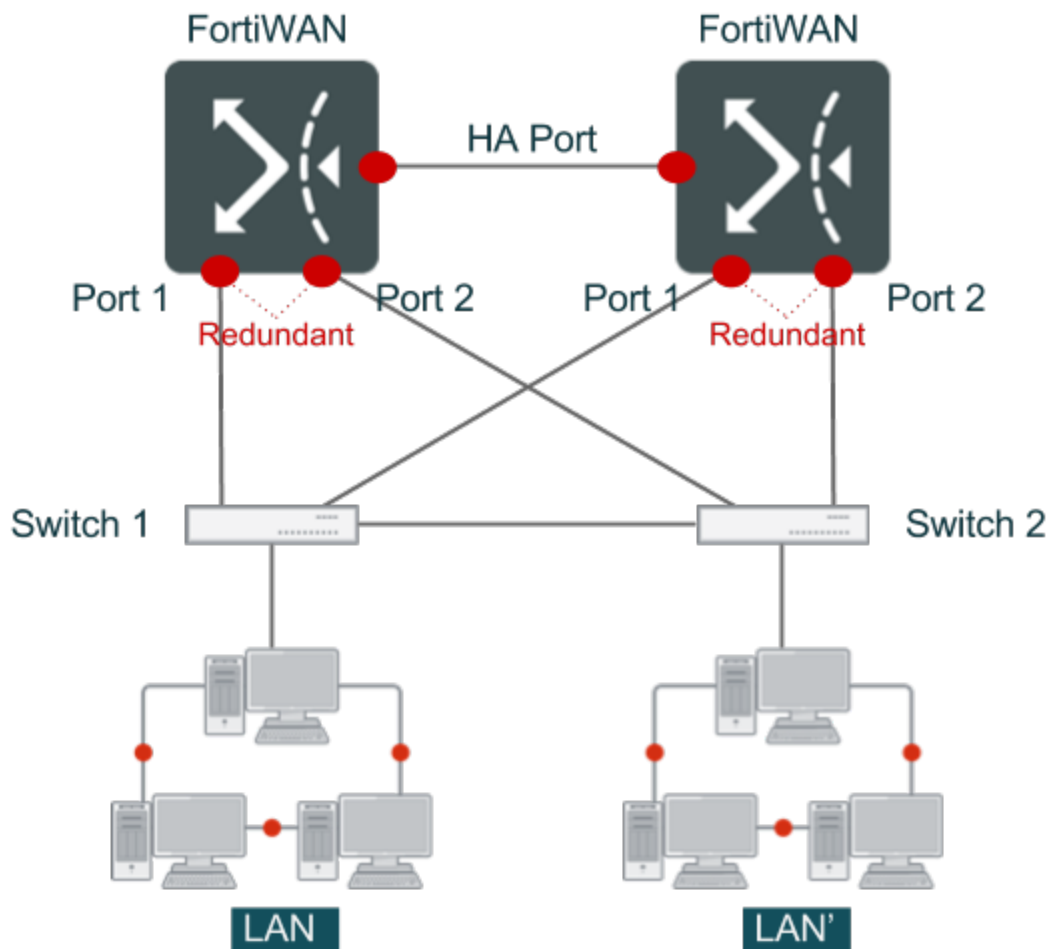
Once the master is down, the slave emits 1 beep and resumes the role of the master to keep network alive.

Switching on the two units together, then the unit with larger Up Time or Serial Number takes the role of master, while the peer unit takes the role of slave.

Note: Ensure the cable is solidly plugged in both units. Otherwise, it may cause errors. After the master locates the slave, system will activate HA mode.

### Redundant LAN Port and/or redundant DMZ port: FortiWAN in HA mode

As illustrated in the topology below, two FortiWAN units work in HA mode, with one active and the other in standby. Port1 and port2 acts as redundant LAN port for each other, putting the two units into hot backup mode. This mode offers a significant solution against single point failure in LAN/DMZ (See "[Configurations for VLAN and Port Mapping](#)").



## High Availability (HA) Scenarios

### Firmware Update Procedure in HA Deployment

Firmware update on both master and slave units under HA deployment can be completed at once (one firmware update instruction). The firmware update procedure in HA deployment is similar to the non-HA (single unit) procedure:

1. Log onto the master unit as Administrator, go to [System]→[Summary], double check and make sure the peer device is under normal condition (See "[Summary](#)").
2. Execute the firmware update with uploading the firmware file (See "[Administrator](#)"). Please wait as this may take a while.

The master unit starts with verifying the uploaded firmware file for master and slave units (system can not be uploaded with a firmware file that is earlier than the version system is running on). The slave unit then receives a duplicate of firmware file from master unit, and starts to update firmware. The master unit holds on updating itself until the update on slave unit completes. Once slave completes its update, the master unit starts updating itself then, while slave gets into reboot procedure. The whole update procedure will complete after the two units recover from system reboot. The asynchronous update procedure on the two units causes the peer unit recovering from reboot earlier than local unit, and the master-slave relationship will switch therefore.

The whole firmware update will be aborted if any abnormality happens during updating on slave. The master unit will not get updating itself without updating successfully on slave unit. Abnormal termination of firmware update does not trigger system reboot, and therefore the master-slave relationship will not switch.

During the firmware update, the heartbeat mechanism over master and slave units stops temporarily until the firmware update succeeds or is terminated by abnormality.

After the firmware update is complete, the firmware version number displayed in fields [System Information] and [Peer Information] on Web UI page [System > Summary] should be updated and identical. The information displayed in field [Peer Information] gives reference to judge the update.

**Version = Updated version number, State = Slave:** Firmware update succeeds on both units.

**Version = Non-updated version number, State = Slave:** Firmware update is aborted by abnormalities. Both units fail to update. Please perform the HA firmware update again (with [Update Slave] being checked).

**Version = Updated version number, State = Incompatible:** The peer unit succeeds in updating, but the local unit fails. Please perform the single unit firmware update (without [Update Slave] being checked).

**Version = Non-updated version number, State = Incompatible:** The local unit succeeds in updating, but the peer unit fails. Please reboot local unit to switch the master-slave relationship of the two units. Reconnect and login to Web UI, and perform the single unit firmware update (without [Update Slave] being checked).

Note: If there are abnormal behaviors in the DMZ or public IP servers, go to [System] → [Diagnostic Tools] → [ARP Enforcement] and execute [Enforce] for troubleshooting. Also notice that if the Ethernet cable for HA between the master and slave is removed or disconnected.

If abnormal behaviors appear consistently, please remove the network and HA cable, and perform the firmware update procedure again to both system individually. Then reconnect them to the network as well as the HA deployment.

If repetitive errors occur during the firmware update process, DO NOT ever switch off the device and contact your dealer for technical support.

## HA Fallback to Single Unit Deployment

The steps to fallback to single unit deployment from HA are:

1. Log onto Web UI via Administrator account. Go to [System] → [Summary] and double check and make sure the peer device is under normal condition (See "[Summary](#)").
2. Turn the Master off if the Master is to be removed. The Slave will take over the network immediately without impacting services. If the Slave is to be removed, then simply turn the Slave off.
3. Remove the device and the associated cables.

Steps of the Slave Take Over are:

1. In the HA setup, the Master unit is in an active state and serving the network at the meanwhile the Slave unit is monitoring the Master.
2. In the case of unit failover (Hardware failure, Power failure, HA cable failure, etc), the Slave takes over the network and beeps once when the switchover is completed. The switchover requires 15 seconds or so since negotiations for states.
3. The switched Master unit becomes the Slave unit in the HA deployment even it is repaired from failures. You can power cycle the Master unit to have another switchover to the units.

## Long-distance HA deployment

Sometimes the two FortiWAN appliances used to establish HA deployment are apart from each other geographically. It requires several Ethernet switches or bridges to connect the two appliances across areas or buildings. Since FortiWAN is designed to join a HA deployment by directly connecting the two RJ-45 ports (HA ports) with a Ethernet cable, it is supposed that there is not any non-HA Ethernet frames broadcasted between the two appliances. The HA messages interchanged for availability detection are raw Ethernet frames of EtherType 0x88B6 (LOCAL2), not 0x0800 (IPv4); and the mechanism of FortiWAN's HA deployment is very sensitive to non-HA Ethernet frames. For this reason, it requires STP and ARP being disabled on the switch (connecting the two FortiWAN units) to avoid misleading the judgment on HA takeover. Besides, please create a port base VLAN on the switch to isolate the HA connectivity from other subnets if necessary.

## Get HA information via SNMP and event notifications via SNMP trap

You can use SNMP manager to get slave unit information and receive notifications when the slave unit fails, recovers and take over the master unit. Configure SNMP for your FortiWAN unit (See "[SNMP](#)") to get the information in a MIB field via SNMP manager. Configure the SNMP manager on your FortiWAN and enable the event types "HA slave failure and recovery" and "HA takeover" to notify (See "[Notification](#)"), then notifications will be delivered to your SNMP manager for the events. The correspondent MIB fields and OIDs are listed as following:

### SNMP field names and OIDs

| MIB Field          | OID                       | Description                                                                  |
|--------------------|---------------------------|------------------------------------------------------------------------------|
| fwnSysHAMode       | 1.3.6.1.4.1.12356.118.1.1 | Boolean values used to indicate if the FortiWAN unit supports HA deployment. |
| fwnSysSlaveVersion | 1.3.6.1.4.1.12356.118.1.2 | Firmware version of the slave unit deployed with this local unit in HA mode. |

| MIB Field               | OID                           | Description                                                                                                                                              |
|-------------------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| fwnSysSlaveSerialNumber | 1.3.6.1.4.1.12356.118.1.3     | Serial number of the slave unit deployed with this local unit in HA mode.                                                                                |
| fwnSysSlaveUptime       | 1.3.6.1.4.1.12356.118.1.4     | Uptime of the slave unit deployed with this local unit in HA mode.                                                                                       |
| fwnSysSlaveState        | 1.3.6.1.4.1.12356.118.1.5     | State of the slave unit deployed with this local unit in HA mode.                                                                                        |
| fwnEventHASlaveState    | 1.3.6.1.4.1.12356.118.3.1.3.1 | Send event notification when the slave unit deployed with the local (master) unit in HA mode fails or recovers from a failure: recovery (1), failure(2). |
| fwnEventHATakeover      | 1.3.6.1.4.1.12356.118.3.1.3.2 | Send event notification when the master (local) unit in HA deployment is took over by its slave unit: true(1), false(2).                                 |

**See also**

- [Summary](#)
- [Configurations for VLAN and Port Mapping](#)
- [Administrator](#)

## Web UI and CLI Overview

FortiWAN provides the Web User Interface (Web UI) which is the primary interface for network deployments, administration, configurations and traffic statistics and analysis. FortiWAN's Command Line interface (CLI) provides basic commands for trouble shooting and system recovery. This section starts with the steps to connect to FortiWAN's Web UI and CLI while the first time using FortiWAN product. Afterward a basic and common concept about using Web UI is introduced.

### Connecting to the Web UI and the CLI

Be aware that the position of LAN port may vary depending on models. FortiWAN-200B, for example, has five network interfaces, with its fourth interface as LAN port and fifth as DMZ port (see [Network interfaces and port mapping](#)).

Before setting up FortiWAN in your network, ensure the following are taken care of:

- Check network environment and make sure the following are ready before FortiWAN installation and setup: well-structured network architecture, and proper IP allocation.
- Use cross-over to connect PC to FortiWAN LAN port instead of straight-through.

## Default LAN port

FortiWAN's LAN port (see [Network interfaces and port mapping](#)) is used to connect to a private LAN subnet and provides the access to the Web UI. The default subnet configured on LAN port is 192.168.0.0/255.255.255.0 and the localhost IP address is 192.168.0.1, which means you can connect to LAN port (192.168.0.1) from a management computer in the subnet 192.168.0.0/255.255.255.0 without changing network setting on LAN port. For example, connect directly a management computer that IP address/netmask is 192.168.0.10/255.255.255.0 to the LAN port.

For the first time accessing to the Web UI, you can get the connection via a computer matching with the default LAN subnet (See the section "Access via a computer that matches the default LAN IP address" below). However, the default subnet configured on LAN port might conflict with or be unreachable from your existing network, especially for the deployments of FortiWAN-VM. If you want to have the connection to LAN port from a subnet that does not match the default LAN IP address, such as an existing subnet 10.10.10.0/255.255.255.0, you have to change the network setting of LAN port via CLI to match the subnet (See the section "Access via a computer that does not match the default LAN IP address" below).

## To connect to the Web UI

The default IP address of LAN port is 192.168.0.1 and the netmask is 255.255.255.0. For the first time accessing the Web UI, you can get the access via a computer connected directly to FortiWAN, or via a computer in a existing LAN subnet connected to FortiWAN.

Requires: Microsoft Internet Explorer 6, Mozilla Firefox 2.0, or Google Chrome 2.0 or newer.

## Access via a computer that matches the default LAN IP address

- Using the Ethernet cable, connect LAN port of the appliance to your computer. For a FortiWAN-VM appliance, connect your computer to the virtual network (vSwitch) of the LAN port of FortiWAN-VM appliance.
- Switch on FortiWAN. It will emit 3 beeps, indicating the system is initialized and activated. Meanwhile, the LAN port LED blinks, indicating a proper connection.
- By default, the LAN IP address is 192.168.0.1. Configure your computer to match the appliance's default LAN subnet. For example, on Windows 7, click the Start (Windows logo) menu to open it, and then click Control Panel. Click Network and Sharing Center, Local Area Connection, and then the Properties button. Select Internet Protocol Version 4 (TCP/IPv4), then click its Properties button. Select Use the following IP address, then change your computer's settings to:
  - IP address: 192.168.0.2 (or 192.168.0.X)
  - Subnet mask: 255.255.255.0
- To connect to FortiWAN's web UI, start a web browser and go to <https://192.168.0.1>. (Remember to include the "s" in <https://>.)
- Login to web UI with the default username, `admin`, and leave the password field blank (case sensitive).

## Access via a computer that does not match the default LAN IP address

- Connect to the CLI (See the section "To connect to the CLI" below).
- Configure the network setting of LAN port to match the existing LAN subnet (See the section "Change network setting to LAN port via CLI" below).

- After system reboots, connect the subnet to the LAN port of FortiWAN appliance.
- To connect to FortiWAN's web UI, start a web browser on a computer in the subnet and go to `https://xxx.xxx.xxx.xxx`, where `xxx.xxx.xxx.xxx` is the IP address assigned to LAN port. (Remember to include the "s" in `https://`.)
- Login to web UI with the default username, `admin`, and leave the password field blank (case sensitive).

**Note:**

1. Make sure the proxy settings of the web browser are disabled. For example, open Internet Explorer and select "Internet Option" on "Tools" menu. Click the "Connection" tab, "LAN settings" and open "Local Area Network Settings" dialog box, then disable "Proxy server".
2. Default account `admin` has the Administrator permission (See "[Administration/Administrator and Monitor Password](#)"). It is strongly recommended to reset the passwords ASAP, and take good care of it.
3. Web UI supports concurrent multiple sign-in (See "[Using the Web UI/Multi-user Login](#)").
4. The default Username/Password, `Administrator/1234` and `Monitor/5678`, used for V4.0.x remain in this version, but will be removed in next version.
5. FortiWAN supports Web UI access from the Internet by connecting to the WAN ports. For example, start the web browser and go to `https://xxx.xxx.xxx.xxx`, where `xxx.xxx.xxx.xxx` is the IP address assigned to a WAN port (see [Configuring Network Interface](#)). However, FortiWAN's Firewall denies any access to FortiWAN's localhost coming from the Internet (WAN) by default (see [Firewall](#)). Therefore, LAN port is the only way for your first time Web UI accessing. Then it is your option to configure network setting to a WAN link (WAN port) and modify the firewall rules to accept localhost accessing from the Internet.

## To connect to the CLI

Requires: Terminal emulator such as HyperTerminal, PuTTY, Tera Term, or a terminal server

- Using the console cable, connect the appliance's console port to your terminal server or computer. On your computer or terminal server, start the terminal emulator
- Use these settings:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None
- Press Enter on your keyboard to connect to the CLI
- Login with the default username, `admin`, and leave the password field blank (case sensitive)

FortiWAN maintains a common local authentication database for its Web UI and CLI. Accounts defined as group Administrator are able to CLI with its username and password.

Note: FortiWAN CLI has limited functionality and cannot fully configure the system. Normal configuration changes should be done via the WebUI.

## Change network setting to LAN port via CLI

1. Connect and log into the CLI (See the section "To connect to the CLI" above).
2. Configure the IP address and netmask of LAN port via command `resetconfig`. Also configure a static route with a default gateway if it's necessary. Type:

```
resetconfig <ip_address/netmask>
```

```
resetconfig <ip_address/netmask> <network_ip/netmask@gateway_ip>
```

where:

`<ip_address/netmask>` is the IPv4 address and netmask assigned to the LAN port. It must correspond to the subnet you would like to connect to. For example, type `resetconfig 10.10.10.1/255.255.255.0`, if 10.10.10.0/255.255.255.0 is the subnet connected to the LAN port. Then IP address of LAN port is changed to 10.10.10.1 from the default.

`<network_ip/netmask@gateway_ip>` is the routing rule assigned to the LAN port, so that packets can be routed to the subnet via the gateway. For example, type `resetconfig 192.168.2.254/255.255.255.0 192.168.1.0/255.255.255.0@192.168.2.1`, if 192.168.2.0/255.255.255.0 is the subnet connected directly to the LAN port and 192.168.2.1 is the gateway to route packets to subnet 192.168.1.0/255.255.255.0. Then IP address of LAN port is changed to 192.168.2.254 from the default.

See "[Console Mode Commands](#)" for details.

3. System reboots for applying the configurations.



## Using the Web UI

### Web UI Overview

The screenshot shows the FortiWAN Web UI interface. Labels point to various components:

- Navigation menu:** Points to the left sidebar menu.
- Model:** Points to the 'Model' field in the header.
- Serial number:** Points to the 'Serial number' field in the header.
- Current login account and the associated IP:** Points to the 'Administrator@10.12.107.20' field in the header.
- System time:** Points to the '2016/06/04 15:36:52' field in the header.
- Current page (may contain sub-panes):** Points to the main content area.

The interface includes a header bar with the FortiWAN logo, model (FWN200B), serial number (FWN2HB-VM-000002), login account (Administrator@10.12.107.20), system time (2016/06/04 15:36:52), and buttons for Apply, Refresh, Help, and Logout. The left sidebar contains a navigation menu with categories like System, Network Setting, WAN Link Health Detection, and Administration. The main content area displays 'System Information' and 'Peer Information' tables, along with a 'WAN Link State' table.

|                   |                          |
|-------------------|--------------------------|
| Version           | V4.03.0-build0704 160704 |
| Model / Bandwidth | FWN200B / 200 Mbps       |
| Serial Number     | FWN2HB-VM-000002         |
| Uptime            | 0 day(s), 00:59:29       |
| Connections       | 249                      |
| CPU Usage %       | 0%                       |
| Packets / Second  | 5                        |
| VRRP State        | VRRP Disabled            |
| Hard Disk         | N/A                      |

|                   |      |
|-------------------|------|
| Version           | None |
| Model / Bandwidth | None |
| Serial Number     | None |
| Uptime            | None |
| State             | None |

| WAN | State | IPv4 Address | IPv6 Address | Note |
|-----|-------|--------------|--------------|------|
| 1   | OK    | 10.12.107.20 |              |      |

Once you log in, you will see the operating page that is divided into three parts, the **header** is located at the upper side of the screen, the **navigation menu** is located on the left side of the screen, and the **content pane** is located on the center of the screen.

**Header** contains information and items which are unrelated to FortiWAN's functions.

- **Current login account:** Display the account you login as and the IP address you login from.
- **System Time:** Display the FortiWAN's system time.
- **Current operating page:** Display the path (Main category > Page name) of the operating page displayed in Content Pane.
- **Apply:** The button for applying configurations. Pages for only displaying information or statistics contain no Apply button.
- **Reload:** The button for reloading current operating page.
- **Help:** The button for getting the Help information of current operating page.
- **Logout:** The button for logging out Web UI.

[System/Summary] shown above indicates page contents are displayed of [System] > [Summary], and [Administrator@125.227.251.80] indicates Administrator account log in from IP 125.227.251.80. Note that do not use your browser's Back button to navigate, pages may not operate correctly.

**Navigation Menu** consists of six main categories: **System, Service, Statistics, Log, Reports and Language**. Each category contains sub-menu of individual functions. To expand a category, simply click it. To display the operating page of a function from a sub-menu, click the name of the function and it will display on the content pane.

- **System:** Contains necessary items to maintain the FortiWAN; they are Summary, Network Setting, WAN Link Health Detection, Optimum Route Detection, Port Speed/Duplex Setting, Backup Line Setting, IP Grouping, Service Grouping, Busyhour Setting, Diagnostic Tools, Date/Time, Remote Assistance and Administration (See "[System Configurations](#)" and "[Configuring Network Interface \(Network Setting\)](#)"). Administration is not available to Monitor permission, it is invisible on the menu to a Monitor account.
- **Service:** Contains the services the FortiWAN provides; they are Firewall, NAT, Persistent Routing, Auto Routing, Virtual Server, Bandwidth Management, Connection Limit, Cache Redirect, Multihoming, Internal DNS, DNS Proxy, SNMP, IP-MAC Mapping and Tunnel Routing (See "[Load Balancing & Fault Tolerance](#)" & "[Optional Services](#)").
- **Statistics:** Contains basic statistics of FortiWAN's system, services and traffic; they are Traffic, BM, Persistent Routing, WAN Link Health Detection, Dynamic IP WAN Link, DHCP Lease Information, RIP & OSPF Status, Connection Limit, Virtual Server Status, FQDN, Tunnel Status and Tunnel Traffic (See "[Statistics](#)").
- **Log:** Contains managements of system logs; they are View, Control, Notification and Reports (See "[Log](#)").
- **Reports:** Contain the advanced analysis and long-term statistics of FortiWAN's system, services and traffic; they are Bandwidth, CPU, Session, WAN Traffic, WAN Reliability, WAN Status, TR Reliability, TR Status, In Class, Out Class, WAN, Service, Internal IP, Traffic Rate, Connection Limit, Firewall, Virtual Server, Multihoming, Dashboard and Settings (See "[Reports](#)").
- **Language:** Support English, Traditional Chinese and Simplified Chinese for options to display Web UI in multiple languages,

**Content Pane** displays related items of a function specified from the left menu.

## Multi-user Login

FortiWAN's Web UI supports multiple sign-in. The maximum limit for users can log-in concurrently is 20 users, account permission (See "[Administration\Administrator and Monitor Password](#)") insensitive. An user get failed to log-in if there have been 20 users in the Web UI concurrently. FortiWAN Web UI does not accept multiple login from the same host and the same browser. Users that attempt to login to Web UI via the same host and browser (different tabs or windows) will be logged out (including the one who is already in Web UI).

Configurations to FortiWAN applied concurrently via Web UI by the multiple users are arranged and processed in order (one by one). It takes time for system to complete every single configuration applying; therefore, when multiple configurations are in the queue to be applied, it might take a little extra time to wait for system getting previous applications complete for the users after clicking the Apply button. Configurations to different functions are queued up together to be applied. For example, an configuration to Auto Routing (made by user A) will be queued if a configuration to Multihoming (made earlier by user B) has being processed.

FortiWAN does not provide multi-thread to run concurrent Tunnel Routing Benchmark (See "[Tunnel Routing - Benchmark](#)"). An alert displays to the users who try to start Tunnel Routing Benchmark Client\Server via WebUI if the Benchmark Client\Server is already running (started earlier by one user).

## Basic concept to configure via Web UI

FortiWAN's services (load balancing, fault tolerance and other optional services) are based on Policy and Filter. Policies (or called Classes as well) are specified items indicating different actions for a service. Policies are applied to different objects classified by the predefined filters. Basically, a object is classified by the combinations of When, Source, Destination and TCP/UDP/ICMP Service. A filter contains the settings of those items When, Source, Destination and Service, and also an associated Policy. Traffic that matches the filter will be applied to the specified policy.

## The common operation buttons

FortiWAN manages most of its rules/filters/policies with top-down evaluation method where the rules are prioritized in descending order.

-  Click this button, to add a new rule below the current rule.
-  Click this button, to delete the rule.
-  Click this button, to move the rule up a row.
-  Click this button, to move the rule down a row.
-  Write a note for this rule.
- ☐ The function is disabled.
- ☒ The function is enabled.
-  This symbol indicates a default policy, rule or filter, which is unmodifiable and indelible.

## Configuration on When

This is for filtering traffic by different time period which is predefined in "[Busyhour Settings](#)".

## Configuration on Source and Destination

This is for filtering the established sessions from/to specified source/destination. The options are:

- IPv4/IPv6 Address** : Matches sessions coming from or going to a single IPv4/IPv6 address. e.g. 192.168.1.4.
- IPv4/IPv6 Range** : Matches sessions coming from or going to a continuous range of IP addresses. e.g. 192.168.1.10-192.168.1.20.

|                         |   |                                                                                                                               |
|-------------------------|---|-------------------------------------------------------------------------------------------------------------------------------|
| <b>IPv4/IPv6 Subnet</b> | : | Matches sessions coming from or going to a subnet.<br>e.g. 192.168.1.0/255.255.255.0.                                         |
| <b>WAN</b>              | : | Matches sessions coming from or going to WAN.                                                                                 |
| <b>LAN</b>              | : | Matches sessions coming from or going to LAN.                                                                                 |
| <b>DMZ</b>              | : | Matches sessions coming from or going to DMZ.                                                                                 |
| <b>Localhost</b>        | : | Matches sessions coming from or going to FortiWAN.                                                                            |
| <b>Any Address</b>      | : | Matches all sessions regardless of its source or destination.                                                                 |
| <b>FQDN</b>             | : | Matches sessions coming from or going to FQDN.                                                                                |
| <b>IP Grouping Name</b> | : | Matches sessions coming from or going to the IP addresses that predefined in IP groups (See " <a href="#">IP Grouping</a> "). |

## Configuration on Input Port

This is for filtering the traffic coming from specified physical ports. Input Port are the item used to evaluate outbound traffic for only Auto Routing (See "[Auto Routing](#)") so far. Ports (normal ports, VLAN ports, redundant LAN\DMZ ports and aggregated LAN\DMZ ports) defined in [Network Setting > VLAN and Port Mapping] (See "[Configurations for VLAN and Port Mapping](#)") are listed for options:

|                             |   |                                                                 |
|-----------------------------|---|-----------------------------------------------------------------|
| <b>Port X</b>               | : | Matches sessions coming from the specified normal port.         |
| <b>Port X.[VLAN Tag]</b>    | : | Matches sessions coming from the specified VLAN port.           |
| <b>LAN Bridge: [Lable]</b>  | : | Matches sessions coming from the specified redundant LAN port.  |
| <b>DMZ Bridge: [Lable]</b>  | : | Matches sessions coming from the specified redundant DMZ port.  |
| <b>LAN Bonding: [Lable]</b> | : | Matches sessions coming from the specified aggregated LAN port. |
| <b>DMZ Bonding: [Lable]</b> | : | Matches sessions coming from the specified aggregated DMZ port. |

## Configuration on Service

This is for filtering the established sessions running specified service. It contains some well-known services for options and user-defined services (TCP@, UDP@ and Protocol#):

- FTP (21)
- SSH (22)
- TELNET (23)
- SMTP (25)
- DNS (53)
- GOPHER (70)
- FINGER (79)

- HTTP (80)
- POP3 (110)
- NNTP (119)
- NTP (123)
- IMAP (143)
- SNMP (161)
- BGP (179)
- WAIS (210)
- LDAP (389)
- HTTPS (443)
- IKE (500)
- RLOGIN (513)
- SYSLOG (514)
- RIP (520)
- UUCP (540)
- H323 (1720)
- RADIUS (1812)
- RADIUS-ACCT (1813)
- pcAnywhere-D (5631)
- pcAnywhere-S (5632)
- X-Windows (6000-6063)
- GRE
- ESP
- AH
- ICMP
- TCP@
- UDP@
- Protocol#
- Any

## Console Mode Commands

This section provides further details on the Console mode commands. Before logging onto serial console via HyperTerminal, please ensure the following settings are in place: Bits per second: 9600; Data bits: 8; Parity: None; Stop bits: 1; Flow control: None (See "[Connecting to the Web UI and the CLI](#)").

Note that for some standard utilities such as `tcpdump` or `traceroute`, the options that are not listed here are not supported by FortiWAN.

### help:

Displays the help menu

```
help [COMMAND]
```

Show a list of console commands.

**arp:**

Manipulate (add and delete entries) or display the IPv4 network neighbor cache.

```
arp [-i <port>] -a [<hostname>]
arp [-i <port>] -e
arp -i <port> -s <hostname> <hw_addr>
arp -i <port> -d <hostname>
```

**-a [<hostname>]:** Display the entries of the specified `hostname`. All the entries will be displayed if no `hostname` is specified. Hostnames will be displayed in alternate BSD style output format.

**-e:** Display entries in default (Linux) style.

**-s <hostname> <hw\_addr>:** Manually create an ARP entry mapping for the host `hostname` with the hardware address `hw_addr`. This requires specifying a port via `-i port`.

**-d <hostname>:** Remove the entries for the specified host `hostname`. This requires specifying a port via `-i port`.

**-i <port>:** Specify an network interface (port) of FortiWAN to display, create or remove entries.

**<port>:** Specify an network interface (port) of FortiWAN in format `port#`, e.g. `port1`, `port2` and etc.

**<hostname>:** Specify the target IP address or domain name.

**<hw\_addr>:** Specify the MAC address.

Note: If domain name is to be used in the `hostname` parameter, the DNS Server must be set in the Web UI [System]->[Network Settings]->[DNS Server].

**arping:**

Discover and prob hosts on a network by sending ARP requests

```
arping <hostname> <link> <index>
```

Send an ARP request to ask the MAC address of an IP address and display the result.

**<hostname>:** Specify the target IP address or domain name (MAC address is not supported). Note that domain name is valid only if parameter `<link>` is specified as "wan".

**<link>:** Specify the link or ports that the ARP request is sent through. The valid values are "wan", "dmz" and "lan".

**<index>:** Specify the index of a WAN link if `<link>` is specified as "wan". The valid values are 1, 2, 3, ...,etc.

Example:

**arping 192.168.2.100 lan** will send an ARP request through LAN ports to ask the MAC address of host 192.168.2.100.

**arping 10.10.10.10 wan 1** will send an ARP request through WAN link 1 to ask the MAC address of host 10.10.10.10.

Note: If domain name is to be used in the `hostname` parameter, the DNS Server must be set in the Web UI [System]->[Network Settings]->[DNS Server].

**callhome:**

Get the logs of automated local configuration (see [Automated Local Configuration](#)).

```
callhome showlog
```

**date:**

Get or set system software/hardware time.

```
date [-h] [HH:MM[:SS] [[YYYY-]MM-DD]]
date [-h] [HH:MM[:SS] [[YYYY/]MM/DD]]
```

where

**-h:** Get hardware time (without date and/or time being specified) or set both software and hardware time (with specified date and/or time).

**HH:MM[:SS]:** Set system software time (without **-h** option) or hardware time (with **-h** option). **HH**, **MM** and **SS** indicate the hour, minute and second respectively. It will set the second field as **00** if **SS** is not specified. Please set **HH** in 24-hour format.

**[YYYY-]MM-DD** or **[YYYY/]MM/DD**: Both are used to set system software date (without **-h** option) or hardware date (with **-h** option). **YYYY**, **MM** and **DD** indicate the year, month and day respectively. It will set the year field as current year if **YYYY** is not specified.

For example:

`date` will get current system software time.

`date -h` will get current system hardware time.

`date 15:20:30` will set system software time to 15:20:30.

`date -h 15:20:30 2017-10-31` will set both software and hardware date and time to October 30, 2017 and 15:20:30.

**diagnose:**

Get diagnostic information of FortiWAN hardware

```
diagnose hardware deviceinfo cpu
diagnose hardware deviceinfo disk
diagnose hardware deviceinfo mem
diagnose hardware deviceinfo nic
```

Get information of FortiWAN's CPU, disk, memory and network interface controllers (NICs).

```
diagnose hardware ethtool
```

Display and change parameters of the network interface controllers (NICs) of FortiWAN by the standard Linux utility `ethtool` (V3.7). Execute `diagnose hardware ethtool -h` to get a short help message.

```
diagnose hardware lspci
```

Get information about PCI buses in FortiWAN system and the devices connected to them.

```
diagnose hardware smartctl
```

Control and monitor the storage system of FortiWAN by the standard utility `smartctl` (V6.3). Execute `diagnose hardware smartctl -h` to get a help message or refer to <https://www.smartmontools.org> for details.

**disablefw:**

Disable all the firewall rules

```
disablefw
```

Disable all the configured firewall rules to allow any traffic accessing or passing through FortiWAN. This command rescues Web UI accessing from being inadvertently locked by incorrect firewall rules deployment. System will re-confirm, press [y] to proceed or [n] to cancel.

**enforcearp:**

Force FortiWAN's surrounding machines to update their ARP tables

```
enforcearp
```

System will send gratuitous ARP packets to update their ARP tables. This is for cases where after the initial installation of FortiWAN, machines or servers sitting in the DMZ are unable to be able to connect to the internet.

**exec**

Execute specified program. The available programs are `conntrack`, `optpath` and `config save tftp`.

```
> help exec
exec: Execute program
Usage:
exec conntrack {help|list|delete} [FILTERS]
exec optpath {help|cache list [NETADDR]}
exec config save tftp FILE SERVER
```

**exec conntrack**

List or clear current conntrack in system.

```
conntrack help
```

Display usage of the conntrack program.

```
conntrack delete [wan=N]
```

Delete the conntracks established on the specified WAN N.

```
conntrack {list|delete} [FILTERS]
```

List or deletes the specified conntracks in system according to the filter, where [FILTERS] is a combination of the following parameters in AND logical conjunction:

```
src=[IP_ADDRESS]
dst=[IP_ADDRESS]
rsrc=[IP_ADDRESS]
rdst=[IP_ADDRESS]
```

[IP\_ADDRESS] IP address of source/destination or reply source/destination

```
proto=[PROTO]
```

[PROTO] Protocol number or icmp, tcp, udp, gre, esp, or ah

```
sport=[PORT]
```

```
dport=[PORT]
```

```
rsport=[PORT]
```

```
rdport=[PORT]
```

[PORT] Port number of source/destination or reply source/destination

**Note** that parameters `sport`, `dport`, `rsport` and/or `rdport` must be used together with `proto`.



**Example:**

```
conntrack delete proto=udp dst=192.168.1.1 dport=53
```

**exec optpath**

When Optimum Route is enabled in Dynamic Detect or a combination of Dynamic Detect and Static IP Table, FortiWAN detects RTTs to a class C network via each of the WAN links and keeps the RTT values in system for a aging period for calculating the best WAN link to the class C network. See [By Optimum Route](#) for details.

```
exec optpath cache list
```

List all the detected RTT values in cache.

**Example:**

```
> exec optpath cache list
Subnet [WAN] RTT(usec) Age(sec) [WAN] RTT Age...
2.22.119.0 [1] 20010 299 [2] 20362 299
5.39.184.0 [1] 81401 226 [2] 79267 226
188.166.57.0 [1] 11631 171 [2] 11551 171
```

Detected RTT to network 2.22.119.0 via WAN1 is 20010 (usec) and cache expires in 299 (sec).

Detected RTT to network 2.22.119.0 via WAN2 is 20362 (usec) and cache expires in 299 (sec).

```
exec optpath cache list [NETADDR]
```

List the detected RTT values to [NETADDR], where [NETADDR] is a class C network, such as 8.8.8.0.

**exec config save tftp**

Save system configurations as a file and download the config file via TFTP.

```
exec config save tftp [FILE_NAME] [SERVER]
```

**Example:**

```
> exec config save tftp FortiWan-20180905.cfg 192.168.1.2
```

Save system configurations as the specified file name "FortiWan-20180905.cfg" and download it to TFTP server 192.168.1.2.

```
> exec config save tftp FortiWan-20180905.cfg tftp.mydomain.com
```

Save system configurations as the specified file name "FortiWan-20180905.cfg" and download it to TFTP server tftp.mydomain.com.

Note that the specified file name must be in .cfg format. This command does the same operation as clicking Save in System > Administration > Configuration File on GUI. See [Configuration File](#) for the details.

**export:**

Display configurations of NAT, Multihoming and Virtual Server

```
export <config_name>
```

Display the configurations of FortiWAN's NAT, Multihoming and Virtual Server in the command line interface. You can export the configurations by copying the displayed content to a text file.

**<config\_name>:** Specify the configuration to be displayed. Values of the parameter are `nat`, `multihoming` and `virtual-server` for options.

### get:

Get the version and serial number information of a FortiWAN apparatus

```
get sys status
```

Display the firmware version, serial number and BIOS version of the FortiWAN apparatus.

### httpctl:

Control the web server that Web UI is running on

```
httpctl restart
httpctl showport
httpctl setport <port>
```

System will restart the web server running on FortiWAN for the Web UI, or display the port number occupied by the web server, or specify port number to the web server.

**restart:** Restart the web server.

**showport:** Display the port number that web server is listening.

**setport:** Set the port number for the web server with indicating parameter `port`.

**<port>:** Specify the port number for `setport`.

### import:

Import the configurations of NAT, Multihoming and Virtual Server

```
import
```

Type `import` [Enter] to import the configurations of NAT, Multihoming and Virtual Server to FortiWAN. You have to manually input the configuration in text after the command prompt "`import>`" line by line.

Example:

```
> import
Please enter configuration. terminate with a line constaining exactly:
1) 'apply' to apply, or
2) 'abort' to abort.
import> nat {
import> wan-array {
import> wan@1 {
import> rule-array {
import> rule { #1
import> source 10.10.10.55-10.10.10.77
import> destination 10.12.10.55-10.12.10.70
import> translated 10.12.104.232
import> }
import> }
import> }
import> }
import> }
import> apply
Start to apply configuration of nat...
Settings are applied for page Service -> Nat
```

&gt;

Type `abort` in command prompt `import>` to leave the prompt any time. Please refer to the exported configurations (displayed by command `export` or saved via Web UI. See "Configuration File" in "[Administration](#)") for the import format.

### init\_reports\_db:

Set Reports database to factory default

```
init_reports_db
```

Set FortiWAN's Reports database to factory default. All the report data will be deleted. Please make sure the database is backed up if it is necessary (See [Reports Database Tool](#) and [Database Data Utility](#)). Note that executing this command will bring system an automatic reboot.

### jframe:

Enable jumbo frames to support specified MTU size for FortiWAN's LAN ports

```
jframe show
```

Get the port number and the MTU size of FortiWAN's LAN ports

```
jframe set <port> <mtu>
```

Enable jumbo frames on the LAN port by specifying a MTU size that is larger than 1500.

**<port>:** The port# of LAN port, such as port1, port2...and etc.

**<mtu>:** The MTU size.

Note that applying for Network Setting resets the MTU on LAN ports to 1500.

### logout:

Exit Console mode

```
logout
```

Exit the Console mode. The system will re-confirm, press `[y]` to proceed or `[n]` to cancel.

### ping:

Test network connectivity

```
ping <hostname> <link> <index>
```

Ping a HOST machine to detect the current WAN link status. HOST is the machine/device to be pinged. The LINK parameter can be WAN, LAN or DMZ. If the LINK is WAN then also specify the WAN port number.

**<hostname>:** The parameter in specifying the target IP address or domain name. Note that domain name is valid only if parameter `<link>` is specified as "wan".

**<link>:** The parameter in specifying the link or ports that the ICMP PING REQUEST packets are sent through. The valid values are "wan", "dmz" and "lan".

**<index>:** The parameter in specifying the index of a WAN link if `<link>` is specified as "wan". The valid values are 1, 2, 3, ...,etc. (0 for private subnet).

Example:

`ping www.hinet.net wan 1` to ping www.hinet.net via WAN #1.

Note: If domain name is used in the `hostname` parameter, DNS Server must be set in the Web UI [System]-> [Network Settings]->[DNS Server] (See "[Set DNS server for FortiWAN](#)").

For more on ICMP related error messages please refer to other ICMP/PING materials.

### **reactivate:**

Reactivate the FortiWAN apparatus

```
reactivate
```

Reactivating the FortiWAN apparatus will:

- Reset all system configurations to factory default (See "[Appendix A: Default Values](#)" for the details)
- Return the system to base-bandwidth (See "License Control" in "[Administration](#)")
- Reset Reports database to factory default. All the report data will be deleted.

Using this command will result in all system data being deleted as well as all bandwidth licenses. Before you attempt a reactivation, please make sure the following are complete:.

- Backup any configuration data (See "Configuration File" in "[Administration](#)").
- Backup Reports database (See "[Reports Database Tool](#)").
- Locate your Bandwidth Upgrade Key if your system is not at base bandwidth, so that the bandwidth license the system had before can be activated by reentering the key.

Note that if your system is not at base bandwidth and you do not have your Bandwidth Upgrade Keys, please contact Fortinet CSS before attempting a reactivation.

### **reboot:**

Restart FortiWAN

```
reboot [-t <second>]
```

Restart FortiWAN immediately or restart it after a time period.

`-t`: Reboot FortiWAN after seconds. Parameter second is for this.

`<second>`: The parameter in specifying the time period (in second) system waits for to reboot.

Example:

```
reboot -t 5 to restart the system after 5 seconds.
```

### **resetconfig:**

Reset system configurations to factory defaults

```
resetconfig
resetconfig [lan_ip/netmask[@port]]
resetconfig [lan_ip/netmask[@port] [network/netmask@gateway] [wan wanspec]]]
```

Reset system configurations to factory default. This will delete all system settings including accounts of Web UI, network settings and all the other system settings and service settings (See "[Appendix A: Default Values](#)" for the details). Please backup all the configurations (See "Configuration File" in "[Administration](#)") before executing this command. This command makes no changes to Reports database and bandwidth license, as opposed to command `reactivate`.

Since automated local configuration is enabled by default, a FortiWAN will trigger the auto-configuration with the Fortinet call-home server immediately after it reboot from the `resetconfig` command (see [Automated Local Configuration](#)). If it successfully get the correct configuration file from the call-home server, the FortiWAN will replace all the default settings with the downloaded configuration file immediately and reboot system again. Finally, after the reboots from `resetconfig`, the FortiWAN is set as what the predefined configurations, not the default values. If automated configuration fails to get the configuration file, you can still see the default settings as usual.

Since command `resetconfig` will return IP address of LAN and WAN ports to the default values such as 192.168.0.1/255.255.255.0, 192.168.1.1/255.255.255.0 and 192.168.2.1/255.255.255.0, users might need to change the IP address of their local computer to reconnect to the Web UI via the LAN or WAN port (See ["Connecting to the Web UI and the CLI"](#)). Note that `resetconfig` resets the port mappings to factory default, please connect to the correct network port (LAN or WAN) for accessing to Web UI (see [Network interfaces and port mapping](#)).

`resetconfig` provides two optional parameters, `ip_address/netmask` and `@port`, to specify a LAN port address and a LAN port mapping (map the LAN port to the specified physical port) while resetting the configurations. All the configurations will be reset to factory default and the LAN settings will be configured to the specified value, so that users can reconnect to Web UI via this port without changing network topology. Furthermore, a static routing entry can be specified to the FortiWAN appliance, so that you can access Web UI across subnets.

System will re-confirm, press `[y]` to proceed or `[n]` to cancel.

**[lan\_ip/netmask[@port]]:** The parameter in specifying the network configuration `lan_ip/netmask` to network port `@port`. The network configuration will be assigned to LAN port by default if parameter `@port` is not specified.

**[network/netmask@gateway]:** The parameter in specifying the static routing entry.

### Example:

Considering that the LAN port of a FortiWAN 200B appliance is mapped to the first physical port (port1), IP address 192.168.100.1/255.255.255.0 is assigned to the LAN port and a static routing rule is created to route packets destined to 192.168.200.0/255.255.255.0 to 192.168.100.254. Administrators in 192.168.100.0/255.255.255.0 and 192.168.200.0/255.255.255.0 can access Web UI via the LAN port. Here are the usages of command `resetconfig` in different ways:

Type "`resetconfig [IP address/Netmask]`" to specify IP configuration to LAN port from resetting system to factory default.

- `resetconfig` resets all the configurations to factory default including LAN settings. In the default port mapping, port1 is mapped to WAN and port4 is mapped to LAN. IP address of the LAN port returns to 192.168.0.1/255.255.255.0. Administrators in 192.168.100.0/255.255.255.0 and 192.168.200.0/255.255.255.0 can not access to Web UI until appropriate changes to cable installation and network topology are done manually.
- `resetconfig 192.168.100.1/255.255.255.0` resets system to factory default, but set 192.168.100.1/255.255.255.0 to LAN port. However, without a specifying, port1 is mapped to WAN and port4 is mapped to LAN by default. Besides, the static routing rule for responding access requests coming from 192.168.200.0/255.255.255.0 is deleted as well. Therefore, it still requires manual changes to cable installation and network topology for administrators in 192.168.100.0/255.255.255.0 and 192.168.200.0/255.255.255.0 can access the Web UI.
- `resetconfig 192.168.100.1/255.255.255.0@port1` resets system to factory default, but map port1 to LAN and set 192.168.100.1/255.255.255.0 to the LAN port. Administrators in 192.168.100.0/255.255.255.0 can

access Web UI via the LAN port without any change, but administrators in 192.168.200.0/255.255.255.0 can not access the Web UI until a correct routing rule is created.

- `resetconfig 192.168.100.1/255.255.255.0@port1`  
192.168.200.0/255.255.255.0@192.168.100.254 resets system to factory default, but map port1 to LAN, set 192.168.100.1/255.255.255.0 to the LAN port and create a routing rule for packets destined to 192.168.200.0/255.255.255.0, where 192.168.100.254 is the router connecting subnets 192.168.100.0/255.255.255.0 and 192.168.200.0/255.255.255.0. Administrators in 192.168.100.0/255.255.255.0 and 192.168.200.0/255.255.255.0 so that can access Web UI via the LAN port without any change to network deployment.

**[wan wanspec]**: This is used to specify FortiWAN's WAN link 1 (WAN1) to a network port where `wanspec` can be:

- `dhcp@PORT`
- `pppoe@PORT ACCOUNT PASSWORD`
- `WAN_IP/MASK@PORT gw GATEWA`

Automated local configuration (see [Automated Local Configuration](#)) requires the Internet access on WAN1, and by default WAN1 is set as a DHCP client and on the first network port (port1). In case that no DHCP network is available or need to change WAN1 to other network port, you can specify WAN1 as followings:

```
resetconfig 192.168.0.1/255.255.255.0@port4 wan dhcp@port2
resetconfig 192.168.0.1/255.255.255.0@port4 wan pppoe@port2 myaccount mypasswd
resetconfig 192.168.0.1/255.255.255.0@port4 wan 1.0.0.1/255.0.0.0@port2 gw 1.0.0.2
```



It require to specify LAN port also to specify WAN1. Even if you would not like to make changes to LAN port, you still type `lan_ip/netmask@port` (such as 192.168.0.1/255.255.255.0@port4) in front of `wan wanspec`.

If you reset FortiWAN to factory default with specifying WAN1, all the other WAN links except WAN1 will become disabled by default.



Executing `resetconfig` without specifying the LAN port settings will reset port mapping to factory default, which implies the WAN links assigned to the default WAN ports are enabled. However, except the LAN port, there will be not port mappings set for WAN and DMZ if `resetconfig` is executed with specifying any parameter. In the case, there will be not default WAN and DMZ ports available (no default WAN links neither) after `resetconfig`, administrators have to re-login to Web UI via the LAN port to set the port mappings (see [Connecting to the Web UI](#)).

## resetpasswd:

Reset FortiWAN's Administrator and Monitor passwords to factory default

```
resetpasswd
```

System will re-confirm, press `[y]` to proceed or `[n]` to cancel.

## setupport:

Configure the transmission mode for all the FortiWAN port(s)

```

setupport show
setupport change <port> auto
setupport change <port> <speed> <mode>

```

**show:** Show the current transmission modes for all the network ports.

**change:** Change the transmission mode of the specified port to AUTO or specified speed and mode.

**<port>:** The parameter in specifying the port number. The valid values are 1, 2, 3, ...,etc.

**<speed>:** The parameter in specifying the transmission speed. The valid values are 10, 100 and 1000.

**<mode>:** The parameter in specifying the transmission mode. The valid values are half and full.

Example:

```

setupport show
setupport change 1 auto
setupport change 2 100 full

```

Note:

Not all network devices support full 100M speed.

This command has no effect on fiber interface.

The `port` is the port number of the FortiWAN port interface; exact number varies according to product models.

### shownetwork:

Show the current status of all the WAN links available

```

shownetwork

```

Display WAN Type, Bandwidth, IP(s) on Local/WAN/DMZ, Netmask, Gateway, and WAN/DMZ Port.

Note: This Console command can only show the current network status. This setting can be changed in the Web UI under "Network Settings" (See ["Configuring Network Interface \(Network Setting\)"](#)).

### showtrstat:

Display tunnel status

```

showtrstat
showtrstat [TR_GROUP_NAME]

```

Display the status of all tunnel groups or the specified tunnel group.

The displayed information is as:

```

[TR_GROUP_NAME]:
Reorder Rate: [Reorder_Rate] Max Queued Time: [Max_Queued_Time]
-----
|Tunnel | Status | RTT | Jitter|
-----
| [Local_IP]--[Remote_IP] | [Status] | [RTT_value] | [Jitter_value] |
-----

```

### shutdown: Shut the FortiWAN system down

```

shutdown

```

This command is used to shut FortiWAN system down, all the system processes and services will be terminated normally. Note that this command might not power the appliance off, please turn on/off the power switch or plug/unplug the power adapter to power on/off the appliance.

### sslcrt: Set or unset SSL certificate for FortiWAN WebUI

```
sslcrt show | sslcert set
```

Type `sslcrt show` to display current SSL certificate that FortiWAN WebUI is working with. The RSA private key will not be displayed here for security issue.

Type `sslcrt set` to set new SSL certificate for working with FortiWAN WebUI. You have to manually input the SSL private key and its correspondent certificate in text after the command prompt `sslcrt>` line by line. The content inputted for the private key and certificate must start with “-----BEGIN CERTIFICATE-----” and “-----BEGIN RSA PRIVATE KEY-----”, and end with “-----END CERTIFICATE-----” and “-----END RSA PRIVATE KEY-----”.

Example:

```
> sslcert set
Please enter the certificate. It should starts with
-----BEGIN CERTIFICATE-----
and end with
-----END CERTIFICATE-----
To abort please enter an empty line:
sslcrt> -----BEGIN CERTIFICATE-----
sslcrt> ...(data encoded in base64)...
sslcrt> -----END CERTIFICATE-----
Please enter the private key. It should starts with
-----BEGIN RSA PRIVATE KEY-----
and end with
-----END RSA PRIVATE KEY-----
To abort please enter an empty line:
sslcrt> -----BEGIN RSA PRIVATE KEY-----
sslcrt> ...(data encoded in base64)...
sslcrt> -----END RSA PRIVATE KEY-----
>
```

Type `sslcrt reset` to reset to factory default, the self-signed certificate.

### sysctl: Controls the system parameters

```
sysctl
```

Display the values of the system parameters.

```
sysctl <parameter>=<value|default>
```

Set the system parameter with the specified value. The system parameters are as followings:

#### VoIP Related - [sip-helper] and [h323-helper]

| sip-helper | h323-helper |
|------------|-------------|
|------------|-------------|

```
sysctl sip-helper=<0|1|default>
sysctl h323-helper=<0|1|default>
```

**sip-helper:** to enable [1] or disable [0] SIP application gateway modules. Type `default` to set it default, which is disabled.



**h323-helper:** to enable [1] or disable [0] H323 application gateway modules. Type `default` to set it default, which is disabled.

Example:

`sysctl sip-helper=0` disables the SIP application gateway modules.

`sysctl sip-helper=default` set the SIP application gateway modules to default, which is disabled.

Note: SIP and H323 application gateway modules execute NAT transparent for SIP and H323. For some SIP and H323 devices that NAT transparent is a built-in function, it is suggested to disable the SIP or H323 gateway module in FortiWAN.

### ICMP Timeout Related - [icmp-timeout] and [icmpv6-timeout]

| icmp-timeout | icmpv6-timeout |
|--------------|----------------|
|--------------|----------------|

```
sysctl icmp-timeout=<value|default>
```

Set ICMP timeout, where `<value>` is the timeout in seconds. Type `default` to set the timeout to default value, which is 3 seconds.

```
sysctl icmpv6-timeout=<value|default>
```

Set ICMPv6 timeout, where `<value>` is the timeout in seconds. Type `default` to set the timeout to default value, which is 3 seconds.

### TCP Timeout Related -

|                            |                        |                         |
|----------------------------|------------------------|-------------------------|
| tcp-timeout-close          | tcp-timeout-close-wait | tcp-timeout-established |
| tcp-timeout-fin-wait       | tcp-timeout-last-ack   | tcp-timeout-max-retrans |
| tcp-timeout-syn-recv       | tcp-timeout-syn-sent   | tcp-timeout-time-wait   |
| tcp-timeout-unacknowledged |                        |                         |

```
sysctl tcp-timeout-close=<value|default>
```

Set timeout for TCP connections in CLOSING state, where `<value>` is the timeout in seconds. Type `default` to set the timeout to default value, which is 10 seconds.

```
sysctl tcp-timeout-close-wait=<value|default>
```

Set timeout for TCP connections in CLOSE WAIT state, where `<value>` is the timeout in seconds. Type `default` to set the timeout to default value, which is 60 seconds.

```
sysctl tcp-timeout-established=<value|default>
```

Set timeout for TCP connections in ESTABLISHED state, where `<value>` is the timeout in seconds. Type `default` to set the timeout to default value, which is 43200 seconds.

```
sysctl tcp-timeout-fin-wait=<value|default>
```

Set timeout for TCP connections in FIN WAIT state where `<value>` is the timeout in seconds. Type `default` to set the timeout to default value, which is 120 seconds.

```
sysctl tcp-timeout-last-ack=<value|default>
```

Set timeout for TCP connections in LAST ACK state, where `<value>` is the timeout in seconds. Type `default` to set the timeout to default value, which is 30 seconds.

```
sysctl tcp-timeout-max-retrans=<value|default>
```

Set timeout for the TCP connections that reach three retransmission without receiving an acceptable ACK from destinations, where <value> is the timeout in seconds. Type `default` to set the timeout to default value, which is 300 seconds.

```
sysctl tcp-timeout-syn-recv=<value|default>
```

Set timeout for TCP connections in SYN RECV state, where <value> is the timeout in seconds. Type `default` to set the timeout to default value, which is 60 seconds.

```
sysctl tcp-timeout-syn-sent=<value|default>
```

Set timeout for TCP connections in SYN SENT state, where <value> is the timeout in seconds. Type `default` to set the timeout to default value, which is 120 seconds.

```
sysctl tcp-timeout-time-wait=<value|default>
```

Set timeout for TCP connections in TIME WAIT state, where <value> is the timeout in seconds. Type `default` to set the timeout to default value, which is 60 seconds.

```
sysctl tcp-timeout-unacknowledged=<value|default>
```

Set timeout for the segments that receive no acceptable ACKs from destinations, where <value> is the timeout in seconds. Type `default` to set the timeout to default value, which is 300 seconds.

## UDP Timeout Related

```
udp-timeout
```

```
udp-timeout-stream
```

```
sysctl udp-timeout=<value|default>
```

Set UDP timeout, where <value> is the timeout in seconds. Type `default` to set the timeout to default value, which is 30 seconds.

```
sysctl udp-timeout-stream=<value|default>
```

Set UDP stream timeout, where <value> is the timeout in seconds. Type `default` to set the timeout to default value, which is 180 seconds.

## Other Timeout

```
frag6-timeout
```

```
generic-timeout
```

```
sysctl frag6-timeout=<value|default>
```

Set timeout to keep an IPv6 fragment in memory, where <value> is the timeout in seconds. Type `default` to set the timeout to default value, which is 60 seconds.

```
sysctl generic-timeout=<value|default>
```

Set generic timeout for layer 4 unknown/unsupported protocols, where <value> is the timeout in seconds. Type `default` to set the timeout to default value, which is 600 seconds.

## Tunnel Routing Related - [generic-receive-offload-<port>]

```
generic-receive-offload-<port>
```

```
sysctl generic-receive-offload-<port>=<0|1|default>
```

Disabling GRO (General Receive Offload) mechanism on the corresponding LAN ports and/or DMZ ports of a Tunnel Routing network can enhance the Tunnel Routing transmission performance (see [How the Tunnel Routing Works](#) and [How to set up routing rules for Tunnel Routing](#)).

**generic-receive-offload-<port>**: Enable [1] or disable [0] GRO (General Receive Offload) mechanism on the specified physical network interface <port>, where <port> is a variable. Type `default` to set the GRO on <port> to default, which is enabled.

**<port>**: Specify an network interface (port) of FortiWAN in format port#, e.g. port1, port2 and etc.

Example:

```
sysctl generic-receive-offload-port1=0
```

disables GRO mechanism on network interface **port1**.

```
sysctl generic-receive-offload-port2=default
```

set GRO mechanism on network interface **port2** to default, which is enabled.

**Note** that disabling GRO module on a network port can enhance the Tunnel Routing transmission performance on the port, but it also results in slight impact to non-Tunnel-Routing transmission on the port when the system is under heavy loading (there might be a slight decrease in transmission performance of non-Tunnel-Routing traffic through the network port). We suggest keeping GRO modules enabled on the network ports that does not participate in the Tunnel Routing transmission.

### Allow/block Reports database port - [enable-database-port]

```
enable-database-port
```

```
sysctl enable-database-port=<0|1>
```

FortiWAN provides an application tool to backup or delete Reports database via TCP 5432. However, for better security, TCP 5432 on WAN ports is blocked by default. This command is used to manually make FortiWAN allow/block TCP 5432 on WAN ports. Please remember to set it blocked when you complete the database operations.

**enable-database-port**: Enable [1] (allow access to TCP 5432 on WAN ports) or disable [0] (block access to TCP 5432 on WAN ports).

```
sysctl enable-database-port
```

Show current setting of `enable-database-port`.

### sysinfo: Display usage FortiWAN's CPU, memory and disk

```
sysinfo
```

Get the usage of FortiWAN's CPU, memory and disk space in percentage.

### tcpdump: Dump network traffic

```
tcpdump [-aAdDeflLnNPqRStuUvxX] [-c count] [-E algo:secret] [-i PORT] [-s snaplen] [-T type] [-y datalinktype] [expression]
```

**<port>**: The parameter in specifying an network interface (port) of FortiWAN in format port#, e.g. port1, port2 and etc.

For details of the options and parameters, please refer to [http://www.tcpdump.org/tcpdump\\_man.html](http://www.tcpdump.org/tcpdump_man.html). Note that options not listed here are not supported by FortiWAN.

**traceroute: Shows the packet routes between FortiWAN's port to a specified destination**

```
traceroute <hostname> <link> <index>
```

Show the packet routes between FortiWAN's ports to the `hostname`.

**<hostname>:** The parameter in specifying the target IP address or domain name. Note that domain name is valid only if parameter `<link>` is specified as "wan".

**<link>:** The parameter in specifying the link or ports that the traceroute packets start from. The valid values are "wan", "dmz" and "lan".

**<index>:** The parameter in specifying the index of a WAN link if `<link>` is specified as "wan". The valid values are 1, 2, 3, ...,etc.

Example:

```
traceroute www.hinet.net wan 1
```

 shows the trace routes from WAN link1 to www.hinet.net.

Note: If domain name is to be used in the `hostname` parameter, the DNS Server must be set in the Web UI [System]->[Network Settings]->[DNS Server] (See "[Set DNS server for FortiWAN](#)").

## Automated Local Configuration

Previous topics give the necessary overview for planning the network topology to introduce FortiWAN into your network. Most of them are about the physical deployment; where to put FortiWAN into the network, how to connect to the subnets and how to cable it. To make FortiWAN able to perform data transmission between networks and function the critical services, it still requires correct configurations. In the subsequent subjects, such as [Configuring Network Interface](#), [Load Balancing & Fault Tolerance](#) and [Optional Services](#), you will learn how to configure the settings.

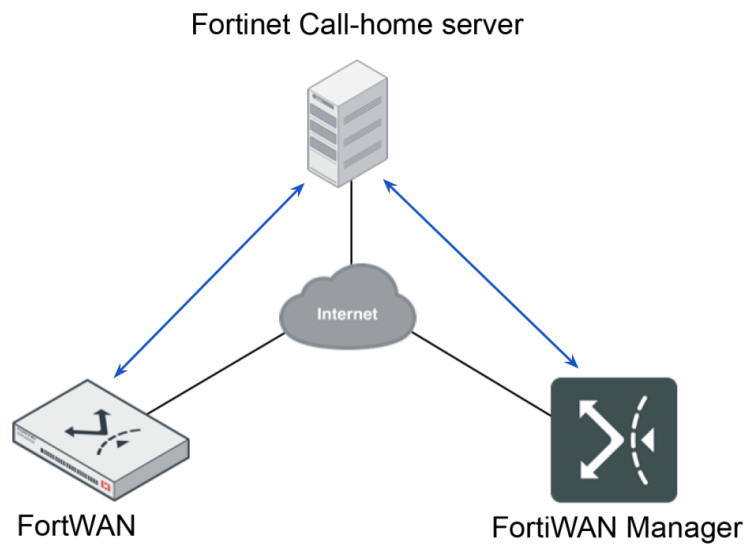
Generally, a network administrator/installer is required to manually complete physical cabling and then configure via GUI one or several FortiWAN devices per site. With the scale extended, more and more appliances need to be deployed over cross-regional sites, even over countries. Headquarter network administrators are facing a problem of local installers understanding the requirements for cabling and configuring the appliances, even for basic Internet access, before the HQ administrator can use FortiWAN-Manager for further configuration. Especially for inter-site intranet demand, deep knowledge is required to handle configurations such as Tunnel Routing, VPNs and internet/intranet routing.

Through FortiWAN Manager 4.5.0 (and later), network administrators can predefine configurations for batches of FortiWAN devices on the Fortinet call-home server in advance. As long as a local installer equips a FortiWAN with Internet access by connecting it to a DHCP-based network, FortiWAN's call-home process can automatically connect and authenticate itself to the call-home server, then download and apply the correct configuration to itself. This is an efficient way for cross-regional deployment over many sites, even countries.

The automated local configuration process involves three roles and two major parts:

### The roles

- **FortiWAN Management** is used to edit configurations and upload the configuration files to **Fortinet call-home server** for FortiWANs.
- **Fortinet call-home server** stores the configuration files of the FortiWAN devices.
- **FortiWAM appliance** automatically connects itself to **Fortinet call-home server** to download the configuration file and applies it.



## Making plans and configurations in advance

Before deploying FortiWAN appliances into local sites, headquarter network administrator needs to make an overall plan how to route internet and intranet traffic of every local site, and according to the plan predefine configurations of [Network Setting](#) (minimum requirement), [Tunnel Routing](#), [IPSec](#), [Auto Routing](#), [Bandwidth Management](#), [Firewall](#), [Multihoming](#) and etc. for every FortiWAN. All the configurations tasks can be centrally done through FortiWAN Manager V4.5.0 or later versions. Those configurations are saved as configuration files and uploaded to Fortinet's Call-home server with the FortiWAN's serial numbers.

At this stage, at least a network administrator familiar to FortiWAN, how the services function and how to configure the settings, is still required. All of the services are introduced in the subsequent subjects and you can refer to FortiWAN Manager's user guide (<http://docs.fortinet.com/fortiwan/admin-guides>) for the details of configuration editor and call-home server usage.

## FortiWAN's automated configuration

FortiWAN's WAN1 and primary DNS are set as a DHCP WAN link (see [Configuring your WAN and DMZ](#) and [Configurations for a WAN link in Bridge Mode: DHCP](#)) and 8.8.8.8 by factory default, which means a FortiWAN can has Internet access as long as connecting FortiWAN's WAN1 port (DHCP client) to any DHCP network (e.g. LAN with DHCP server) and turning the power on. It does not require Web UI login to configure the network settings.

When a FortiWAN is first time started from factory default, it will:

- Use WAN1 to automatically connect and authenticate itself to Fortinet's call-home server over the Internet.
- Download the correct predefined configuration file according to the serial number if it is stored in the call-home server in advanced.
- Restore and apply the downloaded configuration file to itself.
- Disable the automated configuration function and reboot system.

## Steps to deploy FortiWAN via automated local configuration

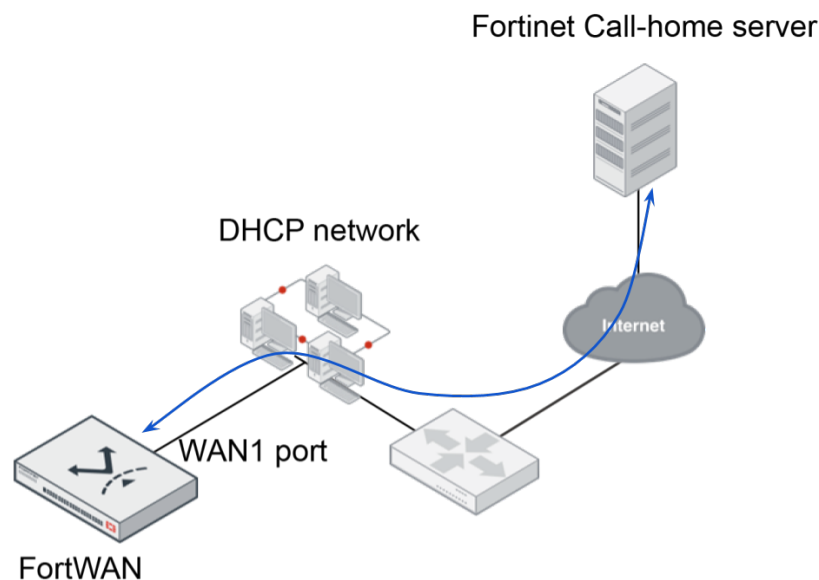
After realizing what FortiWAN's automated local configuration is, here are the exact steps to install a FortiWAN via automated configuration:

### Preparation before starting

1. A network topology plan for installing the FortiWAN in a local site
2. A FortiWAN Manager (V4.5.0 or later)
3. A DHCP network (in headquarter, the local site or anywhere is fine) (See [What if no DHCP network available](#) if no DHCP network is available)
4. A FortiWAN in factory default

### Start installation

1. In headquarter, according to deployment topology plan, use FortiWAN Manager's Config Editor to generate the configuration file for the FortiWAN. Other, similar configuration files can be imported to the Config Editor, modified and saved for new sites, as required (see FortiWAN Manager's user guide for the details).
2. Save the configuration file with the FortiWAN's serial number on Fortinet's call-home server through FortiWAN Manager. Note that this step will require a Call-Home Key. To obtain a Call-Home Key, log in to the FortiCare customer portal, and go to the Asset page for the Serial Number of your FortiWAN. Look on the License & Key page and a Call-Home Key should be displayed. If the Key is not present, please contact Customer Support/FortiCare..
3. Equip the FortiWAN with the Internet access by connecting WAN1 (WAN1 is on port1 by default) to a DHCP network so that WAN1 can be automatically assigned with an IP address from DHCP server. Step 3 ~ step 5 can be done in headquarter, the local site or anywhere.



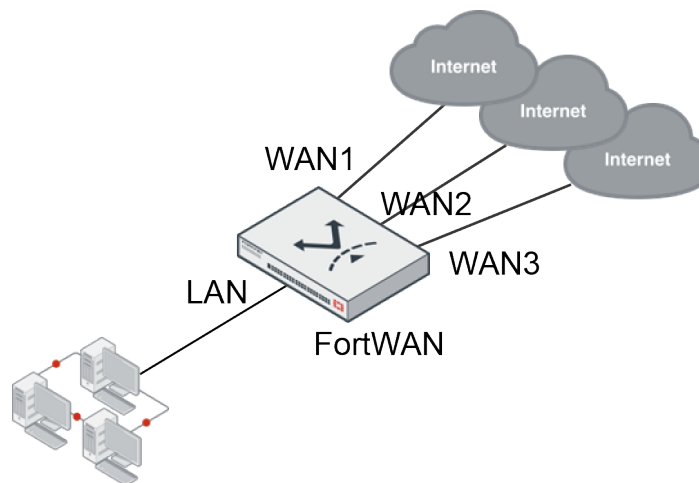
4. Turn the power on.
5. Wait several moments for FortiWAN to authenticate, retrieve its config, install and reboot. If desired or if the process has not completed within 5 minutes, connect and login to the FortiWAN's CLI (see [To connect to the CLI](#))

and execute `callhome showlog`. Normally, you will see:

```
Fortiwan login: admin
Password:
> callhome showlog
2017-10-03 01:30:58 callhome daemon start
2017-10-03 01:31:23 Received config from home server
2017-10-03 01:31:24 Config restored. Disable callhome and reboot...
```

, which means the configuration file is downloaded correctly from the call-home server.

6. According to the configurations, the local installer re-cables this FortiWAN into network of the site.



7. Now you can login to this FortiWAN's Web UI to check the configurations.

The followings are notices about automated local configuration:

- After an automated configuration is successfully done, automated local configuration will become DISABLED until next reset factory default (the CLI command `resetconfig` or the Factory Default button on Web UI page **System > Administration**).
- While automated local configuration is enabled, FortiWAN continues sending the configurations requests periodically if no configuration file is available on the call-home server for the FortiWAN or connection fails. The FortiWAN will not disable automated configuration function (even if a system reboot) until automated configuration is successfully done (configuration is downloaded, restored and system reboots). If, for some reason, FortiWAN cannot connect to the call-home server, obtain the required config file from the central administrator. Then disconnect WAN 1 and configure FortiWAN by connecting to the LAN port as detailed in normal installation procedures (see Quick Start Guide and FortiWAN manual).

### What if no DHCP network available

If there is no DHCP network available, automated configuration can also be done by assigning a static IP to WAN1 or connect it to a PPPoE network to have the Internet access. But this will require a manual execution of the CLI command `resetconfig` (see [resetconfig](#)). You can reset FortiWAN to factory default with specifying WAN1 with static IP or PPPoE client or any other network port.

Here is an example to perform automated configuration via static-IP WAN1:

1. Predefine and save a configuration on the call-home server for the FortiWAN.
2. Connect FortiWAN's port2 to a static network such as 172.60.0.0/255.255.255.0, gateway 172.60.0.254. The same, the FortiWAN is in factory default status.
3. Turn the power on

4. Connect and login to the FortiWAN's CLI and manually execute the command:

```
resetconfig 192.168.0.1/255.255.255.0@port4 wan 172.60.0.10/255.255.255.0@port2 gw
172.60.0.254
```

In this example, the command sets WAN1 on network port2 (changing WAN1 to another port or keeping it on port1 depends on your network), gives it a static IP 172.60.0.10 and the gateway. FortiWAN will reboot immediately.

5. After it restart from reboot, logging to CLI again and execute `callhome showlog`. You will see:

```
> callhome showlog
2017-10-03 01:30:58 callhome daemon start
2017-10-03 01:31:23 Received config from home server
2017-10-03 01:31:24 Config restored. Disable callhome and reboot...
```

, which means the configuration file is downloaded correctly from the call-home server.

---

If `callhome showlog` prints the following logs

```
2017-10-01 23:33:14 callhome daemon start
2017-10-01 23:33:29 Cannot get config from home server (#1)
2017-10-01 23:34:29 Cannot get config from home server (#2)
```

Please make sure the Internet access is available and check if WAN1 port is correctly assigned with an IP address from DHCP server. To check WAN1 port, please login to CLI and execute `shownetwork`.



Current configurations of a FortiWAN will be replaced with the downloaded configuration file if automated configuration is successfully performed.

Resetting a FortiWAN to factory default resets all the settings to default value, for example the LAN port IP is 192.168.0.1. However at the same time it enables automated local configuration trying to get configuration file from the call-home server. Therefore, if the automated configuration is successfully done, this FortiWAN will be finally equipped with the downloaded configurations, not the default values.

---



## Configuring Network Interface (Network Setting)

As an edge router of a network site, FortiWAN is supposed to operate with connected networks, the WAN, LAN and DMZ networks. FortiWAN must guarantee general communication among the connected networks (routing), and so that can provide the advanced load balancing and fault tolerance functions. To establish connectivity between FortiWAN and the networks, you need to complete the following basic network settings:

1. Decide a FortiWAN's network port for connecting the FortiWAN with the network. This network port can be a physical port, an aggregated, redundant or VLAN port. Whether it is a physical or logical port, you have to program it as what the type that the connected network is (WAN, LAN or DMZ). **VLAN and Port Mapping** is the configuration that you can create logical network ports (aggregated, redundant and VLAN ports) and define the port mapping to the physical and logical ports (see [Configurations for VLAN and Port Mapping](#)).
2. Configure the basic IP network setting and static routing information to the network port for the connected network. The settings here are necessary for FortiWAN to guarantee basic communication among the connected networks, packets can be routed correctly between the networks. According to the type of connected network, settings are divided into:
  - **WAN Setting** (DMZ setting is included): WAN Settings is the major part to deploy FortiWAN in various types of WAN links (see [Configuring your WAN](#)).
  - **WAN/DMZ Private Subnet**: This includes settings for deploying private subnets to WAN/DMZ port (see [WAN/DMZ Private Subnet](#)).
  - **LAN Private Subnet**: This includes settings for deploying private subnets to LAN port (see [LAN Private Subnet](#)).

Generally speaking, a network site consists of a WAN link and a private LAN network at least. WAN Setting and LAN Private Subnet are the necessary configurations for FortiWAN to connect the internal and external networks.

Some of FortiWAN's functions, such as system time synchronization, log push, ping and trace commands, require cooperating with external servers. When FortiWAN itself (localhost) communicates with those external servers, such as NTP, FTP, SMTP servers, an appropriate DNS server is required for domain name resolving. Configuration of **DNS Server** is part of the basic network setting (see [Set DNS server for FortiWAN](#)).

Briefly, network setting of a FortiWAN contains the configurations of:

1. DNS for FortiWAN's localhost (DNS Server, see [Set DNS server for FortiWAN](#))
2. Network port programming (VLAN and Port Mapping, see [Configurations for VLAN and Port Mapping](#))
3. Individual network connected to FortiWAN and the relative routing information (WAN Setting, WAN/DMZ Private Subnet and LAN Private Subnet, see [Configuring your WAN and DMZ](#), [WAN/DMZ Private Subnet](#) and [LAN Private Subnet](#))

## Set DNS server to FortiWAN

As an edge router, FortiWAN connects the external and internal networks to provide necessary valuable functions for incoming and outgoing service accesses. Among the functions, domain name resolution plays an important role for service accesses. The following is an overview about the DNS deployment on FortiWAN, according to source of the DNS query.

## For external users who want to access your domain

If you provide network services (such as HTTP, FTP or SMTP) to Internet, no matter how you deploy the servers (deploy them in DMZ or LAN) you will need also provide the resolution of your domain name to users who want to access your services from Internet. You may manage your domain simply by a DNS hosting or FortiWAN's **Multihoming** (See "[Multihoming](#)"). Multihoming is basically a DNS server providing standard name resolution to Internet users, moreover it provides load balancing and fail over to inbound traffic.

## For internal users who want to access internal or external servers

It requires a DNS server for any user to resolve a external domain he want to access through Internet. Usually, this DNS server could be a ISP's DNS server or any registered public DNS server. An user can configure the setting of DNS server on its own computer manually or automatically be allocated by DHCP. This DNS server is also necessary to FortiWAN itself for some operations. Several FortiWAN's functions, such as sending logs and notifications, ping and traceroute commands, require DNS resolution if the target is a FQDN (fully qualified domain name). Through Web UI **System > Network Setting > DNS Server**, you can manually set the DNS server to FortiWAN. FortiWAN's DHCP (also SLAAC and DHCPv6, see "[Automatic addressing within a basic subnet](#)") allocate the DNS servers set here to users in LAN or DMZ subnet if the users' computers are set to automatically get DNS by DHCP.

On the other hand, if you want to maintain an internal DNS server in your site, FortiWAN provides **Internal DNS** (see "[Internal DNS](#)") for managing your domain to internal users (the users in LAN or DMZ subnet). An user in LAN or DMZ subnet need to manually configure the DNS server on his computer for using the FortiWAN's Internal DNS (set DNS server as IP address of the gateway he connects to). It is unable to automatically allocate FortiWAN's internal DNS to users by FortiWAN's DHCP. The Internal DNS is recursive, which allows users to resolve other people's domains (external domains). The DNS servers set here (System > Network Setting > DNS Server) will be asked by Internal DNS while it recursively resolve an unknown domain. Of cause that you can also set up a standalone internal DNS server to manage your domain for internal users, but this is the category of FortiWAN.

The last feature about DNS that FortiWAN provides is **DNS Proxy**, which is a mechanism to redirect outgoing DNS queries to other DNS servers according to WAN links loading. This is not the well-known DNS proxy, but is a solution for ISP peering issue (See "[DNS Proxy](#)" and "[Optimum Route Detect](#)").

Back to **System > Network Setting > DNS Server**, it enables administrators to define the host name the FortiWAN in the network, the IPv4/IPv6 address of domain name servers used by FortiWAN, and the suffix of the domain name. The following is the list of FortiWAN's functions that might require the DNS servers set here.

|                                     |                                                                                                         |
|-------------------------------------|---------------------------------------------------------------------------------------------------------|
| <b>System &gt; Diagnostic Tools</b> | Ping and Trace (See " <a href="#">Diagnostic Tools</a> ")                                               |
| <b>System &gt; Date/Time</b>        | Synchronize system time through NTP server (See " <a href="#">Setting the system time &amp; date</a> ") |
| <b>Service &gt; Internal DNS</b>    | Recursively resolve an unknown domain (see " <a href="#">Internal DNS</a> ")                            |
| <b>Log &gt; Control</b>             | SMTP and FTP Server Settings (See " <a href="#">Log Control</a> ")                                      |
| <b>Log &gt; Notification</b>        | SMTP Server Settings (See " <a href="#">Log Notification</a> ")                                         |
| <b>CLI</b>                          | Ping and Traceroute Commands (See " <a href="#">Console Mode Commands</a> ")                            |

|             |                                                                                                                                                                      |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FQDN</b> | Maintain the FQDN mapping in system for supporting FQDN in management policies (See "Basic concept to configure via Web UI" in <a href="#">"Using the Web UI"</a> ). |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Configure the setting

|                                |                                                                                                                                                                                                                |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hostname</b>                | Name for this FortiWAN appliance.                                                                                                                                                                              |
| <b>IPv4 Domain Name Server</b> | IPv4 DNS servers for this FortiWAN itself to resolve unknown domains. The maximum of three IPv4 addresses is allowed. The DNS servers set here will be used in a top-down order, if the DNS request timed out. |
| <b>IPv6 Domain Name Server</b> | IPv6 DNS servers for this FortiWAN itself to resolve unknown domains. The maximum of three IPv6 addresses is allowed. The DNS servers set here will be used in a top-down order, if the DNS request timed out. |
| <b>Domain Name Suffix</b>      | Primary domain suffix of this FortiWAN appliance.                                                                                                                                                              |

Note: Incomplete DNS server configurations will not influence the performance of the functions listed above. Only IP address is necessary instead of the FQDN.

## Aggregated, Redundant, VLAN Ports and Port Mapping

Go to **System > Network Setting** from the Web UI, click the label **VLAN and Port Mapping** in the upper-right corner to expand the configuration panel. This is a configuration that you can create logical network ports and define the port mapping to the physical and logical ports. The VLAN and Port Mapping panel consists of four tables, **VLAN and Port Mapping**, **Redundant LAN Port**, **Redundant DMZ Port** and **Aggregated Port**, which are described as followings:

### VLAN and Port Mapping

As the previous description, FortiWAN's physical network ports can be further programed as an aggregated port, a redundant port or several VLAN ports, which are generally called logical ports (see [Network interfaces and port mapping](#)). A network ports must function as a WAN, LAN or DMZ port and be connected with a corresponding network (a WAN, LAN or DMZ network), so that the FortiWAN can work correctly for the connected network. Although each of FortiWAN's physical ports is mapped to a port type by default, the default mapping can be changed (even logical ports can be created) according to how you deploy your network site. For example, a FortiWAN 200B's Port 1 could be programed as a LAN port, Port 2 could be programed as a DMZ port, and Port 3 ~ Port 5 could be programed as WAN ports, while Port 1 ~ Port 3 are WAN ports, Port 4 is a LAN port and Port 5 is a DMZ port by default. **VLAN and Port Mapping** is the configuration table for defining the port mapping and creating VLAN IDs on the ports. It consists of three elements; **Port**, **VLAN Tag** and **Mapping**:

### Port

In the **VLAN and Port Mapping** table, each of the FortiWAN's physical ports is listed in the Port column (indicated as Port1, Port2, Port3 ..., corresponding to the numbers presented on the front panel of the FortiWAN device), so that port mapping can be programed and VLAN tags can be created on it. Moreover, the created aggregated ports (an logical port that is created by aggregating two physical ports, see Aggregated Port below for

more details) will also be listed here for defining mappings and VLAN tags to them. As for a FortiWAN-VM appliance, the ports listed in Port column are indicated as vNIC2, vNIC3, vNIC4 ..., mapping of the ports and the vNICs is as below (vNIC 1 is used for HA port and can not be changed):

| Ports | Port 1 | Port 2 | Port 3 | Port 4 | Port 5 | Port 6 | Port 7 | Port 8 | Port 9  |
|-------|--------|--------|--------|--------|--------|--------|--------|--------|---------|
| vNICs | vNIC 2 | vNIC 3 | vNIC 4 | vNIC 5 | vNIC 6 | vNIC 7 | vNIC 8 | vNIC 9 | vNIC 10 |

## Mapping

For the ports listed in the table, there are four options available for mapping them to a function (click the pull-down menus of Mapping column):

|             |                                                                                                                                                                |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WAN</b>  | Specify a physical port or a VLAN port as a WAN port. This option is not available for an aggregated port.                                                     |
| <b>LAN</b>  | Specify a physical port, a VLAN port or an aggregated port as a LAN port.                                                                                      |
| <b>DMZ</b>  | Specify a physical port, a VLAN port or an aggregated port as a DMZ port.                                                                                      |
| <b>None</b> | Specify any port for non-purpose. To aggregate two physical ports, it requires to map the two ports to None first (see <a href="#">Aggregated Port</a> below). |

Whether a physical port or a logical port (aggregated, redundant or VLAN port) is, it must be programmed as one of the port types (WAN, LAN and DMZ) first to be used by other services. A port that is programmed as a WAN, LAN or DMZ port will become an option to setting items of some configurations:

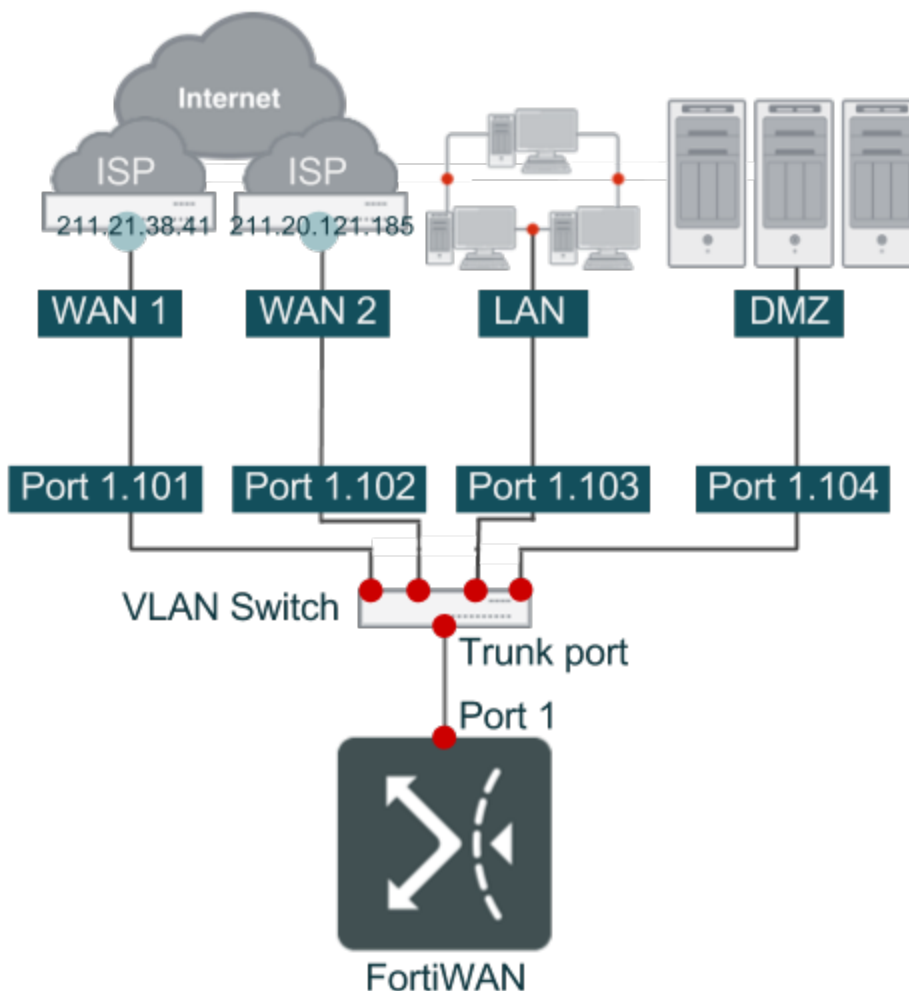
- Port that is programmed as a **WAN port** will be listed in the pull-down menus:
  - [WAN Port] of **WAN Setting** for configuring and deploying a WAN subnet to the ports (see [Configuring your WAN](#)).
  - [WAN Port] of **WAN/DMZ Private Subnet** for configuring and deploying a private WAN subnet to the ports (see [WAN/DMZ Private Subnet](#)).
  - [Input Port] of **Auto Routing's** IPv4/IPv6 Filters for creating a filter rule to evaluate packets by the port receiving the packets (see [Outbound Load Balancing and Failover](#)).
  - [Input Port] of **Bandwidth Management's** IPv4/IPv6 Filters of Outbound BM for creating a filter rule to evaluate packets by the port receiving the packets (see [Bandwidth Management](#)).
- Port that is programmed as a **DMZ port** will be listed in the pull-down menus:
  - [DMZ Port] of **WAN Setting** for configuring and deploying a DMZ subnet to the ports (see [Configuring your WAN](#)).
  - [DMZ Port] of **WAN/DMZ Private Subnet** for configuring and deploying a private DMZ subnet to the ports (see [WAN/DMZ Private Subnet](#)).
  - [Input Port] of **Auto Routing's** IPv4/IPv6 Filters for creating a filter rule to evaluate packets by the port receiving the packets (see [Outbound Load Balancing and Failover](#)).
  - [Input Port] of **Bandwidth Management's** IPv4/IPv6 Filters of Outbound BM for creating a filter rule to evaluate packets by the port receiving the packets (see [Bandwidth Management](#)).

- Port that is programmed as a **LAN port** will be listed in the pull-down menus:
  - [LAN Port] of **LAN Private Subnet** for configuring and deploying a LAN subnet to the ports (see [Configuring your WAN](#)).
  - [Input Port] of **Auto Routing's** IPv4/IPv6 Filters for creating a filter rule to evaluate packets by the port receiving the packets (see [Outbound Load Balancing and Failover](#)).
  - [Input Port] of **Bandwidth Management's** IPv4/IPv6 Filters of Outbound BM for creating a filter rule to evaluate packets by the port receiving the packets (see [Bandwidth Management](#)).

Changes to port mappings here will be updated immediately to the corresponding pull-down menus. If a port has been configured and deployed with a network, or been associated with a filter rule, a change to mapping of the port will fail the original deployments and settings. Please remember to reconfigure relative settings if a port mapping is changed.

## VLAN Tag

FortiWAN supports IEEE 802.1Q, which is also known as VLAN Tagging (Cisco's ISL is not supported). A FortiWAN's physical port can be mapped to several VLAN ports. In a large-scale network that is segmented into smaller groups of subnets by a VLAN switch, FortiWAN allows data being exchanged between these subnets. Moreover, the VLAN switch ports can be programmed as DMZ, WAN or LAN ports. To introduce a VLAN Switch into the network working with FortiWAN, here is a example:



FortiWAN's Port 1 is connected with the VLAN switch, and appropriate VLAN settings have been configured on the VLAN switch. Now, it requires to have VLAN tagging configured on FortiWAN to get the VLAN deployment workable. The steps are:

1. In the VLAN and Port Mapping table, click the Add button in the VLAN Tag field of Port 1 to create a new VLAN tag. A VLAN tag input will then available to replace the original string "no VLAN Tag".
2. Enter the VLAN tag into the input field to define a VLAN to Port1.
3. This VLAN tag can be edited, deleted, moved up/down by buttons aside it.
4. Map the VLAN tag to WAN, LAN or DMZ in Mapping column.
5. Define the next VLAN to Port1 by the same processes.

| Port   | VLAN Tag | Mapping |
|--------|----------|---------|
| Port 1 | 101      | WAN     |
|        | 102      | WAN     |
|        | 103      | LAN     |
|        | 104      | DMZ     |

After the configuration is applied, FortiWAN's port 1 will no longer accept untagged VLAN packets. Through the VLAN switch, both Port 1.101 and port 1.102 are connected with a WAN link (**Port 1.101 and Port 1.102 will be listed in the WAN Port pull-down menu for WAN Setting**), while port 1.103 is connected the LAN subnet (**Port 1.103 will be listed in the LAN Port pull-down menu for Private LAN Subnet setting**) and port 1.104 is connected with the DMZ subnet (**Port 1.104 will be listed in the DMZ Port pull-down menu for DMZ Setting**). You can also define VLAN tags to an aggregated port from the table (it requires to create an aggregated port first for defining VLAN tags to it).

**Note:** This field (VRID) is only available when VRRP mode is enabled in LAN Private Subnet settings. The VRID indicates the virtual router identifier for every VR.

### Redundant LAN/DMZ Port

A logical redundant port pairs an active and a standby physical network port. It means a logical redundant LAN port consists of two physical LAN ports, and a logical redundant DMZ port consists of two physical DMZ port. Under normal usage, the active port passes traffic and the standby port is just backup. Once the active port goes down (or unavailable), the standby port takes over the active role and starts passing traffic. Why a redundant LAN port and a redundant DMZ port are necessary? Because without the redundant ports, even if FortiWAN is working in HA mode, single point failure can still occur over connectivities between LAN/DMZ subnets and FortiWAN's LAN/DMZ ports. Redundant ports increase the reliability of connectivity of FortiWAN's LAN and DMZ. FortiWAN's redundant port supports the Spanning Tree algorithm and sets the highest 0xffff as bridge priority. The configurations thus manage to avoid network failure caused by the possible packet looping.

**Label**

Name of the logical redundant LAN/DMZ port. Only the ASCII characters “0-9 a-z A-Z” are acceptable for a label and the first character must be non-numeric. After applying the settings, the specified label, in the format **Bridge: label name**, will become one of the port options in corresponding pull-down menus used for configurations of LAN setting (see [LAN Private Subnet](#)), DMZ setting (see [Configuring your WAN](#)), Auto Routing and Bandwidth Management (FortiWAN's Auto Routing and Bandwidth Management support managing outbound traffic by input ports where the traffic received on, see [Auto Routing](#) and [Bandwidth Management](#)). All the configurations refer to the logical redundant port instead of its member physical ports.

**Mapping**

There are two menus in the Mapping field for selecting the two member-ports under a LAN/DMZ redundant port. All the physical ports and VLAN tags mapped to LAN/DMZ in the **VLAN and Port Mapping** table are listed here for options. It requires at least two are mapped to LAN/DMZ in **VLAN and Port Mapping** first for creating a LAN/DMZ redundant port, or there will be no items here for options.

Select a LAN/DMZ port from each of the two pull-down menus to add the member-ports to the redundant port. By default, the first configured member-port becomes the active one for the redundant port, while the second one is in hot standby state.

Note that the physical member ports that are redundant to each other must be equal in port speed and duplex (See ["Port Speed/Duplex Settings"](#)).

**Notices to create a redundant port**

Before creating a redundant port, you need to know:

- The two member-ports of a redundant port can be two physical network ports, two VLAN tags, or a pair of one physical port and a VLAN tag.
- It requires to exactly map two member-ports to LAN or DMZ in *VLAN and Port Mapping* table before pairing the two ports to a logical LAN/DMZ redundant port.
- VLAN tags can not be defined to an redundant port.

**Creating an redundant LAN/DMZ port**

To configure an redundant LAN port or redundant DMZ port, perform the following steps:

**Step 1** Map two ports (two physical port, two VLAN ports, or a pair of one physical port and one VLAN port) to LAN or DMZ in *VLAN and Port Mapping* table.

| VLAN and Port Mapping |   |             |         |
|-----------------------|---|-------------|---------|
| Port                  |   | VLAN Tag    | Mapping |
| Port1                 | + | no VLAN Tag | LAN ▼   |
| Port2                 | + | no VLAN Tag | LAN ▼   |

| VLAN and Port Mapping |  |          |         |
|-----------------------|--|----------|---------|
| Port                  |  | VLAN Tag | Mapping |
| Port1                 |  | 101      | LAN ▼   |
|                       |  | 102      | LAN ▼   |

| VLAN and Port Mapping |  |             |         |
|-----------------------|--|-------------|---------|
| Port                  |  | VLAN Tag    | Mapping |
| Port1                 |  | 101         | LAN ▼   |
| Port2                 |  | no VLAN Tag | LAN ▼   |

**Step 2** Create a new redundant port configuration by clicking the add button on *Redundant LAN Port* or *Redundant DMZ Port* table.

**Step 3** Assign the redundant port a name by entering it in Label filed.

**Step 4** Select a member-port from each of the two pull-down menus in Mapping field (the ports mapped to LAN or DMZ in *VLAN and Port Mapping* table are listed here for options).

**Step 5** Apply the settings by clicking Apply.

## Aggregated Port

FortiWAM's port aggregation is implementation of IEEE 802.3ad active mode, which bundles two physical ports into a single logical aggregated port to provide the aggregated bandwidth of the two physical links. If single point failure occurs on connectivity of one of the physical member ports under an aggregated port, traffic will be carried within the remaining port channel. The related parameters of IEEE 802.3ad active mode are sat as follows:

| Parameter        | Value  | Note           |
|------------------|--------|----------------|
| ad_select        | stable | as default     |
| all_slave_active | 0      | as default     |
| downdelay        | 0      | as default     |
| lacp_rate        | slow   | as default     |
| max_bonds        | 1      | as default     |
| miimon           | 100    | as recommended |
| min_links        | 0      | as default     |
| updelay          | 0      | as default     |
| use_carrier      | 1      | as default     |
| xmit_hash_policy | layer2 | as default     |



**Label**

Name of the logical aggregated port. Only the ASCII characters “0-9 a-z A-Z” are acceptable for a label and the first character must be non-numeric. After entering a label here, this label will be listed in **VLAN and Port Mapping** table at the same time so that the logical aggregated port can be mapped to LAN or DMZ, or have VLAN tags defined on it. After applying the settings, the specified label will become one of the port options in corresponding pull-down menus, in the format **Bonding: label name**, used for configurations of LAN setting (see [LAN Private Subnet](#)), DMZ setting (see [Configuring your WAN](#)), Auto Routing and Bandwidth Management (FortiWAN's Auto Routing and Bandwidth Management support managing outbound traffic by input ports where the traffic received on, see [Auto Routing](#) and [Bandwidth Management](#)). All the configurations refer to the logical aggregated port instead of its member physical ports.

**Mapping**

There are two menus in the Mapping field for selecting the two member-ports under a aggregated port. All the physical ports and VLAN tags mapped to **None** in the **VLAN and Port Mapping** table are listed here for options. It requires at least two are mapped to **None** in **VLAN and Port Mapping** first for creating an aggregated port, or there will be no items here for options.

Select a port from each of the two pull-down menus to add the member-ports to the aggregated port. After this, you need to enable the aggregated port by mapping it to LAN/DMZ or defining VLAN tags on it from **VLAN and Port Mapping** table, or the aggregated port is mapped to None by default.

Note that the physical member ports that are aggregated must be equal in port speed and duplex (See ["Port Speed/Duplex Settings"](#)).

**Notices to create a redundant port**

Before creating a redundant port, you need to know:

- The two member-ports of an aggregated port can be two physical network ports, two VLAN tages, or a pair of one physical port and a VLAN tag.
- A logical aggregated port requires two purposeless member-ports (both are mapped to None in *VLAN and Port Mapping* table).
- An aggregated port can only be mapped to a DMZ or LAN port.
- VLAN tags can be defined to an aggregated port.

**Creating an aggregated port**

To configure an aggregated port, perform the following steps:

**Step 1** Disable two ports (two physical port, two VLAN ports, or a pair of one physical port and one VLAN port) by mapping them to None in *VLAN and Port Mapping* table.

| VLAN and Port Mapping |   |             |         |
|-----------------------|---|-------------|---------|
| Port                  |   | VLAN Tag    | Mapping |
| Port1                 | + | no VLAN Tag | None ▼  |
| Port2                 | + | no VLAN Tag | None ▼  |

| VLAN and Port Mapping |             |          |         |
|-----------------------|-------------|----------|---------|
| Port                  |             | VLAN Tag | Mapping |
| Port1                 | + ↓ ↑<br>🗑️ | 101      | None ▼  |
|                       | + ↓ ↑<br>🗑️ | 102      | None ▼  |

| VLAN and Port Mapping |             |             |         |
|-----------------------|-------------|-------------|---------|
| Port                  |             | VLAN Tag    | Mapping |
| Port1                 | + ↓ ↑<br>🗑️ | 101         | None ▼  |
| Port2                 | +           | no VLAN Tag | None ▼  |

**Step 2** Create a new port aggregation configuration by clicking the add button on *Aggregated Port* table.

**Step 3** Assign the aggregated port a name by entering it in Label filed.

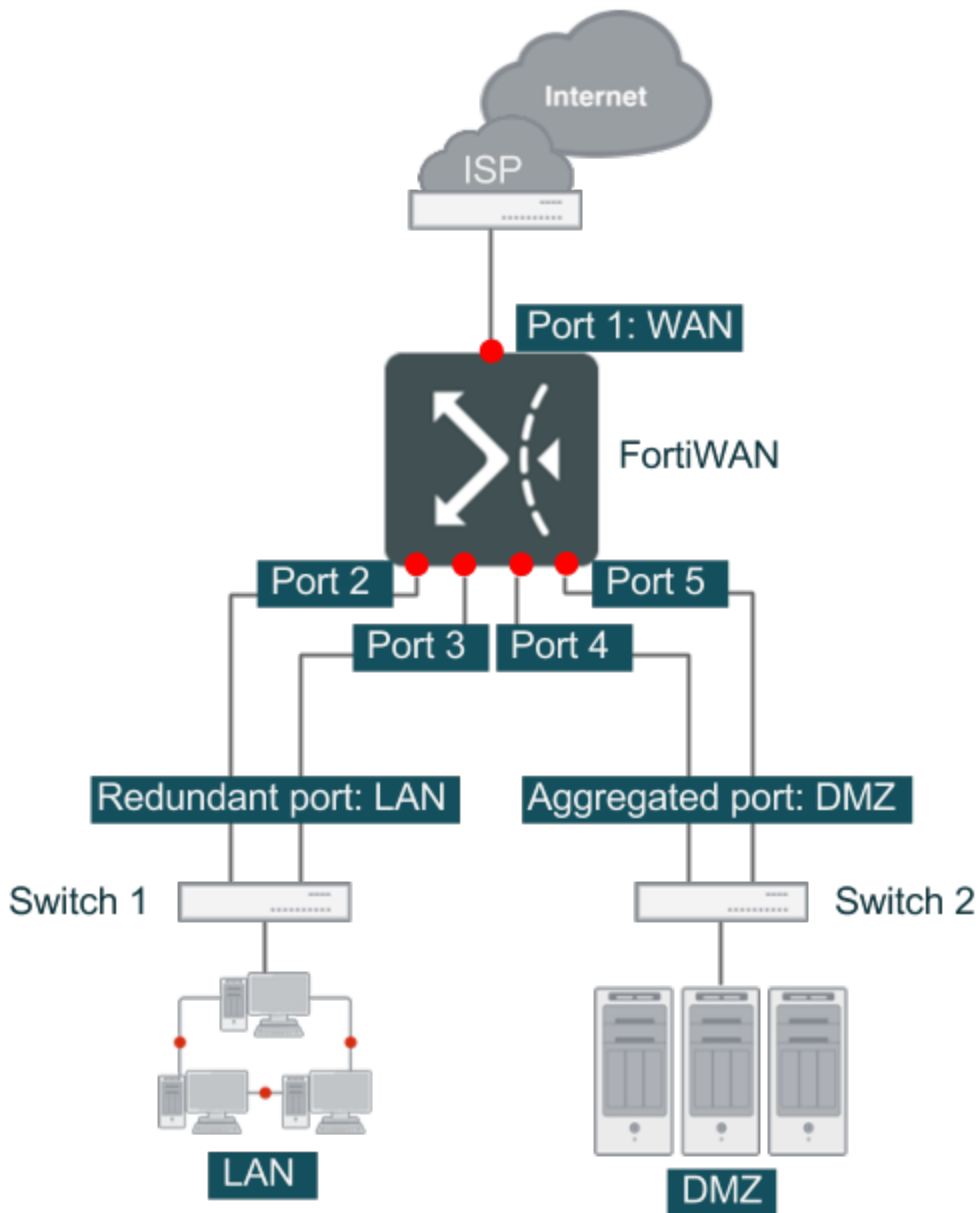
**Step 4** Select a member-port from each of the two pull-down menus in Mapping field (the disabled ports in *VLAN and Port Mapping* table are listed here for options).

**Step 5** The label name of the aggregated port will be listed in *VLAN and Port Mapping* table. Map the logical aggregated port to LAN or DMZ by selecting it from the pull-down menu in Mapping field. You can also define VLAN tags to the aggregated port in VLAN Tag field and Mapping field.

**Step 6** Apply the settings by clicking Apply.

## Scenarios

As illustrated in the topology below, FortiWAN port1 are mapped to WAN port. Port2 and port3 are paired to a logical redundant LAN port which is connected to Switch1, port4 and port5 are paired to a logical aggregated DMZ port which is connected to Switch2.



**Step 1** To configure the settings for the deployment, you need to map Port1, Port2, Port3, Port4 and Port5 to WAN, LAN, LAN, None and None respectively in *VLAN and Port Mapping* table.

| Port  | VLAN Tag    | Mapping |
|-------|-------------|---------|
| Port1 | no VLAN Tag | WAN     |
| Port2 | no VLAN Tag | LAN     |
| Port3 | no VLAN Tag | LAN     |
| Port4 | no VLAN Tag | None    |

| Port  | VLAN Tag    | Mapping |
|-------|-------------|---------|
| Port5 | no VLAN Tag | None    |

**Step 2** Create a new redundant LAN port labeled lan23 and mapped it to Port2 and Port3 in *Redundant LAN Port* table.

| Label | Mapping |
|-------|---------|
| lan23 | Port 2  |
|       | Port 3  |

**Step 3** Create a new aggregated port labeled dmz45 and mapped it to Port4 and Port5 in *Aggregated Port* table.

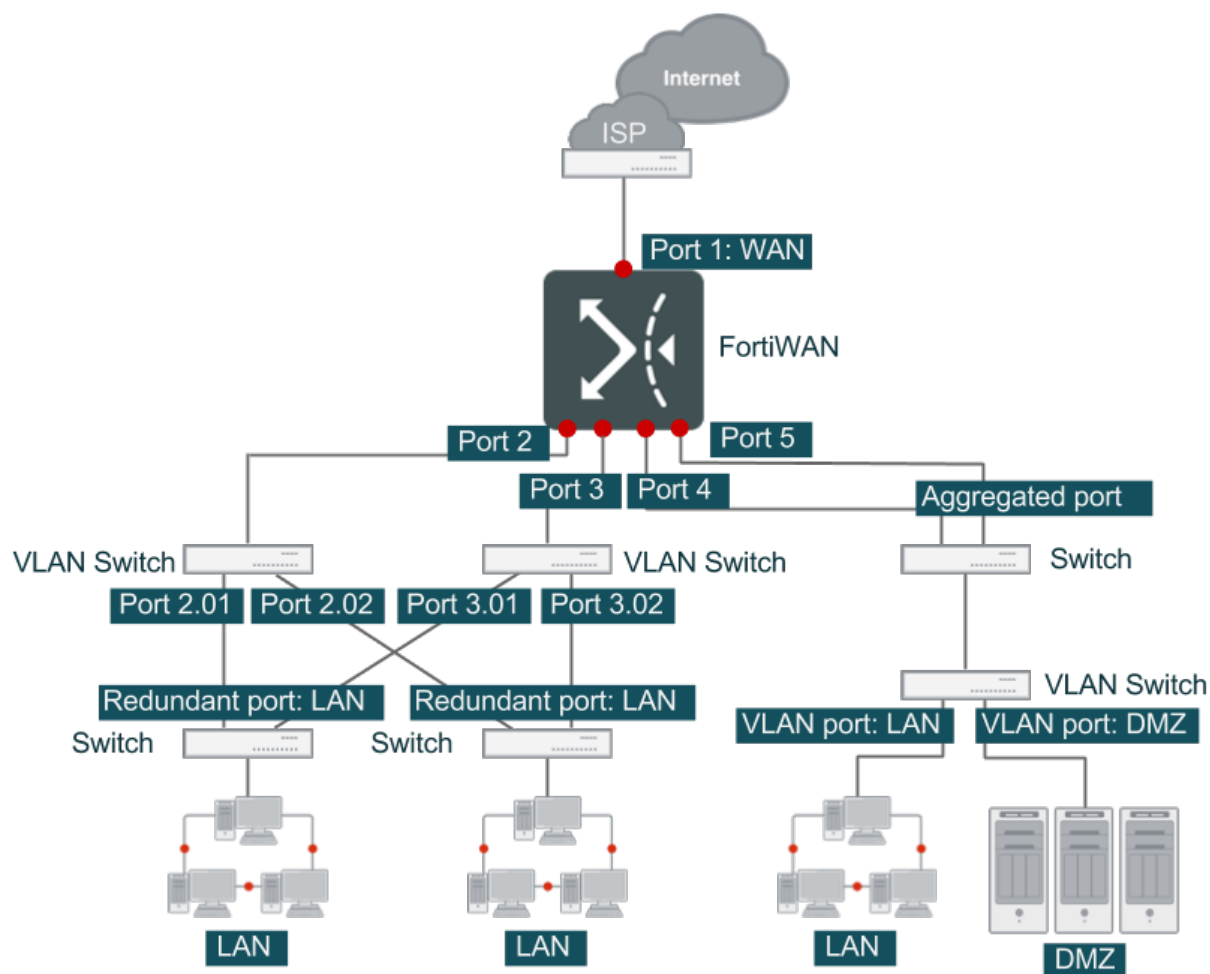
| Label | Mapping |
|-------|---------|
| dmz45 | Port 4  |
|       | Port 5  |

**Step 4** Map the created logical aggregated port dmz45 to DMZ in *VLAN and Port Mapping* table.

| Port  | VLAN Tag    | Mapping |
|-------|-------------|---------|
| Port1 | no VLAN Tag | WAN     |
| Port2 | no VLAN Tag | LAN     |
| Port3 | no VLAN Tag | LAN     |
| Port4 | no VLAN Tag | None    |
| Port5 | no VLAN Tag | None    |
| dmz45 | no VLAN Tag | DMZ     |

After the configurations are applied, labels "Bridge: lan23" and "Bonding: dmz45" will be listed respectively in LAN Port and DMZ Port pull-down menus of LAN and DMZ subnets settings (see [LAN Private Subnet](#) and [Configuring your WAN](#)) for options. Moreover, the two labels will be also listed in Input Port pull-down menu of Auto Routing and Bandwidth Management (see [Auto Routing](#) and [Bandwidth Management](#)) for your options.

You can also have the deployment configured in an advanced way. First, if you need the LAN ports being defined with several VLAN tags and also having them in redundant pairs; second, if you need the aggregated port being mapped to one LAN and one DMZ by defining it with VLAN tags, the configurations will be the following steps:



**Step 1** To configure the settings for the deployment, you need to define Port2 and Port3 with VLAN tags and map all of them to LAN in *VLAN and Port Mapping* table. Leaving Port4 and Port5 being mapped to None as previous.

| Port  | VLAN Tag    | Mapping |
|-------|-------------|---------|
| Port1 | no VLAN Tag | WAN     |
| Port2 | 01          | LAN     |
|       | 02          | LAN     |
| Port3 | 01          | LAN     |
|       | 02          | LAN     |
| Port4 | no VLAN Tag | None    |
| Port5 | no VLAN Tag | None    |

**Step 2** Create a new redundant LAN port labeled lan23tag01 and mapped it to Port2.01 and Port3.01 in *Redundant LAN Port* table.

| Label      | Mapping   |
|------------|-----------|
| lan23tag01 | Port 2.01 |
|            | Port 3.01 |

**Step 3** Create another new redundant LAN port labeled lan23tag02 and mapped it to Port2.02 and Port3.02 in *Redundant LAN Port* table.

| Label      | Mapping   |
|------------|-----------|
| lan23tag02 | Port 2.02 |
|            | Port 3.02 |

**Step 4** Create a new aggregated port labeled agg45 and mapped it to Port4 and Port5 in *Aggregated Port* table.

| Label | Mapping |
|-------|---------|
| agg45 | Port 4  |
|       | Port 5  |

**Step 5** In *VLAN and Port Mapping* table, map the created logical aggregated port agg45 to a LAN and a DMZ by defining it with VLAN tags.

| Port  | VLAN Tag    | Mapping |
|-------|-------------|---------|
| Port1 | no VLAN Tag | WAN     |
| Port2 | 01          | LAN     |
|       | 02          | LAN     |
| Port3 | 01          | LAN     |
|       | 02          | LAN     |
| Port4 | no VLAN Tag | None    |
| Port5 | no VLAN Tag | None    |
| agg45 | 01          | LAN     |
|       | 02          | DMZ     |

## Configuring networks to FortiWAN

As the previous description, FortiWAN is an intelligent WAN load balancing device providing services to increase connection efficiency and reliability between the internal and external networks, but basically as a router it is fundamental to route IP packets among the connected networks. According to different purpose and functionality, a connected network could be one of the three types: WAN, LAN and DMZ networks. When you configure setting of a network to a FortiWAN, you are registering the network to the FortiWAN (majorly adding related routing information about the network to the FortiWAN), so that the FortiWAN can find the path to correctly route packets destined to the network. Network settings establish the necessary routing rules to FortiWAN so that the connected WAN, LAN and DMZ networks can communicate to each other. Besides setting routing rules, network setting requires other necessary information used to guarantee a well-cooperation between the connected network and FortiWAN. No matter what types those connected networks are, there are some common concepts among the settings:

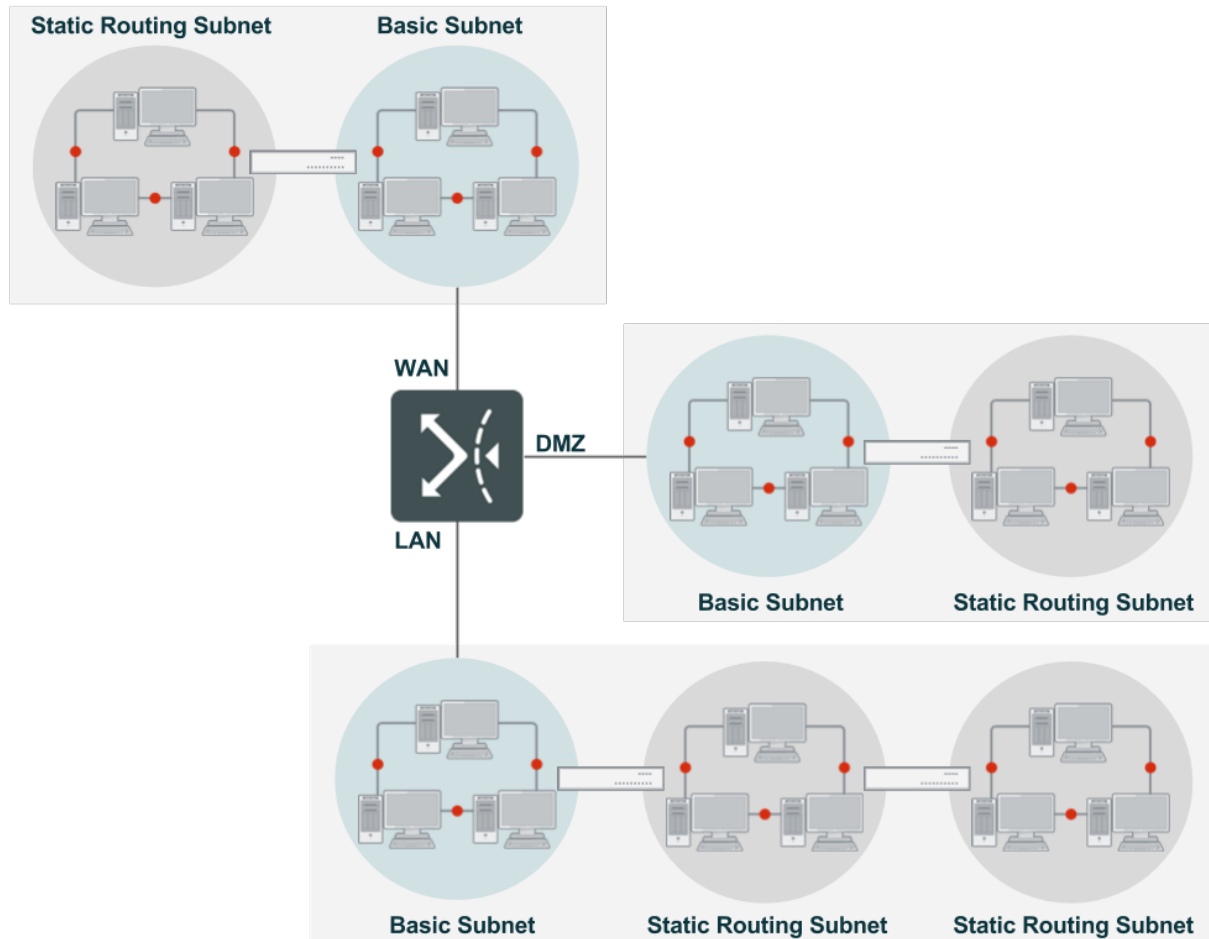
### Static route: basic subnets & static routing subnets

Within a network site, FortiWAN routes communication among the connected WAN (near WAN actually, see [WAN, LAN and DMZ](#) and [Near WAN](#)), LAN and DMZ networks according to established static routing entries, without WAN load balancing and fail-over being involved. Those static routing entries of connected networks are manually added to FortiWAN by network settings. A connected network can contain several subnets. Basically, FortiWAN defines two types of subnets to a connected network for its static route, basic subnet and static routing subnet:

**Basic subnet:** Any subnet connected directly to FortiWAN's network port is called a basic subnet. Setting for a basic subnet tells FortiWAN the network IP, netmask of the subnet and the connected port, so that FortiWAN is aware of the network port used to directly deliver the packets destined to the subnet.

**Static routing subnet:** Any subnet connected directly or indirectly to a FortiWAN's basic subnet is called a static routing subnet. Setting for a static routing subnet tells FortiWAN the network IP, netmask of the subnet and the gateway, so that FortiWAN can find the next hop to forward packets destined to the subnet, although the static routing subnet does not connect directly to the FortiWAN.

Basically, all the network configurations in WAN Setting (see [Configuring your WAN and DMZ](#)), WAN/DMZ Private Subnet (see [WAN/DMZ Private Subnet](#)) and LAN Private Subnet (see [LAN Private Subnet](#)) contain settings of basic subnet and static routing subnet, except IPv4-based bridge-mode WAN links. FortiWAN's basic subnets and static routing subnets are static routes, therefore, any physical change to deployment of the subnets requires corresponding modifications to the routing entries. The basic static route is supposed to be suitable for simple topologies. When you have a large-scale network with complex topologies, dynamic routing would be much suitable for it. FortiWAN supports RIP (v1 and v2), OSPF and VRRP on its LAN ports.



## IPv4/IPv6 dual stack

FortiWAN supports IPv4/IPv6 dual stack, which means a FortiWAN can be configured with both IPv4 and IPv6 connectivity capabilities (FortiWAN does not support a pure IPv6 based network). None of IPv4 network and IPv6 network is dispensable for configuring a dual stack network to FortiWAN. Therefore, the required static routing information for configuring a dual stack network to a WAN, LAN or DMZ port will include IPv4 basic subnet, IPv4 static routing subnet, IPv6 basic subnet and IPv6 static routing subnet.

## Auto addressing

FortiWAN supports auto addressing on each of the WAN, LAN and DMZ ports, so that hosts in any of the connected basic subnet can be automatically assigned IP addresses and relative information. FortiWAN provides the addressing mechanisms including DHCP, DHCP relay, DHCPv6 and SLAAC (see [Automatic addressing within a basic subnet](#)).

## Configuring your WAN and DMZ

In this section we will talk about the configurations for WAN and DMZ network deployments. To have a FortiWAN accessing to the Internet, it requires an ISP network connected to the FortiWAN. The connectivity between a FortiWAN's WAN port and an ISP network is called a WAN link, which is the necessary medium for accessing the



Internet. FortiWAN's DMZ is designed to be associated with a WAN link, therefore, configuration of a DMZ must be included in a WAN link.

Compared with a LAN network, there are more concerns need to be taken care of for a WAN link and its DMZ. Besides port mapping for the WAN ports on a FortiWAN, you need to decide the WAN types and the subsequent subnet deployments for a WAN link as well. Generally, ISP provides a connectivity in various ways. Here is a table telling what you will have from ISP for a connectivity in different types:

FortiWAN supports WAN links in both routing mode and bridge mode (See [WAN types: Routing mode and Bridge mode](#)).

| Internet connectivity type             | IP type | No. of IP | Network scale                                                                      | Modem type              |
|----------------------------------------|---------|-----------|------------------------------------------------------------------------------------|-------------------------|
| <b>Routing Mode</b>                    | Static  | Multiple  | An IP subnet (number of available IP matches the netmask)                          | A gateway (router)      |
| <b>Bridge Mode: One Static IP</b>      | Static  | Single    | One IP of a large-scale subnet (less number of available IP than the netmask)      | A bridge, not a gateway |
| <b>Bridge Mode: Multiple Static IP</b> | Static  | Multiple  | An IP range of a large-scale subnet (less number of available IP than the netmask) | A bridge, not a gateway |
| <b>Bridge Mode: PPPoE</b>              | Dynamic | Single    | One IP of a large-scale subnet                                                     | A bridge, not a gateway |
| <b>Bridge Mode: DHCP Client</b>        | Dynamic | Single    | One IP of a large-scale subnet                                                     | A bridge, not a gateway |

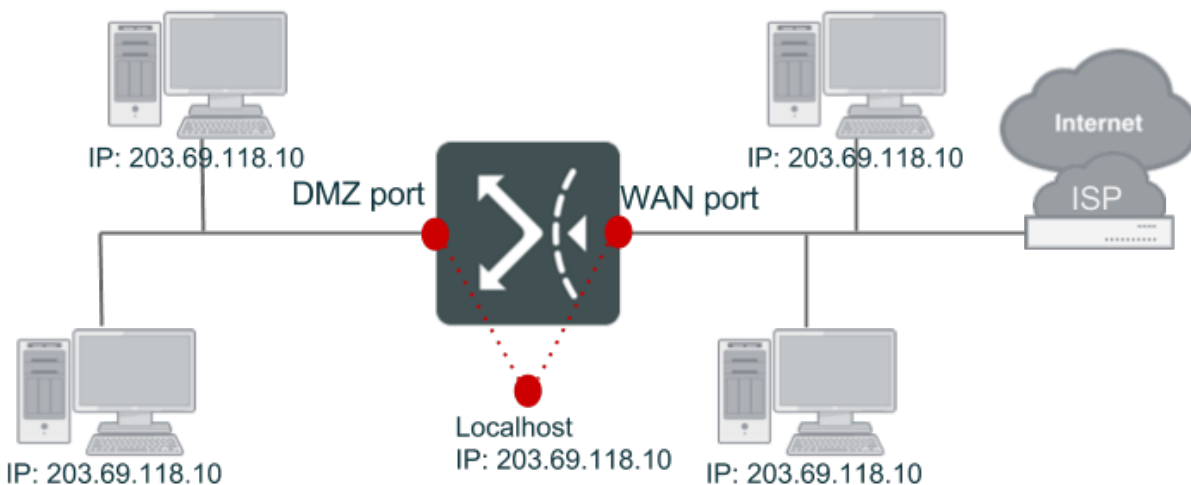
Since ISP provides the available IP addresses in different ways for the above Internet connectivity, FortiWAN has equal mechanisms to identify the near WAN areas and define the static route. Before continuing on the topic, let us review what a near WAN is to FortiWAN first. As previous descriptions, FortiWAN defines the area that is between a FortiWAN's WAN port and the ISP's modem as a near WAN of the WAN link. Individual IP addresses, segments and subnets deployed within this area are considered the near WAN of a WAN link. Opposite to the WAN area (the Internet), although near WAN is located on the WAN side, it can be considered as a part of your network site, just like the LAN and DMZ areas. Within the network site, FortiWAN delivers packets among the near WAN, DMZ and LAN according to the static routes. Services of load balancing, fail-over, traffic shaping and statistics (Auto Routing, Bandwidth Management and NAT) will not be applied to those packets. Only packets that are destined to somewhere not defined in the routing table (the traffic communicating with hosts out of the site) will be handled by Bandwidth Management, Auto Routing and NAT, and forwarded to the gateway (the Internet). Note that traffic within near WAN and traffic communicating with near WAN will not be counted in outbound and inbound traffic of the WAN link, but they do occupy part of bandwidth of the WAN link. You should be careful about usage of your near WAN. A lot of near WAN traffic impacts on FortiWAN's WAN load-balancing and traffic shaping.

Configurations of WAN links are mainly about setting the static routing information to FortiWAN for the near WAN (and DMZ). Comparing with a LAN, setting the static route for near WAN and DMZ of a WAN link is more complex

and variable. According to the distinguishing characteristics of different WAN types, FortiWAN identifies the near WAN and DMZ areas of a WAN link in different ways. Configuring a WAN link as a unsuitable type on FortiWAN will result in a mistake for near WAN identification; miscalculation and misjudgment then happen when performing traffic statistics, traffic shaping and load-balancing. The followings are the mechanisms FortiWAN uses for different WAN types:

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Routing-mode WAN link                        | <ul style="list-style-type: none"> <li>• It requires at least one IPv4 network being configured for a IPv4-based Internet connectivity, or a pair of IPv4 and IPv6 networks for a dual-stack connectivity.</li> <li>• Any IP address of the network is considered either in near WAN or DMZ (except the IP used by localhost).</li> <li>• The whole IPv4/IPv6 network (indicated by the specified netmask) is considered belonging to your site, either in form of a near WAN or a combination of near WAN and DMZ.</li> <li>• A near WAN is considered an IPv4/IPv6 network and the gateway of the WAN link is counted in the near WAN.</li> <li>• Traffic that matches routing entries of the network will bypass Bandwidth Management and Auto Routing. If a bridge-mode Internet connectivity is incorrectly configured as a routing-mode WAN link on FortiWAN, all the IP addresses of the network (usually a large-scale network such as a class C) will be considered belonging to your site. However, the problem is that most of the IP addresses do not actually belong to your site (they are outside of your site, over the Internet); WAN load-balancing, fail-over and traffic shaping should not be bypassed for those traffic.</li> </ul> |
| Bridge-mode WAN link with multiple static IP | <ul style="list-style-type: none"> <li>• It requires exactly specifying the individual IPv4/IPv6 address or IPv4/IPv6 ranges to deploy near WAN and/or DMZ for a IPv4-based or dual-stack WAN link.</li> <li>• Only the specified IPv4/IPv6 addresses are considered belonging to your site (located in near WAN or DMZ). Unspecified IP addresses are considered the outside of your site, belonging to the Internet.</li> <li>• A near WAN is considered a segment of an IPv4/IPv6 network. The gateway of the WAN link will not be count in the near WAN.</li> <li>• Incorrectly configuring a routing-mode Internet connectivity as a bridge-mode WAN link on FortiWAN will result in abnormal behaviors to traffic communicating with the gateway and unspecified IP addresses.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Bridge-mode WAN link with one static IP      | <ul style="list-style-type: none"> <li>• Near WAN and DMZ are not supported for this WAN type on FortiWAN.</li> <li>• Only the IPv6/IPv4 address assigned to localhost of the WAN link is considered belonging to your site. All the other IP addresses (including the gateway) within the same network (indicated by the specified netmask) are considered the outside of your site.</li> <li>• Incorrectly configuring a routing-mode Internet connectivity as a bridge-mode WAN link on FortiWAN will result in abnormal behaviors to traffic communicating with the gateway and unspecified IP addresses.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| PPPoE bridge-mode WAN link                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| DHCP bridge-mode WAN link                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

You have to figure out the type of your link, so that you can correctly configure it to FortiWAN. The netmask and number of IP addresses indicate whether you have an complete IP subnet (routing mode) or just some IP addresses of a large-scale subnet (bridge mode). If you have ISP links belonging to *Routing Mode* and *Bridge Mode: Multiple Static IP*, you will have more than one IP address to use. The localhost of a WAN port will require one IP address, and the rest of the IP addresses are available to hosts connected to the WAN port and a DMZ port. Deploying IP addresses to WAN and DMZ are so that included in configurations of *Routing Mode* and *Bridge Mode: Multiple Static IP*. As for links belonging to *Bridge Mode: One Static IP*, *Bridge Mode: PPPoE* and *Bridge Mode: DHCP Client*, the only IP address must be used by the localhost of the WAN port and there will be no more IP addresses available to other hosts in WAN and DMZ.



[WAN Settings] is the major part to deploy FortiWAN in various types of WAN links. If your network has several WAN links, you have to configure one after another. Select any link from [WAN link] and check [Enable] to start a configuration of the WAN connection (See "[WAN link and WAN port](#)"). A configuration of WAN link is divided into three parts: Basic Settings, Basic Subnet and Static Routing Subnet. Before starting configuration, here are several important concepts you should know.

Configuration of a WAN link, no matter what the WAN type it is, contains the following parts:

### Basic setting

The basic setting will require you to set the maximum upload/download bandwidth of a WAN link, upload/download threshold and the MTU for transmission between FortiWAN and ISP's network. These settings are necessary for FortiWAN Bandwidth Management (see [Bandwidth Management](#)), Auto Routing (see [Auto Routing](#)) and Multihoming ([Multihoming](#)) refer to process the real WAN traffic that is between FortiWAN and the Internet (traffic between FortiWAN and its near WAN is not included).

For bridge-mode WAN links, the basic setting also contains extra fields:

### Bridge Mode: One Static IP

Allocating the only IPv4/IPv6 address to localhost of the WAN port.

Bridge Mode: Multiple Static IP

Allocating the one IPv4/IPv6 address to localhost of the WAN port, and arrange others to network segments in WAN and/or DMZ if necessary. Opposite to routing-mode WAN links, ISP provides you a range of IP addresses of a large-scale network for the bridge-mode WAN link, not a network subnet. These IP addresses can be deployed in WAN and/or DMZ, and the corresponding static route will be established as well, but it is just not a basic subnet (in routing-mode, IP addresses of a WAN link in WAN and/or DMZ are treated as )

Bridge Mode: PPPoE

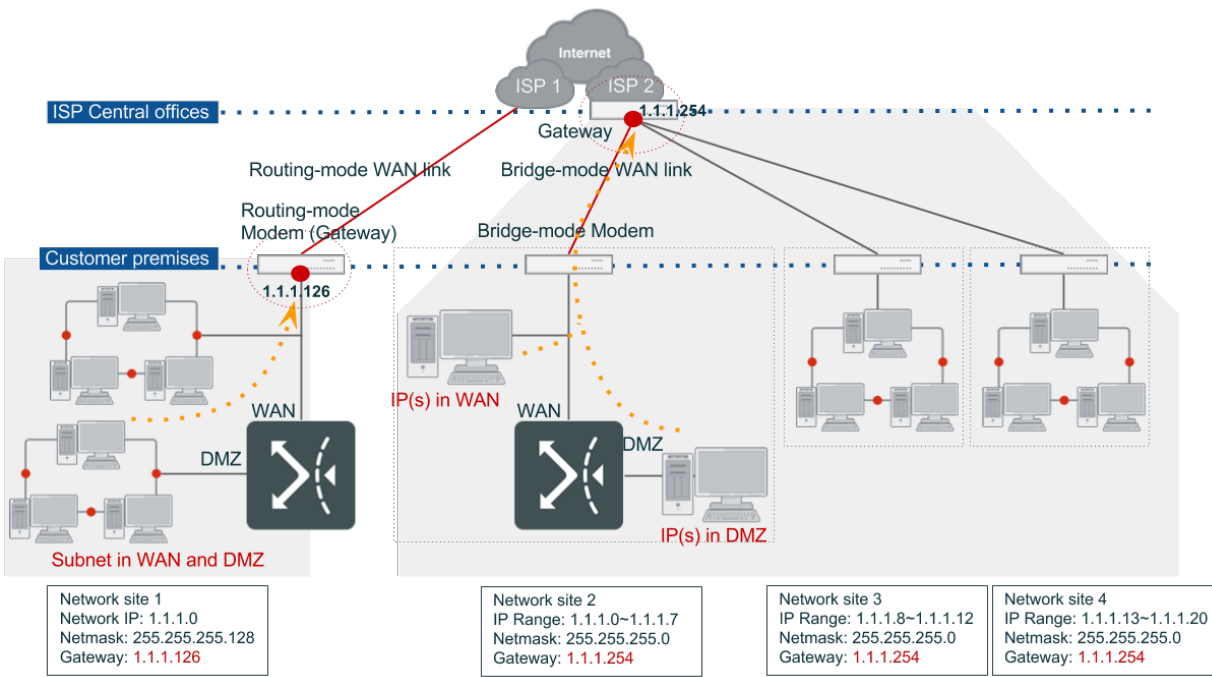
The username and password for PPPoE accessing.

IPv4/IPv6 basic subnet & IPv4/IPv6 static routing subnet

As previous description, FortiWAN need the static route to find path for traffic among LAN, DMZ and near WAN. When you configure a routing-mode WAN link or an IPv4/IPv6 dual stack link, settings of basic subnet and static routing subnet are the route to FortiWAN for IPv4/IPv6 networks connecting to WAN ports and/or DMZ ports.

Routing mode and Bridge mode: multiple static IP

Routing mode and bridge mode (multiple static IP) deploy IP addresses in WAN and DMZ in different ways. The following table lists the difference between the two modes for the WAN link deployments.



|                               | Routing mode                                             | Bridge mode: Multiple static IP                                 |
|-------------------------------|----------------------------------------------------------|-----------------------------------------------------------------|
| Form of given IPs and netmask | An IP subnet (Number of IP matches scale of the netmask) | A range of IPs (Number of IP is less than scale of the netmask) |

|                                                      | Routing mode                              | Bridge mode: Multiple static IP |
|------------------------------------------------------|-------------------------------------------|---------------------------------|
| <b>Gateway</b>                                       | Located on customer premises              | Located on ISP's central office |
| <b>Modem type</b>                                    | Functions as a router (the gateway)       | Functions as a bridge           |
| <b>Deployment of near WAN and/or DMZ</b>             | Supports                                  | Supports                        |
| <b>Static routing subnets in near WAN and/or DMZ</b> | Supports                                  | Not supports                    |
| <b>Configuration for near WAN and/or DMZ</b>         | In Basic Subnet and Static Routing Subnet | In Basic Setting                |

### Start to configure a WAN link

To deploy a WAN link on FortiWAN, go to **System > Network Setting** and expand **WAN Setting** panel on the Web UI. Configurations of all the WAN links start from a common setting block in the panel:

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WAN Link</b> | <p>Select the WAN link that you are configuring to FortiWAN from the drop-down menu. Depending on the model, FortiWAN supports up to 25 or 50 WAN links. All the WAN links are numbered from 1 to 25 or 50, such as WAN link 1, WAN link 2, ... and WAN link 50. Each number indicates a WAN link. The number is nothing about the WAN port that the WAN link is installed to. For example, you can install WAN link 1 to WAN Port 3, or WAN link 3 to WAN Port 1.</p> <p>Number of WAN links that a FortiWAN supports is always more than its physical network port. For example, FortiWAN 200B supports 25 WAN links, but 5 physical network ports are provided only. You will need to create VLAN ports on FortiWAN's ports to install more than 4 WAN links.</p> <p>In configurations of most of FortiWAN's services, such as Auto Routing, Multihoming, Bandwidth Management, Virtual Server, NAT and etc., these WAN links appear as options for associating policies and rules to a WAN link. They are also the options used to switch among WAN links for statistics.</p> |
| <b>Enable</b>   | Check/uncheck to enable/disable the WAN link. Enabling/disabling of a WAN link does not represent the connectivity status of the WAN link. Connectivity statuses of the enabled WAN links will be listed in in <b>WAN Link State</b> panel on Web UI page <b>System &gt; Summary</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Note</b>     | Text descriptions for the WAN link. You can see the notes of the enabled WAN link in <b>WAN Link State</b> panel on Web UI page <b>System &gt; Summary</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## WAN Type

The first step to start a WAN link configuration is deciding the WAN type (See "[WAN types: Routing mode and Bridge mode](#)"). Configuration varies on [WAN Type] in [Basic Settings]. The [WAN Type] could be one of:

- Routing Mode (See "[Configurations for a WAN link in Routing Mode](#)")
- Bridge Mode: One Static IP (See "[Configurations for a WAN link in Bridge Mode: One Static IP](#)")
- Bridge Mode: Multiple Static IP (See "[Configurations for a WAN link in Bridge Mode: Multiple Static IP](#)")
- Bridge Mode: PPPoE (See "[Configurations for a WAN link in Bridge Mode: PPPoE](#)")
- Bridge Mode: DHCP Client (See "[Configurations for a WAN link in Bridge Mode: DHCP](#)")

### See also

- [WAN link and WAN port](#)
- [Configurations for a WAN link in Routing Mode](#)
- [Configurations for a WAN link in Bridge Mode: One Static IP](#)
- [Configurations for a WAN link in Bridge Mode: Multiple Static IP](#)
- [Configurations for a WAN link in Bridge Mode: PPPoE](#)
- [Configurations for a WAN link in Bridge Mode: DHCP](#)

## Routing-mode WAN link

Configuration of a routing-mode WAN link starts from selecting and enabling the WAN link on Web UI (see *Start to configure a WAN link* in [Configuring your WAN and DMZ](#)), and select Routing Mode from the WAN Type drop-down menu in Basic Setting panel. After that, you start configuring the following settings:

### IPv4-based routing-mode WAN link

- **Basic setting** and at least one **IPv4 basic subnet** are necessary.
- IPv4 static routing subnet is for your option.

### IPv4/IPv6 Dual-stack routing-mode WAN link

- **Basic setting**, one **IPv4 basic subnet** and one **IPv6 basic subnet** are necessary.
- IPv4/IPv6 static routing subnets are for your options.

## Basic Setting

Besides the WAN Type, the rest setting fields of Basic Setting of a routing-mode WAN link are as followings:

### WAN Port

A FortiWAN's network port used to connect the WAN link with the FortiWAN (you need to physically install the network cable to this port for the WAN link). All the physical and VLAN ports that are mapped to WAN (see [Aggregated, Redundant, VLAN Ports and Port Mapping](#)) are listed here for your options. The WAN link field is unrelated to the WAN port. For example, you can install WAN link 1 to WAN Port3, or WAN link 3 to WAN Port 1. (See [WAN link and WAN port](#)).

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Down/Up Stream</b>           | The WAN link's transfer speed at which you can download/upload data from/to the Internet. Please input the value in Kbps, e.g. 10240Kbps/640Kbps. FortiWAN Bandwidth Management's default inbound and outbound classes use the two values actively to limit the download and upload rates on the WAN link (see <a href="#">Bandwidth Management</a> ).                                                                                                                                                                                                                                           |
| <b>Down/Up Stream Threshold</b> | Specify upstream/downstream (Kbps) threshold to the WAN link. WAN links with traffic exceeding the thresholds will be considered as failed.<br><br>FortiWAN's Auto Routing and Multihoming will ignore the WAN links failed by exceeding traffic while distributing traffic over WAN links, if the Threshold function is enabled in their load-balancing policies (See <a href="#">Outbound Load Balancing and Failover (Auto Routing)</a> and <a href="#">Inbound Load Balancing and Failover (Multihoming)</a> ).<br><br>Leave it blank or zero if you do not apply threshold to the WAN link. |
| <b>MTU</b>                      | (Maximum Transmission unit) refers to the size of the largest packet or frame that a given layer of a communications protocol can pass onwards on the WAN port. It allows dividing the packet into pieces, each small enough to pass over a single link. It is set to 1500 by default.                                                                                                                                                                                                                                                                                                           |
| <b>IPv4 Gateway</b>             | IPv4 address of the default gateway of the WAN link. This field is mandatory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>IPv6 Gateway</b>             | IPv6 address of the default gateway of the WAN link. This field is optional. Ignore it for IPv4-based links or configure it for IPv4/IPv6 dual stack links.                                                                                                                                                                                                                                                                                                                                                                                                                                      |



Applying network settings involving changes related to MTU of a network interface will restart the interface and disrupt established connections.

## Static routing information

As mentioned previously, FortiWAN requires the correct routing information to deliver packets among the connected near WAN, DMZ and LAN networks. Configurations of basic subnets and static routing subnets of a WAN link are the routing information for the FortiWAN.

A routing-mode WAN link is attached with an IP network which should be deployed as a basic subnet to the WAN link. Since localhost of the WAN port is a part of the subnet, at least one basic subnet is necessary for configuring a routing-mode WAN link. For the reason, IP(s) on Localhost and Netmask fields of a routing-mode WAN link are contained in configuration of Basic Subnet, rather than Basic Setting.

## IPv4/IPv6 Basic Subnet

Basic subnets are the subnets connecting directly to FortiWAN. A DMZ must be associated with a WAN link, therefore, basic subnet of a WAN link can be divided into four types according to combination of WAN and DMZ:

- **Subnet in WAN:** A subnet deployed in WAN. This type requires at least one IP for localhost of the WAN port, and the rest of the subnet can be used for hosts in WAN (near WAN).

- **Subnet in DMZ:** A subnet deployed in DMZ. This type requires at least one IP for localhost of the DMZ port, and the rest of the subnet can be used for hosts in DMZ.
- **Subnet in WAN and DMZ:** A subnet deployed in two segments, WAN and DMZ. Proxy ARP combines the two segments into a logic segment for the IP subnet (see ). Proxy ARP logically combines the specified WAN port and DMZ port into a logical port. This type requires at least one IP for localhost of the WAN port, and the rest of the subnet can be used for hosts in WAN (near WAN) and DMZ.
- **Subnet on Localhost:** A subnet deployed on the localhost of a WAN port (This is not supported for IPv6 basic subnets). All the IP addresses of the subnet will be deployed on the WAN port.

A subnet in WAN and DMZ might be the most practical deployment for a routing-mode WAN link. If the ISP provides only one network with your IPv4 WAN link (this is the most general case for a routing-mode link), you can deploy it as any of the subnet types but a subnet in DMZ. Remember, at least one IP address must be assigned to localhost of a WAN port for the IPv4 link, therefore, at least one subnet must be associated with the WAN port. If you get more than one network from the ISP with the IPv4 link, you still have to deploy at least one of them as a subnet in WAN, a subnet in WAN and DMZ or a subnet on localhost, but there is not limitation to the rest networks. Briefly, if you are given only one network for the WAN link, you can not deploy it as a subnet in DMZ. As for configuring a dual stack link, similarly, it requires at least one IPv4 network and one IPv6 network get deployed individually as a subnet in WAN, a subnet in WAN and DMZ or a subnet on localhost. Next comes the configuration of basic subnet for each type:

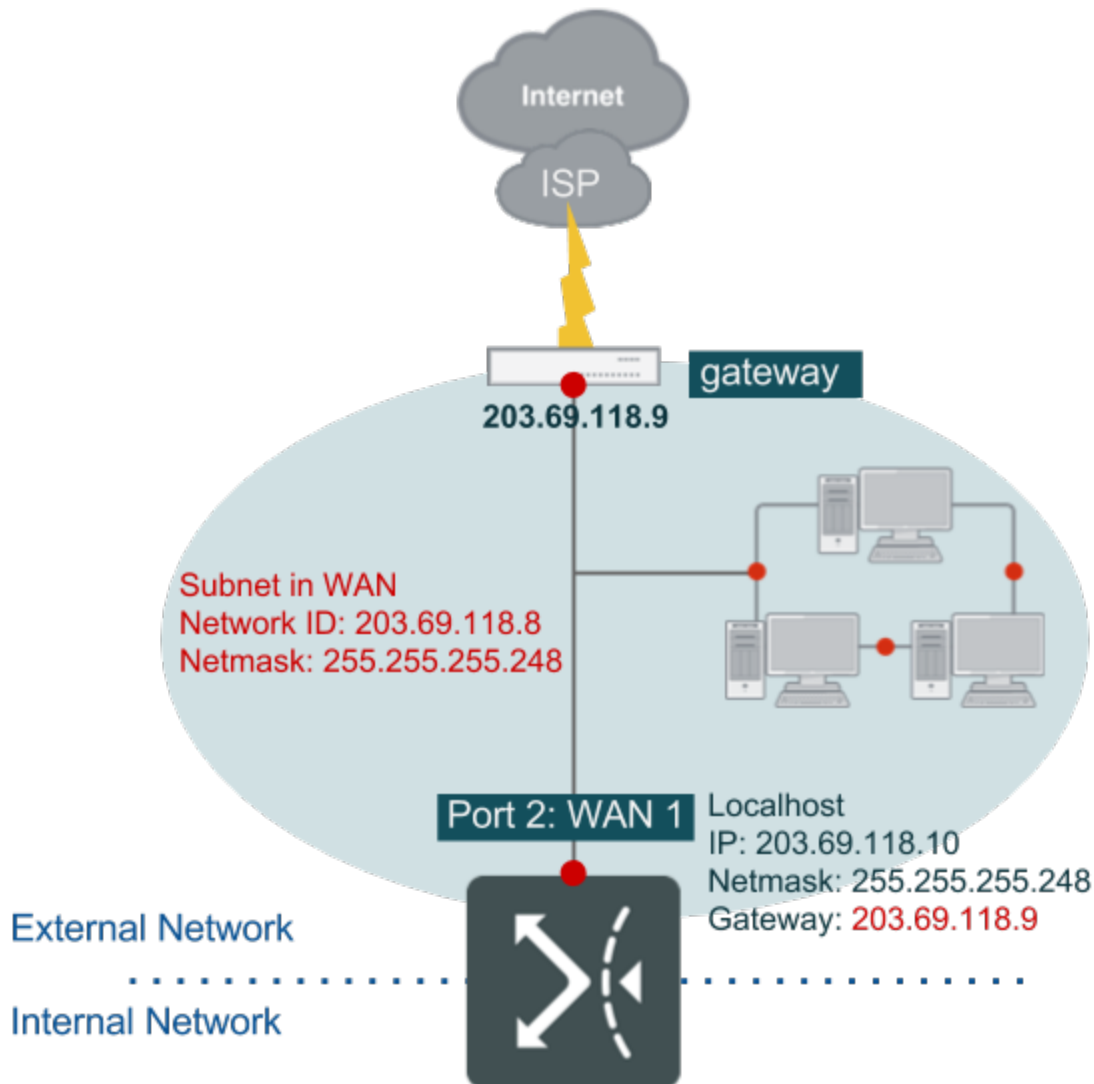
### [IPv4/IPv6 Basic Subnet]: Subnet in WAN

Click the add button on the IPv4 Basic Subnet panel or IPv6 Basic Subnet panel to add a configuration, and select **Subnet in WAN** from the Subnet Type drop-down menu. The rest configuration fields to deploy a IPv4/IPv6 network as a subnet in WAN are as followings:

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IP(s) on Localhost</b>    | <p>The IP address(es) that you want to assign to localhost of the specified WAN port (the WAN port that is specified in Basic Setting panel) for the WAN link. At least one IP address is required here. You can type a range of IP addresses here in format "IPstart-IPend" or click the add button to individually add more IP addresses to the localhost.</p> <p>Note that the rest IP addresses of the network that are not assigned to the localhost here will be automatically considered as being located in WAN area.</p> |
| <b>Netmask/Prefix Length</b> | Netmask/Prefix Length of the IPv4/IPv6 network that you are deploying to the WAN link as a subnet in WAN.                                                                                                                                                                                                                                                                                                                                                                                                                         |

This topology is frequently used for where cluster hosts being deployed in WAN.





In the this diagram, we have a WAN link attached with a given network that netmask is 255.255.255.248, gateway is 203.69.118.9 and the available IP addresses are 203.69.118.10 – 203.69.118.14. The WAN link is connected to FortiWAN's Port2 (mapped to a WAN port) with IP address 203.69.118.10 being assigned to the localhost. In this case, FortiWAN will consider that the rest IP addresses 203.69.118.11 – 203.69.118.14 are located in the WAN area (actually, the near WAN) of the WAN link. The following is the configuration for this case:

| Basic Setting     |               |
|-------------------|---------------|
| WAN Port          | Port2         |
| IPv4 Gateway      | 203.69.118.9  |
| IPv4 Basic Subnet |               |
| Subnet Type       | Subnet in WAN |

|                           |                 |
|---------------------------|-----------------|
| <b>IP(s) on localhost</b> | 203.69.118.10   |
| <b>Netmask</b>            | 255.255.255.248 |

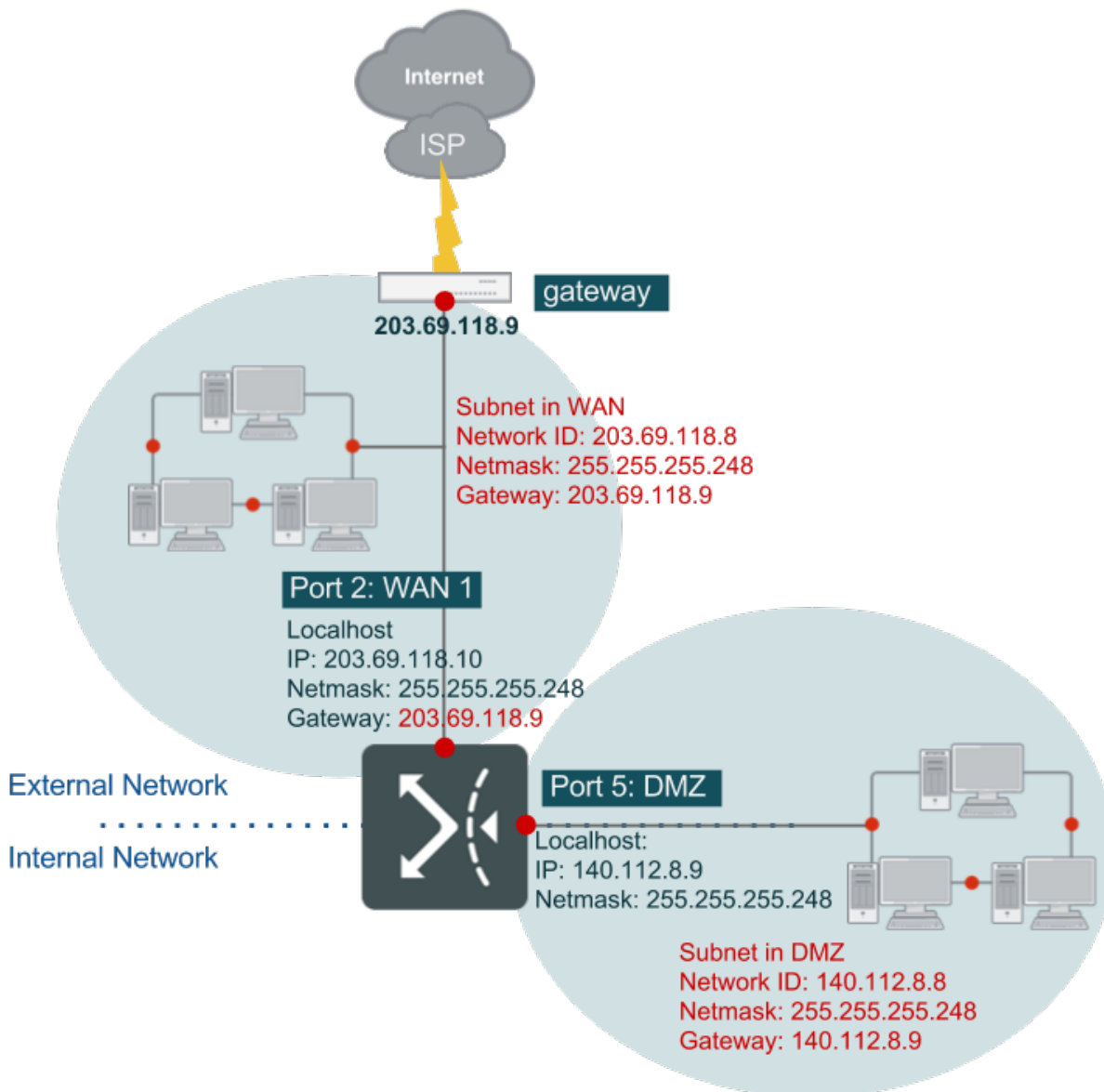
Configuration of the settings implies a route to FortiWAN that any packet destined to 203.69.118.9 – 203.69.118.14 will be directly forwarded through this WAN port, without Auto Routing and Bandwidth Management processes. In this case, subnet 203.69.118.8/29 (203.69.118.9 – 203.69.118.14) is the near WAN of the link.

### [IPv4/IPv6 Basic Subnet]: Subnet in DMZ

Click the add button on the IPv4 Basic Subnet panel or IPv6 Basic Subnet panel to add a configuration, and select **Subnet in DMZ** from the Subnet Type drop-down menu. The rest configuration fields are as followings:

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IP(s) on Localhost</b>                          | <p>The IP address(es) of the IPv4/IPv6 network that you want to assign to localhost of the specified DMZ port (the DMZ port that is specified below) of the WAN link. At least one IP address is required here. You can type a range of IP addresses here in format "IPstart-IPend" or click the add button to individually add more IP addresses to the localhost.</p> <p>Note that the rest IP addresses of the network that are not assigned to the localhost here will be automatically considered as being located in DMZ area.</p> |
| <b>Netmask/Prefix Length</b>                       | Netmask/Prefix Length of the IPv4/IPv6 network that is being deployed as a subnet in DMZ and associated with the WAN link.                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>DMZ Port</b>                                    | A FortiWAN's network port used to connect a subnet of the WAN link with the FortiWAN as a DMZ subnet (you need to physically install the network cable to this port for the DMZ subnet). All the physical, logical and VLAN ports that are mapped to DMZ (see <a href="#">Aggregated</a> , <a href="#">Redundant</a> , <a href="#">VLAN Ports and Port Mapping</a> ) are listed here for your options.                                                                                                                                   |
| <b>Enable DHCP/DHCP Relay/SLAAC/DHCPv6 Service</b> | <p>Click to enable automatic addressing on the specified DMZ port for hosts in the connected IPv4/IPv6 DMZ subnet (see <a href="#">Automatic addressing within a basic subnet</a> for configuration details).</p> <p>Note that only the IP addresses of the IPv4/IPv6 basic subnet defined here are the candidates for related IP pools of automatic addressing.</p>                                                                                                                                                                     |

This topology is frequently used for where a cluster of hosts being deployed in DMZ. The following example for a subnet in DMZ is based on the above example that a WAN link with a subnet being deployed in WAN. Please click the [+] button on IPv4/IPv6 Basic Subnet panel to add a subnet to the WAN link. **Remember a subnet in DMZ must coexist with a subnet in WAN, a subnet in WAN and DMZ or a subnet on localhost.**



As described in the topology, since the cluster of hosts are deployed in DMZ. FortiWAN port5 has to be mapped to DMZ with IP address 140.112.8.9. Thus the hosts in the subnet take the default gateway as 140.112.8.9. In this case, IP addresses 203.69.118.9 – 203.69.118.14 are treated as in near WAN, while IP addresses 140.112.8.9 – 140.112.8.14 in DMZ do not belong to near WAN. Check [Enable DHCP] if hosts in the subnet in DMZ require DHCP service. And enter the starting and ending address in [DHCP Range]. If any host in the subnet uses static IP address, then in [Static Mapping], enter its IP and MAC address. Similarly, if ISP provides another LAN IPv6 subnet, you can deploy it in DMZ. The SLAAC and DHCPv6 in FortiWAN are designed to work together, which SLAAC responses router advertisement (including default gateway and DNS server) to a host and DHCPv6 responses the host an appropriate IPv6 address. Note: FortiWAN assumes that IP addresses that are unlisted in [IP(s) on Localhost] can be used for hosts in the subnet.

In the this diagram, we have another network that ISP provides to the WAN link, which the netmask is 255.255.255.248, gateway is 140.112.8.9 and the available IP addresses are 140.112.8.10 – 140.112.8.14. This network is connected to FortiWAN's Port5 (mapped to a DMZ port) with IP address 203.69.118.10 being assigned

to the localhost. In this case, FortiWAN will consider that the rest IP addresses 203.69.118.11 – 203.69.118.14 are located in the WAN area (actually, the near WAN) of the WAN link. The following is the configuration for this case:

|                            |                 |
|----------------------------|-----------------|
| <b>Basic Setting</b>       |                 |
| <b>WAN Port</b>            | Port2           |
| <b>IPv4 Gateway</b>        | 203.69.118.9    |
| <b>IPv4 Basic Subnet 1</b> |                 |
| <b>Subnet Type</b>         | Subnet in WAN   |
| <b>IP(s) on localhost</b>  | 203.69.118.10   |
| <b>Netmask</b>             | 255.255.255.248 |
| <b>IPv4 Basic Subnet 2</b> |                 |
| <b>Subnet Type</b>         | Subnet in DMZ   |
| <b>IP(s) on localhost</b>  | 140.112.8.9     |
| <b>Netmask</b>             | 255.255.255.248 |
| <b>DMZ Port</b>            | Port5           |

For the details about DHCP, DHCP Relay, SLAAC and DHCPv6, see "[Automatic addressing within a basic subnet](#)".

### [IPv4/IPv6 Basic Subnet]: Subnet in WAN and DMZ

Click the add button on the IPv4 Basic Subnet panel or IPv6 Basic Subnet panel to add a configuration, and select **Subnet in WAN and DMZ** from the Subnet Type drop-down menu. The rest configuration fields are as followings:

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IP(s) on Localhost</b> | The IP address(es) of the IPv4/IPv6 network that you want to assign to localhost of the specified WAN port (the WAN port that is specified in Basic Setting panel) and DMZ port (the DMZ port that is specified below) of the WAN link. The WAN port and DMZ port will be logically combined for Public IP Pass-through. At least one IP address is required here. You can type a range of IP addresses here in format "IPstart-IPend" or click the add button to individually add more IP addresses to the localhost. |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**IP(s) in WAN**

The IP address(es) of the IPv4/IPv6 network that you want to assign to the WAN area (near WAN) of the WAN link. You can leave it blank, type one IP address or a range of IP addresses (in format "IPstart-IPend" ) here. You can also click the add button to individually add more IP addresses to the near WAN.

Note that the rest IP address(es) of the network that are not assigned to the localhost (above) and WAN (here) will be automatically considered as being located in DMZ. Therefore, no matter how you deploy IP addresses in WAN area, at least one IP address, IP address of gateway of the WAN link (what you set in Basic Setting for IPv4 Gateway and/or IPv6 Gateway), must be contained in this field.

**Netmask/Prefix Length**

Netmask/Prefix Length of the IPv4/IPv6 network that you are deploying to the WAN link as a subnet in WAN.

**DMZ Port**

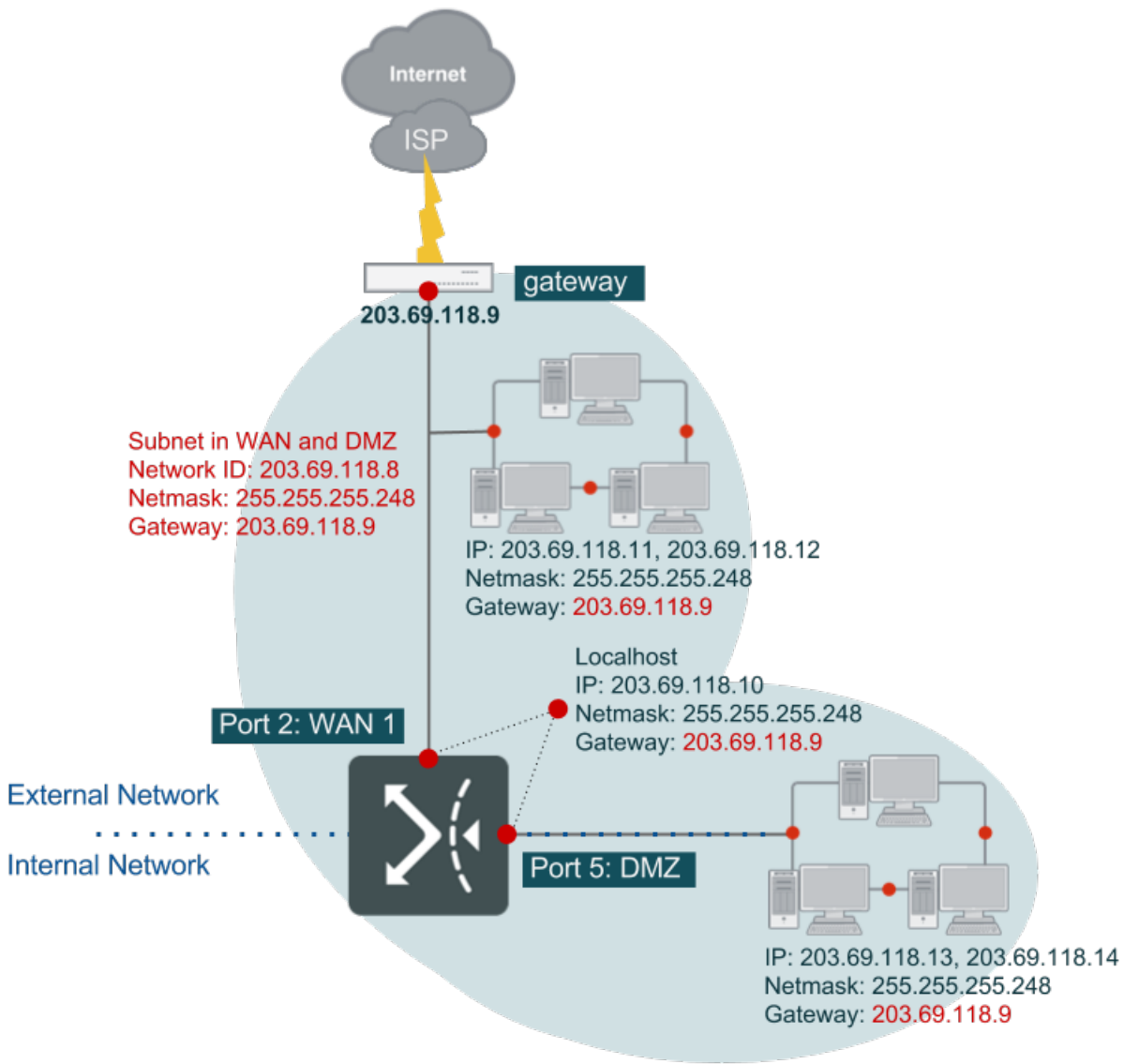
A FortiWAN's network port used to connect a part of the subnet to the WAN link as segment in DMZ (you need to physically install the network cable to this port for the DMZ subnet). All the physical, logical and VLAN ports that are mapped to DMZ (see [Aggregated, Redundant, VLAN Ports and Port Mapping](#)) are listed here for your options.

**Enable DHCP/DHCP Relay/SLAAC/DHCPv6 Service**

Click to enable automatic addressing on the specified DMZ port for hosts in the connected IPv4/IPv6 DMZ segment (see [Automatic addressing within a basic subnet](#) for configuration details).

Note that only the IP addresses assigned to the DMZ part of the defined basic subnet are the candidates for related IP pools of automatic addressing.

This topology is frequently found where a cluster of hosts in one subnet are deployed in both WAN side and DMZ side.



As described in the topology, port2 and port5 are connected in dotted line, indicating an IP range in the same subnet 203.69.118.8/29 spreads across WAN (port2) and DMZ (port5). FortiWAN employs Proxy ARP to connect those hosts becoming in the same network segment (See "[Public IP pass through \(DMZ Transparent Mode\)](#)").

Note that although IP address 203.69.118.9 has been configured as default gateway in Basic Setting table, you are still required to add it in the field [IP(s) in WAN]. When you select [Subnet in WAN and DMZ] from [Subnet Type], FortiWAN will assume the IP addresses that are unlisted in [IP(s) on Localhost] and [IP(s) in WAN] are all in DMZ. Thus, in this example, except 203.69.118.10, 203.69.118.9 and 203.69.118.11-203.69.118.12, the rest IP addresses of subnet 203.69.118.8/29 are assigned to DMZ for Public IP Pass-through. In this case, IP addresses 203.69.118.9 – 203.69.118.12 in WAN side are treated as in near WAN, while IP addresses 203.69.118.13 – 203.69.118.14 in DMZ side do not belong to near WAN.

Check [Enable DHCP] if hosts in the subnet in DMZ require DHCP service. And enter the starting and ending address in [DHCP Range]. If any host in the subnet uses static IP address, then in [Static Mapping], enter its IP and MAC address. Similarly, the configuration to deploy an IPv6 public subnet in WAN and DMZ.

| Basic Setting      |                             |
|--------------------|-----------------------------|
| WAN Port           | Port2                       |
| IPv4 Gateway       | 203.69.118.9                |
| IPv4 Basic Subnet  |                             |
| Subnet Type        | Subnet in WAN and DMZ       |
| IP(s) on localhost | 203.69.118.10               |
| IP(s) in WAN       | 203.69.118.11-203.69.118.12 |
| Netmask            | 255.255.255.248             |
| DMZ Port           | Port5                       |

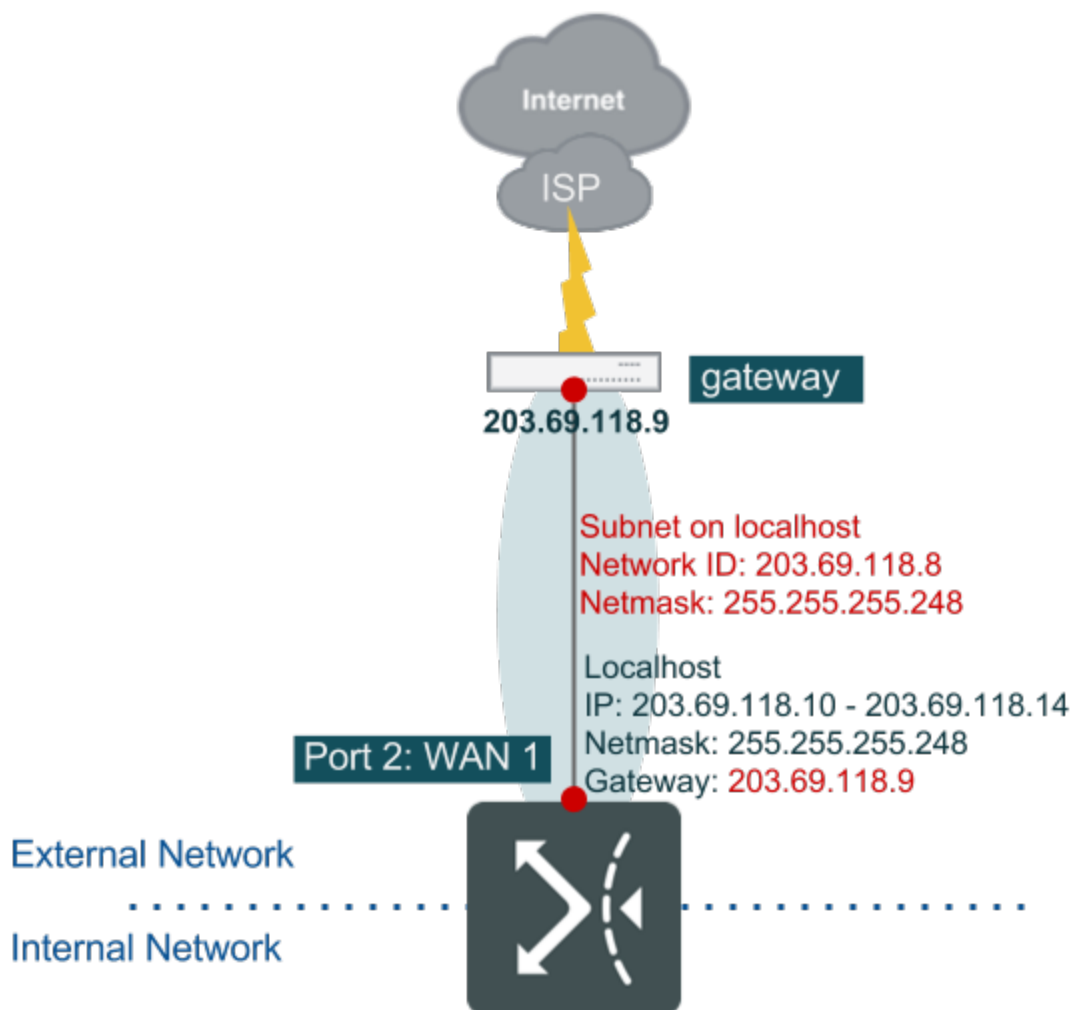
For the details about DHCP, DHCP Relay, SLAAC and DHCPv6, see "[Automatic addressing within a basic subnet](#)".

### [IPv4/IPv6 Basic Subnet]: Subnet on Localhost

Click the add button on the IPv4 Basic Subnet panel (this subnet type is not supported for IPv6 basic subnets) to add a configuration, and select **Subnet on Localhost** from the Subnet Type drop-down menu. The rest configuration fields are as followings:

|            |                                                                                                                                                      |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network IP | The network IP of the subnet that you want to assign to localhost of the specified WAN port (the WAN port that is specified in Basic Setting panel). |
| Netmask    | Netmask of the IPv4 subnet that you are deploying to the WAN link as a subnet on localhost.                                                          |

This topology is found where subnet is designated on FortiWAN to better use Virtual Server.



This deployment is much simpler than other subnet types. Except the gateway, all the IP addresses of the subnet are assigned to the WAN port of the WAN link; there is no IP addresses available for deployment in WAN and/or DMZ areas. All of the IP addresses will indicate the associated WAN link to services NAT, Multihoming and Virtual Server. For this example, the configuration just requires 203.69.118.8 and 255.255.255.248 being entered in [Network IP] and [Netmask] respectively.

#### Basic Setting

|                          |                     |
|--------------------------|---------------------|
| <b>WAN Port</b>          | Port2               |
| <b>IPv4 Gateway</b>      | 203.69.118.9        |
| <b>IPv4 Basic Subnet</b> |                     |
| <b>Subnet Type</b>       | Subnet on Localhost |
| <b>Network IP</b>        | 203.69.118.8        |
| <b>Netmask</b>           | 255.255.255.248     |



Note that, for all of the subnet types described above, the IP addresses (IPv4 or IPv6) specified to field [IP(s) on Localhost] can be used for NAT to transfer the source IP address of packets to. The first IP address on the list of [IP(s) on Localhost] will be used for the NAT default rules of the WAN link. System generates NAT default rules automatically for a WAN link so that a host with private IP address in LAN can access Internet without setting NAT rules manually. **For FortiWAN V4.0.x, system does not generate NAT default rules for IPv6 WAN links, setting NAT rules manually is required** (See "NAT").

## IPv4/IPv6 Static Routing Subnets

A WAN link's static routing subnets are the subnets connected to the WAN link's basic subnets via routers or L3 switches. The same as those basic subnets, FortiWAN needs the corresponding static route (dynamic routing protocols are not supported for WAN links' networks), so that FortiWAN can find the path to forward packets to the static routing subnets. Configuring a static routing subnet to a WAN link here implies adding the routing information to FortiWAN. A routing-mode WAN link supports both IPv4 and IPv6 static routing subnets for pure IPv4-based WAN link and IPv4/IPv6 dual stack WAN link. According to the area a subnet deployed in, the static routing subnets of a WAN link are divided into:

- **Subnet in WAN:** A static routing subnet deployed in WAN, connected to a basic subnet in WAN or basic subnet in WAN and DMZ.
- **Subnet in DMZ:** A static routing subnet deployed in DMZ, connected to a basic subnet in DMZ or basic subnet in WAN and DMZ.

Next comes a few examples to further illustrate configurations in [Basic Subnet] and [Static Routing Subnet].

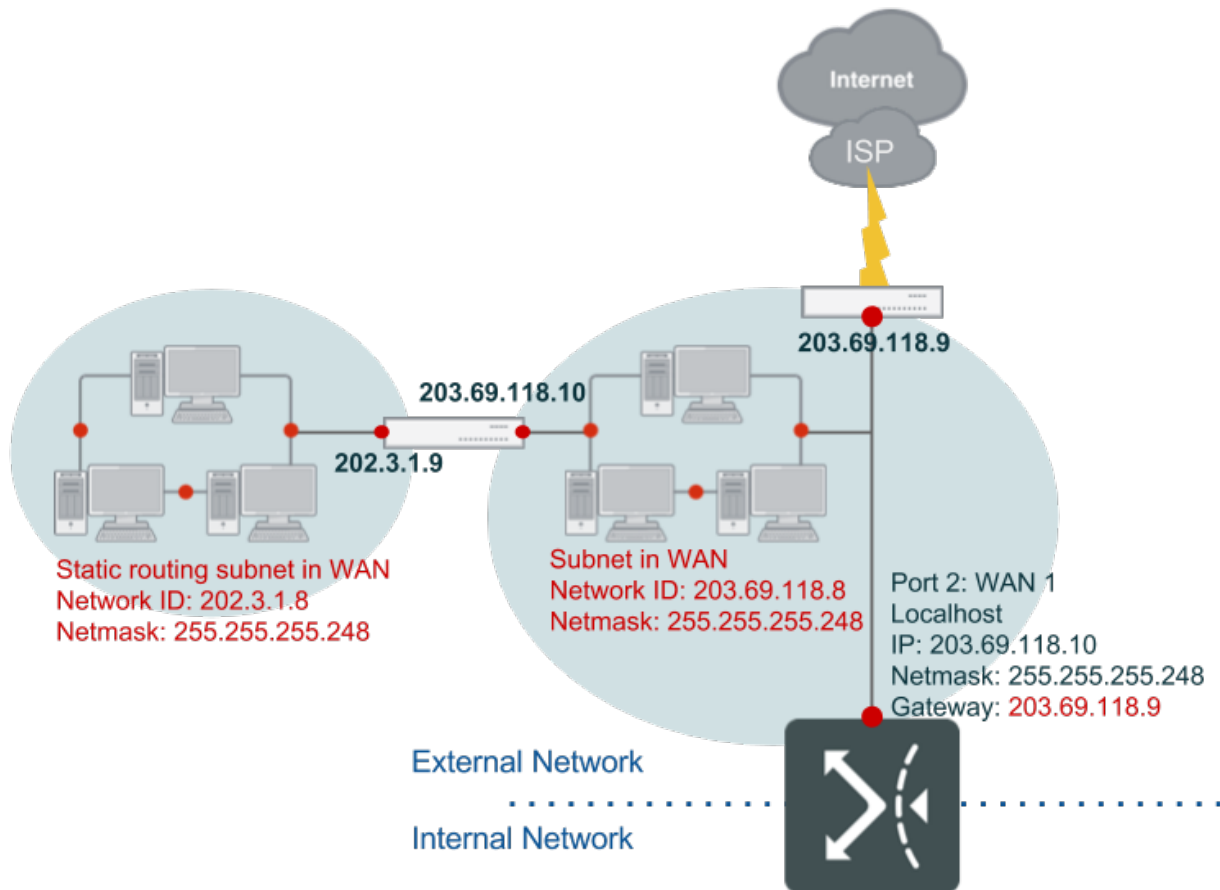
### [IPv4/IPv6 Static Routing Subnet]: Subnet in WAN

Click the add button on the IPv4 Static Routing Subnet panel or IPv6 Static Routing Subnet panel to add a configuration, and select **Subnet in WAN** from the Subnet Type drop-down menu. The rest configuration fields are as followings:

|                   |                                                                                                                                                                                                                                                                                   |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Network IP</b> | The network IP of the IPv4 static routing subnet that you want to deploy in (near) WAN area of the WAN link. This field is in IPv4 Static Routing Subnet panel.                                                                                                                   |
| <b>Netmask</b>    | Netmask of the IPv4 static routing subnet that you want to deploy in (near) WAN area of the WAN link. This field is in IPv4 Static Routing Subnet panel.                                                                                                                          |
| <b>Subnet</b>     | The IPv6 static routing subnet that you want to deploy in (near) WAN area of the WAN link in format such as 2000::123f:0:0:1/32. This field is in IPv6 Static Routing Subnet panel.                                                                                               |
| <b>Gateway</b>    | IPv4/IPv6 address of the gateway (router) connecting a basic subnet with the static routing subnet. This IP address is the path that FortiWAN uses to forward packets destined to the static routing subnet to. This field is in both IPv4 and IPv6 Static Routing Subnet panels. |
| <b>Proxy ARP</b>  | Check to enable Proxy ARP on FortiWAN for the static routing subnet; FortiWAN will answer the ARP queries for a network address that is in the static routing subnet. This field is in IPv4 Static Routing Subnet panel.                                                          |

This topology is rarely seen in actual network where static routing subnet is located on the WAN. In other words, the subnet in WAN does not connect to FortiWAN directly, but needs a router instead to transfer packets. In this

example, a subnet 202.3.1.8/29 located on the WAN connects to the basic subnet 203.69.118.8/29 via a router (202.3.1.9 and 203.69.118.10). Subnet 202.3.1.8/29 is so that a static routing subnet of the WAN link. Configuration of the static routing subnet indicates the route to FortiWAN for packets destined to subnet 202.3.1.8/29.



As described in the UI, FortiWAN transfers packets to the gateway 203.69.118.10 to deliver them to subnet 202.3.1.8/255.255.255.248.

| Basic Setting      |               |
|--------------------|---------------|
| WAN Port           | Port2         |
| IPv4 Gateway       | 203.69.118.9  |
| IPv4 Basic Subnet  |               |
| Subnet Type        | Subnet in WAN |
| IP(s) on localhost | 203.69.118.10 |

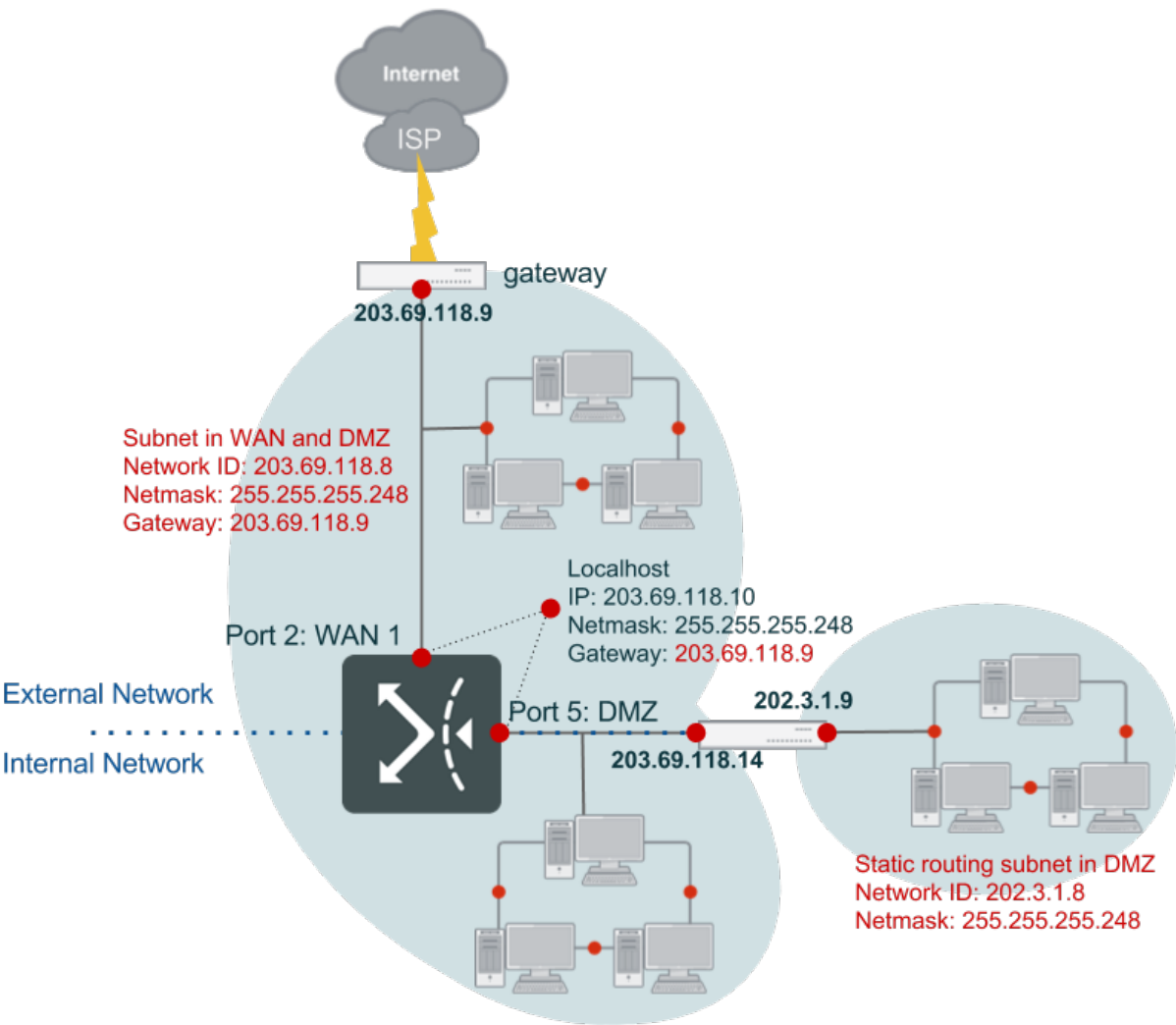
|                                   |                 |
|-----------------------------------|-----------------|
| <b>Netmask</b>                    | 255.255.255.248 |
| <b>IPv4 Static Routing Subnet</b> |                 |
| <b>Subnet Type</b>                | Subnet in WAN   |
| <b>Network IP</b>                 | 202.3.1.8       |
| <b>Netmask</b>                    | 255.255.255.248 |
| <b>Gateway</b>                    | 203.69.118.10   |

### [IPv4/IPv6 Static Routing Subnet]: Subnet in DMZ

Click the add button on the IPv4 Static Routing Subnet panel or IPv6 Static Routing Subnet panel to add a configuration, and select **Subnet in DMZ** from the Subnet Type drop-down menu. The rest configuration fields are as followings:

|                   |                                                                                                                                                                                                                                                                                   |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Network IP</b> | The network IP of the IPv4 static routing subnet that you want to deploy in DMZ area of the WAN link. This field is in IPv4 Static Routing Subnet panel.                                                                                                                          |
| <b>Netmask</b>    | Netmask of the IPv4 static routing subnet that you want to deploy in DMZ area of the WAN link. This field is in IPv4 Static Routing Subnet panel.                                                                                                                                 |
| <b>Subnet</b>     | The IPv6 static routing subnet that you want to deploy in DMZ area of the WAN link in format such as 2000::123f:0:0:1/32. This field is in IPv6 Static Routing Subnet panel.                                                                                                      |
| <b>Gateway</b>    | IPv4/IPv6 address of the gateway (router) connecting a basic subnet with the static routing subnet. This IP address is the path that FortiWAN uses to forward packets destined to the static routing subnet to. This field is in both IPv4 and IPv6 Static Routing Subnet panels. |
| <b>Proxy ARP</b>  | Check to enable Proxy ARP on FortiWAN for the static routing subnet; FortiWAN will answer the ARP queries for a network address that is in the static routing subnet. This field is in IPv4 Static Routing Subnet panel.                                                          |

This topology is very similar with the Static Routing Subnet: Subnet in WAN in last example. The only difference is, the subnet is in DMZ area.



As described in the UI, FortiWAN transfers packets to the gateway 203.69.118.14 to deliver them to subnet 139.3.1.8/255.255.255.248

| Basic Setting      |                             |
|--------------------|-----------------------------|
| WAN Port           | Port2                       |
| IPv4 Gateway       | 203.69.118.9                |
| IPv4 Basic Subnet  |                             |
| Subnet Type        | Subnet in WAN and DMZ       |
| IP(s) on localhost | 203.69.118.10               |
| IP(s) in WAN       | 203.69.118.11-203.69.118.13 |

|                                   |                 |
|-----------------------------------|-----------------|
| <b>Netmask</b>                    | 255.255.255.248 |
| <b>DMZ Port</b>                   | Port5           |
| <b>IPv4 Static Routing Subnet</b> |                 |
| <b>Subnet Type</b>                | Subnet in WAN   |
| <b>Network IP</b>                 | 202.3.1.8       |
| <b>Netmask</b>                    | 255.255.255.248 |
| <b>Gateway</b>                    | 203.69.118.14   |

**See also**

- [WAN link and WAN port](#)
- [VLAN and port mapping](#)
- [Configurations for VLAN and Port Mapping](#)
- [Outbound Load Balancing and Failover \(Auto Routing\)](#)
- [Inbound Load Balancing and Failover \(Multihoming\)](#)
- [Scenarios to deploy subnets](#)
- [Public IP pass through \(DMZ Transparent Mode\)](#)
- [IPv6/IPv4 Dual Stack](#)

**Bridge-mode (multiple static IP) WAN link**

Configuration of a multiple-static-IP bridge-mode WAN link starts from selecting and enabling the WAN link on Web UI (see *Start to configure a WAN link* in [Configuring your WAN and DMZ](#)), and select Bridge Mode: Multiple Static IP from the WAN Type drop-down menu in Basic Setting panel. After that, you start configuring the following settings:

**IPv4-based bridge-mode WAN link**

- Only **Basic setting** is necessary.
- IPv4 basic subnets and IPv4 static routing subnets are not supported here.

**IPv4/IPv6 Dual-stack bridge-mode WAN link**

- Only **Basic setting** is necessary.
- IPv4 basic subnets and IPv4 static routing subnets are not supported here; IPv6 basic subnets and IPv6 static routing subnets are optional.

Different from routing mode, configuration of static routing is contained in Basic Setting for a bridge-mode WAN link. Similar to routing mode, FortiWAN uses ProxyARP to combine the WAN area and DMZ area as one logical network segment.

## Basic Setting

Besides the WAN Type, the rest setting fields of Basic Setting of a multiple-static-IP bridge-mode WAN link are as followings:

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WAN Port</b>                 | A FortiWAN's network port used to connect the WAN link with the FortiWAN (you need to physically install the network cable to this port for the WAN link). All the physical and VLAN ports that are mapped to WAN (see <a href="#">Aggregated, Redundant, VLAN Ports and Port Mapping</a> ) are listed here for your options. The WAN link field is unrelated to the WAN port. For example, you can install WAN link 1 to WAN Port3, or WAN link 3 to WAN Port 1. (See <a href="#">WAN link and WAN port</a> ).                                                                                  |
| <b>Up/Down Stream</b>           | The WAN link's transfer speed at which you can download/upload data from/to the Internet. Please input the value in Kbps, e.g. 10240Kbps/640Kbps. FortiWAN Bandwidth Management's default inbound and outbound classes use the two values actively to limit the download and upload rates on the WAN link (see <a href="#">Bandwidth Management</a> ).                                                                                                                                                                                                                                           |
| <b>Up/Down Stream Threshold</b> | Specify upstream/downstream (Kbps) threshold to the WAN link. WAN links with traffic exceeding the thresholds will be considered as failed.<br><br>FortiWAN's Auto Routing and Multihoming will ignore the WAN links failed by exceeding traffic while distributing traffic over WAN links, if the Threshold function is enabled in their load-balancing policies (See <a href="#">Outbound Load Balancing and Failover (Auto Routing)</a> and <a href="#">Inbound Load Balancing and Failover (Multihoming)</a> ).<br><br>Leave it blank or zero if you do not apply threshold to the WAN link. |
| <b>MTU</b>                      | (Maximum Transmission unit) refers to the size of the largest packet or frame that a given layer of a communications protocol can pass onwards on the WAN port. It allows dividing the packet into pieces, each small enough to pass over a single link. It is set to 1500 by default.                                                                                                                                                                                                                                                                                                           |
| <b>IPv4 IP(s) on Localhost</b>  | The IPv4 addresses that are deployed on localhost (See " <a href="#">Scenarios to deploy subnets</a> "). IP addresses specified here can be used for NAT to transfer the source IP address of packets to. The first IP address listed here will be used to generate the NAT default rules of the WAN link (See " <a href="#">NAT</a> ").                                                                                                                                                                                                                                                         |
| <b>IPv4 IP(s) in WAN</b>        | The IPv4 addresses that are deployed in WAN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>IPv4 IP(s) in DMZ</b>        | The IPv4 addresses that are deployed in DMZ.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Different from configuration of Routing mode's basic subnets, it requires exactly specifying IPs to fields IP(s) in WAN and IP(s) in DMZ for a Bridge mode WAN link if you want to deploy those IP addresses in the WAN and DMZ areas. FortiWAN would not automatically classifies the rest IPs of a subnet as IPs in WAN or IPs in DMZ for bridge-mode WAN links (FortiWAN does it for a routing-mode WAN link), since the bridge mode is supposed to work with certain IPs of a large-scale network (see [WAN types: Routing mode and Bridge mode](#)) and FortiWAN is not aware of what the IPs are that an ISP provides you for the WAN link (the remaining IPs of the large-scale subnet are not valid to be deployed in your network).

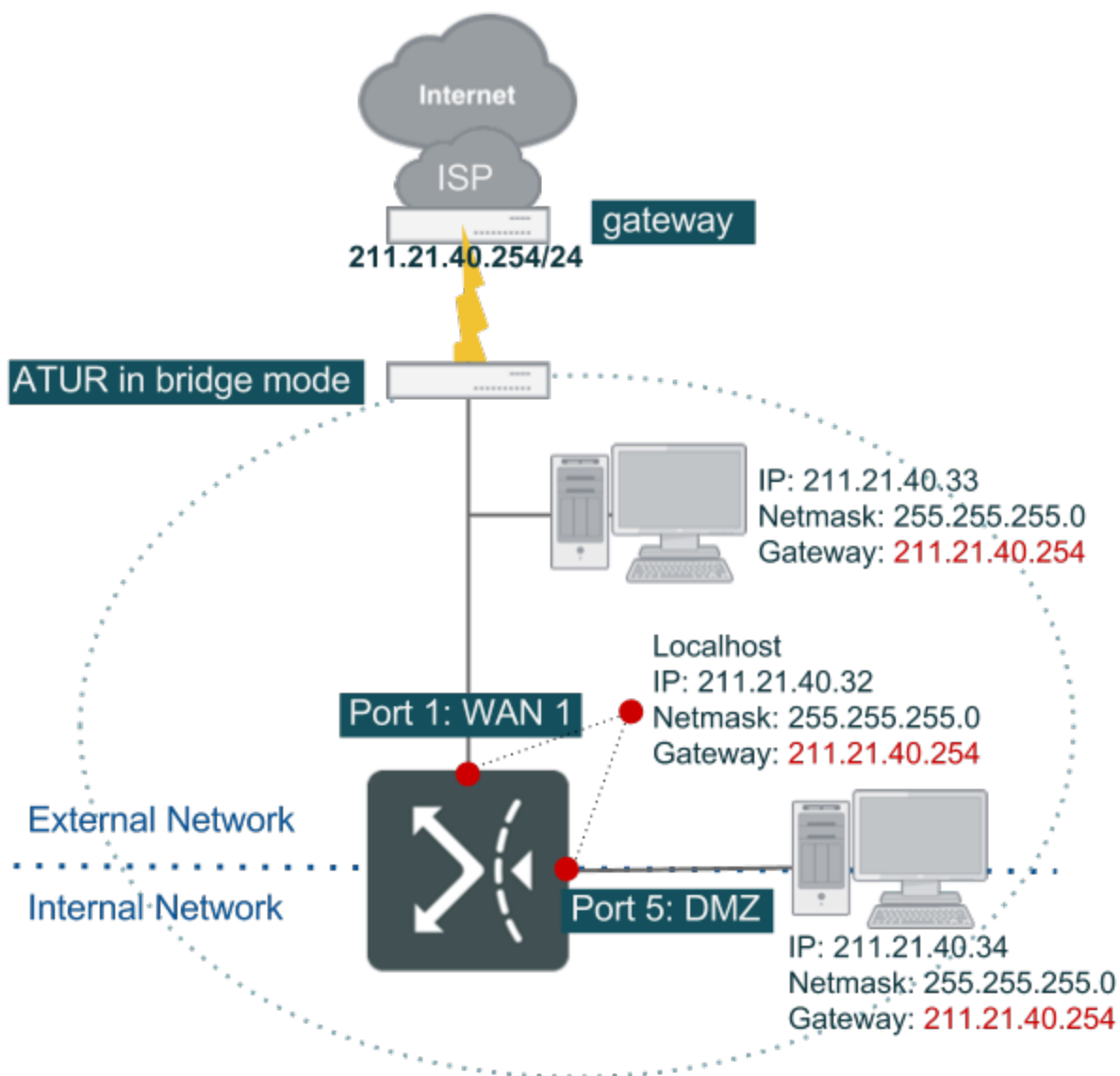
|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IPv4 Netmask</b>                                | The IPv4 netmask that ISP provides.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>IPv4 Gateway</b>                                | The IPv4 address of the default gateway.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>IPv6 IP(s) on Localhost</b>                     | The IPv6 addresses that are deployed on localhost (See " <a href="#">Scenarios to deploy subnets</a> "). IP addresses specified here can be used for NAT to transfer the source IP address of packets to. The first IP address listed here will be used to generate the NAT default rules of the WAN link. <b>For FortiWAN V4.0.x, system does not generate NAT default rules for IPv6 WAN links, setting NAT rules manually is required</b> (See " <a href="#">NAT</a> "). |
| <b>IPv6 IP(s) in WAN</b>                           | The IPv6 addresses that are deployed in WAN.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>IPv6 IP(s) in DMZ</b>                           | The IPv6 addresses that are deployed in DMZ.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>IPv6 Prefix</b>                                 | The IPv6 prefix that ISP provides.                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>IPv6 Gateway</b>                                | The IPv6 address of the default gateway.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Subnet</b>                                      | The IPv6 subnet deployed on the WAN link.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>DMZ Port</b>                                    | The network port of FortiWAN used to connect the DMZ area. All the physical and logical ports that are mapped to DMZ (see <a href="#">Configurations for VLAN and Port Mapping</a> ) are listed here for options. Hosts deployed in the DMZ are required to connected to this port. Public IP pass-through (see <a href="#">Public IP Pass-through</a> ) is supported to combine the selected WAN port and DMZ port.                                                        |
| <b>Enable DHCP/DHCP Relay/SLAAC/DHCPv6 Service</b> | <p>Click to enable automatic addressing on the specified DMZ port for hosts in the connected IPv4/IPv6 DMZ segment (see <a href="#">Automatic addressing within a basic subnet</a> for configuration details).</p> <p>Note that only the IP addresses defined in fields <b>IPv4 IP(s) in DMZ</b> and <b>IPv6 IP(s) in DMZ</b> are the candidates for related IP pools of automatic addressing.</p>                                                                          |



Applying network settings involving changes related to MTU of a network interface will restart the interface and disrupt established connections.

The SLAAC and DHCPv6 in FortiWAN are designed to work together, which the SLAAC responses router advertisement (including default gateway and DNS server) to a host and DHCPv6 responses the host an appropriate IPv6 address.

This topology can be seen where a group of valid IP addresses ranging 211.21.40.32~211.21.40.34 have been given by ISP and assigned to port1 on FortiWAN. And their default gateway is 211.21.40.254 given by ISP as well. If there are other hosts deployed on the WAN, then configure their IP addresses in [IP(s) in WAN]. And if there are hosts deployed on the DMZ, then configure their IP addresses in [IP(s) in DMZ].



#### Basic Setting

|                                |               |
|--------------------------------|---------------|
| <b>WAN Port</b>                | Port1         |
| <b>IPv4 IP(s) on Localhost</b> | 211.21.40.32  |
| <b>IPv4 IP(s) in WAN</b>       | 211.21.40.33  |
| <b>IPv4 IP(s) in DMZ</b>       | 211.21.40.34  |
| <b>IPv4 Netmask</b>            | 255.255.255.0 |
| <b>IPv4 Gateway</b>            | 211.21.40.254 |



|                 |       |
|-----------------|-------|
| <b>DMZ Port</b> | Port5 |
|-----------------|-------|

### Static routing information

FortiWAN assumes that the near WAN and DMZ areas of a bridge-mode WAN link (both of IPv4-based and dual-stack) are parts of a large-scale network, not a complete network, with the exception of extra IPv6 subnets being available for dual-stack WAN links. Static routing information is set to FortiWAN by assigning individual IP in Basic Setting, rather than specifying a network in Basic Subnet. FortiWAN's bridge-mode accepts complete IPv6 networks to be deployed to the DMZ. In case that ISP provides multiple IPv6 subnets for a dual-stack connectivity, it is an option for you to use. Configurations of IPv6 basic subnets and IPv6 static routing subnets are so that the routing information for the FortiWAN.

### [IPv6 Basic Subnet]: Subnet in DMZ

This is the only type that FortiWAN provides for basic subnets of a bridge-mode WAN link. Click the add button on the IPv6 Basic Subnet panel to add a configuration, and select **Subnet in DMZ** from the Subnet Type drop-down menu. The rest configuration fields are as followings:

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IP(s) on Localhost</b>          | <p>The IP address(es) of the IPv6 network that you want to assign to localhost of the specified DMZ port (the DMZ port that is specified below) of the WAN link. At least one IP address is required here. You can type a range of IP addresses here in format "IPstart-IPend" or click the add button to individually add more IP addresses to the localhost.</p> <p>Note that the rest IP addresses of the network that are not assigned to the localhost here will be automatically considered as being located in DMZ area.</p> |
| <b>Prefix Length</b>               | Prefix Length of the IPv6 network that is being deployed as a subnet in DMZ and associated with the WAN link.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>DMZ Port</b>                    | A FortiWAN's network port used to connect a subnet of the WAN link with the FortiWAN as a DMZ subnet (you need to physically install the network cable to this port for the DMZ subnet). All the physical, logical and VLAN ports that are mapped to DMZ (see <a href="#">Aggregated</a> , <a href="#">Redundant</a> , <a href="#">VLAN Ports and Port Mapping</a> ) are listed here for your options.                                                                                                                              |
| <b>Enable SLAAC/DHCPv6 Service</b> | <p>Click to enable automatic addressing on the specified DMZ port for hosts in the connected IPv6 DMZ subnet (see <a href="#">Automatic addressing within a basic subnet</a> for configuration details).</p> <p>Note that only the IP addresses of the IPv6 basic subnet defined here are the candidates for related IP pools of automatic addressing.</p>                                                                                                                                                                          |

### [IPv6 Static Routing Subnet]: Subnet in DMZ

This is the only type that FortiWAN provides for static routing subnets of a bridge-mode WAN link. Click the add button on the IPv6 Static Routing Subnet panel to add a configuration, and select **Subnet in DMZ** from the Subnet Type drop-down menu. The rest configuration fields are as followings:

|                |                                                                                                                                                                                                            |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Subnet</b>  | The IPv6 static routing subnet that you want to deploy in DMZ area of the WAN link in format such as 2000::123f:0:0:1/32.                                                                                  |
| <b>Gateway</b> | IPv6 address of the gateway (router) connecting a basic subnet with the static routing subnet. This IP address is the path that FortiWAN uses to forward packets destined to the static routing subnet to. |

**See also**

- [WAN link and WAN port](#)
- [VLAN and port mapping](#)
- [Configurations for VLAN and Port Mapping](#)
- [Outbound Load Balancing and Failover \(Auto Routing\)](#)
- [Inbound Load Balancing and Failover \(Multihoming\)](#)
- [Scenarios to deploy subnets](#)
- [Public IP pass through \(DMZ Transparent Mode\)](#)
- [IPv6/IPv4 Dual Stack](#)

**Bridge-mode (one static IP) WAN link**

Configuration of a one-static-IP bridge-mode WAN link starts from selecting and enabling the WAN link on Web UI (see *Start to configure a WAN link* in [Configuring your WAN and DMZ](#)), and select Bridge Mode: One Static IP from the WAN Type drop-down menu in Basic Setting panel. After that, you start configuring the following settings:

**IPv4-based bridge-mode WAN link**

- Only **Basic setting** is necessary.
- IPv4 basic subnets and IPv4 static routing subnets are not supported here.

**IPv4/IPv6 Dual-stack bridge-mode WAN link**

- Only **Basic setting** is necessary.
- IPv4 basic subnets and IPv4 static routing subnets are not supported here; IPv6 basic subnets and IPv6 static routing subnets are optional.

Different from routing mode, configuration of static routing is contained in Basic Setting for a bridge-mode WAN link.

**Basic Setting**

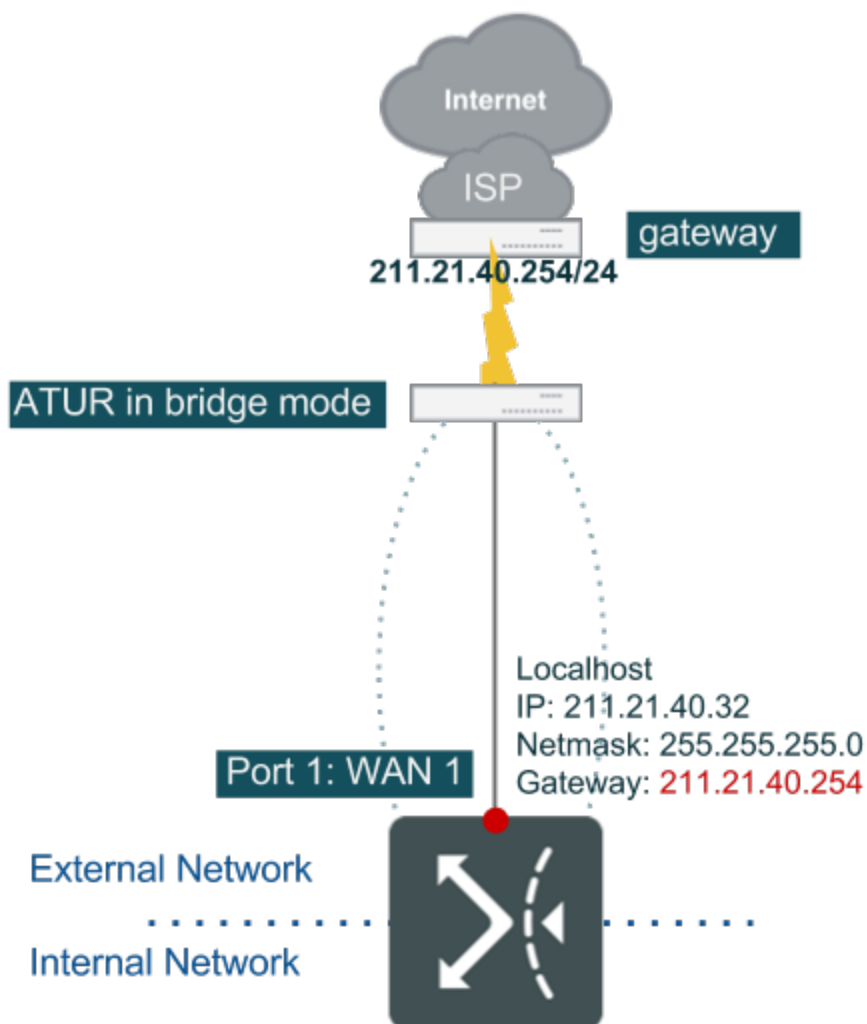
Besides the WAN Type, the rest setting fields of Basic Setting of a one-static-IP bridge-mode WAN link are as followings:

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WAN Port                 | A FortiWAN's network port used to connect the WAN link with the FortiWAN (you need to physically install the network cable to this port for the WAN link). All the physical and VLAN ports that are mapped to WAN (see <a href="#">Aggregated, Redundant, VLAN Ports and Port Mapping</a> ) are listed here for your options. The WAN link field is unrelated to the WAN port. For example, you can install WAN link 1 to WAN Port3, or WAN link 3 to WAN Port 1. (See <a href="#">WAN link and WAN port</a> ).                                                                                        |
| Up/Down Stream           | The WAN link's transfer speed at which you can download/upload data from/to the Internet. Please input the value in Kbps, e.g. 10240Kbps/640Kbps. FortiWAN Bandwidth Management's default inbound and outbound classes use the two values actively to limit the download and upload rates on the WAN link (see <a href="#">Bandwidth Management</a> ).                                                                                                                                                                                                                                                 |
| Up/Down Stream Threshold | <p>Specify upstream/downstream (Kbps) threshold to the WAN link. WAN links with traffic exceeding the thresholds will be considered as failed.</p> <p>FortiWAN's Auto Routing and Multihoming will ignore the WAN links failed by exceeding traffic while distributing traffic over WAN links, if the Threshold function is enabled in their load-balancing policies (See <a href="#">Outbound Load Balancing and Failover (Auto Routing)</a> and <a href="#">Inbound Load Balancing and Failover (Multihoming)</a>).</p> <p>Leave it blank or zero if you do not apply threshold to the WAN link.</p> |
| MTU                      | (Maximum Transmission unit) refers to the size of the largest packet or frame that a given layer of a communications protocol can pass onwards on the WAN port. It allows dividing the packet into pieces, each small enough to pass over a single link. It is set to 1500 by default.                                                                                                                                                                                                                                                                                                                 |
| IPv4 Localhost IP        | The IPv4 address that ISP provides (See " <a href="#">Scenarios to deploy subnets</a> "). IP addresses specified here can be used for NAT to transfer the source IP address of packets to, and will be used to generate the NAT default rules of the WAN link (See " <a href="#">NAT</a> ").                                                                                                                                                                                                                                                                                                           |
| IPv4 Netmask             | The IPv4 netmask that ISP provides.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| IPv4 Gateway             | The IPv4 address of the default gateway.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| IPv6 Localhost IP        | <p>The IPv6 address that ISP provides (See "<a href="#">Scenarios to deploy subnets</a>"). IP addresses specified here can be used for NAT to transfer the source IP address of packets to, and will be used to generate the NAT default rules of the WAN link.</p> <p><b>For FortiWAN V4.0.x, system does not generate NAT default rules for IPv6 WAN links, setting NAT rules manually is required</b> (See "<a href="#">NAT</a>").</p>                                                                                                                                                              |
| IPv6 Prefix              | The IPv6 prefix that ISP provides.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| IPv6 Gateway             | The IPv6 address of the default gateway.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |



Applying network settings involving changes related to MTU of a network interface will restart the interface and disrupt established connections.

[Bridge Mode: One Static IP] is used when ISP gives one static IPv4 address to a user. Usually, the IPv4 address a user obtained is one IP address of a C class IPv4 network; it is indicated by the netmask 255.255.255.0. The default gateway that ISP assigned is located at ISP's network, while the ATU-R works in bridge mode. FortiWAN's Bridge Mode: One Static IP is suggested to apply for this case. IPv6/IPv4 dual static is supported for FortiWAN's Bridge Mode: One Static IP. In the dual static similar as previous case, ISP might provide you a WAN IPv6 subnet and a LAN IPv6 subnet. You can deploy the LAN IPv6 subnet as a basic subnet in DMZ. Although the deployment is under FortiWAN's Bridge Mode, FortiWAN routes packets between WAN and DMZ for the IPv6 subnets. Basic subnets are not supported for IPv4 network deployed in Bridge Mode. The following topology is widely seen where a user gets one static IP from ISP.



**See also**

- [WAN link and WAN port](#)
- [VLAN and port mapping](#)
- [Configurations for VLAN and Port Mapping](#)
- [Outbound Load Balancing and Failover \(Auto Routing\)](#)
- [Inbound Load Balancing and Failover \(Multihoming\)](#)
- [Scenarios to deploy subnets](#)
- [IPv6/IPv4 Dual Stack](#)

**Configurations for a WAN link in Bridge Mode: PPPoE**

[Bridge Mode: PPPoE] is used for PPPoE WAN link (ISP provides dynamic or static IP addresses via PPPoE). In [Basic Settings], you shall configure upstream and downstream, user name, password and service name given by ISP. Left [IP Address] blank if you are assigned an dynamic IP address; otherwise, enter your static IP address. Select an FortiWAN WAN port to which PPPoE ADSL Modem is connected, e.g. port1. Checks [Redial Enable] to enable redial. As some ISPs automatically reconnect to the network within a certain time interval, [Redial Enable] will avoid simultaneous redialing of WAN links, which properly staggers WAN redial time. In case of connecting several DHCP/PPPoE WAN links to the same ISP, the connections might fail if they are deployed on the same physical WAN port via VLAN because the same MAC address. Via [Clone MAC Enable] you can configure MAC address clone on FortiWAN for this deployment.

**Basic Setting**

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WAN Port</b>                 | The physical port (network interface) on FortiWAN used to connect the WAN link. For the deployment of multiple WAN links on one WAN port, set this field with the same value for those WAN links. For example, select Port1 for configurations of WAN link1, WAN link2 and WAN link3 for deploying the three WAN links on WAN port1. Note: The port has to be mapped to [WAN] beforehand in [VLAN and Port Mapping] (See " <a href="#">WAN link and WAN port</a> ", " <a href="#">VLAN and port mapping</a> " and " <a href="#">Configurations for VLAN and Port Mapping</a> "). |
| <b>Up/Down Stream</b>           | The WAN link's transfer speed at which you can upload/download data to/from the Internet e.g. 512Kbps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Up/Down Stream Threshold</b> | Specify upstream/downstream (Kbps) threshold for the WAN link. WAN link with traffic that exceeds the threshold values will be considered as failed. FortiWAN's Auto Routing and Multihoming (See " <a href="#">Outbound Load Balancing and Failover (Auto Routing)</a> " and " <a href="#">Inbound Load Balancing and Failover (Multihoming)</a> ") use the value while balancing traffic between WAN links if the Threshold function is enabled. Leave it blank or zero if you do not apply threshold to the WAN link.                                                         |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MTU</b>              | (Maximum Transmission unit) refers to the size of the largest packet or frame that a given layer of a communications protocol can pass onwards. It allows dividing the packet into pieces, each small enough to pass over a single link.                                                                                                                                                                                                             |
| <b>User Name</b>        | Fill in the Username provided by ISP.                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Password</b>         | Fill in Password provided by ISP.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Service Name</b>     | Fill in service name provided by ISP. Left it blank if ISPs do not require it.                                                                                                                                                                                                                                                                                                                                                                       |
| <b>IPv4 Address</b>     | Fill in the IPv4 address provided by ISP. Left it blank if ISPs do not require it.                                                                                                                                                                                                                                                                                                                                                                   |
| <b>IPv6 Enable</b>      | Check to enable IPv6 over PPPoE.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Redial Enable</b>    | Since some ISPs tend to turn off PPPoE connection at a certain schedule, FortiWAN will automatically re-establish every disconnected PPPoE link when detected. In order to prevent simultaneous re-connection of multiple links, different re-connection schedules can be configured for different WAN links to avoid conjunction. After reconnection schedule is configured (HH:MM), the system will perform PPPoE reconnection as scheduled daily. |
| <b>Clone MAC Enable</b> | Configure MAC address clone.                                                                                                                                                                                                                                                                                                                                                                                                                         |



Applying network settings will restart a network interface if this interface is using PPPoE or DHCP and disrupt established connections.

#### See also

- [WAN link and WAN port](#)
- [VLAN and port mapping](#)
- [Configurations for VLAN and Port Mapping](#)
- [Outbound Load Balancing and Failover \(Auto Routing\)](#)
- [Inbound Load Balancing and Failover \(Multihoming\)](#)

### Configurations for a WAN link in Bridge Mode: DHCP

[Bridge Mode: DHCP Client] is used when FortiWAN WAN port gets a dynamic IP address from DHCP host. IPv6 is not supported in this WAN type.

## Basic Setting

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WAN Port</b>                 | The physical port (network interface) on FortiWAN used to connect the WAN link. For the deployment of multiple WAN links on one WAN port, set this field with the same value for those WAN links. For example, select Port1 for configurations of WAN link1, WAN link2 and WAN link3 for deploying the three WAN links on WAN port1. Note: The port has to be mapped to [WAN] beforehand in [VLAN and Port Mapping]. (See " <a href="#">WAN link and WAN port</a> ", " <a href="#">VLAN and port mapping</a> " and " <a href="#">Configurations for VLAN and Port Mapping</a> ") |
| <b>Up/Down Stream</b>           | The WAN link's transfer speed at which you can upload/download data to/from the Internet e.g. 512Kbps                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Up/Down Stream Threshold</b> | Specify upstream/downstream (Kbps) threshold for the WAN link. WAN link with traffic that exceeds the threshold values will be considered as failed. FortiWAN's Auto Routing and Multihoming (See " <a href="#">Outbound Load Balancing and Failover (Auto Routing)</a> " and " <a href="#">Inbound Load Balancing and Failover (Multihoming)</a> ") use the value while balancing traffic between WAN links if the Threshold function is enabled. Leave it blank or zero if you do not apply threshold to the WAN link.                                                         |
| <b>MTU</b>                      | (Maximum Transmission unit) refers to the size of the largest packet or frame that a given layer of a communications protocol can pass onwards. It allows dividing the packet into pieces, each small enough to pass over a single link.                                                                                                                                                                                                                                                                                                                                         |
| <b>Clone MAC Enable</b>         | Configure MAC address clone.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



Applying network settings will restart a network interface if this interface is using PPPoE or DHCP and disrupt established connections.

### See also

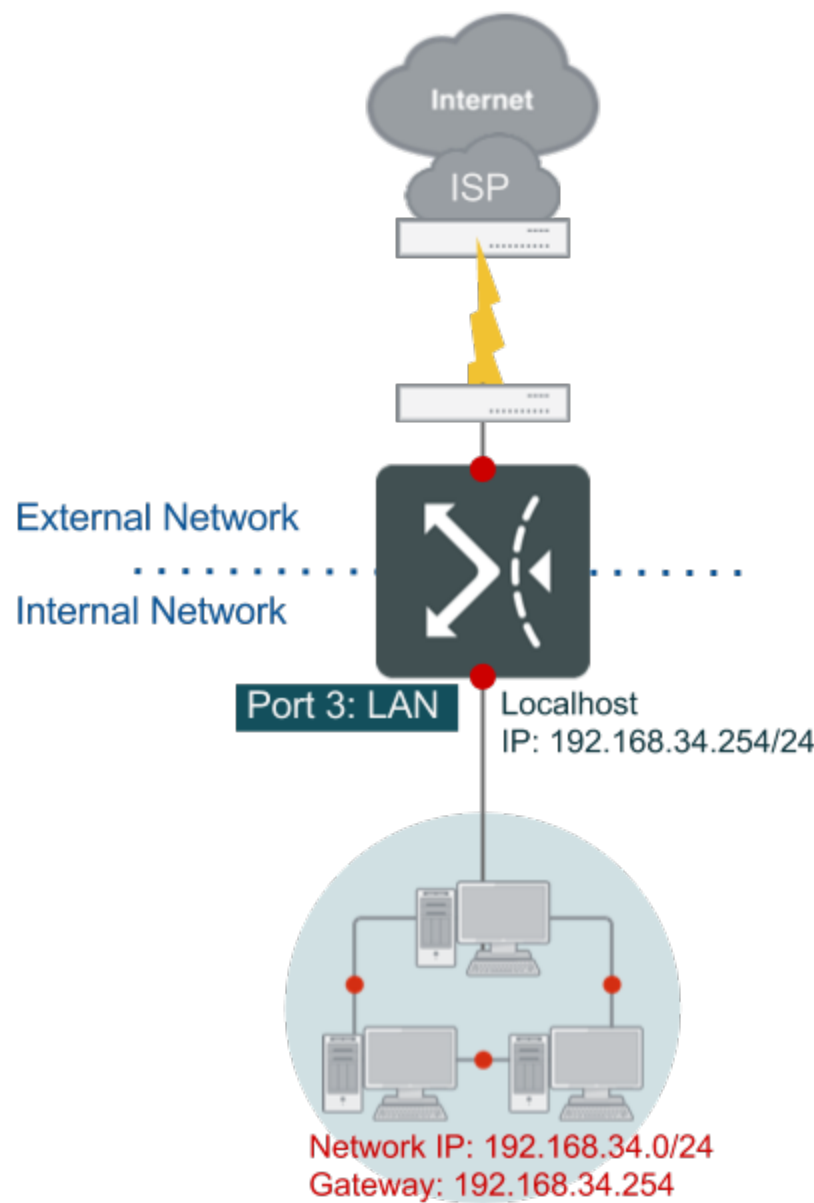
- [WAN link and WAN port](#)
- [VLAN and port mapping](#)
- [Configurations for VLAN and Port Mapping](#)
- [Outbound Load Balancing and Failover \(Auto Routing\)](#)
- [Inbound Load Balancing and Failover \(Multihoming\)](#)

## LAN Private Subnet

[LAN Private Subnet] is the second most important part for deploying FortiWAN in your network. In contrast with configurations on WAN Settings to active the WAN link transmission from FortiWAN to Internet (external network), LAN Private Subnet is the configuration for deploying the internal network on FortiWAN's LAN ports. There are two parts for setting LAN private subnet: **Basic Subnet** and **Static Routing Subnet**, which respectively are the subnets connected directly to FortiWAN's LAN ports and the subnets connected indirectly to FortiWAN via a router. (See "[Scenarios to deploy subnets](#)")

Basic Subnet

Here is a simple example to demonstrate a configuration for the basic subnet in the typical LAN environment.



As the illustration, FortiWAN port3 has been mapped to LAN port via [System / Network Setting / VLAN and Port Mapping] (See "[VLAN and Port Mapping](#)"), and is assigned with private IP 192.168.34.254. Enter this IP address in the field [IP(s) on Localhost]. For hosts in LAN, port3 (192.168.34.254) serves as gateway as well. Enter the netmask (255.255.255.0) for the subnet in the field [Netmask]. Select the LAN port.

| IPv4 Basic Subnet  |                |
|--------------------|----------------|
| IP(s) on Localhost | 192.168.34.254 |



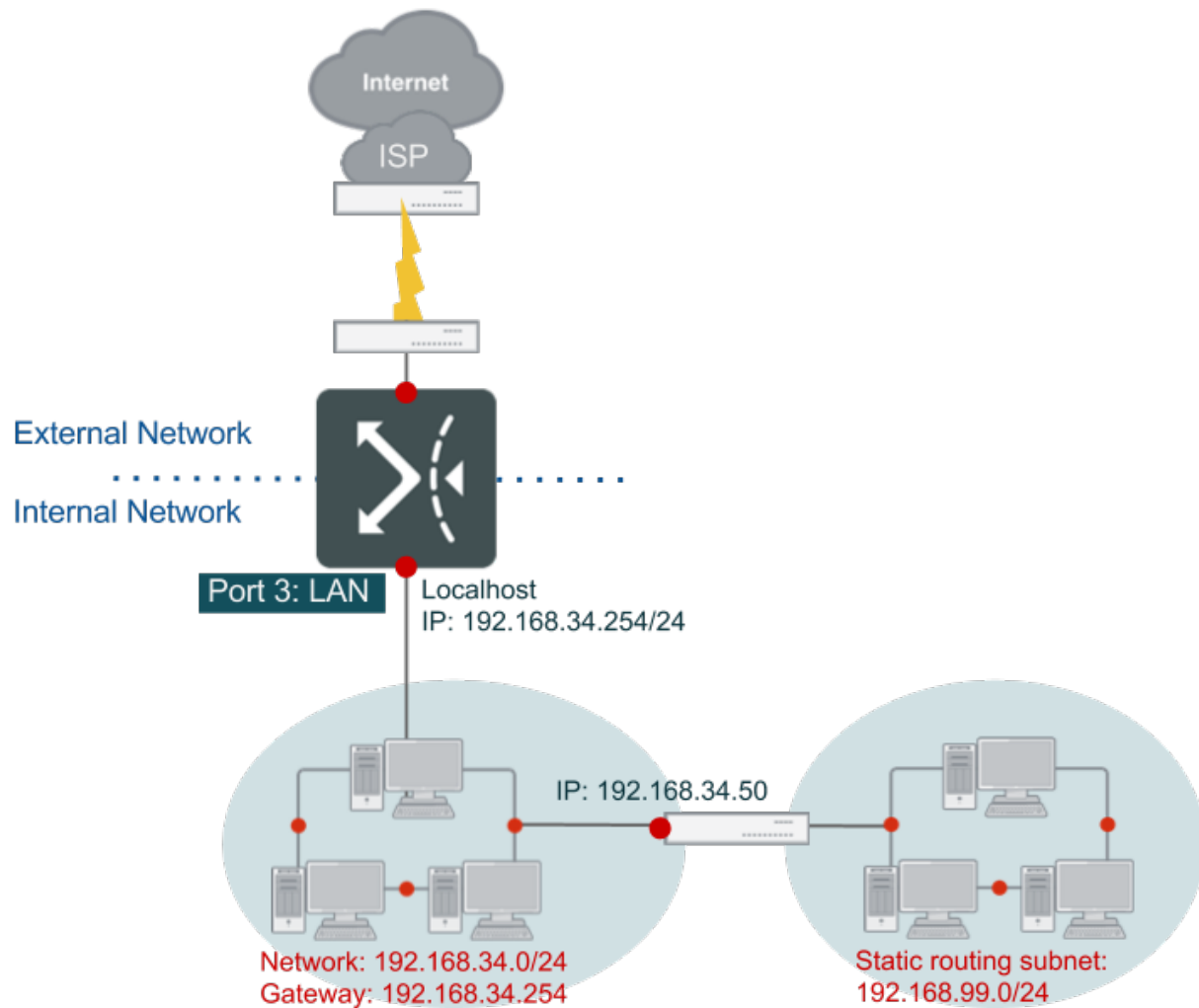
|                 |               |
|-----------------|---------------|
| <b>Netmask</b>  | 255.255.255.0 |
| <b>LAN Port</b> | Port3         |

Check the field in [Enable DHCP], to allocate IP address (any of 192.168.34.175~192.168.34.199) dynamically via DHCP to PCs in LAN. If any host in LAN requires static IP addresses, then enter in [Static Mapping] the IP addresses to designate, and MAC addresses of the PCs as well. Check the field in [NAT Subnet for VS], which is an optional choice. When users in LAN or DMZ access the WAN IP of virtual server, their packets may bypass FortiWAN and flow to internal server directly. This function can translate the source IP address of the users' packets into IP address of FortiWAN, to ensure the packets flow through FortiWAN. If no check is made, the system will determine which IP address it may translate into by itself. Similarly, to deploy an IPv6 private LAN on FortiWAN port4 which has been mapped to LAN port, with IPv6 address 2001:a:b:cd08::1 served as gateway for PCs in LAN. Check the field in [Enable SLAAC] or [Enable DHCPv6 Service] to allocate IP addresses dynamically to PCs in LAN. [NAT Subnet for VS] is not supported in IPv6 private LAN. The SLAAC and DHCPv6 in FortiWAN are designed to work together, which the SLAAC responses router advertisement (including default gateway and DNS server) to a host and DHCPv6 responses the host an appropriate IPv6 address.

For the details about DHCP, DHCP Relay, SLAAC and DHCPv6, see "[Automatic addressing within a basic subnet](#)".

## Static Routing Subnet

[Static Routing Subnet] is useful when in LAN a router is used to cut out a separate subnet which does not connect to FortiWAN directly. The topology is similar to [Static Routing Subnet: Subnet in DMZ] mentioned previously, and the only difference is this example is set in LAN rather than in DMZ. In this topology below, a subnet 192.168.99.x is located in the LAN and connects to router 192.168.34.50, while another subnet 192.168.34.x is located on the LAN port as well, but connects to FortiWAN directly. The configurations here indicate how FortiWAN to route packets to subnet 192.168.99.x.



#### IPv4 Static Routing Subnet

|                   |               |
|-------------------|---------------|
| <b>Network IP</b> | 192.168.99.0  |
| <b>Netmask</b>    | 255.255.255.0 |
| <b>Gateway</b>    | 192.168.34.50 |

## RIP

FortiWAN supports the Routing Information Protocol (RIP v1, v2), RIP employs hop count as the metric, and uses timer broadcast to update the router. As RIP features configuration simplicity and operation convenience, it has been widely used across all fields. RIP version 1 (v1) was designed to suit the dynamic routing needs of LAN technology-based IP internetworks, and to address some problems associated with RIP v1, a refined RIP, RIP version 2 (v2) was defined. RIP v2 supports sending RIP announcements to the IP multicast address and supports the use of authentication mechanisms to verify the origin of incoming RIP announcements.

Check the field in [RIP] if you have enabled RIP on your private subnet router. Check the field in [RIP v1] if you have enabled RIP v1 on your private subnet router behind FortiWAN. Thus, FortiWAN can forward packets from

the RIP v1-enabled private subnet. Otherwise, check the field in [RIP v2] if you have enabled RIP v2 on your private subnet router. Thus, FortiWAN can forward RIP v2 packets. Moreover, if you have enabled RIP v2 authentication, type the password in [Password]. Otherwise, keep [Password] blank.

## OSPF

Apart from RIP, FortiWAN also supports OSPF (Open Shortest Path First), to assign LAN port router with given preference. Like RIP, OSPF is designated by the Internet Engineering Task Force (IETF) as one of several Interior Gateway Protocols (IGPs). Rather than simply counting the number of hops, OSPF bases its path descriptions on "link states" that take into account additional network information. Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network so that all will have the same routing table information.

|                               |                                                                                                                                                                            |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>OSPF Interface</b>         | Displays the LAN port in the network. Check the box to enable OSPF over the port.                                                                                          |
| <b>Area Setting</b>           | Network is logically divided into a number of areas based on subnets. Administrators can configure area ID, which accepts numbers or IPs only.                             |
| <b>Authentication Setting</b> | Routers in different areas require authentication to communicate with each other. Authentication types: Null, Simple Text Password, MD5.                                   |
| <b>Router Priority</b>        | Set router priority. Router that sends the highest OSPF priority becomes DR (Designated Router). The value of the OSPF Router Priority can be a number between 0 and 255.  |
| <b>Hello Interval</b>         | Set the interval, in seconds, to instruct the router to send out OSPF keepalive packets to inform the other routers.                                                       |
| <b>Dead Interval</b>          | Set the length of time, in seconds, that OSPF neighbors will wait without receiving an OSPF keepalive packet from a neighbor before declaring the neighbor router is down. |
| <b>Retransmit Interval</b>    | Set the interval, in seconds, between retransmissions of Link ups. When routers fail to transmit hello packets, it will retransmit packets in the defined interval.        |
| <b>Authentication Type</b>    | This specifies whether the router will perform authentication of data passing the LAN. Choices are: Null, Simple Text Password, MD5.                                       |

FortiWAN provides statistics for the RIP & OSPF service, see "[RIP & OSPF Status](#)".

## VRRP

VRRP is a Virtual Router Redundancy Protocol that runs on a LAN port. A system can switch between VRRP or HA mode; when switched, the system will reboot first for changes to take effect. When VRRP mode is enabled, the HA mode will be automatically disabled, and also a VRID field will appear available for input in [VLAN and Port Mapping] setting page (See "[VLAN and Port Mapping](#)"). In general, VRRP is faster in detecting the master unit compared to HA mode. Although FortiWAN's VRRP implementation is based on VRRP version 3, some restrictions may apply:

- Always in non-preempt mode.
- Always in non-accept mode.

- IPv6 is not supported.
- Active-active mode is not supported.

When FortiWAN switches to master mode, it automatically starts WAN link health detection. When it switches to backup mode, it automatically stops WAN link health detection and sets WAN status to "failed".

In addition, DHCP servers in LAN and DMZ should let clients use FortiWAN virtual IP and the default gateway (as FortiWAN's DHCP service does). If RIP and OSPF is used in LAN, FortiWAN uses real IP at OSPF and virtual IP at RIP to exchange route information. Clone-MAC settings will be ignored if VRRP function is enabled. FortiWAN doesn't exchange NAT table with VRRP peers. When VRRP master changes, existing connection might break.

|                               |                                                                                                                                                   |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Local Priority</b>         | The priority field specifies the sending VRRP router's priority for the virtual router. Select a number from 1 to 254 as the priority for the VR. |
| <b>Advertisement Interval</b> | Set the time interval in centi-seconds between advertisements. (Default is 100)                                                                   |
| <b>Virtual address</b>        | Enter a virtual IP address for the virtual router.                                                                                                |
| <b>Double-check Link</b>      | Click the checkbox to enable. When enabled, the backup router will check whether the master is responding ARP on the specified WAN port.          |

#### See also

- [Scenarios to deploy subnets](#)
- [VLAN and Port Mapping](#)
- [Summary](#)
- [RIP & OSPF Status](#)

## WAN/DMZ Private Subnet

After having gone through public subnet configurations, let's move to private subnet settings. This section lists a few typical topology structures for private subnet. Similarly, FortiWAN supports two different types of private subnet according to the deployment, direct or indirect connecting to FortiWAN. The two settings are configured from [Basic Subnet] and [Static Routing Subnet]. FortiWAN supports both IPv4 and IPv6 for the two private subnet types.

On its UI, [IPv4 Basic Subnet] and [IPv6 Basic Subnet] could be one of:

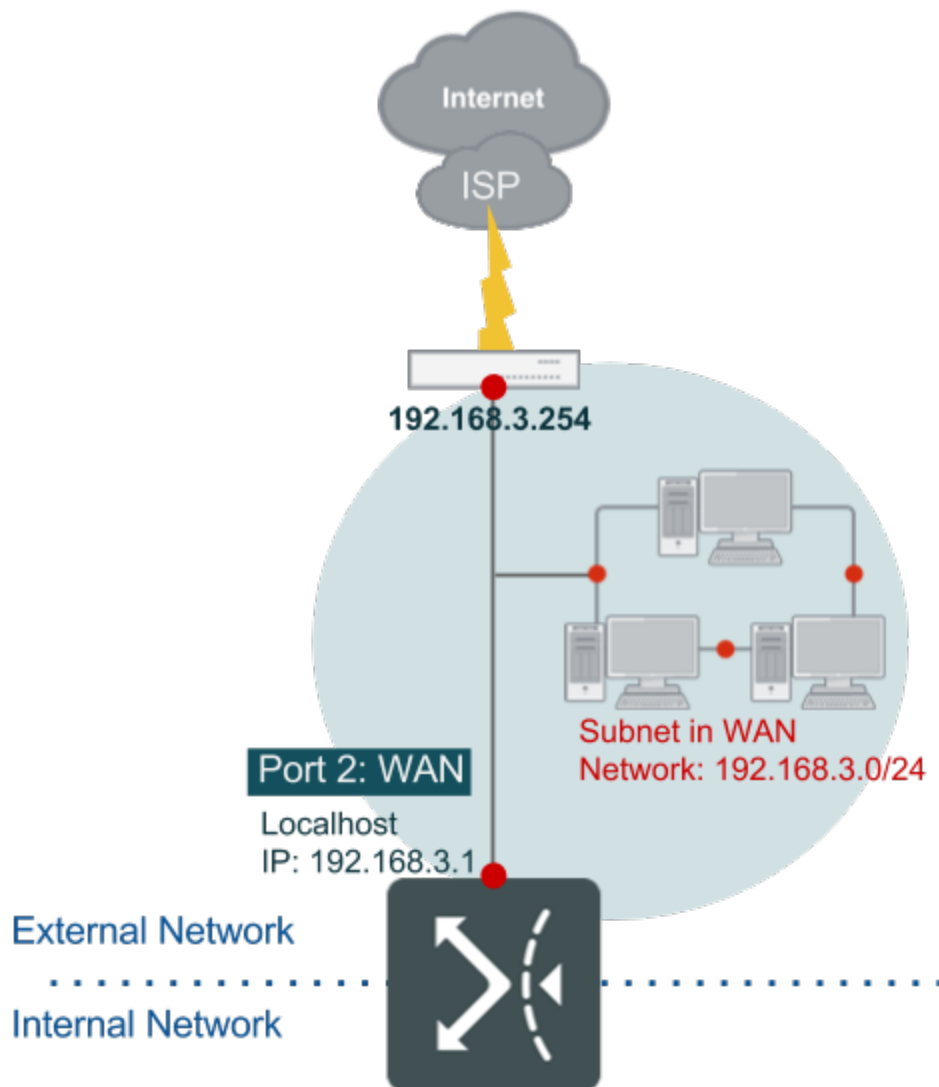
- Subnet in WAN
- Subnet in DMZ
- Subnet in WAN and DMZ
- Subnet on Localhost (Not support in [IPv6 Basic Subnet])

And [IPv4 Static Routing Subnet] and [IPv6 Static Routing Subnet] could be one of:

- Subnet in WAN
- Subnet in DMZ

**[Basic Subnet]: Subnet in WAN**

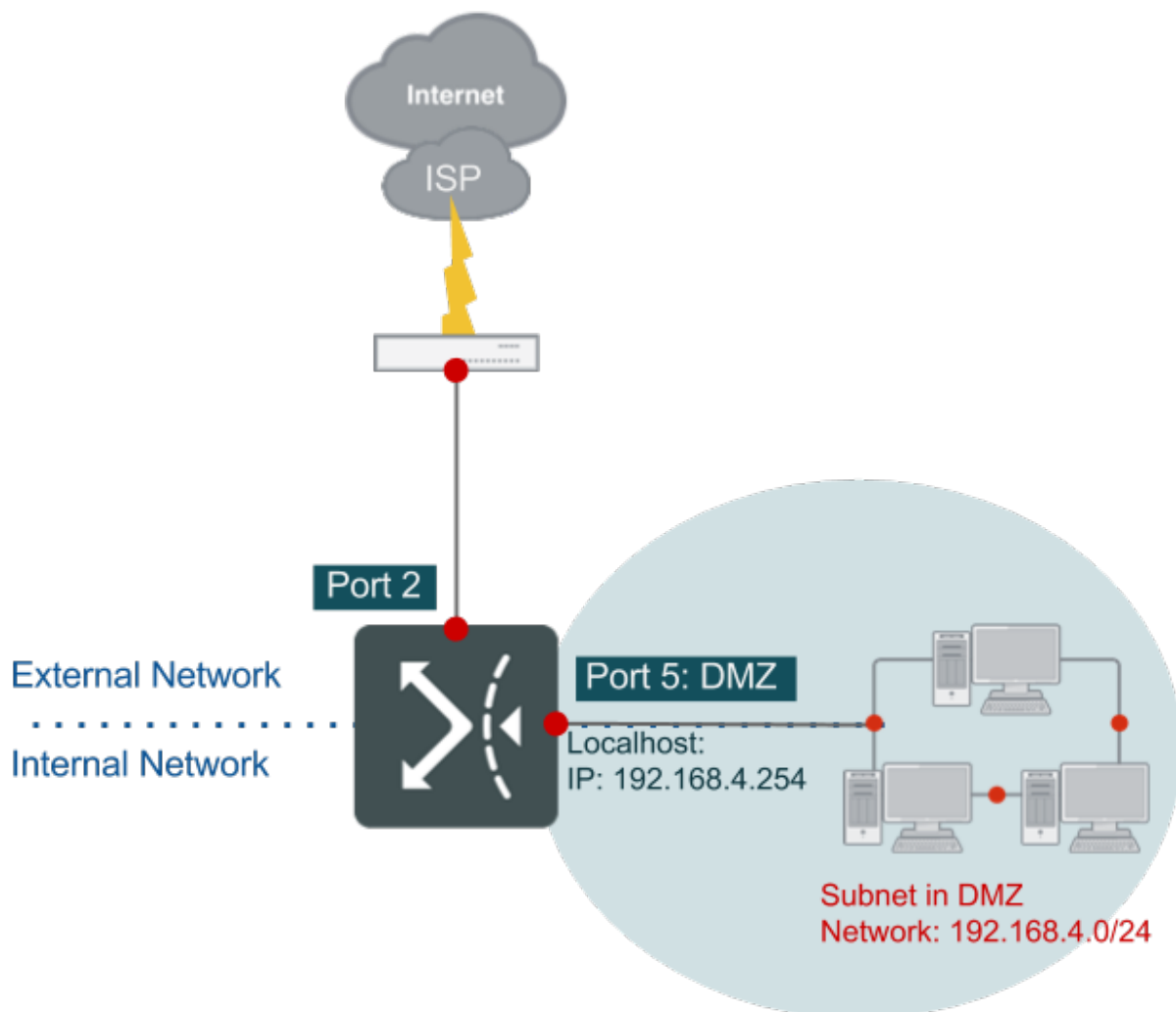
This topology is frequently found where cluster hosts in the IPv4 private subnet are located on the WAN. In this example, FortiWAN port2 has been mapped to WAN port, with IP 192.168.3.1. Select [Subnet in WAN] from [Subnet Type] in [Basic Subnet]. Then enter 192.168.3.1 in [IP(s) on Localhost] and the netmask offered by ISP in [Netmask].



Note: FortiWAN assumes that IP addresses that are unlisted in [IP(s) on Localhost] are all in WAN.

**[Basic Subnet]: Subnet in DMZ**

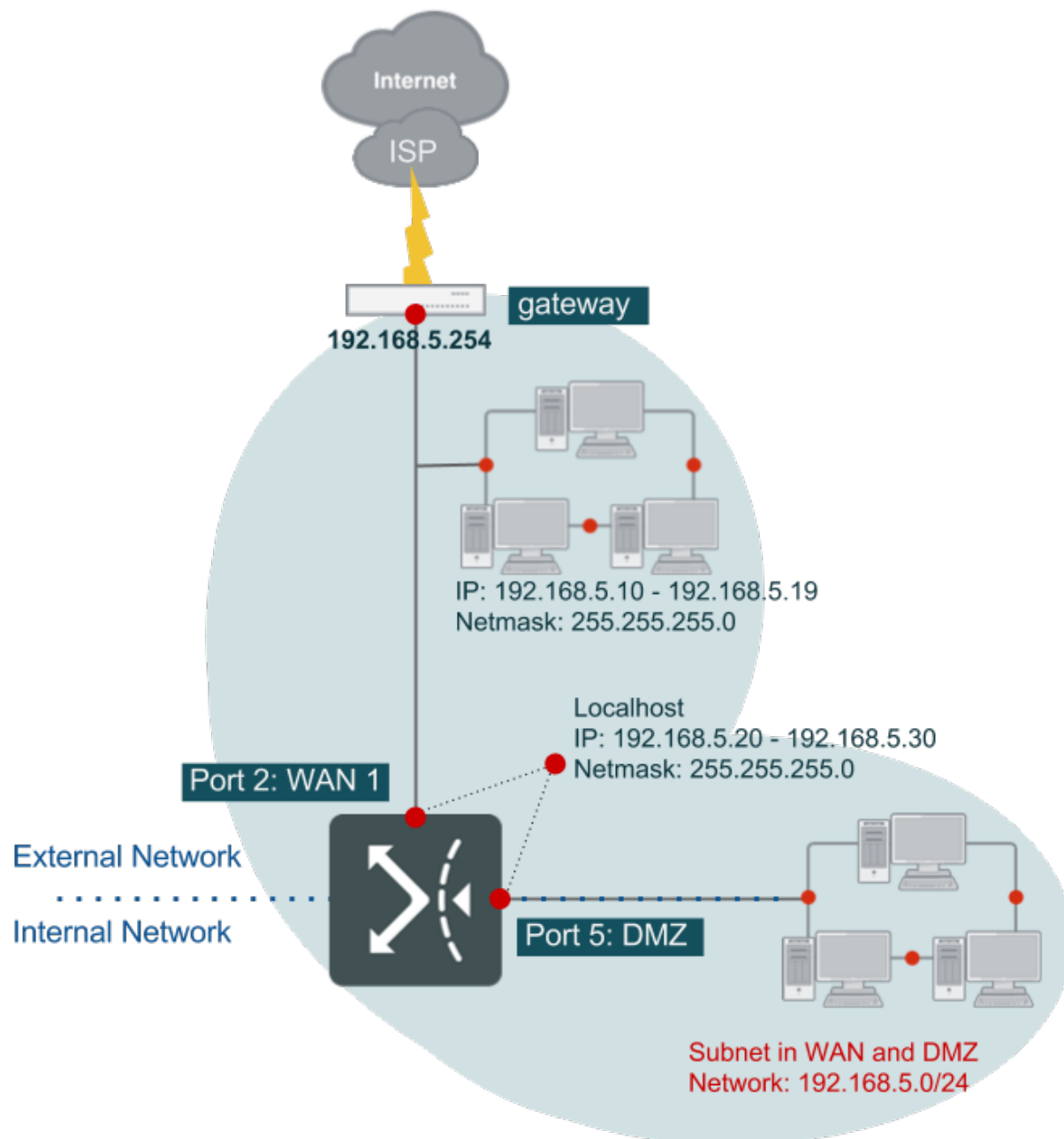
This topology is frequently found where cluster hosts in IPv4 private subnet are located on the DMZ. In this example, FortiWAN port5 has been mapped to DMZ port, with private IP 192.168.4.254. And subnet 192.168.4.X is located on the DMZ as a whole. From UI, select [Subnet in DMZ] from [Subnet Type] in [Basic Subnet].



Check [Enable DHCP] if hosts in the subnet in DMZ require DHCP service. And enter the starting and ending address in [DHCP Range]. If any host in the subnet uses static IP address, then in [Static Mapping], enter its IP and MAC address. Note: FortiWAN assumes IP addresses that are unlisted in [IP(s) on Localhost] are all in DMZ. Thus there is no need to configure them.

#### [Basic Subnet]: Subnet in WAN and DMZ

This topology is found where cluster hosts in IPv4 private subnet are located in both WAN and DMZ. FortiWAN hereby assumes IP addresses that are unlisted in [IP(s) on Localhost] and [IP(s) in WAN] are all in the DMZ. Port2 and port5 are connected in dotted line, indicating the subnet spreads across WAN (port2) and DMZ (port5). FortiWAN employs Proxy ARP to connect the whole subnet together. In this example, more than one IP addresses are needed for FortiWAN in bridging. These IP addresses therefore have to be on the same network segment. Enter 192.168.5.20-192.168.5.30 in [IP(s) on Localhost], and 192.168.5.10-192.168.5.19 in [IP(s) in WAN].

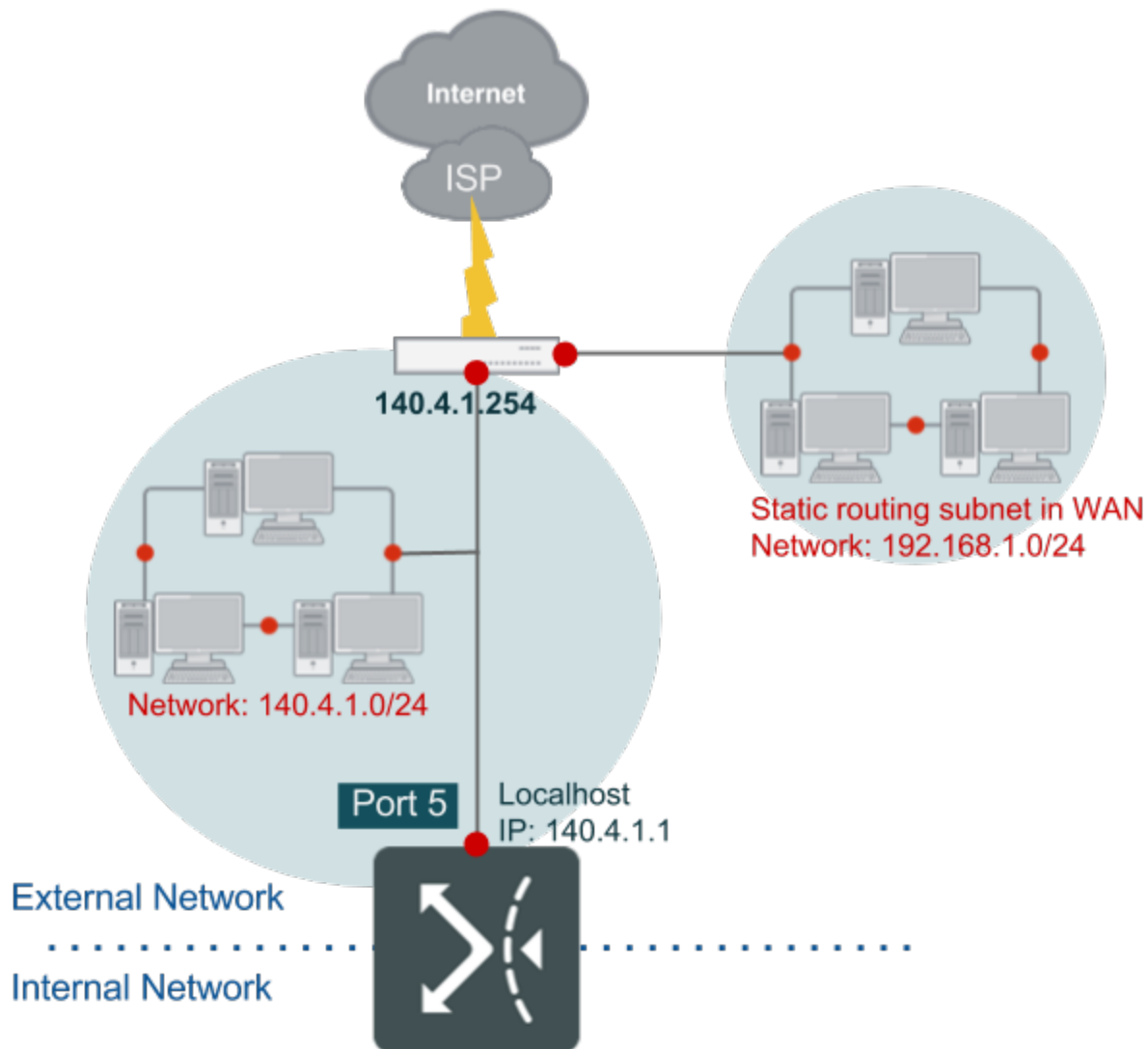


### [Basic Subnet]: Subnet on Localhost

This topology is found where a whole IPv4 private subnet is designated on FortiWAN. And the IP addresses in this subnet can be utilized by Virtual Server. An IPv6 private subnet is not supported for this subnet type.

### [Static Routing Subnet]: Subnet in WAN

This topology is found where IPv4 private static routing subnet is located on the WAN. In other words, the private subnet on the WAN does not connect to FortiWAN directly. Instead, it connects to a router which helps to transfer its packets.

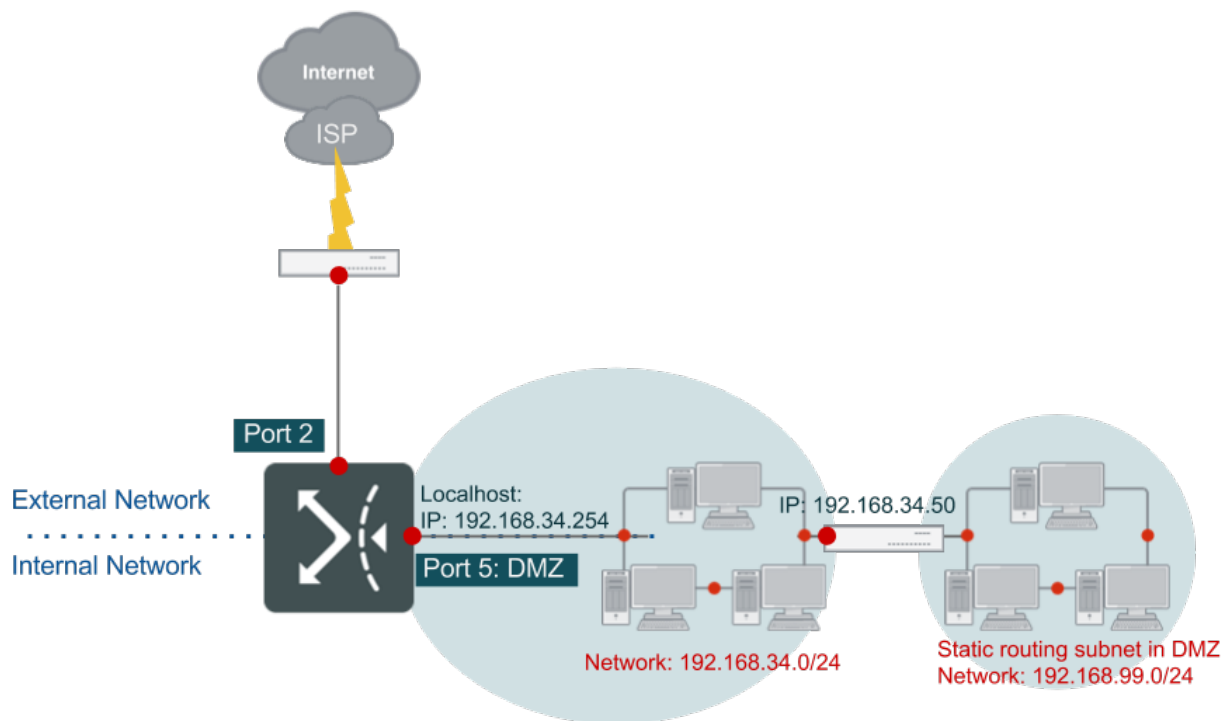


Hence, in [Static Routing Subnet], [Gateway] IP address is that of the router.

### [Static Routing Subnet]: Subnet in DMZ

In this topology, in DMZ you create an IPv4 private subnet using one router (its IP, say, 192.168.34.50). But the subnet (its IP 192.168.99.0/24) does not connect to FortiWAN directly. Configure the subnet on FortiWAN to process its packets.





## Automatic addressing within a basic subnet

FortiWAN functions for various network topologies which consists of connectivity of multiple subnets (basic subnet). Deployments of basic subnets varies for purposes, but they can be simply divided, according to the location, into three basic types: WAN-sided subnet, DMZ-sided subnet and LAN-sided subnet, which are supposed to connect to the WAN port, DMZ port and LAN port of FortiWAN. FortiWAN so that services the hosts in the subnets. For this reason, mechanisms to automatically address the hosts in those basic subnets are provided. FortiWAN's automatic addressing is designed to serve the hosts in DMZ-sided and LAN-sided subnets. Hosts in WAN-sided subnets can only be addressed manually. DMZ-sided subnets are divided further into Subnet-in-DMZ, and Subnet-in-WAN-and-DMZ. FortiWAN's automatic addressing is designed according to IPv4 network and IPv6 network, which is described as follows:

### IPv4 Automatic addressing

FortiWAN provides standard **DHCP** and **DHCP Relay** to allocate IPv4 addresses to or relay DHCP messages for hosts in the following subnets or IP range:

|                 |                                                                                                                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DMZ Side</b> | <ul style="list-style-type: none"> <li>• Routing Mode, IPv4 Basic Subnet: Subnet in DMZ</li> <li>• Routing Mode, IPv4 Basic Subnet: Subnet in WAN and DMZ</li> <li>• Bridge Mode: Multiple Static IP, IPv4 IP(s) in DMZ</li> </ul> |
| <b>LAN Side</b> | <ul style="list-style-type: none"> <li>• LAN Private Subnet</li> </ul>                                                                                                                                                             |

## DHCP

FortiWAN acts a DHCP server on the specified LAN port or DMZ port if checkbox **Enable DHCP** is checked. FortiWAN receives DHCP requests and responds related information from/to hosts (DHCP clients) in the subnets connect to the LAN or DMZ ports.

### Domain Name Server

The DNS that FortiWAN responds to the DHCP clients within the DHCP OFFER messages if the clients are sat to automatically get DNS information through DHCP.

- **Single DNS server:** the DNS servers defined in **System > Network Setting > DNS Server > IPv4 Domain Name Server** are listed here for your options.
- **ALL:** answer the DHCP clients with all the defined DNS servers information.
- **None:** answer the DHCP clients without containing any DNS server information.

This option is only available for LAN private subnet. For the DMZ-sided subnets (hosts in the two subnets are supposed to be deployed with public IP addresses), system behaves answering the DHCP clients with all the defined DNZ servers information.

### Domain Name Suffix

The domain name suffix that FortiWAN responds to the DHCP clients within the DHCP OFFER messages if the clients are sat to automatically get DNS information from DHCP.

- **Single domain name suffix:** the domain name suffixes defined in **System > Network Setting > DNS Server > Domain Name Suffix** are listed here for your options.
- **ALL:** answer the DHCP clients with all the defined domain name suffixes.
- **None:** answer the DHCP clients without containing any domain name suffixes.

This option is only available for LAN private subnet.

**TFTP Server Name**

This option is used to deliver a TFTP server name to DHCP clients. When the DHCP server see the request in a DHCP discover from a DHCP client, it returns the TFTP server name in its DHCP offer to the client as DHCP option 66. Usually, option 66 is used for IP phone auto-provisioning. You will need to refer to a vender's documentation to configure this option.

Specify the IP address or the hostname of a TFTP server directly here according to what the device vender provides. FortiWAN DHCP will directly return what is specified here to requests without any encoding/decoding. The DHCP server will ignore the request for option 66 from a DHCP client if this field is leaved blank. Note that FortiWAN does not support DHCP option 67 (Bootfile Name) and option 150 (TFTP Server Address).

**Vendor Encapsulated Options**

This option is used to transmit Vender Specific Information between the DHCP server and clients. Usually, the information could be the configuration data to the DHCP clients. For example an IP address of a WLAN controller or a DLS (Deployment Service) server, or an identifier if the DHCP clients are wireless APs, IP phones or other devices. When the DHCP server see the request in a DHCP discover (option 43 or number 43 included in option 55) from a DHCP client, it returns the vender specific information in its DHCP offer to the client as DHCP option 43.

The vender encapsulated option ca contain either a single vender-specific value or multiple vender-specific sub-options. The RFC allows a vender to define its own sub-option codes. All the sub-options are included in the DHCP offer as Type-Length-Value blocks embedded within the option 43. You will need to refer to a vender's documentation to form the options to their specification.

Specify the information directly here in hexadecimal numbering format according to what the device vender provides. FortiWAN DHCP will directly return what is specified here to requests without any encoding/decoding. The DHCP server will ignore the request for option 43 from a DHCP client if this field is leaved blank. Note that FortiWAN does not support DHCP option 60 (Vender Class Identifier), DHCP server will not return option 43 based on option 60.

**DHCP Range**

The address pools that DHCP server assigns and manages IP addresses from. Define the IP ranges by specifying IPv4 Starting Address and IPv4 Ending Address.

**Static Mapping**

DHCP server assigns and manages IP addresses according to clients' MAC addresses. An IP address that is mapped to a MAC address is only available to the client with the MAC address. It will not be assigned to other client even it is idle. Define the mapping by specifying MAC Address and the correspondent IPv4 Address.

**Client ID Mapping**

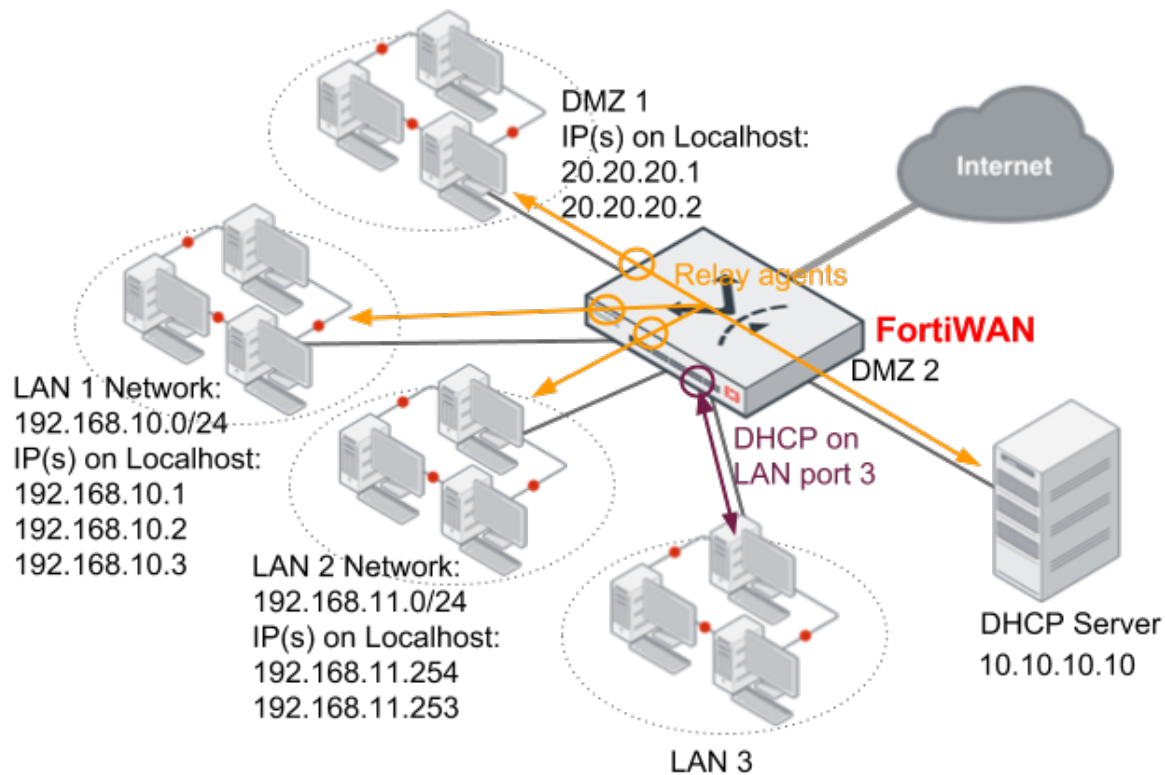
DHCP server assigns and manages IP addresses according to the client ID of DHCP client (the Client Identifier, options code 61, in the options field of DHCP request). An IP address that is mapped to a client ID here is only available to this client. It will not be assigned to other clients even it is idle. Define the mapping by specifying Client ID and the correspondent IPv4 Address. Corresponding setting of client ID on a DHCP client is required.

Note that IP addresses defined in **DHCP Range**, **Static Mapping** or **Client ID Mapping** must be also defined in filed **IPv4 IP(s) in DMZ** for a **bridge-mode (multiple static IP) WAN link**, the **DMZ side** of basic subnets (subnet in WAN and DMZ, and subnet in DMZ) for a **routing-mode WAN link** and the basic subnets of private LAN subnets.

**DHCP Relay**

DHCP relay is a proxy forwarding DHCP requests and responses between hosts and DHCP server across different subnets. A router called DHCP relay agent acts the proxy receiving DHCP requests from hosts in the same subnet and resending them to the DHCP server located in another subnet. The DHCP relay agent then delivers the DHCP messages responded by the DHCP server to the hosts in the subnet, so that the hosts are assigned the IP addresses and related information.

FortiWAN is the DHCP relay agent in the network once the DHCP Relay function is enable. Address allocation for multiple subnets (subnet in LAN, subnet in DMZ, subnet in WAN and DMZ and IPs in DMZ) can be managed by a centralized DHCP server. As the example below, FortiWAN relays the DHCP messages between the connected subnets and the standalone DHCP server, so that one DHCP server manages the address allocation for the three subnets, LAN 1, LAN 2 and a DMZ 1. As for subnet LAN 3, it employs FortiWAN's DHCP server on LAN port 3. The enabled DHCP server on LAN port 3, which is independent from the standalone DHCP server, serves only subent LAN 3. Note that you can only enable either DHCP or DHCP Relay for a subnet.



To implement the deployment, you need to enable DHCP Relay for each of the subnets (enable DHCP Relay on each of the ports). In the example above, DHCP Relay is enabled on ports of LAN 1, LAN 2 and subnet in DMZ 1, and all the DHCP requests received on the ports will be forwarded to the DHCP server in the subnet DMZ 2. A LAN port or DMZ port with DHCP Relay being enabled on will forward the DHCP requests it received (coming from the subnet it connects to) to the DHCP server.

FortiWAN supports up to two DHCP servers in a DHCP relay deployment. Once two DHCP servers are configured, the relay agent will forward a DHCP request to both of the DHCP servers. The first response received by the relay agent will be first apply to the DHCP client, and the subsequent responses will be ignored then.

|                            |                                                                                                                                    |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>DHCP Relay Server 1</b> | IP address of the first standalone DHCP server.                                                                                    |
| <b>DHCP Relay Server 2</b> | IP address of the second standalone DHCP server. Leave it blank if only one DHCP server is required for the DHCP relay deployment. |

**DHCP Relay Agent IP**

The IP address of the DHCP Relay agent on the port. It indicates the source of a relayed DHCP request to the DHCP server. This IP will be contained in a relayed DHCP message, so that the DHCP server could recognize the relay agent that the relayed DHCP request came from and respond the corresponding IP address to the DHCP client (according to this DHCP Relay Agent IP and the addressing policy).

The DHCP Relay Agent IP must be an IP address deployed on the localhost of the LAN port or DMZ port. You might deploy multiple IP addresses to a LAN port or a DMZ port (the field **IP(s) on Localhost** of a LAN subnet, a subnet in DMZ or a subnet in WAN and DMZ), then any of them could be took as the DHCP Relay Agent IP.

Next are the configurations of DHCP Relay on the LAN 1, LAN 2 and DMZ ports in the example above.

**LAN 1 subnet**

From the example above, we have configured the localhost of LAN 2 port with three IP addresses 192.168.10.1, 192.168.10.2 and 192.168.10.3 for subnet 192.168.10.0/24. To enable DHCP Relay on this port, you need to check the check-box "Enable DHCP Relay" on the Web UI and configure the settings as follows:

|                            |                                            |
|----------------------------|--------------------------------------------|
| <b>DHCP Relay Server 1</b> | 10.10.10.10                                |
| <b>DHCP Relay Agent IP</b> | 192.168.10.1, 192.168.10.2 or 192.168.10.3 |

The DHCP server (10.10.10.10) recognizes the relay agent (the LAN 1 port) that relayed the DHCP message through the "DHCP Relay Agent IP" contained in the relayed message. Then according to the DHCP addressing policy, it selects an IP belongs to 192.168.10.x from its IP pool and responds to the relay agent on LAN 1 port.

**LAN 2 subnet**

From the example above, we have configured the localhost of LAN 1 port with three IP addresses 192.168.11.254 and 192.168.11.253 for subnet 192.168.11.0/24. To enable DHCP Relay on this port, you need to check the check-box "Enable DHCP Relay" on the Web UI and configure the settings as follows:

|                            |                                  |
|----------------------------|----------------------------------|
| <b>DHCP Relay Server 1</b> | 10.10.10.10                      |
| <b>DHCP Relay Agent IP</b> | 192.168.11.254 or 192.168.11.253 |

The DHCP server (10.10.10.10) recognizes the relay agent (the LAN 2 port) that relayed the DHCP message through the "DHCP Relay Agent IP" contained in the relayed message. Then according to the DHCP addressing policy, it selects an IP belongs to subnet 192.168.11.x from its IP pool and responds to the relay agent on LAN 2 port.

## DMZ 1

As the previous description, DHCP relay agent enabled on a DMZ port forwards the DHCP messages between DMZ and a DHCP server. In FortiWAN, a DMZ can be deployed according the following WAN types:

- **Routing Mode - IPv4 Basic Subnet:** Subnet in DMZ
- **Routing Mode - IPv4 Basic Subnet:** Subnet in WAN and DMZ
- **Bridge Mode - Multiple Static IP:** IPv4 IP(s) in DMZ

No matter which WAN type a DMZ is deployed, it is necessary to configure the "IP(s) on Localhost" field to the DMZ port via Web UI. From the example above, we have configured the localhost of DMZ 1 port with three IP addresses 20.20.20.1 and 20.20.20.2. To enable DHCP Relay on this port, you need to check the check-box "Enable DHCP Relay" on the Web UI and configure the settings as follows:

|                            |                          |
|----------------------------|--------------------------|
| <b>DHCP Relay Server 1</b> | 10.10.10.10              |
| <b>DHCP Relay Agent IP</b> | 20.20.20.1 or 20.20.20.2 |

The DHCP server (10.10.10.10) recognizes the relay agent (the DMZ 1 port) that relayed the DHCP message through the "DHCP Relay Agent IP" contained in the relayed message. Then according to the DHCP addressing policy, it selects an IP belongs to subnet 20.20.20.x from its IP pool and responds to the relay agent on DMZ 1 port.

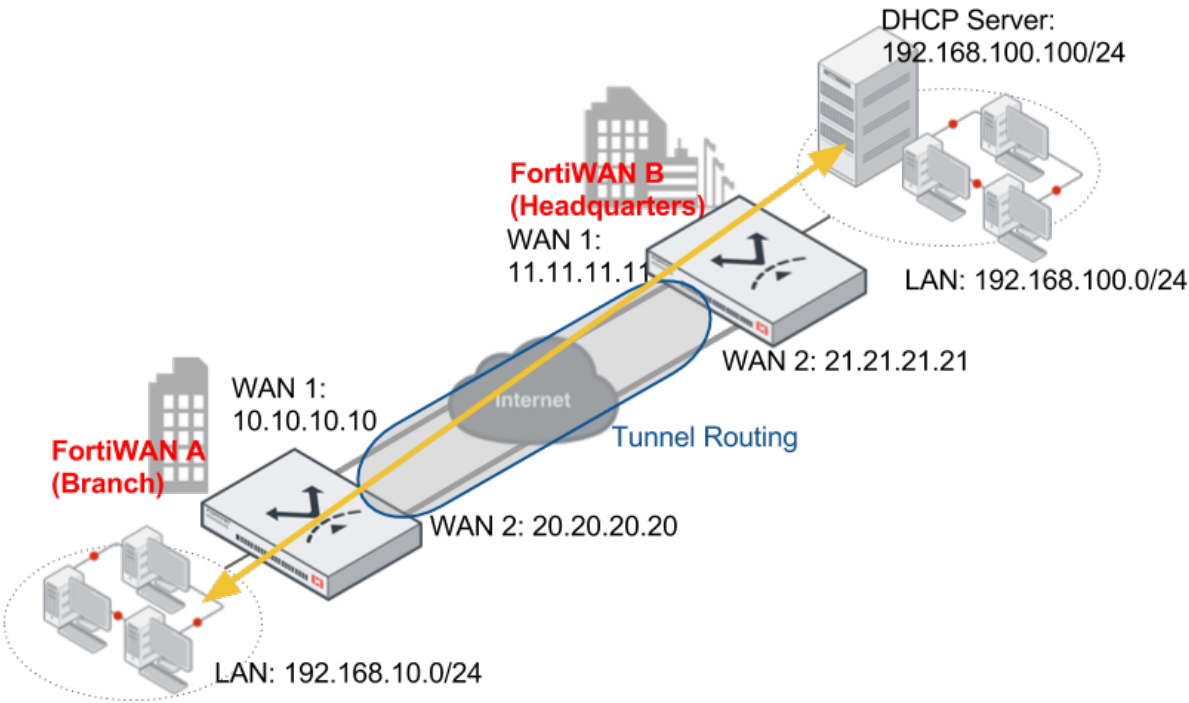
**Note that the DHCP server working with FortiWAN's DHCP Replay must be a standalone server.**

FortiWAN's DHCP function is not supported to work with DHCP Relay; a port with DHCP being enabled can not cooperate with the ports that DHCP Relay is enabled on. The centralized DHCP server working in a DHCP Relay deployment must be well-configured in the IP pools for the multiple IP subnets it is managing.

## DHCP Relay over FortiWAN Tunnel Routing network

FortiWAN's DHCP Relay is capable of forwarding DHCP messages through Tunnel Routing (See "[Tunnel Routing](#)") so that the centralized IP addressing over a FortiWAN Tunnel Routing network can be implemented. This is useful for the application that a headquarters centrally manages IP allocation to its regional branches. The following shows the example that a DHCP server located in the headquarters site (deployed in the LAN subnet) manages the IP addressing to its branches through Internet.

With Tunnel Routing connectivity, a VPN network is established among networks of the two sites. DHCP relay in the VPN network serves for the subnets just as normal. FortiWAN A (the branch) delivers the relayed DHCP requests from its private subnet 192.168.10.0/24 to the DHCP server located in remote private subnet 192.168.100.0/24 over Internet; conversely, FortiWAN B (the headquarters) delivers the DHCP responses to the branch site over Internet and FortiWAN A will forward the response to its LAN to allocate a host the IP address. DHCP messages are delivered by Tunnel Routing encapsulation and decapsulation, just like normal Tunnel Routing transmission. The localhost of LAN port on FortiWAN A is configured to 192.168.10.254. Configuration of IP pool for subnet 192.168.10.0/24 is required on the DHCP server. The related configurations on the two FortiWAN units are as follows:



Configurations on FortiWAN A

Go to **Network Setting > LAN Private Subnet > IPv4 Basic Subnet** and select the subnet 192.168.10.0/24 to configure.

Check the checkbox **Enable DHCP Relay** and configure the setting below.

|                     |                 |
|---------------------|-----------------|
| DHCP Relay Server 1 | 192.168.100.100 |
| DHCP Relay Agent IP | 192.168.10.254  |

Go to **Service > Tunnel Routing** and define a Tunnel Group with the two tunnels below:

| Local IP    | Remote IP   |
|-------------|-------------|
| 10.10.10.10 | 11.11.11.11 |
| 20.20.20.20 | 21.21.21.21 |

Define the Routing Rule.

| Source                     | Destination                 | Service | Group      |
|----------------------------|-----------------------------|---------|------------|
| 192.168.10.0/255.255.255.0 | 192.168.100.0/255.255.255.0 | Any     | Group Name |

Configurations on FortiWAN B

Go to **Service > Tunnel Routing** and define a Tunnel Group with the two tunnels below:



| Local IP    | Remote IP   |
|-------------|-------------|
| 11.11.11.11 | 10.10.10.10 |
| 21.21.21.21 | 20.20.20.20 |

Define the Routing Rule.

| Source                      | Destination                | Service | Group      |
|-----------------------------|----------------------------|---------|------------|
| 192.168.100.0/255.255.255.0 | 192.168.10.0/255.255.255.0 | Any     | Group Name |

Note that the DHCP Relay can only work with Tunnel Routing or Tunnel Routing over IPSec Transport Mode. **It does not support relaying DHCP requests through IPSec Tunnel Mode** (See "IPSec VPN").

### IPv6 Automatic Addressing

FortiWAN provides **stateless** and **stateful** mechanisms to allocate IPv6 addresses to hosts in the following subnets or IP range:

|                 |                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DMZ Side</b> | <ul style="list-style-type: none"> <li>• Routing Mode, IPv6 Basic Subnet: Subnet in DMZ</li> <li>• Routing Mode, IPv6 Basic Subnet: Subnet in WAN and DMZ</li> <li>• Bridge Mode: One Static IP, IPv6 Basic Subnet: Subnet in DMZ</li> <li>• Bridge Mode: Multiple Static IP, IPv6 IP(s) in DMZ</li> <li>• Bridge Mode: Multiple Static IP, IPv6 Basic Subnet: Subnet in DMZ</li> </ul> |
| <b>LAN Side</b> | <ul style="list-style-type: none"> <li>• LAN Private Subnet</li> </ul>                                                                                                                                                                                                                                                                                                                  |

**Stateless Address Autoconfiguration (SLAAC)** is a standard mechanism to equip hosts with IPv6 addresses and related routing information through the IPv6 router advertisements (RA). SLAAC has two properties:

- SLAAC is a stateless mechanism which is short of the IP management. SLAAC is incapable of controlling the mapping between a host and an IPv6 address.
- DNS information is absent from the traditional Router Advertisement messages. SLAAC with options of RDNSS and DNSSL included in RA messages (what is called SLAAC RDNSS) can convey information about DNS recursive servers and DNS Search Lists.

Comparing with SLAAC, **DHCPv6** takes the advantage of IP management, so that is called stateful. By specifying the IP pool and static IP mapping, administrators are able to control how the IPv6 addresses be allocated via DHCPv6. FortiWAN provides both SLAAC RDNSS and DHCPv6 for the stateless and stateful IPv6 automatic addressing

### Stateless IPv6 addressing: SLAAC

Enabling the stateless IPv6 addressing for the "IPv6 Basic Subnets" or "IPv6 (IPs) in DMZ" by checking the checkbox **Enable SLAAC**.

**DNS Server**

The recursive DNS servers used to serve the IPv6 subnet you are configuring (the Subnet field below). FortiWAN conveys it through router advertisement (RA) messages. Depending on the subnet type (DMZ-sided or LAN-sided), this could be the DNS server serving the global IPv6 subnets (public) that your ISP provides or the DNS server for the unique local IPv6 subnet (private).

- **Single DNS server:** the IPv6 addresses defined in **System > Network Setting > DNS Server > IPv6 Domain Name Server** are listed here for your options
- **ALL:** answer the hosts with all the defined IPv6 DNS servers information.
- **None:** answer the hosts without containing any IPv6 DNS server information.

This option is only available for IPv6 LAN private subnet. For the DMZ-sided subnets (hosts in the subnets are supposed to be deployed with IPv6 global addresses), system behaves answering the hosts with all the defined DNS servers information.

**Subnet**

The subnet deployed on the port (LAN port or DMZ port) you are configuring. SLAAC services the subnet. The subnet is used by SLAAC to allocate the prefix information to the hosts, so that an IPv6 address can be determined (with the Host ID) on a host. Depending on the subnet type, it could be a global IPv6 subnet or a unique local IPv6 subnet.

**DNS Search List**

A search list to be used when trying to resolve a name by means of the DNS. This option is only available for IPv6 LAN private subnet.

**Stateful IPv6 addressing: DHCPv6**

To enable the stateful IPv6 addressing for the "IPv6 Basic Subnets" or "IPv6 (IPs) in DMZ", **you are required to enable and configure both SLAAC and DHCPv6 on Web UI**. FortiWAN will not respond for any Router Advertisement (RA) if it SLAAC is disabled. The stateful IPv6 addressing via DHCPv6 requires RA to discover the default gateway for hosts, and therefor hosts fail to get default gateway if SLAAC is disabled. Please enable and configure the SLAAC as the introduction above if DHCPv6 is enable and make sure the network interface of a host is set to automatically get the IPv6 address through DHCPv6.

FortiWAN acts a DHCPv6 server on the specified LAN port or DMZ port if checkbox **Enable DHCPv6 Service** is checked. All the hosts running as DHCPv6 client could gain the routing and DNS information from DHCPv6 server. DHCPv6 provides configuring and management to the IPv6 addresses to be assigned, which is a shortage of SLAAC.

**DNS Server**

The DNS servers used to serve the IPv6 subnet you are configuring (the Subnet field below). FortiWAN responds to the DHCPv6 clients within the DHCPv6 messages if the clients are set to automatically get DNS information through DHCPv6. Depending on the subnet type (DMZ-sided or LAN-sided), this could be the DNS server serving the global IPv6 subnets (public) that your ISP provides or the DNS server for the unique local IPv6 subnet (private).

- **Single DNS server:** the IPv6 addresses defined in **System > Network Setting > DNS Server > IPv6 Domain Name Server** are listed here for your options.
- **ALL:** answer the hosts with all the defined IPv6 DNS servers information.
- **None:** answer the hosts without containing any IPv6 DNS server information.

This option is only available for IPv6 LAN private subnet. For subnet in DMZ and subnet in WAN and DMZ (hosts in the subnets are supposed to be IPv6 global address deployment), system behaves answering the hosts with all the defined DNS servers information.

**DHCP Range**

The address pools that DHCPv6 server assigns and manages IPv6 addresses from. Define the DHCP ranges by specifying IPv6 Starting Address and IPv6 Ending Address.

**Static Mapping**

DHCPv6 server assigns and manages IPv6 addresses according to client IDs. An IPv6 address that is mapped to a client ID is only available to this client. It will not be assigned to other clients even it is idle. Define the mapping by specifying Client ID and the correspondent IPv6 Address.

**DNS Search List**

A search list to be used when trying to resolve a name by means of the DNS. This option is only available for IPv6 LAN private subnet.

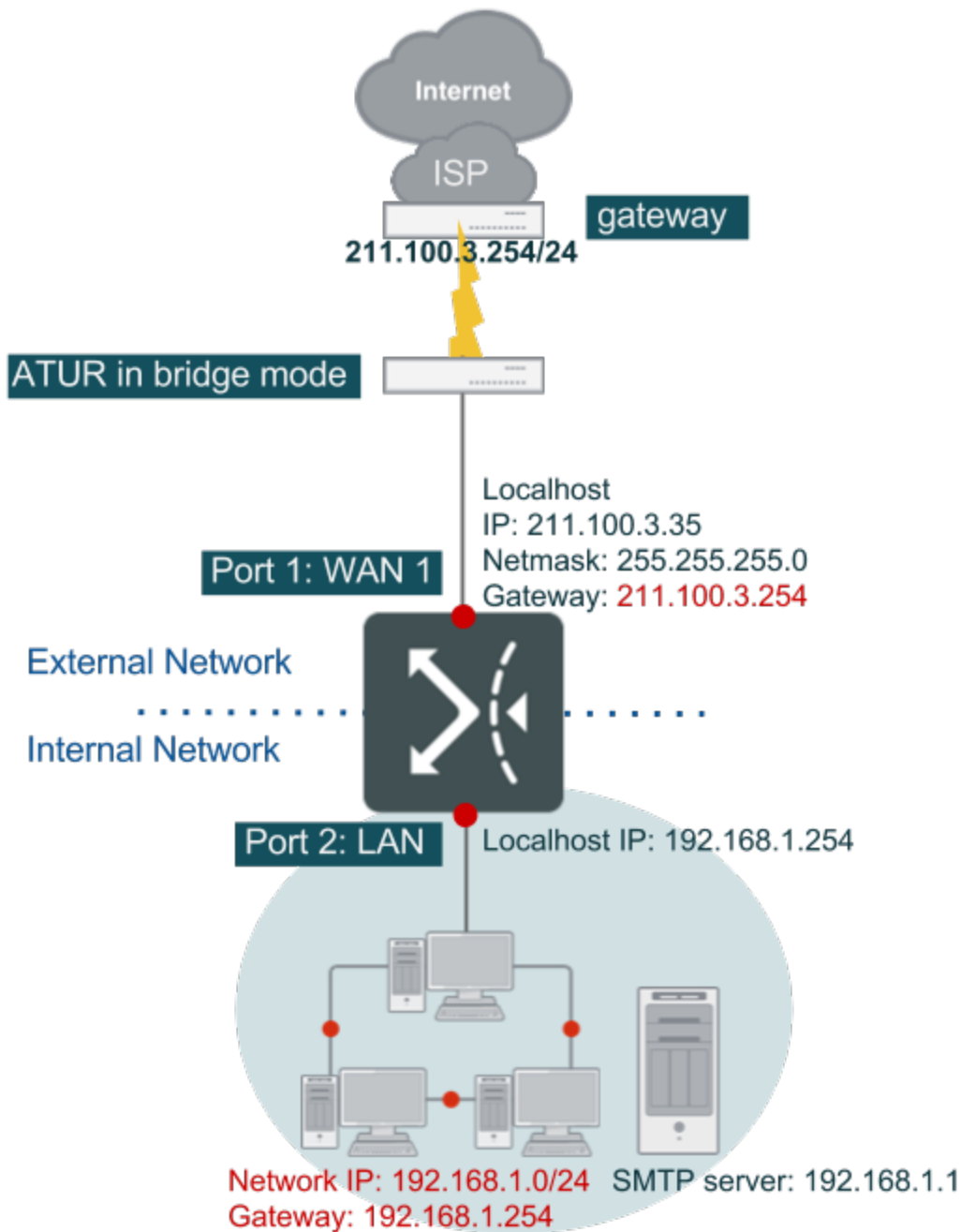
Note that IPv6 addresses defined in **DHCP Range** and **Static Mapping** must be also defined in filed **IPv6 IP(s) in DMZ** for a **bridge-mode (multiple static IP) WAN link**, the **DMZ side** of IPv6 basic subnets (subnet in WAN and DMZ, and subnet in DMZ) for a **routing-mode WAN link** and the IPv6 basic subnets of private LAN subnets.

## Deployment Scenarios for Various WAN Types

This Section provides various network scenarios for the different WAN types and explains how FortiWAN can easily be integrated into any existing networks.

### WAN Type: Bridge Mode with a Single Static IP

Single Static IP is a common and simple WAN network scenario, where the ISP provides a single public static (fixed) IP for the WAN link. Note: ISP often provides ATU-R, sometimes known as ADSL Modems with bridge model.



In this example it is assumed that WAN port 1 is connected to the bridge-mode ATU-R.

Please refer to the ATU-R User manual provided by your ISP to connect the ATU-R to FortiWAN's WAN #1. Connect LAN to FortiWAN's LAN port via a switch or hub. In this example, FortiWAN's Port2 is treated as LAN port. Please map FortiWAN's LAN port to the Port2 in [System] → [Network Setting] → [VLAN and Port Mapping]. Note: FortiWAN is treated as a normal PC when connecting to other networking equipments.

### WAN configuration:

1. Enter FortiWAN's Web-based UI.
2. Go to [System] → [Network Setting] → [WAN Settings].

3. In the WAN LINK scroll menu, select "1", and choose "Enable" in the Basic Settings.
4. In the WAN type scroll menu, select [Bridge Mode: One static IP].
5. Select [Port 1] in the WAN Port field.
6. Enter the up/down stream bandwidth associated with this WAN link. Example: If the ADSL Line on WAN1 is 512/64, then enter [64] and [512] in the Up Stream and Down Stream fields respectively. Note: The up/down stream values entered will ONLY affect the BM and statistics reporting. Bandwidth will not increase if the values are greater than the actual bandwidth.
7. Enter [211.100.3.35] in the Localhost IP field.
8. Enter [255.255.255.0] in the Netmask field.
9. Enter [211.100.3.254] in the Default Gateway IP field.
10. Apply the bridge mode configuration.
11. If the configuration above has been correctly established, in the [System] → [Summary] page, the status color on the WAN Link State for WAN Link #1 will turn green.

### LAN configuration:

1. Go to [System] → [Network Setting] → [LAN Private Subnet].
2. Enter [192.168.1.254] in the IP(s) on Localhost field.
3. Enter [255.255.255.0] in the Netmask field.
4. Select [Port2] in the LAN Port field.
5. Check NAT Subnet for VS.
6. Configuration complete.

### Virtual Server Configuration:

Assume an SMTP server with IP 192.168.1.1 provides SMTP services to the outside via the virtual server. FortiWAN will perform NAT on this machine so that the outside clients can get SMTP services via FortiWAN's public IP on WAN1. The settings for this are in [Service] → [Virtual Server].

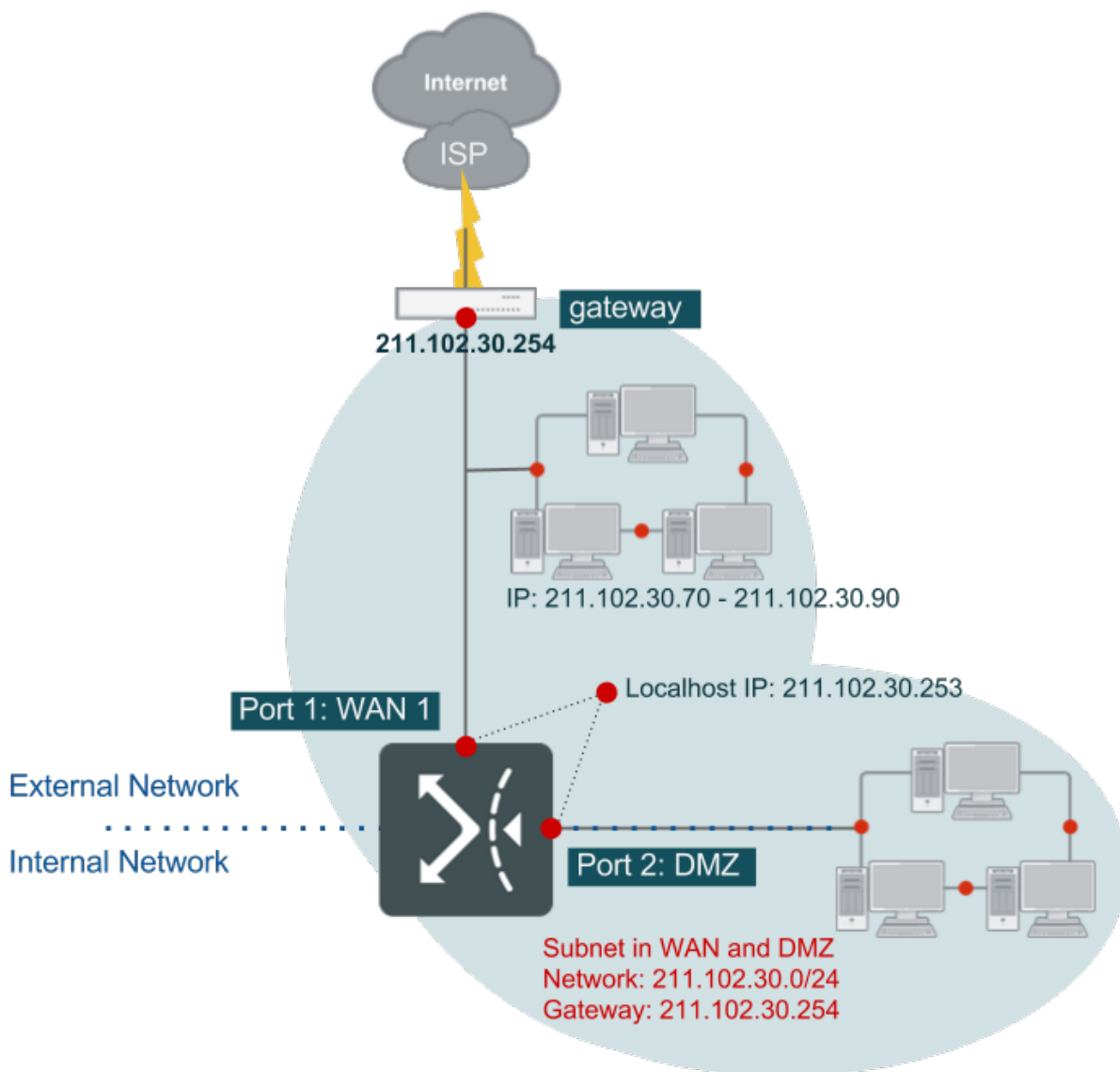
1. Click [+] to create a new rule.
2. Check [E] to enable this rule.
3. Select [All-Time] in the "When" field.
4. Enter [211.100.3.35] in the WAN IP field.
5. Select [SMTP(25)] in the Service field.
6. Select [Round-Robin] in the Algorithm field.
7. Click [+] to create a new server in Server Pool.
8. Enter [192.168.1.1] in the Server IP field.
9. Select [SMTP(25)] in the Service field.
10. Enter [1] in the Weight field.
11. Selection of the L field is optional. (If an Administrator wishes to log Virtual Server activities, please select "L").
12. Configuration complete.

Administrators can set up different types of services inside the LAN and use the Virtual Server to make these services available to public once the configurations are completed.

## WAN Type: Routing Mode Example 1

This is a typical example where ISP provides a network segment (a class C segment for example) to the user. Under such a condition, FortiWAN use one or more IP addresses, while the rest of the public IP addresses (from the assigned segment) will be under DMZ.

Servers with public IP addresses can be deployed in two places in the network (as illustrated in the figure below). It can be deployed either between the ATU-R and FortiWAN, i.e., behind the ATU-R but in front FortiWAN or inside the FortiWAN DMZ segment.



In this example, the router is assumed to be connected to FortiWAN's WAN port1.

### Network Information from ISP:

Client side IP segment is 211.102.30.0/24, Gateway (i.e. the IP for the router) is 211.102.30.254, while the netmask is 255.255.255.0.

FortiWAN's IP is assumed as 211.102.30.253.

Servers in between ATU-R and FortiWAN occupy the IP range between 211.102.30.70-100.102.30.99.

WAN port is on port #1.

DMZ port is on port #2.

ISP supplies the router.

### **Hardware Configuration:**

Connect the router with FortiWAN in WAN1 by referring to router's user manual. Note: FortiWAN is viewed as a normal PC when connected to other network equipment.

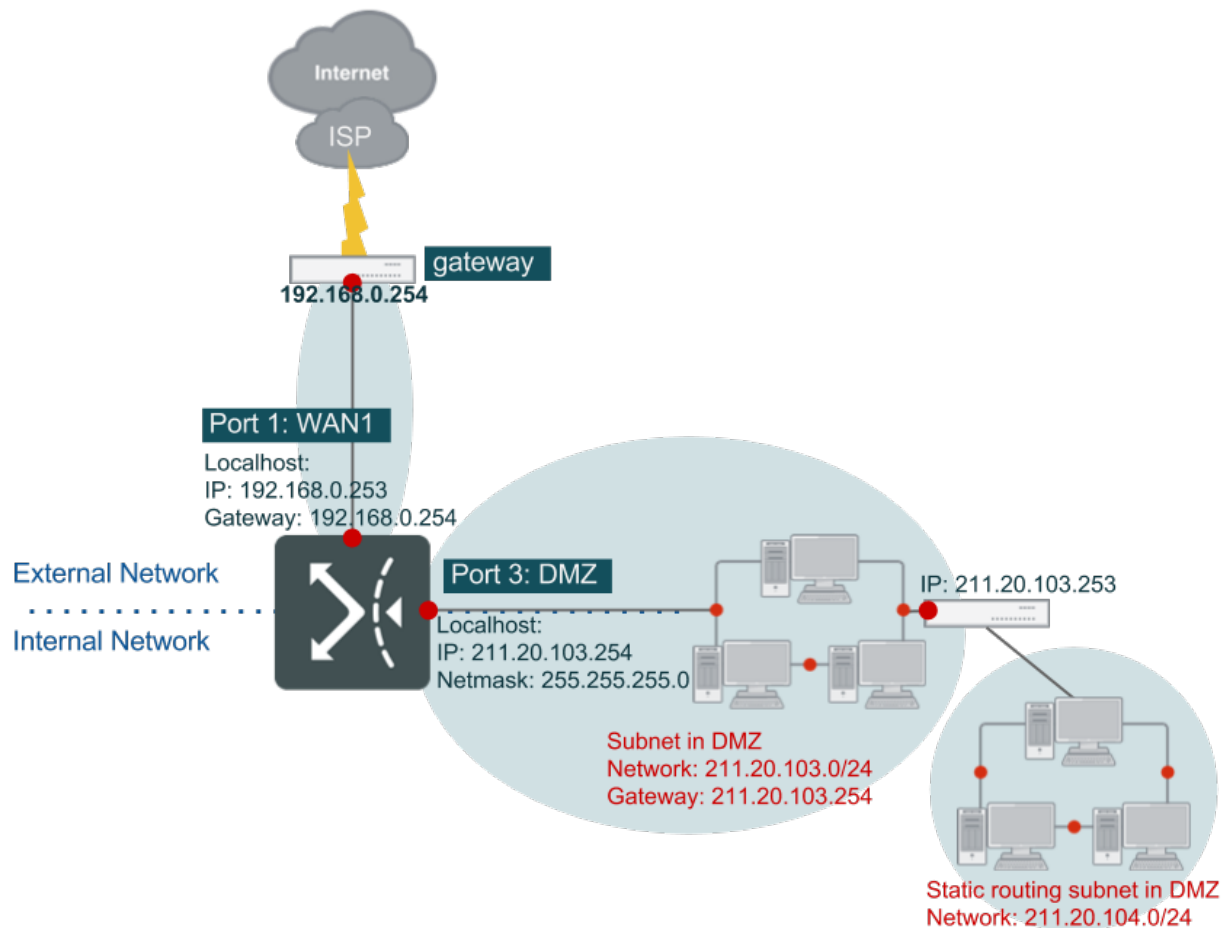
### **Configuration Steps:**

1. Log onto the FortiWAN Web UI.
2. Go to [System] → [Network Settings] → [WAN Settings].
3. Under the WAN Link menu, select "1" and select "Enable" in Basic Settings.
4. In the WAN Type scroll menu, select [Routing Mode].
5. Set WAN port to port #1.
6. Enter the corresponding up/down stream bandwidth. For example, if the type of ADSL connection is 512/64K, then enter [64] and [512] in the Up Stream and Down Stream parameter fields respectively. Note: The Up and Down Stream parameters will not affect the physical bandwidth provided by the ISP. It will only affect the BM and Statistical pages.
7. Set the IPv4 Gateway to 211.21.30.254.
8. In the IPv4 Basic Subnet section select the Subnet Type as "Subnet in WAN and DMZ", as follows:
  - For IP(s) on Localhost field, enter [211.102.30.253].
  - For IP(s) in WAN field, enter [211.102.30.70-211.102.30.99].
  - In the Netmask field, enter [255.255.255.0].
  - In the DMZ Port field, enter [Port 2].
9. Configuration complete.

Note: This example shows all addresses are in DMZ (211.102.30.1-211.102.30.69, 211.102.30.100-211.102.30.252), except those specified in the "IP(s) in WAN" .

### **WAN Type: Routing Mode Example 2**

This example shows the scenario where a private subnet between the WAN router and FortiWAN. In addition, the public IP subnet inside the FortiWAN DMZ port requires a router.



### Sample Configuration:

- Assume the private IP subnet (192.168.0.0/24) is between the WAN link router and FortiWAN WAN port.
- FortiWAN's port 1 IP (192.168.0.253) is connected to the WAN link router (192.168.0.254).
- FortiWAN's Port 3 is DMZ with a public IP subnet (211.20.103.254/24).
- The LAN part behind FortiWAN has another public IP subnet (211.20.104.0/24 behind a router (211.20.103.253).

### Configuration Steps:

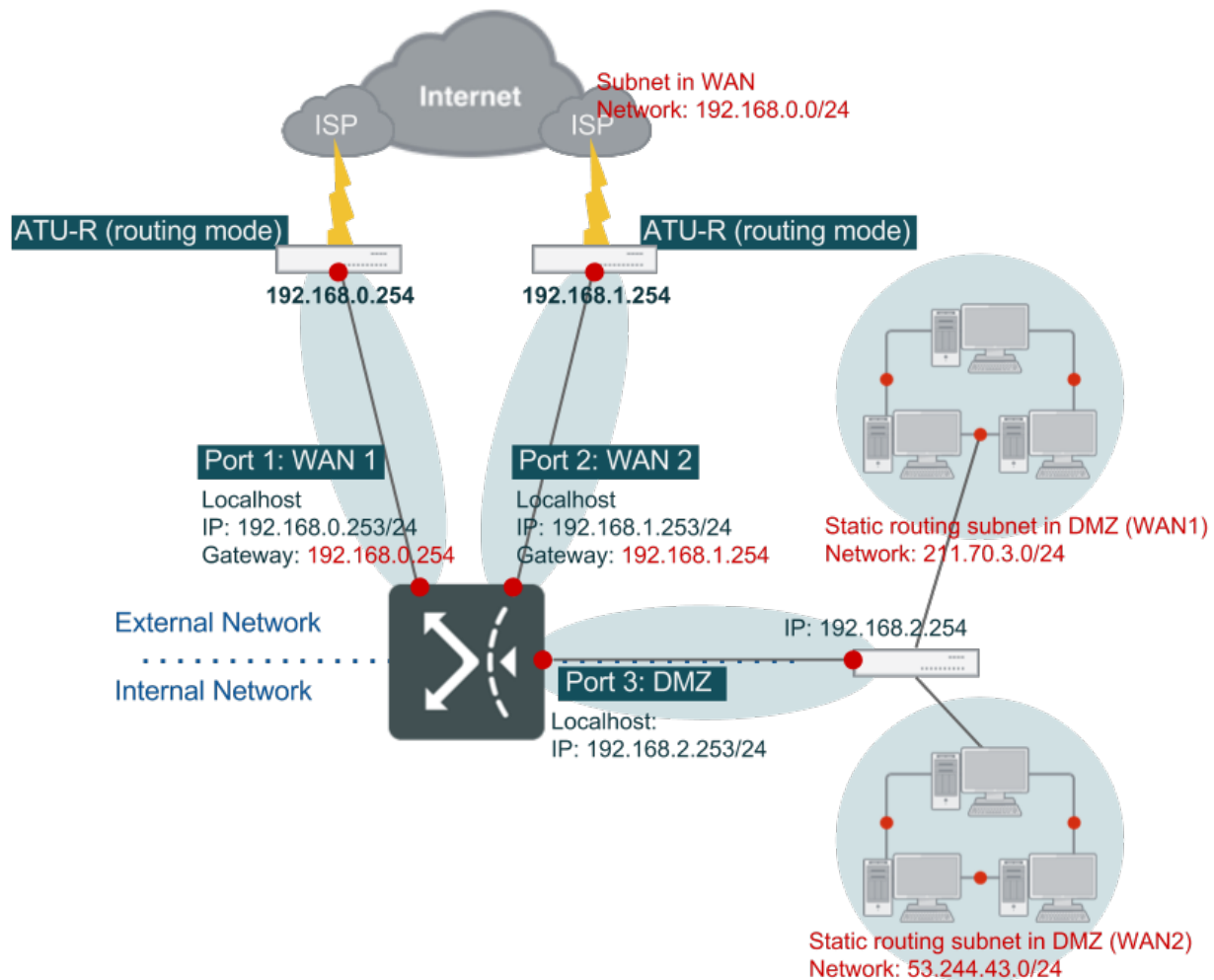
1. In the UI: [System] → [Network Settings] → [WAN Settings] sub-function.
2. Select "1" on the WAN Link menu and select [Enable].
3. In the WAN Type scroll menu, select [Routing Mode].
4. In the WAN Port field, enter [Port 1].
5. Enter the corresponding up and down stream bandwidths.
6. In the IPv4 Gateway field, enter [192.168.0.254].
7. In the IPv4 Basic Subnet function, use [+] to create new rules, and select [subnet in DMZ] in the Subnet Type field.
8. In the IP(s) on Localhost field, enter [211.20.103.254].
9. In the Netmask field, enter [255.255.255.0].



10. In the DMZ Port field, enter [Port 3].
11. In the IPv4 Static Routing Subnet field, use [+] to add new rules with Subnet Type as [Subnet in DMZ]. In this example, there is a router in the DMZ port for the public IP subnet and the subnet does not connect to the FortiWAN directly. Therefore the subnet info should be filled in the "Static Routing Subnet" field.
12. In the Network IP field, enter [211.20.104.0].
13. In the Netmask field, enter [255.255.255.0].
14. In the Gateway field, enter [211.20.103.253].
15. Go to [WAN/DMZ Private Subnet] sub-function page and select [+] in the IPv4 Basic Subnet and add the following rules:
16. Set the Subnet Type as "Subnet in WAN".
17. In the IP(s) on Localhost field, enter [192.168.0.253].
18. In the Netmask field, enter [255.255.255.0].
19. In the WAN Port field, select [Port 1], and the configuration is complete.

### **WAN Type: Routing Mode Example 3**

In this example, both WAN links have its own routers and FortiWAN is connected to these routers using private IP addresses, as illustrated below. In addition, FortiWAN Port 3 has been assigned another private IP connecting to the LAN Core Switch (L3 switch), therefore there is a public IP subnet connected behind the Core Switch inside the LAN.



### Configuration Example:

1. FortiWAN Port 1 (192.168.0.253) is connected to WAN1's router (192.168.0.254/24).
2. FortiWAN Port 2 (192.168.1.253) is connected to WAN2's router (192.168.1.254/24).
3. FortiWAN Port 3 (192.168.2.253) is connected to the LAN Core Switch (192.168.2.254/24).
4. WAN1's Public IP subnet is placed behind the Core Switch as (211.70.3.0/24).
5. WAN2's Public IP subnet is also placed behind the Core Switch as (53.244.43.0/24).

### Configuration Steps:

1. Go to FortiWAN Web UI: [System] → [Network Settings] → [WAN Settings] management page.
2. Select [1] in the WAN Link menu.
3. Click Enable to activate the WAN link.
4. Select [Routing Mode] in the WAN Type menu.
5. Select [Port 1] in the WAN Port field.
6. Enter the corresponding up/down-stream bandwidth.
7. In the IPv4 Gateway field, enter [192.168.0.254].

8. In the Static Routing Subnet field, use [+] to add a new rule with Subnet Type as "Subnet in DMZ". In this example, there is a Core Switch in the DMZ port for the public IP subnet and the subnet does not connect to the FortiWAN directly. Therefore the subnet info should be filled in the "Static Routing Subnet" field.
9. In the Network IP field, enter [211.70.3.0].
10. In the Netmask field, enter [255.255.255.0].
11. In the IPv4 Gateway field, enter [192.168.2.254].
12. In the WAN Link menu, select 2 to switch to WAN2.
13. Click on Basic Settings to enable the WAN link.
14. In the WAN type menu, select [Routing Mode].
15. In the WAN Port field select [Port 2].
16. Enter the corresponding up and down stream bandwidth parameters.
17. In the IPv4 Gateway field, enter [192.168.1.254].
18. In the Static Routing Subnet field, use [+] to add a new rule with the Subnet Type field as "Subnet in DMZ".
19. In the Network IP field, enter [53.244.43.0].
20. In the Netmask field, enter [255.255.255.0].
21. In the Gateway IP field, enter [192.168.2.254].
22. WAN/DMZ Private Subnet Management Page
23. In the WAN and DMZ ports, all three subnets should be completed as below:
24. In the IPv4 Basic Subnet field, click on [+] to add a new rule with 192.168.0.0/24 as the IP, and select "Subnet in WAN" under Subnet Type.
25. In the IP(s) on Localhost field, enter [192.168.0.253].
26. In the Netmask field, enter [255.255.255.0].
27. In the WAN port field, select [Port 1].
28. WAN Port 1 settings are complete; proceed onto WAN Port 2.
29. In the IPv4 Basic Subnet field, click on [+] to add a new rule with 192.168.1.0/24 as the subnet IP address, and select "Subnet in WAN" under Subnet Type.
30. In the IP(s) on Localhost field, enter [192.168.1.253].
31. In the Netmask field, enter [255.255.255.0].
32. In the WAN port field, select [Port 2].
33. The WAN Port2 settings are complete, proceed onto the DMZ port.
34. In the IPv4 Basic Subnet field, click on [+] to add a new rule. Select "Subnet in DMZ" under Subnet Type.
35. In the IP(s) on Localhost field, enter [192.168.2.253].
36. In the Netmask field, enter [255.255.255.0].
37. In the DMZ Port field, select [Port3].
38. Configuration is complete.

The example above illustrates a common FortiWAN deployment scenario where a private IP subnet is placed inside a WAN and DMZ, and a public IP subnet is connected to FortiWAN DMZ via a Core Switch.

## MIB fields for WAN links and VLANs

You can use SNMP manager to get information of defined WAN links and VLANs and receive notifications when a WAN link fails or recovers. Configure SNMP for your FortiWAN unit (See ["SNMP"](#)) to get the information in a MIB field via SNMP manager. Configure the SNMP manager on your FortiWAN and enable the event types "" and "" to

notify (See "[Notification](#)"), then notifications will be delivered to your SNMP manager for the events. The correspondent MIB fields and OIDs are listed as following:

### SNMP field names and OIDs for WAN link

| MIB Field       | OID                             | Description                                                                                                                                                                                                                                                               |
|-----------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fwnWanNumber    | 1.3.6.1.4.1.12356.118.2.1.1     | Maximum of WAN links that the system supports.                                                                                                                                                                                                                            |
| fwnWanTable     | 1.3.6.1.4.1.12356.118.2.1.2     | This is a table containing one element of object fwnWanEntry used to describe the properties and management information of every WAN link deployed on the system                                                                                                          |
| fwnWanEntry     | 1.3.6.1.4.1.12356.118.2.1.2.1   | An object used to describe the properties and management information of every WAN link deployed on the system: Index, Descr, Status, IP, HealthReq, HealthRep, UpLimit, DownLimit, ConnTime, InOctets, OutOctets, TotalOctets, InOctets64, OutOctets64 and TotalOctets64. |
| fwnWanIndex     | 1.3.6.1.4.1.12356.118.2.1.2.1.1 | Index (unique positive integer) of every WAN link.                                                                                                                                                                                                                        |
| fwnWanDescr     | 1.3.6.1.4.1.12356.118.2.1.2.1.2 | Label of every WAN link, such as WAN1, WAN2, WAN3, ect.                                                                                                                                                                                                                   |
| fwnWanStatus    | 1.3.6.1.4.1.12356.118.2.1.2.1.3 | State of every WAN link: ok(1), failed(2), disabled(3), backup(4) and unkown(5).                                                                                                                                                                                          |
| fwnWanIP        | 1.3.6.1.4.1.12356.118.2.1.2.1.4 | First one of the IP addresses deployed on the WAN port (localhost) of every WAN link.                                                                                                                                                                                     |
| fwnWanHealthReq | 1.3.6.1.4.1.12356.118.2.1.2.1.7 | Number of health detection (ping packets or TCP connect requests) sent out for every WAN link.                                                                                                                                                                            |
| fwnWanHealthRep | 1.3.6.1.4.1.12356.118.2.1.2.1.8 | Number of acknowledgements replied to every WAN link for the health detection.                                                                                                                                                                                            |
| fwnWanUpLimit   | 1.3.6.1.4.1.12356.118.2.1.2.1.9 | Maximum upload speed (in kbps) of every WAN link.                                                                                                                                                                                                                         |

| MIB Field               | OID                              | Description                                                                                                                                 |
|-------------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| fwnWanDownLimit         | 1.3.6.1.4.1.12356.118.2.1.2.1.10 | Maximum download speed (in kbps) of every WAN link.                                                                                         |
| fwnWanConnTime          | 1.3.6.1.4.1.12356.118.2.1.2.1.12 | The time period that a WAN link has been available since the last recovery from failure or disability.                                      |
| fwnWanInOctets          | 1.3.6.1.4.1.12356.118.2.1.2.1.5  | Number (32bit unsigned integer) of octets received on the interface (RX) of every WAN link during system's uptime.                          |
| fwnWanOutOctets         | 1.3.6.1.4.1.12356.118.2.1.2.1.6  | Number (32bit unsigned integer) of octets transmitted from the interface (TX) of every WAN link during system's uptime.                     |
| fwnWanTotalOctets       | 1.3.6.1.4.1.12356.118.2.1.2.1.11 | Sum (32bit unsigned integer) of octets received and transmitted on/from the interface (RX and TX) of every WAN link during system's uptime. |
| fwnWanInOctets64        | 1.3.6.1.4.1.12356.118.2.1.2.1.13 | Number (64bit unsigned integer) of octets received on the interface (RX) of every WAN link during system's uptime.                          |
| fwnWanOutOctets64       | 1.3.6.1.4.1.12356.118.2.1.2.1.14 | Number (64bit unsigned integer) of octets transmitted from the (TX) interface of every WAN link during system's uptime.                     |
| fwnWanTotalOctets64     | 1.3.6.1.4.1.12356.118.2.1.2.1.15 | Sum (64bit unsigned integer) of octets received and transmitted on/from the interface (RX and TX) of every WAN link during system's uptime. |
| fwnEventWanLinkRecovery | 1.3.6.1.4.1.12356.118.2.2.2.1.1  | Index of a WAN link will be sent as an event notification when the WAN link recovers from a failure.                                        |
| fwnEventWanLinkFailure  | 1.3.6.1.4.1.12356.118.2.2.2.1.2  | Index of a WAN link will be sent as an event notification when the WAN link fails.                                                          |

**SNMP field names and OIDs for VLAN**

| MIB Field          | OID                             | Description                                                                                                                                                  |
|--------------------|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fwnVlanNumber      | 1.3.6.1.4.1.12356.118.2.2.1     | Number of VLAN defined on the system.                                                                                                                        |
| fwnVlanTable       | 1.3.6.1.4.1.12356.118.2.2.2     | This is a table containing one element of object fwnVlanEntry used to describe the properties and management information of every VLAN defined on the system |
| fwnVlanEntry       | 1.3.6.1.4.1.12356.118.2.2.2.1   | An object used to describe the properties and management information of every VLAN defined on the system                                                     |
| fwnVlanDescr       | 1.3.6.1.4.1.12356.118.2.2.2.1.1 | Label of every VLAN. It consists of the port that the VLAN is defined on and the VLAN tag, such as port1.101, port1.102, port2.203, ect.                     |
| fwnVlanInOctets    | 1.3.6.1.4.1.12356.118.2.2.2.1.2 | Number (32bit unsigned integer) of octets received on the interface (RX) of every VLAN during system's uptime.                                               |
| fwnVlanOutOctets   | 1.3.6.1.4.1.12356.118.2.2.2.1.3 | Number (32bit unsigned integer) of octets transmitted from th interface (TX) of every VLAN during system's uptime.                                           |
| fwnVlanTotalOctets | 1.3.6.1.4.1.12356.118.2.2.2.1.4 | Sum (32bit unsigned integer) of octets received and transmitted on/from the interface (RX and TX) of every VLAN during system's uptime.                      |
| fwnVlanInOctets64  | 1.3.6.1.4.1.12356.118.2.2.2.1.5 | Number (64bit unsigned integer) of octets received on the interface (RX) of every VLAN during system's uptime.                                               |
| fwnVlanOutOctets64 | 1.3.6.1.4.1.12356.118.2.2.2.1.6 | Number (64bit unsigned integer) of octets transmitted from the interface (TX) of every VLAN during system's uptime.                                          |

| MIB Field            | OID                             | Description                                                                                                                             |
|----------------------|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| fwnVlanTotalOctets64 | 1.3.6.1.4.1.12356.118.2.2.2.1.7 | Sum (64bit unsigned integer) of octets received and transmitted on/from the interface (RX and TX) of every VLAN during system's uptime. |
| fwnVlanIndex         | 1.3.6.1.4.1.12356.118.2.2.2.1.8 | Index (unique positive integer) of every VLAN.                                                                                          |

# System Configurations

This topic elaborates on [System] and its submenus. Simple examples are given to illustrate how to configure [system] settings.

## Dashboard

**System > Dashboard** is the first-displayed page after you log in to the Web UI. Various system information, hardware states and real-time reporting are summarized in the dashboard, so that you can have an overview of a FortiWAN appliance at a glance. The provided widgets are:

- System Information
- License Information
- System Resources
- WAN Link State
- Throughput
- Connections
- Recent 10 System Log

The dashboard only displays current states and statistics between a very short period (about six minutes). For medium-term and long-term statistics and deep look inside the items, please see [Statistics](#) and [Reports](#).

### System Information

The System Information widget displays basic system information of a single FortiWAN appliance or a HA pair of FortiWAN appliances. The **Host** column indicates information of local appliance, while the **Peer** column indicates the information of peer unit if HA network is deployed. The **Peer** column keeps blank while no HA peer device is deployed. System information is auto-refreshed every 5 seconds.

It displays the following system information:

| Fields          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HA State</b> | <p>A symbol located on the upper-left corner of the panel indicates the HA state between the local FortiWAN unit and the peer unit.</p> <p>: The HA mode is disabled. The FortiWAN you are connecting to is a standalone device.</p> <p>: The HA mode is enabled. Both the master and slave units are working correctly.</p> <p>: The HA mode is enabled, and two units are during HA initiation (HA negotiation is processing).</p> <p>: The HA mode is enabled, but errors occur between the two HA units.</p> |



| Fields                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Version</b>        | <p><b>Host:</b> Firmware version that local FortiWAN appliance is running.</p> <p><b>Peer:</b> Firmware version that HA peer is running. Available only when HA is deployed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Model</b>          | <p><b>Host:</b> Model of local FortiWAN appliance.</p> <p><b>Peer:</b> Model of HA peer. Available only when HA is deployed.</p> <p>The bandwidth capability of current FortiWAN is relative to the model and the license you applied. To see the bandwidth capability please check the License Control panel in <b>System &gt; Administration</b> (See subsection "License Control" in "<a href="#">Administration</a>").</p>                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Serial Number</b>  | <p><b>Host:</b> Serial number of local FortiWAN appliance.</p> <p><b>Peer:</b> Serial number of HA peer. Available only when HA is deployed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Uptime</b>         | <p><b>Host:</b> Time period for which local FortiWAN appliance has been up and running.</p> <p><b>Peer:</b> Time period for which HA peer has been up and running. Available only when HA is deployed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>State</b>          | <p>When the FortiWAN appliance is deployed alone, it displays <b>None</b> in both Host and Peer columns.</p> <p>When the FortiWAN appliance is deployed as HA mode, it displays the HA state in the Host and Peer columns. The state will be:</p> <ul style="list-style-type: none"> <li>• Normally, this field displays <b>Master</b> or <b>Slave</b>.</li> <li>• When during the procedure of booting, this field displays <b>Rebooting</b> or <b>Booting</b>.</li> <li>• When a system panic happens, this field displays <b>Panic</b>.</li> <li>• When peer unit is lost (power-off or Ethernet cable disconnected), this field displays <b>None</b>.</li> <li>• When firmware version, FortiWAN model or throughput license is inconsistent between the two HA units, this field displays <b>Incompatible</b>.</li> </ul> |
| <b>Connections</b>    | The number of connections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>State</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Packets/Second</b> | The number of the packets that are processed per second.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>VRRP State</b>     | The state of VRRP (Virtual Router Redundancy Protocol) - Enabled or Disabled. Note that enabling VRRP will disable existing HA deployment. (See <a href="#">LAN Private Subnet</a> )                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hard Disk</b>      | FortiWAN's hard disk for Reports is being consumed by increasing report database. Once the disk space is used up, Reports will fail to continue log processing. This field monitors the disk space status of Reports by displaying the total space and consumed space. (See " <a href="#">Reports</a> ")                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

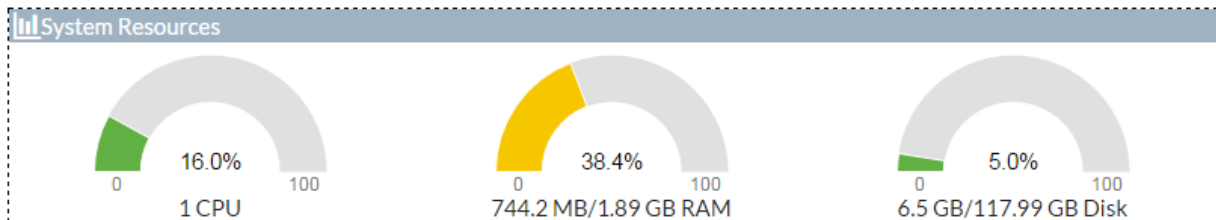
## License Information

The License Information widget displays license state of a FortiWAN-VM. This widget is visible only when you are running a FortiWAN-VM unit. License information is auto-refreshed every 5 seconds.

| Fields         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>License</b> | <p>The following license states will be displayed:</p> <ul style="list-style-type: none"> <li>• <b>Trial License is in use. (Expire in x days x hours x mins):</b> This is a trail or evaluation license.</li> <li>• <b>Valid:</b> This is a permanent license.</li> <li>• <b>Expired:</b> This license is expired.</li> </ul> <p>Click <b>Update</b> button and upload your FortiWAN-VM license file to update the FortiWAN-VM appliance. You can request a evaluation or trial license from Fortinet Customer Support or you can purchase a permanent license from your Fortinet channel partner.</p> |

## System Resources

The System Resources widget displays instance usage of CPU, RAM and hard disk. Information of system resources is auto-refreshed every 5 seconds.



| Fields             | Description                                                                                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CPU Usage %</b> | <p>Information of CPU usage includes:</p> <ul style="list-style-type: none"> <li>• Number of available CPU: depends on the model it would be 1 CPU, 2 CPU or 4 CPU.</li> <li>• CPU usage in percentage</li> <li>• CPU usage in color-code: Green (&lt; 30%), Yellow (30% ~ 60%), Orange (60% ~ 90%) and Red (90% ~ 100%)</li> </ul> |
| <b>Memory</b>      | <p>Information of memory usage includes:</p> <ul style="list-style-type: none"> <li>• Consumed memory / available memory</li> <li>• Memory usage in percentage</li> <li>• Memory usage in color-code: Green (&lt; 30%), Yellow (30% ~ 60%), Orange (60% ~ 90%) and Red (90% ~ 100%)</li> </ul>                                      |

| Fields           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hard Disk</b> | <p>FortiWAN's hard disk is being consumed by increasing report database and system logs. Once the disk space is used up, Reports and system log will fail to continue log processing. (See <a href="#">Log</a> and <a href="#">Reports</a>)</p> <p>Information of memory usage includes:</p> <ul style="list-style-type: none"><li>• Consumed disk space/ available disk space</li><li>• Disk usage in percentage</li><li>• Disk usage in color-code: Green (&lt; 30%), Yellow (30% ~ 60%), Orange (60% ~ 90%) and Red (90% ~ 100%)</li></ul> |

## WAN Link State

The WAN Link State widget displays states of FortiWAN's WAN links. The number of WAN links that a FortiWAN supports depends on the model. For example, FortiWAN 200B supports a maximum of 25 WAN links, while FortiWAN 1000B supports a maximum of 50 WAN links. Each of WAN links is color-coded to indicate its state in this widget:

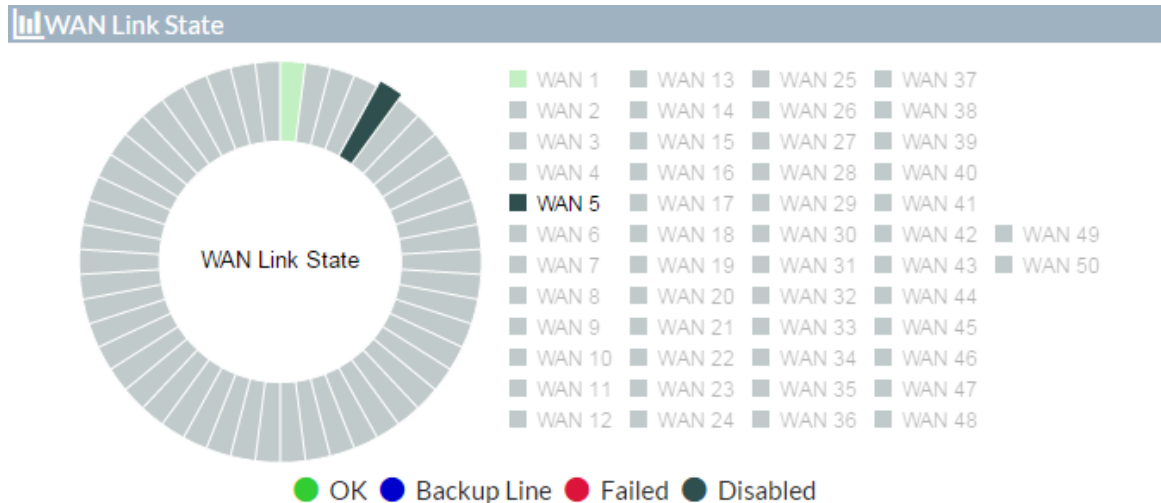
- **Green**: An active WAN link
- **Blue**: A backup line
- **Red**: A failed WAN link
- **Deep green**: A disabled WAN link

This widget consists of three fields:

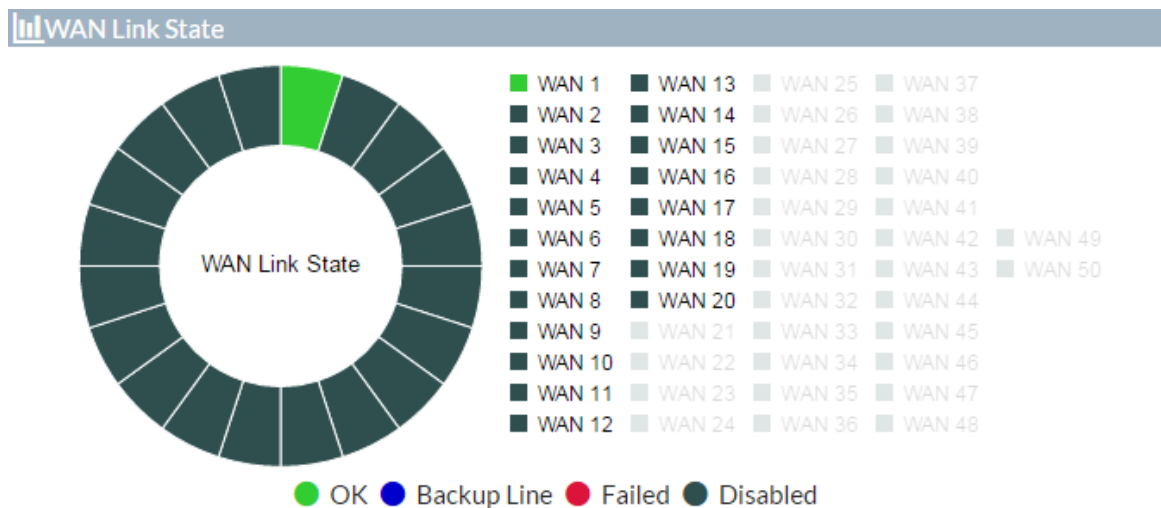
- A matrix in the right side of the widget.
- A circle matrix in the center of the widget
- A small panel in the left side of the widget (available only when mouse crosses over the circle matrix)

### The right-side matrix

All the WAN links are listed with a WAN link number and a state color. The number indicates the WAN link and the color indicates its state. When you move mouse over a WAN link, a corresponding element of the circle matrix pops up to enlarge the colored state.

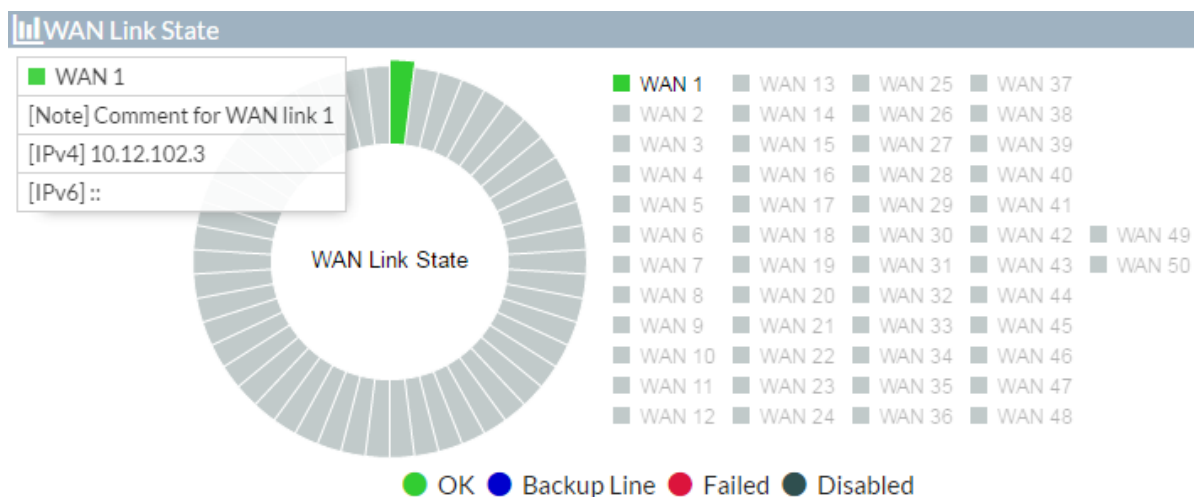


Clicking a WAN link can remove/add the WAN link from/into the state widget. You can remove the disabled WAN links to have a clear WAN link state widget for the active WAN links.



### The circle matrix

All the selected WAN links are circled. Each element in the circle indicate a WAN link with its state color. When you move mouse over an element, a small panel displaying information of the WAN link pops up on the left side of the widget.



### The WAN link information panel

The following information of the specified WAN links is displayed:

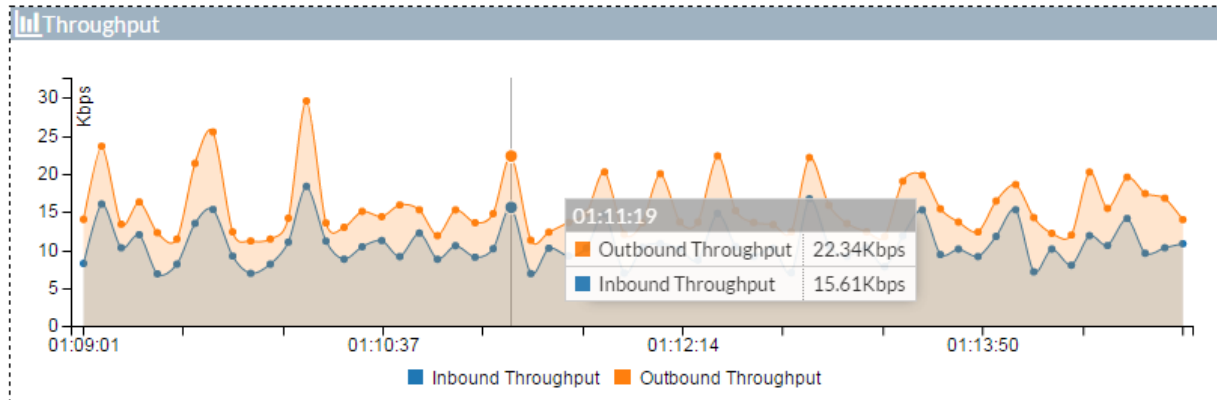
| Fields          | Description                                                                            |
|-----------------|----------------------------------------------------------------------------------------|
| <b>WAN link</b> | The WAN link number and its state (in color).                                          |
| <b>Note</b>     | The annotation of the WAN link (see <a href="#">Configuring your WAN</a> ).            |
| <b>IPv4</b>     | The IPv4 address deployed on the WAN port (see <a href="#">Configuring your WAN</a> ). |
| <b>IPv6</b>     | The IPv6 address deployed on the WAN port (see <a href="#">Configuring your WAN</a> ). |

### Throughput

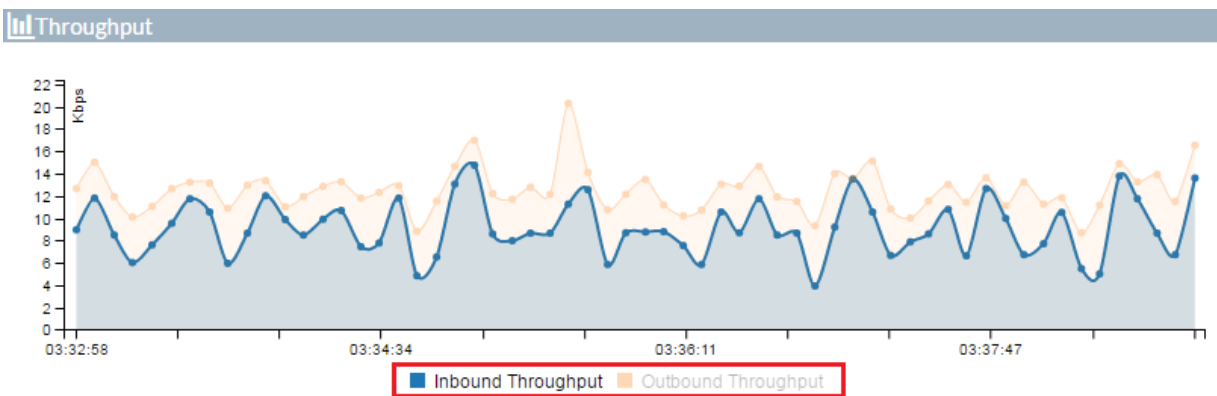
The Throughput widget displays the total bandwidth usage in the past 6 minutes. The inbound and outbound throughput are indicated with a blue line and a orange line respectively. The statistics is auto-refreshed every 6 seconds.

When you move mouse over the line chart, a small panel displaying the exact bandwidth usage at the moment pops up:

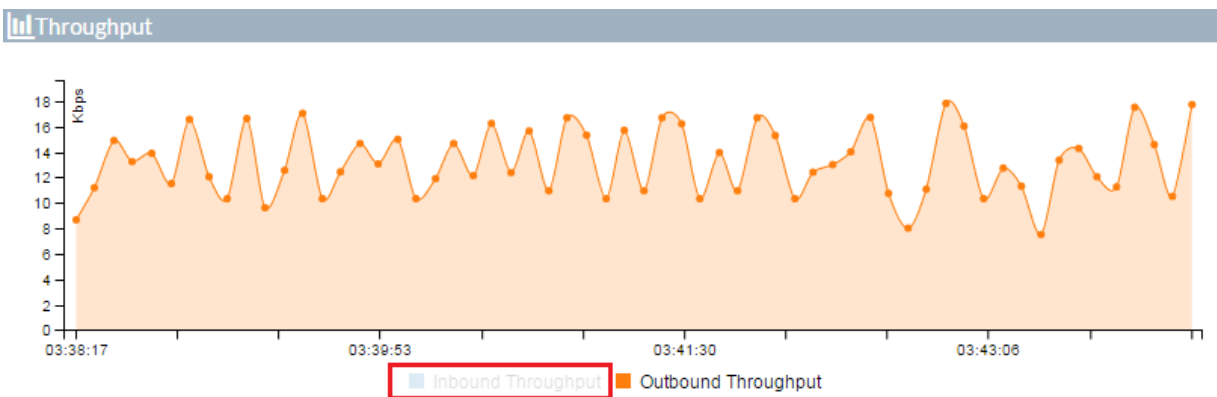
- Time
- Outbound Throughput
- Inbound Throughput



Moving mouse over the Inbound Throughput or Outbound Throughput options under the line chart can highlight the corresponding statistics line in the chart.



The statistics lines can be hid from the widget by clicking the Inbound Throughput and Outbound Throughput options. Clicking it again brings the lines back to the chart.

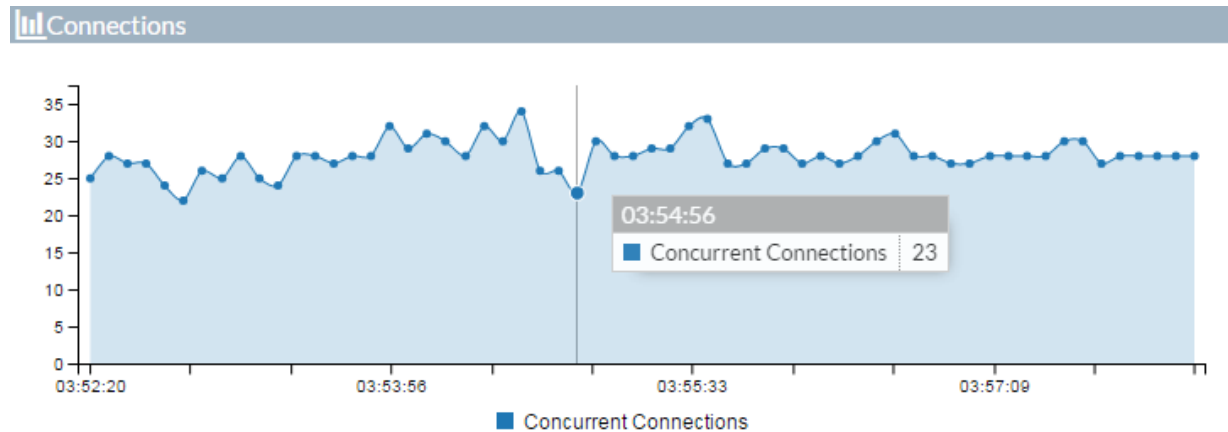


## Connections

The Connections widget displays statistics of concurrent connections in the past 6 minutes. The statistics is auto-refreshed every 6 seconds.

When you move mouse over the line chart, a small panel displaying the exact number of concurrent connections at the moment pops up:

- Time
- Concurrent Connections



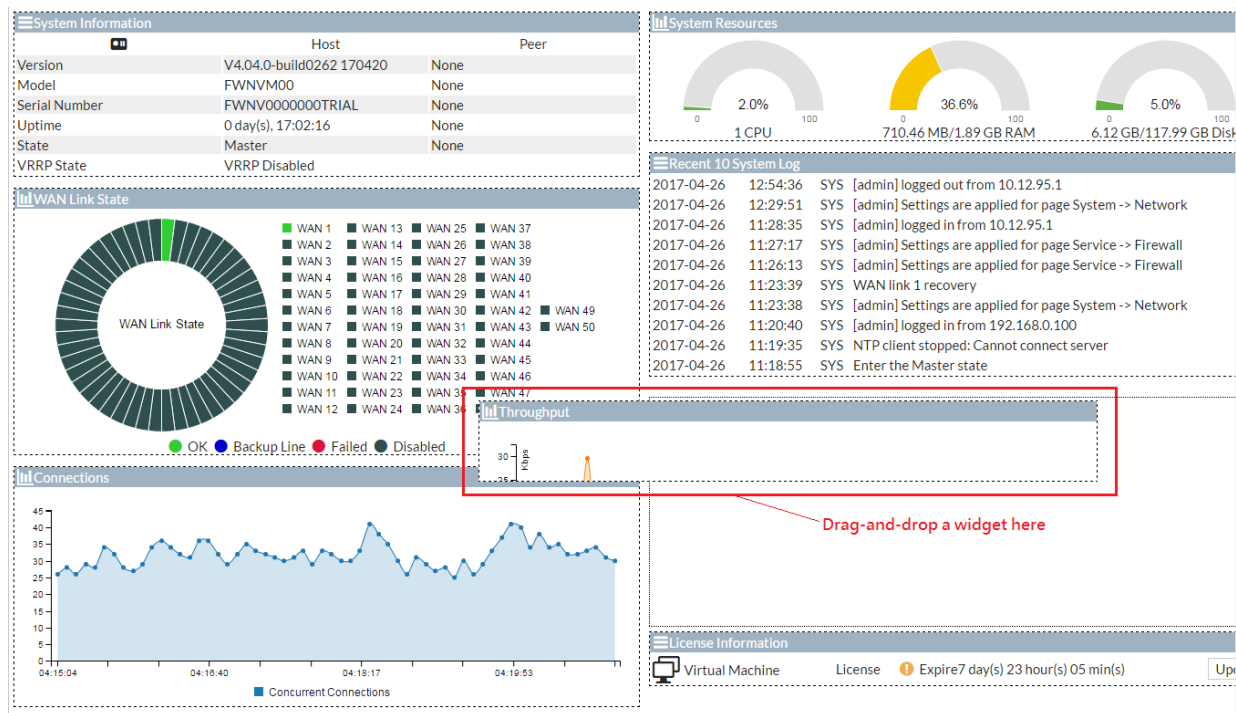
After FortiWAN just starts up, you may see more than 100 concurrent connections in this widget for a while. These connections are because of the standard procedure to detect WAN links and the related networks after FortiWAN starts up, such as ICMP-based health detection.

## Recent 10 System Log

The Recent 10 System Log widget displays the latest 10 system logs. It is auto-refreshed every 5 seconds. Go to **Log > View** for more system logs.

## Positioning widgets

Each of the widgets can be positioned to suit your need via mouse drag-and-drop. When you drag a widget to somewhere between any two widgets, a white block expands. Dropping the widget in the white block sets it to the new position. You can only arrange the widgets into a maximum of two columns.



## Get system information, peer information and WAN link state via SNMP

You can use SNMP manager to get the system information, HA peer information and WAN link state. Configure SNMP for your FortiWAN unit (See "SNMP") and you can get the information in a MIB field via SNMP manager. The correspondent MIB fields and OIDs are listed as following:

### SNMP field names and OIDs

| MIB Field               | OID                       | Description                                                                  |
|-------------------------|---------------------------|------------------------------------------------------------------------------|
| fwnSysSlaveVersion      | 1.3.6.1.4.1.12356.118.1.2 | Firmware version of the slave unit deployed with this local unit in HA mode. |
| fwnSysSlaveSerialNumber | 1.3.6.1.4.1.12356.118.1.3 | Serial number of the slave unit deployed with this local unit in HA mode.    |
| fwnSysSlaveUptime       | 1.3.6.1.4.1.12356.118.1.4 | Uptime of the slave unit deployed with this local unit in HA mode.           |
| fwnSysSlaveState        | 1.3.6.1.4.1.12356.118.1.5 | State of the slave unit deployed with this local unit in HA mode.            |
| fwnSysConnections       | 1.3.6.1.4.1.12356.118.1.6 | Number of connections that are being processed in the system.                |



| MIB Field             | OID                             | Description                                                                           |
|-----------------------|---------------------------------|---------------------------------------------------------------------------------------|
| fwnSysCpuLoad         | 1.3.6.1.4.1.12356.118.1.7       | Current CPU load (in percentage) of the system.                                       |
| fwnSysUsers           | 1.3.6.1.4.1.12356.118.1.8       | Number of IP addresses connecting to the FortiWAN unit from the LAN and DMZ subnets.  |
| fwnSysPktPerSec       | 1.3.6.1.4.1.12356.118.1.9       | Number of packets transferred via the system every second.                            |
| fwnSysConnectionRates | 1.3.6.1.4.1.12356.118.1.10      | Number of connections that are established with the FortiWAN unit every second.       |
| fwnWanStatus          | 1.3.6.1.4.1.12356.118.2.1.2.1.3 | State of every WAN link: ok(1), failed(2), disabled(3), backup(4) and unknown(5).     |
| fwnWanIP              | 1.3.6.1.4.1.12356.118.2.1.2.1.4 | First one of the IP addresses deployed on the WAN port (localhost) of every WAN link. |

### See also

- [FortiWAN in HA \(High Availability\) Mode](#)
- [LAN Private Subnet](#)
- [Configuring your WAN](#)
- [Reports](#)

## Optimum Route Detection

FortiWAN's Optimum Route is a particular load balancing algorithm which determines the best WAN link for Auto Routing and Multihoming by involving real Internet conditions in calculation, while the other algorithms, such as By Round-Robin, By Connection and By Upstream/Downstream/Total Traffic, only focus on the loading between the FortiWAN device and ISP's gateways. Optimum Route is used mainly to avoid the inefficient transmission due to bad peering between ISPs. Peering between two ISPs is an interconnection of administratively separated Internet networks (belonging to the two ISPs individually) for the purpose of exchanging traffic between the users in each network. It allows the two ISP to directly hand off the traffic between each other's customers, which might be the most efficient way to communicate between two networks if it is settlement-free. However, two situations might cause the transmission between two ISP networks inefficient;

- If there is no agreement by the two ISP networks to peer, the transit service, which is a method to carry that traffic across one or more third-party networks (a few exchange points), will be required.
- An ISP restricts the bandwidth for peering with another ISP on the purpose of competition in business. The peering point thus becomes a bottleneck and might make the transmission extremely slow between each other's customers.

Although the other balancing algorithms determine a good WAN link among multiple WAN links (multiple ISP networks) for inbound and outbound traffic, they are not aware of the real situations between those ISPs. For example, two WAN links of a FortiWAN device are connected to ISP-A and ISP-B networks and the peering between each other is bad. Those non-optimum-route balancing algorithms might determine ISP-B WAN link for Auto Routing to transfer the traffic which is destined to a server located in ISP-A network (see [Auto Routing](#)). If the bad peering between ISP-A and ISP-B is the only exchange point, which is the bottleneck, for delivering the traffic, the transmission will become slow. Conversely, those balancing algorithms may also determine the IP of ISP-B WAN link for Multihoming (see [Multihoming](#)) to answer DNS queries coming from ISP-A network. Then the users in ISP-A network suffer the bad peering when accessing services on FortiWAN through ISP-B network.

Algorithm Optimum Route is just the opposite of those algorithms. It determines the optimum WAN link by going deep into the real Internet conditions in two modes: static IP table and dynamic detect.

- **Static IP table:** A static IP table is a set of the IP addresses of an ISP network. Optimum Route evaluates the destination IP of out-going sessions against the IP tables for Auto Routing, and evaluates the source IP of DNS queries against the IP tables for Multihoming. If the evaluated IP matches the IP table of an ISP, which implies the ISP network that the evaluated IP belongs to is recognized, this ISP WAN link will be the optimum routing. Conceptually, it directly asks traffic being delivered directly through a WAN link connected to the ISP network that traffic source or destination belong to, so that traffic will not suffer a peering. This can be also implemented by specifying the source or destination filter with IP groups (See ["IP Grouping"](#)) in Multihoming or Auto Routing rules.
- **Dynamic detect:** It dynamically evaluates WAN links according to the detected round-trip time (RTT) and the bandwidth loading. Bad peering brings bad RTT value.

The following configurations define how Optimum Route detect to determine an optimum WAN link. To use the Optimum Route algorithm in Auto Routing and Multihoming, it requires specifying the algorithm "By Optimum Route" for a Auto Routing policy and A/AAAA Record policy, and applying the policy to corresponding filter rules and A/AAAA records. Without this, Optimum Route would never work even if the detection is configured. FortiWAN provides DNS Proxy to cooperate with Optimum Route to resolve an advanced issue caused by bad peering (See ["DNS Proxy"](#)).

## Optimum Route Policy

Options for optimum route detection

|                        |                                                                                                                                                    |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Static IP Table</b> | Uses static IP table only.                                                                                                                         |
| <b>Dynamic Detect</b>  | Uses dynamic detection only.                                                                                                                       |
| <b>Static, Dynamic</b> | Uses static detection first, then switches over to dynamic detection if static detection fails. [Static, Dynamic] is the default detection method. |
| <b>Dynamic, Static</b> | Uses dynamic detection first, then switches over to static detection if dynamic detection fails.                                                   |

## Static IP-ISP Table

Enables to match the IP address entries in the table to work out the optimum route. Administrators can add, delete or inquire the desirable IP entry in the table.

The static IP-ISP tables are the reference for Optimum Route to recognize the ISP network that the source or destination IP of traffic belongs to and so that point the traffic to corresponding WAN link, which is the optimum routing. A static IP-ISP table contains the IP subnets of an ISP network. You have to maintain these IP subnets in a text file for creating an IP-ISP table. Each line of the text file indicates a IP subnet in format `Network IP/Prefix`, for example:

```
3.0.0.0/8
211.1.0.0/16
```

Note that it is strongly suggested that an IP file contains the IP subnets of only ISP, or Optimum Route might not run as expected. Please prepare the IP files for the IP-ISP tables. Another component of static IP-ISP table is the WAN parameter, which indicates the FortiWAN's WAN links connecting to the ISP's network. Once traffic matches the IP subnets of an IP-ISP table, Optimum Route determines a WAN link from the candidates. It is not such strictly limited that an ISP's IP subnets can only be recorded in one IP-ISP record (just make sure an IP-ISP table contains only one ISP). The IP subnets of an ISP can be separated into multiple IP-ISP tables, just remember Optimum Route evaluates traffic against the tables top down by first match, and it picks up one of the corresponding WAN links if a table is matched.

|                   |                                                   |
|-------------------|---------------------------------------------------|
| <b>Table Name</b> | Name for the IP-ISP Table, such as an ISP's name. |
|-------------------|---------------------------------------------------|

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Setting</b>   | Set the IP subnets of an ISP to the table.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                  | <p data-bbox="391 243 503 277"><b>Upload</b></p> <p data-bbox="617 243 1490 441">Upload the IP file of a ISP to save the ISP's IP subnets to the static IP-ISP table. Click "Browse" to locate the IP file and click "Upload" to upload the file. You are required to upload an IP file (click "Upload") first, then apply (click "Apply") the settings of the IP-ISP table. Note that an IP table file is necessary to create a static IP-ISP table.</p> <p data-bbox="617 451 1490 630">After saving the IP subnets to the table, you might continue maintaining (add or remove) the IP subnets of the ISP. You can make it by editing the subnets in the following field Rule Setting or manually editing the IP file and re-upload it to the table. IP file re-uploading overwrites the original IP subnets of the table.</p>                                                                                                                                                                                                                                                                                                           |
|                  | <p data-bbox="391 642 560 676"><b>Rule Setting</b></p> <p data-bbox="617 642 1490 787">After uploading the IP file to the table, you can manually edit it by adding/removing subnets to/from the IP table if necessary. Without uploading an IP file to the table first, it is ineffective to add/remove IP subnets to/from the table.</p> <div data-bbox="617 798 1490 1029"> <p data-bbox="618 800 836 833"><b>Subnet Address</b></p> <p data-bbox="860 800 1489 1018">Specify a subnet address to add/remove to/from the table. The acceptable format is [network address/netmask] or [network address/prefix], such as 202.99.0.0/255.255.255.0 or 202.99.0.0/24. A single IP or an unusual subnet mask like "/255.255.255.255" or "/32" is unacceptable.</p> </div> <p data-bbox="617 1039 714 1073"><b>Action</b></p> <p data-bbox="860 1039 1490 1073">Select the action for the specified subnet.</p> <p data-bbox="860 1083 1490 1165"><b>Add to:</b> Add the specified subnet to the static IP-ISP table.</p> <p data-bbox="860 1176 1490 1257"><b>Remove from:</b> Remove the specified subnet from the static IP-ISP table.</p> |
| <b>Parameter</b> | Select the WAN links that are connected to the ISP network that this IP-ISP table indicates. Check the field of WAN link to select it. Multiple selection is allowed if more than one WAN link is connected to the same ISP network. Be ensure that the selected WAN links are exactly connected to the ISP network that the table indicates, or the Optimum Route might not run as excepted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>IP Query</b>  | Inquire if a single IP address is in the static IP table.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

When the source or destination IP of a packet matches an static IP-ISP table, Optimum Route determines a WAN link from the intersections of the WAN parameters here and the corresponding WAN parameters of a Auto Routing policy or Multihoming A/AAAA record policy, according to the traffic loading on the WAN ports. For example:

Auto Routing policy: Label=By\_OR, Algorithm=By Optimum Route, Parameter=1,2,3 (checked)

The matched IP-ISP table: Table Name=ISP\_A, Parameter=2,3,4 (checked)

Traffic matches a Auto Routing filter rule is processed by Auto Routing according to the corresponding policy "By\_OR". Optimum Rout is set to detect network by static IP-ISP table. Packet destination IP of the traffic matches the ISP's network of IP-ISP table "ISP\_A", which WAN links 2, 3 and 4 are connected to the ISP network. Optimum Route determines a WAN link for Auto Routing from WAN link 2 and WAN link3, which are the intersections of WAN links 1, 2, 3 (WAN parameters set in the AR policy) and WAN links 2, 3, 4 (WAN parameters set in the IP-ISP table). If traffic loading on WAN port 2 is currently heavier than WAN port 3, WAN link 3 will be the optimum link that Optimum Route decides for Auto Routing. The traffic will then be transferred through WAN link 3 by Auto Routing. For Multihoming with algorithm By Optimum Rout, the process is similar.

Here are the situations cause Optimum Route by IP-ISP table detection returning nothing to Auto Routing and Multihoming:

- Optimum Route returns nothing when the evaluated packet source and destination IP does not match any of the IP-ISP tables. This might because of incomplete collection of IP subnets of ISP networks. You can make the IP-ISP tables more complete by continuing IP subnets collecting and adding them to the tables. The more complete the IP subnets are, the better effect Optimum Route brings.
- Even if traffic matches an IP-ISP table, Optimum Route returns nothing when there is no intersection of Optimum Route's WAN parameters and Auto Routing (or Multihoming) policy's WAN parameters. Please make sure at least one intersected WAN link between the policies.

The traffic will be processes by Auto Routing according to the specified fail-over policy (see [Auto Routing](#)), if Optimum Route returns nothing to Auto Routing for the traffic. Multihoming will answer the IP address defined to the first WAN link in the A/AAAA record policy (see [Multihoming](#)), if Optimum Route returns nothing to Multihoming for the query.

## Dynamic Detect

Optimum Route's dynamic detection detects the round-trip time (RTT) of traffic targets and involves it to a dynamic calculation to determine the optimum WAN link for Auto Routing and Multihoming. Optimum Route spreads detection packets to a target through all the enabled WAN links to collect the transmission latency between the FortiWAN device and the target via each WAN link (ISP). In Optimum Route, this RTT will also represent the latency for data transmission through each WAN link between the FortiWAN device and the class C that the detection target belongs to. Fort example, if Optimum Route detects 20 ms, 30 ms and 40 ms RTTs between FortiWAN and a target 211.21.1.100 through WAN link 1, 2 and 3, a reference table as follow will be maintained and cached for a wile:

```
Subnet=211.21.1.0/24, WAN1=20ms, WAN2=30ms, WAN3=40ms
```

During the cache period, Optimum Route uses the values directly to calculate the optimum WAN link for any subsequent traffic that the target belongs to subnet 211.21.1.0/24. As for the target we are talking about, Optimum Route takes the destination IPs of out-going session packets as the targets if they matches the relevant Auto Routing policies, and takes the source IPs of DNS queries as the targets if they matches the relevant Multihoming A/AAAA record policies.

To determine an optimum WAN link, Optimum Route evaluates on availability of the candidates by calculating the weight of each WAN link. The calculation of weight involves the detected RTT and current traffic loading, which are combined in specified ratio. It seems making sense that the less the RTT is the optimum the WAN link is, but practically it is not necessarily that data transmission to a target through a WAN link with less RTT but serious traffic congestion on the WAN port is better than through a WAN link with higher RTT but the WAN port is in full-availability.

To enable dynamic detection for Optimum Route, it requires to have the following settings configured. It contains three parts:

- The protocol and procedure used for detecting RTT.
- The time period for caching detected RTT.
- The ratio of RTT and traffic loading for availability evaluation.

|                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Detection Protocol</b>                             | <p>ICMP and TCP are the protocols used to detect the RTT (Default: ICMP). ICMP (ping) or TCP (TCP connect request) packets are sent to a target through each of the enabled WAN links. So that system gets RTTs from the responses. Here are the options for the detection protocol:</p> <p><b>ICMP:</b> Using ICMP for detections.</p> <p><b>TCP:</b> Using TCP for detections</p> <p><b>ICMP, TCP:</b> Using ICMP for detections first. System will try TCP detection if the ICMP detections are declared failed.</p> <p><b>TCP, ICMP:</b> Using TCP for detections first. System will try ICMP detection if the TCP detections are declared failed.</p> |
| <b>Detection Period, in Seconds</b>                   | The time interval between retries if there is no response received for current detection. (Default: 3 seconds).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Number of Retries</b>                              | The times that system will retry if detections continue receiving no responses (Default: 3 retries). Retry will stop as long as a response is received, or system will declare the RTT detection is failed if all the retries receive no responses.                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Cache Aging Period, in Minutes</b>                 | The time period to cache the detected results (Default: 2880mins, ie. 2days). After the cache is cleaned, system will re-trigger detections for the same request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Weight of Round Trip Time :<br/>Weight of Load</b> | A parameter used to calculate the optimum route. It shows how much round trip time (RTT) and link load account for in calculating the optimum route. Note: The smaller the field value is, the less it accounts for in optimum route calculation.                                                                                                                                                                                                                                                                                                                                                                                                          |

## Port Speed/Duplex Settings

[Port Speed/Duplex Settings] enables to configure port speed and duplex transfer mode. Generally it is set to auto-detect by default which works properly in most cases. Manual speed/duplex mode configuration is still necessary in event that some old devices are either not supporting auto-detect, or incompatible with FortiWAN.

**Port Name** : The list of all physical ports on FortiWAN.

- Status** : The physical connection status of the port. It shows whether the port has been connected to other detectable network devices e.g. a hub.
- Speed** : The current speed of the port. It can be a value either manually set or auto-detected.
- Duplex** : The current duplex of the port. It can be a value either manually set or auto-detected.
- Settings** : You can opt for desirable settings, which can be manually set or auto-detected.
- MAC Address** : The MAC address of the port.
- HA** : Click to enable HA (switch between master and slave units) based on the status of network ports. While HA is enabled in FortiWAN, the port status of both master and slave FortiWAN units will be compared to determine which unit should be selected as master. Once the number of functioning network ports on the master unit becomes lower than that on the slave unit, the slave unit will then be switched as master instead. (Only the status of selected network ports will be compared.) Note: This field is not available if VRRP has been enabled in [Networking Setting > LAN Private Subnet] setting page.

## Backup Line Settings

In the deployment of multiple links, a link might serve as backup line which is inactive unless it matches the enabling criteria. The choice of backup lines mostly depends on cost, especially in areas where charges are based on data traffic. Backup lines in standby do not cost a cent, thus only basic fees are charged. Contrary to backup lines, main lines are lines commonly in use. The concept is to be used below.

FortiWAN provides log mechanism to the Backup Line service, see "[Log](#)".

### Threshold Parameters

- Backup Line Enable Time** : The interval to enable backup lines after main lines have broken down.
- Backup Line Disable Time** : The interval to disable backup line after main lines have returned to normal.

### Backup Line Rules table

Field Purpose / Description

- Main Line** : Select main lines, which can be multiple links.
- Backup Line** : Select backup lines.

- Algorithm** : 5 options to activate backup lines:
- All fail: when all lines defined in [Main line] are down
  - One fails: when one of the lines defined in [Main line] is down
  - Inbound bandwidth usage reached: when the inbound bandwidth consumption of all lines defined in [Main Line] reaches the defined level
  - Outbound bandwidth usage reached: when the outbound bandwidth consumption of all lines defined in [Main Line] reaches the defined level
  - Total traffic reached: when the total bandwidth consumption of all lines defined in [Main Line] reaches the defined level
- Parameter** : When the latter 3 options are chosen in [Algorithm], you can define here the bandwidth usage of the main lines over which backup lines are to be enabled.

## IP Grouping

IP Grouping is the configuration collect a group of IP addresses together for management purpose. An IP group could be the IP addresses belonging to a department, a physical region or some servers. It simplifies the configurations to most of the FortiWAN's policies. The predefined IP groups can be applied to the IP-based policies of the following FortiWAN's features:

- Firewall
- NAT
- Persistent Routing
- Auto Routing
- Virtual Server
- Bandwidth Management
- Connection Limit
- Cache Redirect
- Multihoming

### Geo IP database

The built-in Geo IP database contains mappings between geographical regions or countries and all public IP addresses that are known to originate from them. By specifying countries to IP groups and applying them to policies, FortiWAN can recognize the countries that connections originate from or destined to, and take the corresponding actions to the traffic according to the policies. For example, you can

- apply a geo IP to the destination field of a Auto Routing policy to route all the traffic destined to the country to specified WAN links.
- apply a geo IP to the source field of a Firewall policy to block all the accesses originated from the country.
- apply a geo IP to the source field of a Virtual Server policy to redirect all the connections originated from the country to the specified backend servers.

You can simply apply a geo IP to a policy to cover all the IP addresses of the country in the policy, rather than exactly knowing each of the IP addresses and manually setting policies for each of them.



## Configuring IP groups

To add an IP group, click the add button to create a configuration panel and complete the following fields:

| Fields                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Group Name</b>              | <p>Group name.</p> <p>The group name will be listed in the drop-down menus of the Source and Destination fields of the features that support IP Grouping.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Enabled</b>                 | <p>Check the field to enable the IP group.</p> <p>An IP group is available to the features only if it is enabled. Disabled IP groups will not be listed in the drop-down menus of the relative Source and Destination fields.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>IPv4/IPv6 Rules Setting</b> | <p>An IP group can contain multiple IP rule settings. Click the add button to create a new setting and complete the following fields.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>E</b>                       | <p>Check the field to add the IP address(es) to the IP group.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>IP Address</b>              | <p>Specify IPv4/IPv6 address(es) to the IPv4/IPv6 group by entering:</p> <ul style="list-style-type: none"> <li>• An single IPv4/IPv6 address</li> <li>• An IPv4/IPv6 range</li> <li>• An IPv4/IPv6 subnet</li> <li>• A Geo IP</li> <li>• A FQDN</li> </ul> <p>A Geo IP contains the mappings between a geographical region and all public IP addresses that are known to originate from it. For example, assigning the <b>Geo IP: Canada</b> to an IP group implies adding all the public IP addresses belonging to Canada to the IP group.</p>                                                                                                                                                                                                                                                                                             |
| <b>Action</b>                  | <p>Specify whether the specified IP address(es) belongs to the group or not.</p> <ul style="list-style-type: none"> <li>• <b>belong to:</b> by default the IP address(es) specified in the IP Address field belong to the group.</li> <li>• <b>not belong to:</b> set the IP address(es) specified in the IP Address field an exception to the group. This is usually used together with other IP rule settings in the same group. For example, when you have a complicated IP group containing lots of IP ranges, subnets or geo IPs and you just need to remove several IP addresses from the group, simply adding several IP rule settings to the group with selecting the not belong to option will be easier than finding the corresponding IP ranges or subnets and separating them. This is especially useful for geo IPs.</li> </ul> |

To collapse or expand configurations of an IP group or IP rule settings, click the arrow buttons on the banners.

## Service Grouping

[Service Grouping] lets you create and manage service groups exclusively and efficiently. You can group an ICMP, a TCP/UDP Port, and a group of TCP/UDP Ports, particular applications and server ports. These predefined service groups are available and easy to use in the drop-down list of the fields of [Source] and [Destination] on such [Service] submenus as [Firewall], [NAT], [Virtual Server], [Auto Routing], [Inbound BM], [Outbound BM].

**Group Name** : Assign a name to a service group e.g. MSN File Transfer. The name will appear in the drop-down list of [Source] and [Destination] in [Service] submenus mentioned previously.

**Enable** : Check the field to enable a service group. Once the service group has been enabled, it will show in the drop-down list of [Source] and [Destination] in [Service] submenus mentioned previously.

**Show/Hide IPv4/IPv6 Detail** : Click the button to show or hide the table details. After Hide Detail has been clicked, the table only shows the name of the service group and whether it has been enabled.

IPv4/IPv6 Rule Settings Table:

**E** : Check the field to add the list of services to the current service group.

**Service** : Enter a single or a set of ICMP / ICMPv6 or TCP / UDP ports. Single port follows the the format: port (xxx). A set of ports follow the format: xxx-yyy e.g. 6891-6900.

**Action** : Two options, to belong and not to belong, to determines whether service port defined in [Service] belongs to the service group. For exceptions in a set of service ports that belongs to the service group, the action of not to belong makes the configuration easier than separating the set of service ports into several groups.

Here is an example to elaborate on how to configure [Service Grouping]. Create a service group "MSN File Transfer", which uses TCP 6891-6900. Then enter TCP@6891-6900 in the [Service] field.

## Busyhour Settings

[Busyhour Settings] plays a crucial role in managing bandwidth. .Generally opening hours Mon-Fri: 09h00 to 18h00 is configured to be busy hours, for this period sees the advent of bandwidth-intensive applications in both intranet and extranet.

**Default Type** : Time segment unspecified in [Rules] below fall into this Default type either as idle or busy hours.

**Rules** : Defines time segment. The time segments are matched in sequence on a first-match basis. If none of the rules match, the default type is used. If time segment in [Default Type] is defined as idle hours, then unspecified time segment in this [Rules] is taken as idle hours as well.

**E** : Check the field box to add time segments in this list to [Rules].

**Day of Week** : Select a day of the week.

**From** : Start time.

**To** : End time.

**Type** : Defines the time segment, either busy or idle hours.

For the case that time period 09:00-18:00 from Monday to Saturday belongs to busy hour and only Sunday belongs to idle hour, set an idle rule for 00:00-00:00 on Sunday beyond a busy rule for Any day 09:00-18:00. The rule would be first matched from the top down.

As is shown in the figure, Sunday and hours beyond Mon-Sat: 09h00-18h00 are set to be idle hours. Remaining hours of the week belong to busy hours.

## Diagnostic Tools

Click the tabs [IPv4] and [IPv6] on the upper side to choice diagnostic tools for IPv4 and IPv6.

### IPv4

#### IPv4 ARP

Enforcement [ARP Enforcement] forces FortiWAN's attached PCs and other devices to update ARP table. Click [Enforce] and system will send out ARP packets force ARP updates throughout the attached devices. Generally the function is used only when certain devices in DMZ cannot access the Internet after FortiWAN has been installed initially.

#### IP Conflict Test

[IP Conflict Test] checks if any PC's IP address runs into conflict with that in WAN or DMZ settings in [Network Settings].

Click [Test] to start testing. And IP conflict message may be one of:

- Test completed, no IP conflict has been found.
- There is an IP conflict with a PC in DMZ, a public IP which has been assigned to WAN in [Network Settings] is now used in DMZ, for example. And the MAC address of this IP is also listed in the message.
- There is an IP conflict with a PC in WAN; a public IP has been assigned to DMZ in [Network Settings] is now used in WAN, for example. And the MAC address of this IP is also listed in the message.

## Clean IPv4 Session Table (Only Non-TCP Sessions)

The function is used to clean up non-TCP session tables in FortiWAN. In FortiWAN, protocols are managed with a session timer. Old sessions may be continuously retried by users that they keep unexpired. These old sessions, are always being valid and active instead of new ones. Hence, new sessions will not get into use unless session tables are cleaned up.

## IPv4 Ping & Trace Route

### Ping

[Ping] is used to detect network status. Enter an IP address or host name of target device. Select a port (WAN, LAN, or DMZ). If WAN port is selected, specify the WAN link number index. Details of ICMP error message and ping are outside the scope of this manual. Please refer to other documents for more information.

Note: If you ping a domain name, ensure DNS server have been specified in [System]->[Network Settings]->[DNS Server] (See "[Set DNS server for FortiWAN](#)").

### Trace

[Trace] is used to trace the route path of a packet from a specific port to destination host. Enter an IP address or host name of target device in [Target]. Select a link port (WAN, LAN, or DMZ). If WAN port is selected, specify the WAN link number index. [Host] can be an IP address or domain name of the target device.

Note: If you trace route with a domain name, ensure DNS server has been specified in [System]->[Network Settings]->[DNS Server] (See "[Set DNS server for FortiWAN](#)").

### Arping

[Arping] is used to detect the MAC address of a PC. Enter an IP address or host name of target device. Select a port (WAN, LAN, or DMZ). If WAN port has been selected, specify the WAN link number index. Details of ARP and error message are out of the scope of this manual; please refer to other documents for more information.

Note: If you arping with a domain name, ensure DNS server has been specified in [System]->[Network Settings]->[DNS Server] (See "[Set DNS server for FortiWAN](#)").

## IPv4 ARP Table Show & Clear

[IPv4 ARP Table Show & Clear] is used to display or clear the ARP information of certain port. Select a [port] and click [Show], to display the ARP information of this port. Or select a [port], click [Clear] to clean up the ARP information of this port, and confirm the message to clear. After this, a message shows that ARP table has been cleared successfully.

## Nslookup Tool

[Nslookup Tool] is used to inquire domain name of hosts. Enter a host in Target Domain. Select a host type from optical [Type] list: Any, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SOA, SRV, TXT; and select a server from optical [Server] list: Internal DNS, Multihoming, etc. Click [Nslookup] to start the inquiring session, and the domain name of target host will show in the field. Click [Stop] to halt the session.

## IPv6

### IPv6 Neighbor Discovery Enforcement

When IPv6 Neighbor Discovery is enforced, FortiWAN will send out a “neighbor discovery” packet to neighbor servers or network devices within the same network to request for a reply of IPv6 and MAC address of devices found.

### Clean IPv6 Session Table (Only Non-TCP Sessions)

The function is used to clean up non-TCP session tables in FortiWAN. In FortiWAN, protocols are managed with a session timer. Old sessions may be continuously retried by users that they keep unexpired. These old sessions, are always being valid and active instead of new ones. Hence, new sessions will not get into use unless session tables are cleaned up.

### IPv6 Ping & Trace Route

#### Ping

[Ping] is used to detect network status. Enter an IP address or host name of target device. Select a port (WAN, LAN, or DMZ). If WAN port is selected, specify the WAN link number index. Details of ICMP error message and ping are outside the scope of this manual. Please refer to other documents for more information.

Note: If you ping a domain name, ensure DNS server have been specified in [System]->[Network Settings]->[DNS Server] (See "[Set DNS server for FortiWAN](#)").

#### Trace

[Trace] is used to trace the route path of a packet from a specific port to destination host. Enter an IP address or host name of target device in [Target]. Select a link port (WAN, LAN, or DMZ). If WAN port is selected, specify the WAN link number index. [Host] can be an IP address or domain name of the target device.

Note: If you trace route with a domain name, ensure DNS server has been specified in [System]->[Network Settings]->[DNS Server] (See "[Set DNS server for FortiWAN](#)").

#### Arping

[Arping] is used to detect the MAC address of a PC. Enter an IP address or host name of target device. Select a port (WAN, LAN, or DMZ). If WAN port has been selected, specify the WAN link number index. Details of ARP and error message are out of the scope of this manual; please refer to other documents for more information.

Note: If you arping with a domain name, ensure DNS server has been specified in [System]->[Network Settings]->[DNS Server] (See "[Set DNS server for FortiWAN](#)").

### IPv6 Neighbor Table Show & Clear

[IPv6 Neighbor Table Show & Clear] is used to display or clear the IPv6 and MAC address of neighbor servers or devices. Select a [port] and click [Show], to display the neighbor information of this port. Or select a [port], click [Clear] to clean up the neighbor information of this port, and confirm the message to clear. After this, a message shows that neighbor table has been cleared successfully.

## Nslookup Tool

[Nslookup Tool] is used to inquire domain name of hosts. Enter a host in Target Domain. Select a host type from optical [Type] list: Any, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SOA, SRV, TXT; and select a server from optical [Server] list: Internal DNS, Multihoming, etc. Click [Nslookup] to start the inquiring session, and the domain name of target host will show in the field. Click [Stop] to halt the session.

## Tcpdump

- Interface** : Tcpdump can capture FortiWAN data packets and download captured packets to local host for analysis and debug. Firstly, select an interface from [Interface] to capture packets. In its drop-down list, tunnel will display if Tunnel Routing has been configured. Option [Any] enables all interfaces to capture packets.
- Timeout** : Set [Timeout] value. Once time is over, capture will stop. Lastly, click [Start] to start capturing and download intercepted packets to local host. It should be noted that FortiWAN does not store the Tcpdump packets. Click [Stop] to stop capturing.

## Setting the system time & date

[Date/Time] lets you configure time, date, and time zone. [Date] follows the year/month/day date format, and [Time] uses 24-hour time system in the hour:minute:second format. [Time Zone] is represented by continent and city, [America] and [New York], for example. FortiWAN uses NTP time server for accurate time synchronization, simply by clicking the [Synchronize Time] button. And other time servers are also included in the drop-down list which can be added or deleted at your preference.

## Remote Assistance

Enabling this function allows Fortinet's technical support specialist to enter your system for further troubleshooting when assistance is needed. FortiWAN allows technical support specialist to access the Web UI and backend system remotely, so as to assist users promptly upon the occurrence of problems. Remote assistance opens both TCP ports 443 for web UI and 23 for SSH debug.

Note: To enter the backend system via SSH login, a debug patch file is required.

- Enable** : Click the checkbox to enable Remote Assistance.
- Server** : Enter the server IP address given by Fortinet's technical support specialist.
- Security Code** : Displays the security code required for remote logins. This security code is automatically generated after clicking Apply to complete Remote Assistance settings, and is updated after every system reboot.

## Administration

Go to **System > Administration**, **Administration** lets you perform administrative tasks, including changing passwords of Administrator and Monitor. Every FortiWAN is shipped with the same default passwords. For security concerns, it is thus strongly recommended that the passwords shall be changed.

By default, FortiWAN uses 443 as the Web UI login port. And it allows administrators to change the port, to avoid possible port conflict caused for virtual server services.

**Update/downgrade** section enables to update or downgrade firmwares once new firmwares are available (from our website or dealers). Simply click the Update/Downgrade button and follow exactly the on-screen instructions.

**Configuration Files** gives you the ability to back up configuration files, by clicking the [Save] button. Or you can click [Restore] to reload the previous backup files to FortiWAN. System configurations can be recovered from failures via the backup configuration files.

In **Maintenance**, you can restore factory default configurations and reboot FortiWAN. Due to the limitation of HTML syntax, no hint displays after reboot has been completed. Thus you have to wait about two minutes before navigating to Web UI in browser.

## Administrator and Monitor Password

FortiWAN maintains a common local authentication database for its Web UI, CLI and SSH login (See "[Connecting to the Web UI and the CLI](#)"). Accounts for authentication are classified into two groups, Administrator and Monitor, with different permissions. Accounts belonging to Administrator have the permission to monitor and modify system parameters via Web UI, CLI and SSH login, while limited operations are allowed (monitor system information and traffic statistics via Web UI ONLY) to accounts belonging to Monitor. Configurations applying, system administrations (managements introduced in this topic), Tunnel Routing Benchmark, CLI access and SSH login are invalid for Monitor group. Note that page **System > Administration** is not available to Monitor accounts.

### Default account/password

While the first time you login to Web UI, you see the default accounts here. "Administrator" and "admin" are the default accounts of group Administrator, and "Monitor" is the default account of group Monitor. Passwords of accounts "Administrator" and "Monitor" are "1234" and "5678" respectively; password of account "admin" is null (See "[Appendix A: Default Values](#)"). All the accounts (default and customized) of group Administrator are able to log into Web UI, CLI and SSH login. All the accounts are case sensitive.

### Create, modify and delete the account and password for Administrators or Monitors.

|                       |                                                                                                                                                   |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Account</b> | You can select and configure an account (old or new). If you select the current login account, [Add Account] button will change to [Set Account]. |
| <b>New Account</b>    | Allows you to add a new account. Enter the new account ID here.                                                                                   |
| <b>New Password</b>   | Enter the new password after you have added or modified an account.                                                                               |
| <b>Password</b>       | Verification Confirm the new password.                                                                                                            |



FortiWAN employs the same local authentication database for both Web UI and CLI, which implies it will be unable to reset password to default if the administrator password get lost. FortiWAN provides a special process to recover the password, see [Appendix C: What if your password is lost?](#).

## Event notifications via SNMP trap

You can receive notification via SNMP trap for any modification of the FortiWAN's account. Configure the SNMP manager on your FortiWAN and enable the event type "Account change" to notify (See "[Notification](#)"), then notification will be delivered to your SNMP manager for the events. The correspondent MIB fields and OIDs are listed as following:

### SNMP field names and OIDs

| MIB Field                       | OID                           | Description                                                                                |
|---------------------------------|-------------------------------|--------------------------------------------------------------------------------------------|
| fwnEventAdminAccountPwChanged   | 1.3.6.1.4.1.12356.118.3.1.1.1 | Send event notification when the password of an account in Administrator group is changed. |
| fwnEventAdminAccountAdded       | 1.3.6.1.4.1.12356.118.3.1.1.2 | Send event notification when an account is added into Administrator group.                 |
| fwnEventAdminAccountRemoved     | 1.3.6.1.4.1.12356.118.3.1.1.3 | Send event notification when an account is removed from Administrator group.               |
| fwnEventMonitorAccountPwChanged | 1.3.6.1.4.1.12356.118.3.1.1.4 | Send event notification when the password of an account in Monitor group is changed.       |
| fwnEventMonitorAccountAdded     | 1.3.6.1.4.1.12356.118.3.1.1.5 | Send event notification when an account is added into Monitor group.                       |
| fwnEventMonitorAccountRemoved   | 1.3.6.1.4.1.12356.118.3.1.1.6 | Send event notification when an account is removed from Monitor group.                     |

## RADIUS Authentication

Except FortiWAN's local authentication database described above, FortiWAN supports RADIUS authentication for Web UI login. Please make sure the following settings are complete on the RADIUS server working with FortiWAN.

Add Fortinet's Vender Specific Attribute (VSA) to `/etc/raddb/dictionary`:

```
VENDOR Fortinet 12356
```



```

BEGIN-VENDOR Fortinet
...
ATTRIBUTE Fortinet-FWN-AVPair 26 string
...
END-VENDOR Fortinet

```

"12356" is Fortinet's vender ID, "Fortinet-FWN-AVPair" is the attribute used for working with FortiWAN and "26" is the attribute ID. If the RADIUS server serves with other Fortinet products, please add the correspondent attributes between BEGIN-VENDOR Fortinet and END-VENDOR Fortinet.

Construct user database on RADIUS server for authentication. For example, we have accounts "Administrator/1234" and "admin/(null)" belong to Administrator group, and "Monitor/5678" belongs to Monitor group.

Add the followings to /etc/raddb/users:

```

Administrator User-Password := "1234"
Fortinet-FWN-AVPair := "user-group=Administrator"
admin User-Password := ""
Fortinet-FWN-AVPair := "user-group=Administrator"
Monitor User-Password := "5678"
Fortinet-FWN-AVPair := "user-group=Monitor"

```

Please make sure "user-group" is specified for every account, or FortiWAN denies the login even the account and password are authorized by RADIUS server.

To enable FortiWAN's RADIUS authentication, please click the checkbox and complete the configuration below.

|                    |                                                                                                                                                                                                                                                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Priority</b>    | <p>Determines priority to the two authentications:</p> <p>RADIUS, Local Database: Authorize a login via RADIUS first, then try local database if the authentication failed in RADIUS.</p> <p>Local Database, RADIUS: Authorize a login via local database first, then try RADIUS if the authentication failed in local database.</p> |
| <b>Server IP</b>   | IP address of the RADIUS server.                                                                                                                                                                                                                                                                                                     |
| <b>Server Port</b> | UDP port number of the RADIUS server (The standard port is 1812, but it might be 1645 for earlier RADIUS).                                                                                                                                                                                                                           |
| <b>Secret</b>      | The secret (password) shared with the RADIUS server.                                                                                                                                                                                                                                                                                 |
| <b>NAS IP</b>      | Enter the correspondent NAS-IP-Address attribute for Request/Response Authenticator if it is necessary, or leave it blank. See RFC2865 for details.                                                                                                                                                                                  |
| <b>NAS Port</b>    | Enter the correspondent NAS-Port attribute for Request/Response Authenticator if it is necessary, or leave it blank. See RFC2865 for details.                                                                                                                                                                                        |
| <b>Apply</b>       | Click to apply the configuration.                                                                                                                                                                                                                                                                                                    |

## Firmware Update (via Web UI)

Click [**Update**] or [**Downgrade**] and follow the on-screen instructions to perform firmware update/downgrade. Note that firmware downgrade will reset current configurations to factory default, please backup current

configurations in advance. Firmware update and downgrade support jump directly to a version from current version without applying all the updates or downgrades that have been released between the versions.

Updating the FortiWAN Firmware:

- Before proceeding with the firmware update, ALWAYS backup system configurations.
- Obtain the latest firmware upgrade pack from <https://support.fortinet.com>.
- Log onto the Web UI with administrator account and go to [System]→ [Administration].
- Click on "Update".
- Use [**Browse...**] to select the path of the new firmware image.
- For **High Availability (HA) deployment** (See "[FortiWAN in HA \(High Availability\) Mode](#)"), check [**Update Slave**] to perform firmware update on the slave unit at the same time. Please double check and make sure the peer device is under normal condition (from page [System > Summary]) before HA firmware update.
- Click [**Upload File**] to start updating.
- The firmware update will take a while, so please be patient. During the update process, be sure NOT to turn off the system or unplug the power adapter. DO NOT click on the [Upload] button more than once.
- Update is completed when the "Update succeeded" message appears. FortiWAN unit(s) will reboot automatically then.

Errors that occur during the update can be caused by any reason below:

- **General error** – Please contact your dealer if this happens repeatedly.
- **Invalid update file** – The file uploaded for firmware update is invalid, please make sure the uploaded file is correct.
- **MD5 checksum error** – Image file is damaged. Please reload and try again.
- **Incompatible version/build** – Firmware version incompatible. System requires a higher version firmware for update and a lower version firmware for downgrade. Check with your dealer for the correct firmware version.
- **Incompatible model/feature** – Firmware image does not match the FortiWAN system. Check with your dealer for the correct model and version.
- **Incompatible platform** – Firmware image does not match the current FortiWAN platform. Check with your dealer for the correct model and version.
- **Update error** – If this error message appears during firmware update, please do not turn off the device and contact your dealer immediately.
- **Unknown error** – Contact your dealer.

When a firmware update has being processed in system, users (multi-account login, see "[Using the Web UI](#)") are unable to perform concurrent firmware updates at the same time.

## Firmware Upgrade/Downgrade via CLI

The CLI upgrade procedure replaces the firmware on the default partition and reboots.

### Before you begin:

- Read the release notes for the version you plan to install. If information in the release notes is different from this documentation, follow the instructions in the release notes.
- You must be able to use TFTP to transfer the firmware file to the FortiWAN. Download and install a TFTP server, like tftpd (Windows, Mac OS X, or Linux), on a server on the same subnet as the FortiWAN.
- Download the firmware file from the Fortinet Customer Service & Support website: <https://support.fortinet.com/>
- Copy the firmware image file to the root directory of the TFTP server.

- Back up your configuration before beginning this procedure (see [Configuration File](#)).
- Connect to CLI (see [To connect to the CLI](#))



TFTP is not secure, and it does not support authentication. You should run it only on trusted administrator-only networks, and never on computers directly connected to the Internet. Turn off tftpd off immediately after completing this procedure.

#### To install firmware via the CLI:

1. Connect your management computer to the FortiWAN console port using an RJ-45-to-DB-9 serial cable.
2. Use an Ethernet cable to connect FortiWAN's HA port to the TFTP server directly, or connect it to the same subnet as the TFTP server.
3. Restart the FortiWAN through the reboot command (initiate a connection to the CLI and log in as the user admin) or turning the power off and on.
4. Press any key when you see the following information on the screen:

```
FortiBootLoader
FortiWAN-200B (18:52-01.08.2015)
Ver:00010001
Serial number:FWN2HB3616000032
Total RAM: 2048MB
Boot up, boot device capacity: 971MB.
Press any key to display configuration menu...
...
```

5. You will see the menu as the following:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
```

```
Enter Selection [G]:
Enter G,F,B,Q, or H:
```

6. Enter **G** for upgrading firmware image from TFTP server.
7. Configure the following settings:

```
Enter TFTP server address [192.168.1.168]: The IP address of the TFTP server, such
as 192.168.0.12.
```

```
Enter local address [192.168.1.188]: The IP address assigned to the HA port for TFTP
transmission, such as 192.168.0.2.
```

```
Enter firmware image file name [image.out]: The file name of the firmware image file,
such as FWN2HB-V400-build0267-FORTINET.out.
```

8. It starts get the firmware image file from the TFTP server
9. Enter **D** to locate the firmware in default partition when you see the following information:

```
MAC:000D48309D17
#####
#####
Total 94177227 bytes data downloaded.
Verifying the integrity of the firmware image..
```

```
Total 103376kB unzipped.
Save as Default firmware/Backup firmware:[D/B]?
```

#### 10. The FortiWAN starts to boot with the new firmware image:

```
Programming the boot device now.
.....
.....
Reading boot image 4265472 bytes.
Initializing FortiWAN...
fortiwan login:
```

---

The same steps can also be used for firmware downgrade.

Please make sure that you are using the correct firmware image file corresponding to your FortiWAN model, or it might block the FortiWAN from booting. This procedure replaces the firmware image on the default partition without validating the image.

Incompatible configurations may also cause failure to system booting after firmware downgrade, for example that configuration of link aggregation on releases later than 4.3 is incompatible to 4.1 and 4.0.



If the FortiWAN fails to boot up after upgrading/downgrading firmware from TFTP, you can:

- Reboot the FortiWAN.
  - Press any key when you see `Press any key to display configuration menu...` on the console.
  - Select `B` to boot the FortiWAN with the backup firmware.
- 

## Configuration File

Click [Save] to back up the current configurations of all functions in one binary file on your PC. Click [Show] to display a binary configuration file (.cfg) as readable content. Click [Restore] to recover whole system with the backed up configurations. Note that Restore will apply the configurations to system and then perform synchronization to the slave unit if HA mode is deployed. After this, system automatically reboot. The configuration file here is in binary format and should NOT be edited outside of FortiWAN tools and systems. The configuration file here contains all the configurations of FortiWAN's functions. You can have individual configuration file of every single function via the export function in every function page. Do NOT to turn off the power while restoring the configuration file, or repetitively clicking on the [Restore] button.

Configuration File for individual function Export and Import:

- Log on to FortiWAN as administrator. On every single function page of Web UI, click [Export Configuration] to back up the configuration in an editable text file.
- To import the previously saved configuration file, click [Browse] on the function page of Web UI to select the configuration file previously saved, and then click [Import Configuration] to import previous configurations. The imported configuration will be displayed on the Web UI, but not be applied to system. Click [Apply] button to apply it to system.

During the configuration file restoration process, if an error occurs, it is most likely the result of one of the following:

- The total WAN bandwidth setting in the restored configuration file exceeds the max bandwidth defined for the current system. The bandwidth can be either upload stream and download stream.
- The restored configuration file contains port numbers exceeding the port numbers defined by the system.
- The restored configuration file contains VLAN parameters not supported by the machine.
- The total number of WAN links in the restored configuration file exceeds the current system definition.
- Incompatible versions and/or systems.

Note:

- FortiWAN does not guarantee full compatibility of configuration files for different models.
- After the firmware upgrade, it is encouraged to backup the configuration file.

Configuration file backup and restore are available in the following function page:

| Function Page                          | File Name                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [System > Network]                     | network.txt                                                                                                                                                                                                                                                                                                                                    |
| [System > WAN Link Health Detection]   | wan-link-health-detection.txt                                                                                                                                                                                                                                                                                                                  |
| [System > Optimum Route Detection]     | optimum-route.txt                                                                                                                                                                                                                                                                                                                              |
| [System > Port Speed / Duplex Setting] | port-speed.txt                                                                                                                                                                                                                                                                                                                                 |
| [System > Backup Line Setting]         | backup-line.txt                                                                                                                                                                                                                                                                                                                                |
| [System > IP Grouping]                 | <ul style="list-style-type: none"> <li>• Click [Import] &amp; [Export], you may backup and restore configurations of ip list in a file named ip-list.txt.</li> <li>• Click [Import Configuration] &amp; [Export Configuration], you may backup and restore configurations of IP Grouping saved in ip-group.txt.</li> </ul>                     |
| [System > Service Grouping]            | <ul style="list-style-type: none"> <li>• Click [Import] &amp; [Export], you may backup and restore configurations of service list in a file named service_list.txt.</li> <li>• Click [Import Configuration] &amp; [Export Configuration], you may backup and restore configurations of Service Grouping saved in service-group.txt.</li> </ul> |
| [System > Busyhour Setting]            | busy-hour.txt                                                                                                                                                                                                                                                                                                                                  |
| [Service > Firewall]                   | firewall.txt                                                                                                                                                                                                                                                                                                                                   |
| [Service > NAT]                        | nat.txt                                                                                                                                                                                                                                                                                                                                        |
| [Service > Persistent Routing]         | persistent-routing.txt                                                                                                                                                                                                                                                                                                                         |
| [Service > Auto Routing]               | auto-routing.txt                                                                                                                                                                                                                                                                                                                               |

| Function Page                    | File Name                                                |
|----------------------------------|----------------------------------------------------------|
| [Service > Virtual Server]       | virtual-server.txt                                       |
| [Service > Bandwidth Management] | bandwidth-management.txt                                 |
| [Service > Connection Limit]     | connection-limit.txt                                     |
| [Service > Cache Redirect]       | cache-redirect.txt                                       |
| [Service > Multihoming]          | multihoming.txt                                          |
| [Service > Internal DNS]         | Internal-nameserver.txt                                  |
| [Service > SNMP]                 | snmp.txt                                                 |
| [Service > IP-MAC Mapping]       | ip-mac-mapping.txt                                       |
| [Service > DNS Proxy]            | dnsproxy.txt                                             |
| [Service > Tunnel Routing]       | tunnel-routing.txt                                       |
| [Log > Control]                  | log-control.txt (This file includes Mail/FTP passwords.) |
| [Log > Notification]             | notification.txt (This file includes email/password)     |
| [Log > Link Report]              | link-report.txt                                          |

## Maintenance

Click [Factory Default] to reset configurations to factory default. Or you can perform “resetconfig” command in console. Click [Reboot] to reboot FortiWAN. For information on console command, please refer to [Console Mode Commands](#).

## Web UI Port

Type the port number in [New Port] and then click [Setport]. Enter the new port number when you log in again into Web UI. Additionally, the new port shall avoid conflict with FortiWAN reserved ports when configuring the port. Otherwise, FortiWAN will display error message of port settings failure and resume to the correct port number that was configured last time.

| Port | Service | Port | Service  | Port | Service |
|------|---------|------|----------|------|---------|
| 1    | tcpmux  | 102  | iso-tsap | 530  | courier |
| 7    | echo    | 103  | gppitnp  | 531  | Chat    |

| Port | Service   | Port | Service       | Port  | Service           |
|------|-----------|------|---------------|-------|-------------------|
| 9    | discard   | 104  | acr-nema      | 532   | netnews           |
| 11   | systat    | 109  | pop2          | 540   | uucp              |
| 13   | daytime   | 110  | pop3          | 556   | remotefs          |
| 15   | netstat   | 111  | sunrpc        | 563   | nnntp+ssl         |
| 17   | qotd      | 113  | auth          | 587   |                   |
| 19   | chargen   | 115  | sftp          | 601   |                   |
| 20   | ftp-data  | 117  | uucp-path     | 636   | ldap+ssl          |
| 21   | ftp-cntl  | 119  | nnntp         | 993   | imap+ssl          |
| 22   | ssh       | 123  | NTP           | 995   | pop3+ssl          |
| 23   | telnet    | 135  | loc-srv/epmap | 1111  | FortiWAN reserved |
| 25   | smtp      | 139  | netbios       | 1900  | FortiWAN reserved |
| 37   | time      | 143  | imap2         | 2005  | FortiWAN reserved |
| 42   | name      | 179  | BGP           | 2049  | nfs               |
| 43   | nickname  | 389  | ldap          | 2223  | FortiWAN reserved |
| 53   | domain    | 465  | smtp+ssl      | 2251  | FortiWAN reserved |
| 77   | priv-rjs  | 512  | print/exec    | 3535  | FortiWAN reserved |
| 79   | finger    | 513  | login         | 3636  | FortiWAN reserved |
| 87   | ttylink   | 514  | shell         | 4045  | Lockd             |
| 95   | supdup    | 515  | printer       | 6000  | x11               |
| 101  | hostriame | 526  | tempo         | 49152 | FortiWAN reserved |

## License Control

License Control provides users with all the License Key configurations, including:

### Bandwidth Upgrade License:

FortiWAN provides various bandwidth capabilities for individual model. Bandwidth upgrade on models is supported via a license key. You could ask your distributor for bandwidth upgrade license keys.

- FortiWAN 200B provides 200 Mbps, 400 Mbps and 600 Mbps bandwidth capability.
- FortiWAN 1000B provides 1 Gbps, and 2 Gbps.
- FortiWAN 3000B provides 3 Gbps, 6 Gbps, and 9 Gbps bandwidth capability.

Product Model Bandwidth Capability

| Product Model  | Bandwidth Capability           |
|----------------|--------------------------------|
| FortiWAN 200B  | 200 Mbps / 400 Mbps / 600 Mbps |
| FortiWAN 1000B | 1 Gbps / 2 Gbps                |
| FortiWAN 3000B | 3 Gbps / 6 Gbps / 9 Gbps       |

Note: Conditional bandwidth upgrade is provided for old models. Please contact customer support to gain further information.

## Login Session Management

The administration login sessions to Web UI and CLI can be managed individually by configuring the inactivity timeout duration. A login session will be expired and logged off after the given time of inactivity.

Go to **System > Administration > Idle Timeout**, and configuration the following settings:

|                    |                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Web Timeout</b> | Set the timeout duration in seconds for Web UI login sessions. The valid value is a integer between 60~28800. Click the Apply button to save the setting. |
| <b>CLI Timeout</b> | Set the timeout duration in seconds for CLI login sessions. The valid value is a integer between 60~28800. Click the Apply button to save the setting.    |

For CLI login sessions, pressing Enter can reset the timer. For Web UI login sessions, the following actions will reset the timer:

- Switching GUI page from the main menu.
- Click the Apply or Reload button on the upper bar.
- Click the Import/Export buttons on the Web UI pages.
- Click the Synchronize Time button on System > Date/Time page.
- Click the buttons on System > Administrator page.
- Operations of TR Benchmark and Diagnostic Tools.
- Click the Show, Refresh, Clear All/Clear, Reset, Re-Connect All/Reconnect buttons on related Statistics pages.



- Switch Log Type or click the Refresh, Clear, Push Now, Send Test E-mail Now button on related Log pages.
- Click the buttons on Reports > Settings pages.
- Change Date, execute an export action, open the Email window, execute email send now, save an email server or schedule, add to an existing schedule, apply filters or execute Drill-in on all the Reports pages.

# Load Balancing & Fault Tolerance

With the rapid proliferation and decreasing prices of broadband solutions, more and more small and medium enterprises are opting for the use of multiple WAN links from various ISPs. The benefits include:

- Single link failure does not result in a total loss of internet connectivity, thus WAN reliability increases.
- Traffic can be evenly dispersed across multiple WAN links, resulting in increased efficiency and improved performance of bandwidth.
- Multiple WAN links for fault tolerance and load balancing has two advantages:
  - The outbound traffic, i.e. traffic originating from LAN traveling outwards, can be load-balanced across multiple WAN links. This is [Auto Routing](#).
  - Traffic from the WAN, i.e. traffic originating from WAN traveling towards the LAN, can be load-balanced across multiple WAN links. This is [Multihoming](#).

## Load Balancing Algorithms

Load balancing algorithm is one of the important components for achieving purpose of traffic load balancing via FortiWAN's various services, such as Auto Routing, Multihoming, Tunnel Routing, Virtual Server and DNS Proxy. These services distribute inbound or outbound traffic over multiple resources (WAN links or internal servers) according to predefined policies, which consist of a load balancing algorithm and the participating resources. A Load balancing algorithm dynamically evaluates on the availability of the participants against factors such as weight, connections or traffic, and picks an appropriate one for the load balancing services assign traffic to. When traffic (sessions or packets) matches a filter rule or policy of a load balancing service, the corresponding algorithm (specified to the policy) determines the appropriate one from the specified resources for the service to handle the traffic. All the load balancing services detect and label the unavailable resources by their own mechanism, such as WAN link health detection (see [WAN Link Health Detection](#)). The algorithms will ignore the failed resources and work with the available ones.

The followings are the algorithms that FortiWAN provides for services Auto Routing, Multihoming, Tunnel Routing, Virtual Server and DNS Proxy.

|                  | Auto Routing | Multihoming | Tunnel Routing | Virtual Server | Proxy DNS |
|------------------|--------------|-------------|----------------|----------------|-----------|
| Round-Robin      | O            | O           | O              | O              | O         |
| By Connection    | O            |             |                | O              |           |
| By Upstream      | O            | O           | O              |                | O         |
| By Downstream    | O            | O           |                |                | O         |
| By Total Traffic | O            | O           |                |                | O         |

|                  | Auto Routing | Multihoming | Tunnel Routing | Virtual Server | Proxy DNS |
|------------------|--------------|-------------|----------------|----------------|-----------|
| By Optimum Route | O            | O           |                |                |           |
| By Response Time |              |             |                | O              |           |
| By Static        |              | O           |                |                |           |
| By Fixed         | O            |             |                |                |           |
| Fail-Over        |              | O           |                |                |           |
| Hash             |              |             |                | O              |           |

**See also**

[Outbound Load Balancing and Failover \(Auto Routing\)](#)

[Inbound Load Balancing and Failover \(Multihoming\)](#)

[Tunnel Routing](#)

[Virtual Server & Server Load Balancing](#)

[DNS Proxy](#)

**Round Robin (weighted)**

Weight Round Robin picks one of the participating resources in circular order according to the specified weights. Round Robin works without considering resource's ability such as processing connections, available bandwidth and response time. In FortiWAN, algorithm Round Robin serves for Auto Routing, Multihoming, Tunnel Routing, Virtual Server and DNS Proxy (it is called By Weight in DNS Proxy). To create a load balancing policy with Round Robin, you need specify the participants (WAN links or internal servers) and assign the weight to each of them. For example, if three WAN links (WAN1, WAN2 and WAN3) are defined in an Auto Routing policy with weight 3:1:2, Round Robin returns one of the three WAN links to Auto Routing in the order of WAN1, WAN1, WAN1, WAN2, WAN3, WAN3. So that Auto Routing can distribute sessions to WAN links in the order. If some of the participants get failed, Round Robin will ignore them and work with the rest participants. For example, if WAN2 goes to failure, then Round Robin return the WAN link to Auto Routing in the order of WAN1, WAN1, WAN1, WAN3, WAN3.

Round Robin works similarly for Multihoming, Tunnel Routing, Virtual Server and DNS Proxy. For the details of configuring a policy of a service, see the section relevant to each of them.

**By Connection**

By connection picks one of the participating resource (WAN links or internal servers) for Auto Routing and Virtual Server, but the processes that By Connection works for Auto Routing and Virtual Server are totally different. For Auto Routing, an idea of weighted Round Robin is involved in the By Connection algorithm. The goal of Auto Routing's By Connection is to guarantee the number of connections being processed by each participating WAN link in a fixed weight. By Connection counts the number of connections running on each participating WAN link and picks one for a new-coming connection to keep the ration of connections running on the WAN links closely

fixed after adding the new connection to the picked one. For example, there are three WAN links (WAN1, WAN2 and WAN3) are defined in an Auto Routing policy with weight 1:1:2. By Connection will respectively return WAN1, WAN2 and WAN3 to Auto Routing for the first three connections, if all the three WAN links are idle. So far, the count of connections running on WAN1, WAN2 and WAN3 goes to 1:1:1. To match the specified weight 1:1:2 of the policy, By Connection will return WAN3 for the forth connection. Next, By Connection returns WAN1 and WAN2 respectively for the fifth and sixth connections and so the count goes to 2:2:2. Obviously, By Connection will return WAN3 for the next two (seventh and eighth) connections, so that the count will be 2:2:4 which is in the ratio 1:1:2. Considering the two connections on WAN2 are closed (the counts become 2:0:4), By Connection must return WAN2 for the next two connections to keep the counts be in ratio 1:1:2. If some of the participants get failed, By Connection will ignore them and work with the rest participants. For example, if WAN2 goes to failure, By Connection will work by keeping the connection count on WAN1 and WAN3 in weight 1:2.

|                                         | WAN1 | WAN2 | WAN3 |
|-----------------------------------------|------|------|------|
| <b>Weight</b>                           | 1    | 1    | 2    |
| Connection 1                            | V    |      |      |
| Connection 2                            |      | V    |      |
| Connection 3                            |      |      | V    |
| Connection 4                            |      |      | V    |
| <b>Connection counts</b>                | 1    | 1    | 2    |
| Connection 5                            | V    |      |      |
| Connection 6                            |      | V    |      |
| Connection 7                            |      |      | V    |
| Connection 8                            |      |      | V    |
| <b>Connection counts</b>                | 2    | 2    | 4    |
| The two connections on WAN2 are closed. |      |      |      |
| <b>Connection counts</b>                | 2    | 0    | 4    |
| Connection 9                            |      | V    |      |
| Connection 10                           |      | V    |      |
| <b>Connection counts</b>                | 2    | 2    | 4    |
| Connection 11                           | V    |      |      |
| <b>Connection counts</b>                | 3    | 2    | 4    |

|                                                                               | WAN1 | WAN2 | WAN3 |
|-------------------------------------------------------------------------------|------|------|------|
| One of the connections on WAN2 and one of the connections on WAN4 are closed. |      |      |      |
| <b>Connection counts</b>                                                      | 3    | 1    | 3    |
| Connection 12                                                                 |      | V    |      |
| Connection 13                                                                 |      | V    |      |
| Connection 14                                                                 |      |      | V    |
| Connection 15                                                                 |      |      | V    |
| Connection 16                                                                 |      |      | V    |
| <b>Connection counts</b>                                                      | 3    | 3    | 6    |

As for Virtual Server, By connection treats service requests coming from the same source IP address as the same connection. The algorithm determine an internal server from server pool for incoming requests of a connection by hashing source IP address of the connection. The hash mechanism that By connection uses is the same as algorithm Hash (see section Hash later). Every internal server in the server pool has the same weight for By connection's hash mechanism.

## By Downstream Traffic

By Downstream Traffic picks one of the participating resources (WAN links) according to the weight mainly relevant to their data downloading availability. Each of the participating WAN links is weighted every three seconds by summing 80% available inbound bandwidth and 20% available outbound bandwidth up. For example, there is an Auto Routing policy with participants WAN1, WAN2 and WAN3. If, at some time, the available inbound bandwidth on WAN1, WAN2 and WAN3 is 4Mbps, 10Mbps and 6Mbps, and the available outbound bandwidth on WAN1, WAN2 and WAN3 is 8Mbps, 5Mbps and 20Mbps, the weight of each WAN link is so that calculated as:

$$\text{WAN1: } 0.8 \times (4/10) + 0.2 \times (8/20) = 0.4$$

$$\text{WAN2: } 0.8 \times (10/10) + 0.2 \times (5/20) = 0.85$$

$$\text{WAN3: } 0.8 \times (6/10) + 0.2 \times (20/20) = 0.68$$

Before the weights are updated next time, By Downstream Traffic returns one of the three WAN links for the load balancing policy in circular order with weight 40:85:68. Weights will be updated by calculating with real-time available bandwidth every three seconds. By Downstream Traffic serves for Auto Routing, Multihoming and DNS Proxy.

## By Upstream Traffic

By Upstream Traffic serves Auto Routing, Multihoming, Tunnel Routing and DNS Proxy. However, the process that By Upstream Traffic works for Tunnel Routing is different from Auto Routing, Multihoming and DNS Proxy. For working with Auto Routing, Multihoming and DNS Proxy, By Upstream Traffic picks one of the participating

resources (WAN links) according to the weight mainly relevant to their data uploading availability. Each of the participating WAN links is weighted every three seconds by summing 80% available outbound bandwidth and 20% available inbound bandwidth up. For the same example, there is an Auto Routing policy with participants WAN1, WAN2 and WAN3. If, at some time, the available inbound bandwidth on WAN1, WAN2 and WAN3 is 4Mbps, 10Mbps and 6Mbps, and the available outbound bandwidth on WAN1, WAN2 and WAN3 is 8Mbps, 5Mbps and 20Mbps, the weight of each WAN link is so that calculated as:

$$\text{WAN1: } 0.8 \cdot (8/20) + 0.2 \cdot (4/10) = 0.4$$

$$\text{WAN2: } 0.8 \cdot (5/20) + 0.2 \cdot (10/10) = 0.4$$

$$\text{WAN3: } 0.8 \cdot (20/20) + 0.2 \cdot (6/10) = 0.92$$

Before the weights are updated next time, By Upstream Traffic returns one of the three WAN links for the load balancing policy in circular order with weight 40:40:92. Weights will be updated by calculating with real-time available bandwidth every three seconds.

As for working with Tunnel Routing, By Upstream Traffic divides the available uploading bandwidth of each participating WAN link by the number of GRE tunnel deployed on the WAN link, and picks one with the most available uploading bandwidth. For example, there is a Tunnel Routing Group consisting of three GRE tunnels deployed on WAN1, WAN2 and WAN3 respectively. Other Tunnel Routing Groups deploy 2 GRE tunnels on WAN1, 3 GRE tunnels on WAN2 and 1 GRE tunnel on WAN3. Totally, there are 3 tunnels on WAN1, 4 tunnels on WAN2 and 2 tunnels on WAN3. If, at a time, the available uploading bandwidth of WAN1, WAN2 and WAN3 is 6Mbps, 20Mbps and 12Mbps, By Upstream Traffic will pick WAN3 for transferring packets matching this Tunnel Routing Group because:

$$\text{WAN1: } 6\text{Mbps}/3 = 2\text{Mbps}$$

$$\text{WAN2: } 20\text{Mbps}/4 = 5\text{Mbps}$$

$$\text{WAN3: } 12\text{Mbps}/2 = 6\text{Mbps}$$

By Upstream Traffic for Tunnel Routing is not a Round-Robin based algorithm, it always picks the resource with most available uploading bandwidth.

## By Total Traffic

By Total Traffic serves Auto Routing, Multihoming and DNS Proxy. By Total Traffic picks one of the participating resources (WAN links) according to the weight evenly relevant to their data downloading and uploading availability. Each of the participating WAN links is weighted every three seconds by summing 50% available inbound bandwidth and 50% available outbound bandwidth up. For example, there is an Auto Routing policy with participants WAN1, WAN2 and WAN3. If, at some time, the available inbound bandwidth on WAN1, WAN2 and WAN3 is 4Mbps, 10Mbps and 6Mbps, and the available outbound bandwidth on WAN1, WAN2 and WAN3 is 8Mbps, 5Mbps and 20Mbps, the weight of each WAN link is so that calculated as:

$$\text{WAN1: } 0.5 \cdot (4/10) + 0.5 \cdot (8/20) = 0.4$$

$$\text{WAN2: } 0.5 \cdot (10/10) + 0.5 \cdot (5/20) = 0.625$$

$$\text{WAN3: } 0.5 \cdot (6/10) + 0.5 \cdot (20/20) = 0.8$$

Before the weights are updated next time, By Total Traffic returns one of the three WAN links for the load balancing policy in circular order with weight 400:625:800. Weights will be updated by calculating with real-time available bandwidth every three seconds.

## Notices of By Upstream Traffic, By Downstream Traffic and By Total Traffic

What the available bandwidth that algorithms By Upstream, Downstream and Total Traffic using for Auto Routing and Multihoming will depend on how Bandwidth Management (see [Bandwidth Management](#)) is configured. Considering that a Bandwidth Management class limits the usage of maximum downloading and uploading bandwidth of a 20Mbps/10Mbps WAN link to 6Mbps and 3Mbps respectively. For traffic classified to this BM class, the available downloading and uploading bandwidth for algorithms By Upstream, Downstream and Total Traffic to evaluate this WAN link will never exceed the bandwidth limits 6Mbps/3Mbps, even if the WAN link is wholly idle.

Algorithms By Upstream, Downstream and Total Traffic measure the transmission ability of a WAN link only between the FortiWAN device and the gateway of its ISP network (last mile). The available bandwidth of a WAN link is measured on the network interface of the WAN link. Algorithms By Upstream, Downstream and Total Traffic do not guarantee transmission ability between the ISP network and destinations.

## By Optimum Route

Relative to algorithms By Upstream, Downstream and Total Traffic, By Optimum Route evaluates a WAN link with not only its traffic loading but also the round-trip time (RTT) between FortiWAN and the destinations. The evaluation involves bandwidth usage of a WAN link and the RTT, which responses the network conditions closer to reality. For example a WAN link with the most available bandwidth might not be the best choice for data transferring to a destination, if it has the worst RTT. Conversely, the WAN link with fewer available bandwidth might be picked by Optimum Route if the RTT is good. By Optimum Route works for Auto Routing and Multihoming to mainly avoid the peering issue between ISP networks. Optimum Route works via various detections and measures. It requires to have the details configured first to make sure it works appropriately (See [Optimum Route Detection](#)).

## By Response Time

By Response Time is only used by Virtual Server (see [Virtual Server & Server Load Balancing](#)) for distribute incoming service requests to internal servers to achieve server load balancing. By Response Time measures the response time of each internal server by sending a detection packets, and picks one server with the lowest response time for Virtual Server routes the matched requests to it.

## By Static

By Static is only used by Multihoming for responding fixed IP addresses to DNS requests for an A/AAAA record without considering the traffic loading and connectivity state of each WAN link. By Static deprives Multihoming of inbound load balancing and WAN link failover; retrogrades it back to general DNS service. Note that the external clients will access to the responded IP addresses, and the accesses might be stuck or failed if the WAN link is congested or unavailable.

## By Fixed

By Fixed is only used by Auto Routing for routing outbound traffic to a fixed WAN link without considering the traffic loading on the WAN link. Different from Multihoming's By Static, By Fixed will not return the WAN link to Auto Routing if it is unavailable. It requires a fail-over policy (configured in a filter rule) to achieve WAN link failover when the fixed WAN link is failed. By Fixed deprives Auto Routing of outbound load balancing.

## Fail-Over

The Fail-Over algorithm is only used by Multihoming to response the IP address of the first-available WAN link to a DNS request. When this algorithm is applied, Multihoming check the health status of each WAN link candidate of an A/AAAA policy from top to bottom, and always responses the first-available WAN link to DNS queries.

## Hash

Hash is only used by Virtual Server for distribute incoming service requests to weighted internal servers to achieve server load balancing. The source IP addresses of a service request will be translated from dot-decimal address to a decimal value first. This value is then hashed by calculating the remainder of the division of the value by the sum of weights (modulo operation), and the remainder indicates the internal server that the service request should be directed to. For example, if there are three servers (serv1, serv2 and serv3) weighted with 1:2:3 in the server pool, requests that their IP addresses are congruent modulo 6 (sum of the servers' weight: 1+2+3) will be assigned to the same server according to the weights (remainder 0 indicates serv1, reminders 1 and 2 indicate serv2, reminders 3, 4 and 5 indicate serv3). The following table lists the examples how the hash function works for Virtual Server:

| Source IP of request | Decimal value | Hash value (mod 6) | Assigned server |
|----------------------|---------------|--------------------|-----------------|
| 172.16.254.1         | 2886794753    | 5                  | serv3           |
| 172.16.254.2         | 2886794754    | 0                  | serv1           |
| 172.16.254.3         | 2886794755    | 1                  | serv2           |
| 172.16.254.4         | 2886794756    | 2                  | serv2           |
| 172.16.254.5         | 2886794757    | 3                  | serv3           |
| 172.16.254.6         | 2886794758    | 4                  | serv3           |
| 125.227.251.80       | 2112093008    | 2                  | serv2           |
| 125.227.251.88       | 2112093016    | 4                  | serv3           |
| 125.227.251.96       | 2112093024    | 0                  | serv1           |



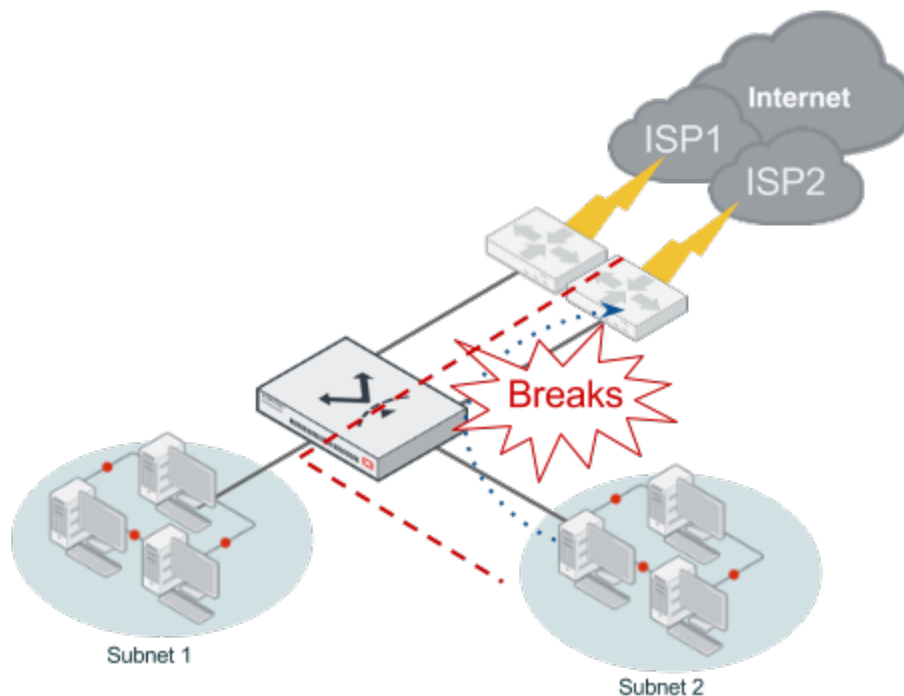
## Outbound Load Balancing and Failover (Auto Routing)

### Auto Routing Mechanism

Auto Routing load-balances the outbound traffic across multiple WAN links according to a pre-defined routing policies. During WAN link failures, auto routing will also adjust the routing methods to distribute the outbound traffic ONLY among the WAN links in fit and working conditions, thus avoiding the failed link(s).

The traditional method of backing up WAN links by having a secondary WAN link taking over the failed link. Basically having a main line and a second line as backup, aided by any standard router's backup policy, minimum fault tolerance can be achieved. This kind of approach means certain lines remain idle for most of the time and it is a waste of resources. In addition, the router configurations can be tedious.

Another approach for multiple WAN links backup is by dividing the LAN into multiple segments, each doing its own thing as they are all independent WAN links. Under standard conditions, each segment has its own way using separate routers. When one of the WAN links fails, the administrator has to change the router configuration to bypass the failed link. The obvious drawback to this approach is the unnecessary workload for administrators. Whenever WAN link status changes, the LAN environment settings (such as gateway, netmask, router policies, proxy settings, etc) all need to be adjusted.

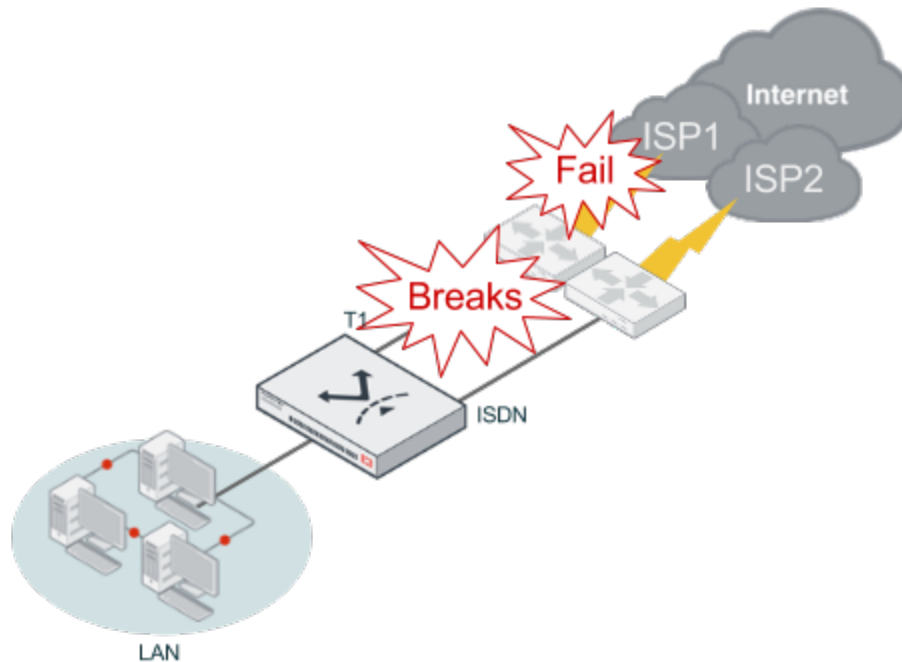


### Fault Tolerance Mechanism

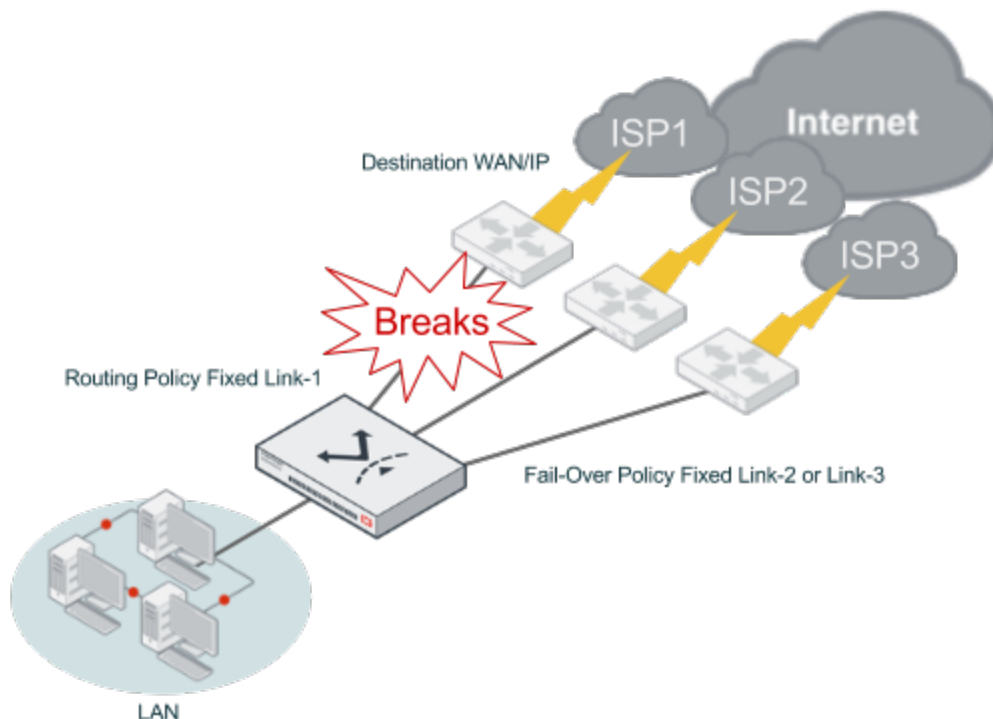
As previously stated, without WAN load-balancer such as FortiWAN, the traditional way of using multiple WAN links always involves human intervention.

FortiWAN has an internal "Virtual Trunk" circuit, which is essentially a combination of the multiple WAN links. Auto routing is capable of adjusting the 'Virtual Trunk' to include only the WAN links that are functioning normally

and to direct outbound traffic through the “Virtual Trunk circuit” without human intervention. Network users will therefore not be able to notice any change of status in WAN links (See [“WAN Link Health Detection”](#)).



The figure above illustrates auto routing securing uninterrupted connection to the internet even during WAN link failures. Compared to the traditional multiple WAN link usage, auto routing can effectively use all available WAN links to balance outbound traffic even when all the WAN links are in perfect working condition. Auto routing cannot prevent data loss on a WAN link when it fails, but all subsequent sessions will be automatically routed to other working links.



FortiWAN provides mechanisms to record, notify and analysis on events refer to the Auto Routing service, see ["Log"](#), ["Statistics: Traffic"](#), ["Statistics: Bandwidth"](#) and ["Reports"](#).

## Configurations

It allows administrators to determine the way traffic is routed to WAN links. Multiple WAN links have a variety of ideal auto-routing methods for any network environment. Auto routing is configured in 2 steps: **Policies** and **Filters**.

### Policy

An Auto Routing policy defines how to dynamically distribute outbound traffic (sessions) over multiple WAN links according to traffic loading of the WAN links, which achieve the outbound load balancing. The basic items to define a policy are the load balancing algorithm and the related WAN parameters. By associating an Auto Routing filter rule with a policy, Auto Routing can determine a good WAN link among the candidates and route the outgoing sessions that match the filter rule to the WAN link.

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Label</b>     | Enter a name to the auto routing policy. The label (policy name) will be listed in the <b>Routing Policy</b> drop-menu later for assigning a policy to a filter.                                                                                                                                                                                                                                                                                                                                                          |
| <b>T</b>         | <p>Check to enable threshold function to the policy.</p> <p>Administrators can configure the downstream and upstream threshold of each WAN link on the configuration page of WAN Setting (See <a href="#">"Configuring your WAN"</a>). WAN links with traffic that exceeds the threshold values will be considered as failed to Auto Routing, and traffic flow will be re-directed to other WAN links based on the selected algorithm.</p>                                                                                |
| <b>Algorithm</b> | <p>Select an load balancing algorithm from the drop-down menu for this routing policy. System distributes sessions that match this policy among WAN links according to the algorithm. The algorithms for options are:</p> <ul style="list-style-type: none"><li>• Fixed</li><li>• Round-Robin</li><li>• By Connection</li><li>• By Downstream Traffic</li><li>• By Upstream Traffic</li><li>• By Total Traffic</li><li>• By Optimum Route</li></ul> <p>See <a href="#">Load Balancing Algorithms</a> for the details.</p> |

**Parameter**

Select the WAN links from the WAN parameters for this routing policy to distribute sessions among. Numbering schemes indicate the WAN links. According to the algorithm, system dynamically routes each matched session to one of the participating WAN links. The WAN parameters varies from the chosen algorithm:

- For algorithms **Fixed**, **By Upstream Traffic**, **By Downstream Traffic**, **By Total Traffic** and **By Optimum Route**, check the check-box under a number scheme to apply the WAN link to this policy. Selecting multiple WAN links is allowed and it implies traffic is balanced among the selected WAN links. When you create a new policy by click the add button for configuring it, the WAN parameters are checked by default if the corresponding WAN links have been enabled (see [Configuring your WAN](#)). Uncheck the check-box of a WAN link to remove it from this routing policy.
- For algorithms **Round-Robin** and **By Connection**, apply a WAN link to this policy by defining the weight (or ratio) on the input box under a number scheme. Selecting multiple WAN links is allowed and it implies traffic is balanced among the selected WAN links. When you create a new policy by click the add button for configuring it, weights are defined as 1 to the WAN parameters by default if the corresponding WAN links have been enabled (see [Configuring your WAN](#)). Change the weight of a WAN link to 0 (zero) to remove it from this routing policy.

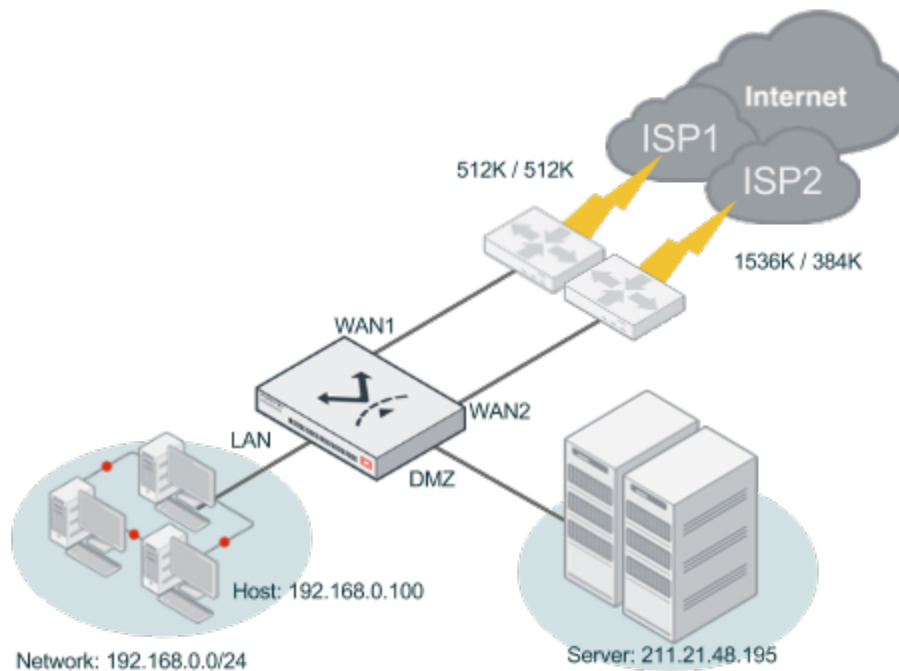
**Filter**

Auto Routing filters are used to evaluate against the outbound sessions (sessions from LAN and DMZ to the Internet through the FortiWAN). The routing policy and fail-over of a matching filter rule are applied to the evaluated sessions. Base on the specified policies, Auto Routing determines which WAN port to use for forwarding packets of the sessions. A filter rule consists of a set of filter terms (When, Input Port, Source, Destination and Service) and the related policies (Routing policy and Fail-over policy) for action.

|                    |                                                                                                                                                                                    |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>E</b>           | Check to enable the rule.                                                                                                                                                          |
| <b>When</b>        | Select a time period for this filter term to evaluate the outbound sessions by the receiving time, or leave it as All-Time. See <a href="#">Busyhour Settings</a> for details.     |
| <b>Input Port</b>  | Select a interface that packets are received on for this filter term to evaluate the outbound sessions, or leave it as Any Port. See <a href="#">Using the web UI</a> for details. |
| <b>Source</b>      | Define the source that packets come from for this filter term to evaluate the outbound sessions, or leave it as Any Address. See <a href="#">Using the web UI</a> for details.     |
| <b>Destination</b> | Define the destination that packets are destined to for this filter term to evaluate the outbound sessions, or leave it as WAN. See <a href="#">Using the web UI</a> for details.  |
| <b>Service</b>     | Define the service that the packets belong to for this filter term to evaluate the outbound sessions, or leave it as Any. See <a href="#">Using the web UI</a> for details.        |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Routing Policy</b>   | Specify a routing policy for sessions that match this filter rule, or leave it as Default Policy. A matched session will be dynamically routed to a WAN link according to the policy. All the predefined routing policies are list here for options.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Fail-over Policy</b> | <p>Once all the WAN links defined to a routing policy get failed, the fail-over policy will take effect. The fail-over policy could be one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Predefined routing policy</b> - Select another predefined routing policy as fail-over policy. The backup routing policy takes over to determine a WAN link for this session if the original routing policy fails.</li> <li>• <b>Tunnel: TUNNEL_GROUP_NAME</b> - This option is available only when Tunnel Routing is enabled. Select a predefined tunnel group as the fail-over policy. Once the fail-over policy takes over the original routing policy, packets of the session will be delivered to the remote FortiWAN device through Tunnel Routing. With defining appropriate Auto Routing policy and filter rule on the remote FortiWAN, packets of the session can be transferred through a WAN link of the remote FortiWAN. See <a href="#">Tunnel Routing</a> for details.</li> <li>• <b>NEXT-MATCH</b> - When NEXT-MATCH takes over original routing policy, system continues evaluating the subsequent filter rules against the session and move on to the next matched policy where packets fall into. At least, it matches the default filter rule and goes to the default policy.</li> <li>• <b>NO-ACTION</b> - Take no actions when the original routing policy get failed, and packets of the session will be dropped.</li> </ul> |
| <b>L</b>                | Check to enable logging. Whenever the rule is matched, system will record the event to log file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Example 1



The auto routing policies to be established accordingly:

1. Always route connections through WAN#1, which is an ADSL WAN link with 512k downstream/512k upstream.
2. Always route connections through WAN#2, which is an ADSL WAN link with 1.5M downstream/384k upstream.
3. Route connections with algorithm "Optimum Route".
4. Route connections based on the current downstream traffic of WAN links.
5. Route connections based on the total traffic of each WAN link.

Policy table will look like:

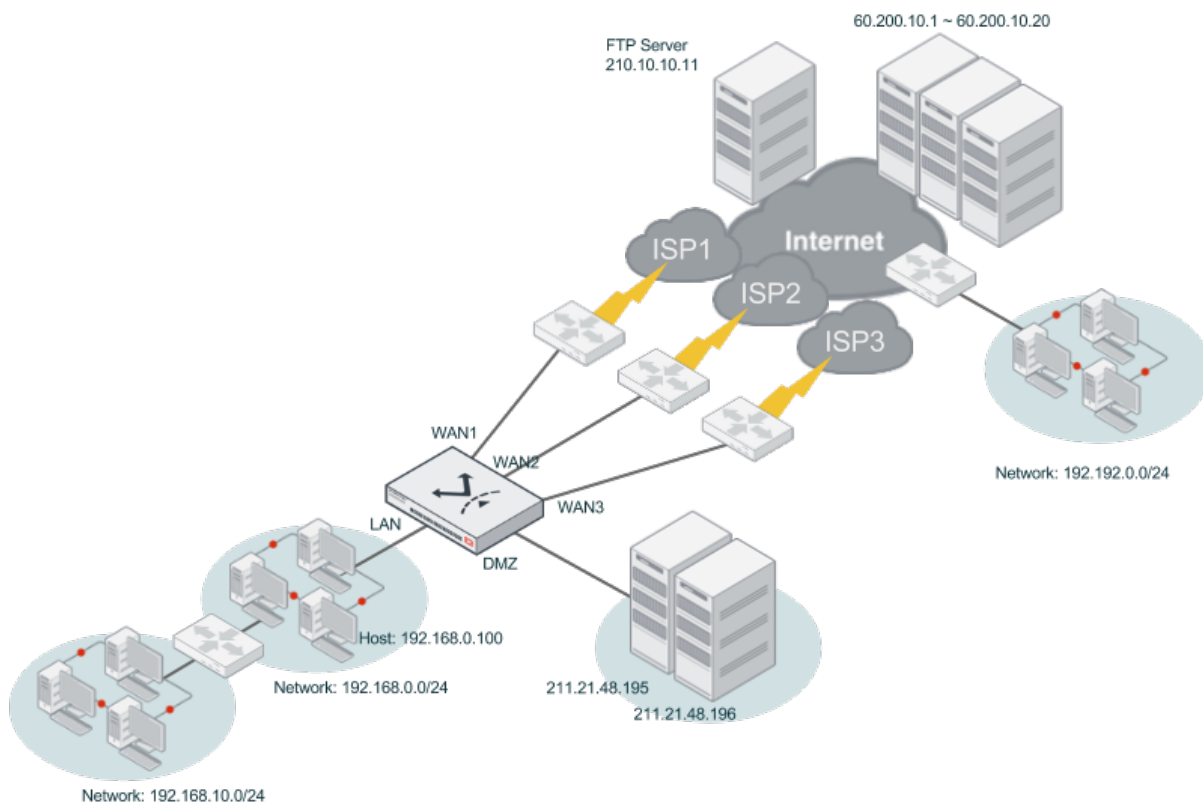
| Label            | Algorithm             | Parameter                    |
|------------------|-----------------------|------------------------------|
| WAN1 (512/512)   | Fixed                 | Check WAN#1                  |
| WAN2 (1536/384)  | Fixed                 | Check WAN#2                  |
| By Optimum Route | By Optimum Route      | Check both WAN #1 and WAN #2 |
| By Downstream    | By Downstream Traffic | Check both WAN #1 and WAN #2 |
| By Total         | By Total Traffic      | Check both WAN #1 and WAN #2 |

Note: Labeling the policies alone does not mean the policy has been set up. Configuring WAN link bandwidth must be done under [System] -> [Network Settings].

Defining filters for the following:

1. When LAN users access web server on the internet, use policy "By Optimum Route" to route connections to the best-conditioned link.
2. When LAN users access the FTP server on the internet, use policy "WAN1(512/512)" to route connections. If WAN#1 fails, the connections will be routed "By Optimum Route". Note: In this case, "By Optimum Route" will only route connections through WAN#2 as WAN #1 has failed.
3. The connections from 211.21.48.195 in DMZ to SMTP server on the internet will be routed by policy "WAN1 (512/512)". If WAN#1 fails, it will be routed by "WAN2 (1536/384)".
4. The connections from 211.21.48.195 in DMZ to POP3 server on the internet will be routed by "WAN1 (512/512)". If WAN#1 fails, no action will be taken. Note: When WAN #1 fails, connection to the external POP server will also fail.

## Example 2



The auto routing policies to be established accordingly:

1. Always route connections through WAN#1 (fixed algorithm).
2. Always route connections through WAN#2 (fixed algorithm).
3. Always route connections through WAN#3 (fixed algorithm).
4. Route connections evenly among the three WAN links with "Round-Robin".
5. Route connections through the three WAN links by "Round-Robin" with weight ratio WAN#1:WAN#2:WAN#3 = 1:2:3. Note: if there are six connections to be established, the first connection will be routed through WAN#1, the second and third through WAN#2, and the last three through WAN#3.

6. Route connections through WAN#1 and WAN#2 depending on the bandwidth left in the downstream traffic of each WAN link.
7. Route connections through WAN#2 and WAN#3 depending on the bandwidth left in the total traffic of each WAN link.

| Label             | Algorithm        | Parameter                                            |
|-------------------|------------------|------------------------------------------------------|
| WAN1              | Fixed            | Check WAN #1                                         |
| WAN2              | Fixed            | Check WAN #2                                         |
| WAN3              | Fixed            | Check WAN #3                                         |
| Round-Robin 1:1:1 | Round-Robin      | Enter "1" for WAN #1, WAN #2, and WAN #3             |
| Round-Robin 1:2:3 | Round-Robin      | Enter "1" for WAN #1, "2" for WAN #2, "3" for WAN #3 |
| By Downstream     | By Downstream    | Check both WAN #1 and WAN #2                         |
| By Total          | By Total Traffic | Check both WAN #2 and WAN #3                         |

Defining filters for the following:

1. The connections from 192.168.0.100 to FTP 210.10.10.11 are routed by the policy "WAN3". If WAN #3 fails, they will be routed by policy "by Downstream".
2. The connections from sub-network 192.168.10.0/24 to web servers on the internet are routed by the policy "Round-Robin1:1:1".
3. The connections from 192.168.0.100~192.168.0.200 to sub-network 192.192.0.0/24 on TCP port 8000 are routed by the policy "WAN2". If WAN #2 fails, they will be routed by the policy "WAN3".
4. The connections from the LAN to the Internet are routed by the policy "by Downstream". If both WAN #1 and WAN #2 fail, they will be routed by "WAN3".
5. The connections from 211.21.48.196 to FTP 210.10.10.11 are routed by policy "Round-Robin1:2:3".
6. The connections from 211.21.48.195 to any SMTP server on the internet are routed by policy "WAN3". If WAN #3 fails, they will be routed by "WAN3". Note: In this case, the host at 211.21.48.195 will not be able to establish connections to any SMTP server on the internet when WAN #3 fails, even though some other WAN links still keep alive. For more details, refer to "Fail-over" policy.
7. The connections from DMZ to the internet are routed by policy "By Downstream". If both WAN #1 and WAN #2 fail, it will be routed by "By Total". Note: Usually, when both WAN #1 and WAN #2 fail, fail-over policy will take effect. Somehow in the case above when both WAN links fail, then all traffic will be routed to WAN #3.
8. The connections from an arbitrary host to the hosts at 60.200.10.1~60.200.10.10 will be routed by policy "WAN2". If WAN #2 fails, they will be routed by "WAN1".
9. The connections from an arbitrary host to any host on the Internet will be routed by the policy "by Downstream".

### See also

- [WAN Link Health Detection](#)
- [Configuring your WAN](#)



- [Load Balancing & Fault Tolerance](#)
- [Busyhour Settings](#)
- [Using the web UI](#)

## Inbound Load Balancing and Failover (Multihoming)

### Multihoming

Multihoming is a technique when external users request any server's IP address; Multihoming promptly returns DNS response according to the link quality. This provides unmatched availability of bandwidth and load-balances incoming traffic across the multiple ISP lines.

Simultaneously using multiple IP address provided by the ISP connections can result in problems with inbound traffic. For example, if the network is currently using an IP provided by ISP1, and a problem occurs with this ISP, then the inbound query will not be received because the external traffic only knows the IP address provided by ISP1. Also, by using the IP provided ISP1, ISP2 cannot manage the inbound traffic of ISP1. Therefore the concern with multiple ISP links is how to effectively display IP address to the external environment.

Multihoming uses DNS fault-tolerance technique to resolve this problems with the simultaneous use of multiple ISP connections. For example, if the web server for external traffic uses a single ISP connection, then any problems with that connection will affect the network. However, if the DNS periodically assigns different IP addresses provided by different ISP connections, then the external traffic will always have a valid IP to connect to. The actual implementation is assigning a name of different IP, and any query to this name will receive an IP address. As a result, different users can access the web server through different IPs, which is the purpose of Multihoming.

Assuming, there are three WAN links (therefore three different IPs) for the web site of [www.example.com](http://www.example.com), the DNS record has three entries:

```
www IN A 211.21.10.3
www IN A 63.98.110.123
www IN A 192.136.1.243
```

All DNS requests to [www.example.com](http://www.example.com) will be sent to FortiWAN. Multihoming will constantly measure the health conditions as well as the state of each WAN link and compute the optimal return answer to the DNS queries, defined as the SwiftDNS technology. The SwiftDNS technology will not only ensure fault tolerance for inbound traffic, it also supports powerful and flexible load balancing algorithms as in the Auto Routing mechanism to enable users with heavy web presence to maximize the reliability and efficiency of their web services.

The SwiftDNS Multihoming mechanism requires network administrators to understand the details of the system behavior. The fundamental concept of the DNS mechanism is shown in the next section. A step by step deployment tutorial will also be provided.

### Introduction to DNS

DNS server differs from the host file based on name resolution. Host file contains information of IP address mapping information. It is only useful for intranet where the information of host machines is relatively static. Name resolution by DNS server is dynamic because it can adapt to changes easily. The way it works is based on DNS server hierarchy on the Internet. If a DNS server cannot resolve a name (the information is not in its cache), it will ask other DNS servers. There is a protocol on how and where to ask other DNS servers.

A name resolution request may go through a number of DNS servers. When an answer is found, it will be saved in cache so that the same request can be answered immediately without asking other DNS servers again. Each name resolution result saved in cache has a TTL (Time To Live). After the period of TTL, it will be discarded in order to avoid stale information.

The whole internet has a large DNS hierarchy. The top of the hierarchy is called Root. It consists of a set of Root DNS servers coordinated by ICANN. The next level below Root is Top Level Domain (TLD). TLD registration database contains information about top level domains such as CA, COM, EDU, GOV, NET, etc. The next level below TLD is Second Level Domain (such as whitehouse.gov, Microsoft.com, inforamp.net, etc.) followed by Third Level Domain, and so on.

You can apply for domains for your organization. First, go to the Internet's Network Information Center (InterNIC) to find out if the domain has been registered already. You can also consult the ICANN-accredited registrar database. Second, register the domain with a registrar. You have to provide at least two DNS servers to serve DNS requests. If your registration has been approved, then any DNS request to your domain will be forwarded to the DNS servers you are registered with. For example, xtera.com is registered and InterNIC has put the name "xtera" into the COM DNS servers.

Once the domain is registered, sub-domains can be created. Example: a part of the network can be named "sales.xtera.com". InterNIC's approval is not required for creating sub-domains. However, it is important to put DNS information about sales.xtera.com into the DNS servers of xtera.com.

Here is an example of how DNS hierarchy works. A user at a university sees a link to sales.xtera.com on a web page and clicks it. The browser will ask the local DNS server dns.utexas.edu about sales.xtera.com. Suppose it is not in the cache of dns.utexas.edu. The DNS server goes to a Root DNS server to find the DNS server for COM TLD. The DNS server for COM TLD tells dns.utexas.edu to go to dns1.xtera.com. Finally dns.utexas.edu is given the IP address of sales.xtera.com by dns1.xtera.com.

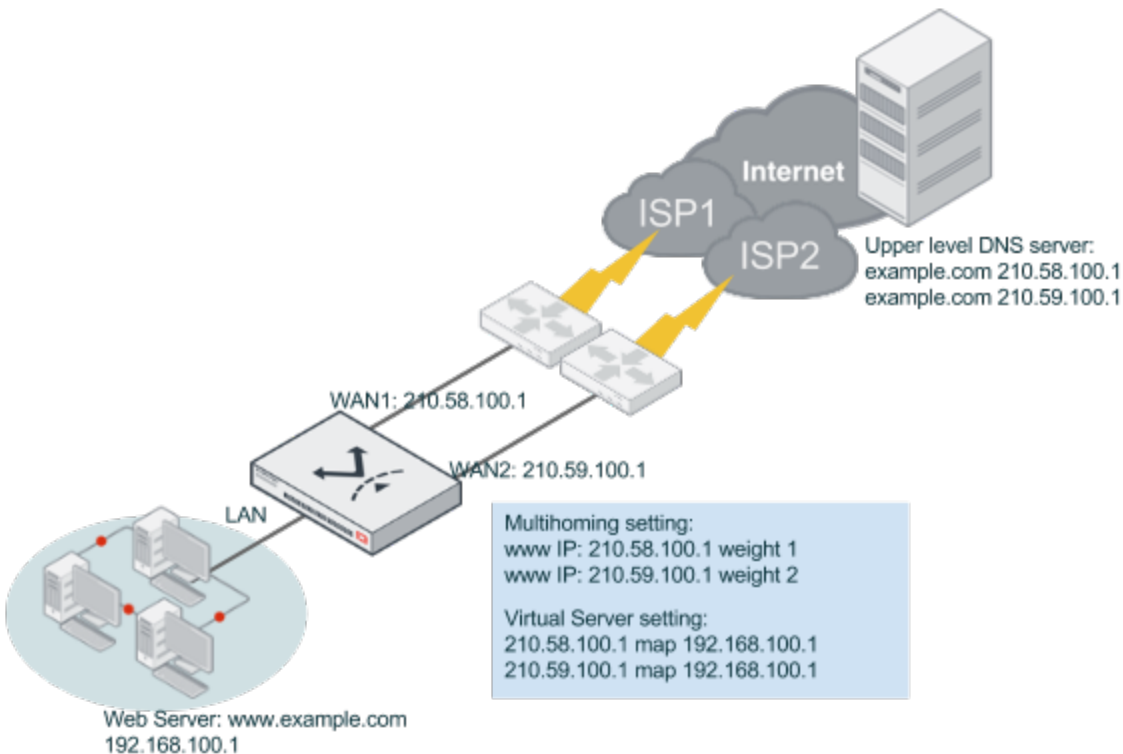
## SwiftDNS

One of the problems with traditional DNS servers are facing is TTL. A long TTL means a long update time when IPs have been changed. Before the update time is up (i.e. TTL is expired), DNS requests may be answered with incorrect information. FortiWAN employs SwiftDNS for multihoming based on the health state of the link and a traffic re-directing algorithm. SwiftDNS dynamically answers DNS requests to prevent broken or congested links. In order to solve the TTL issue stated above, SwiftDNS maintains a very short TTL and actively sends out updates to internal DNS in case of link status changes.

## How does SwiftDNS work?

Here is an example to illustrate how SwiftDNS works. When Multihoming is enabled, SwiftDNS becomes active. In this case, the upper level DNS server for example.com has two NS records and they are for Primary DNS server at 210.58.100.1 and Secondary DNS server at 210.59.100.1. Both of them are pointing to FortiWAN.

In this case, a web site at 192.168.100.1 in LAN is exposed to these two IPs. When both ISP links are working properly, FortiWAN replies to DNS requests for www.example.com with 210.58.100.1 and 210.59.100.1 at ratio of 1:2 (weight ratio).



Assuming ISP1 is down and a DNS request for www.example.com comes in, it would not be able to go through 210.58.100.1 but it will be able to reach 210.59.100.1. Multihoming detects the link status of WAN1 and answer the request with 210.59.100.1.

## Prerequisites for Multihoming

In order to multihome properly, review the requirements below.

Prerequisites for Multihoming:

- Multiple WAN links (minimum of 2).
- Registered domain names for public servers. Please make sure DNS requests for the domains can be delivered to FortiWAN.
- Public servers must be configured as virtual servers, or have public IPs

Besides, Multihoming is a **non-recursive** name server which is an authoritative DNS service that allows others to find your domain only. Multihoming does not answer for unknown domains.

## DNSSEC Support

The DNS Security Extensions (DNSSEC) is a specification that adds data authentications and integrity to standard DNS. To resist tampering with DNS responses, DNSSEC introduces PKI (Public Key Infrastructure) to sign and authenticate DNS resource record sets within the zone. A signed zone includes a collection of new resource records: RRSIG, DNSKEY and DS.

- RRSIG contains the DNSSEC signature for the corresponded DNS records (A, AAAA, MX, CNAME and etc.) within the zone.

- DNSKEY contains the public key corresponded to the private key used to generate RRSIG records. A DNS resolver uses it to verify DNSSEC signatures in RRSIG.
- DS (Delegation Signer) references to the public key used to verify the RRSIG in your zone. Every DS record should be signed by your parent zone and stored in the parent zone to establish trust chain between DNS zones.

Multihoming supports basic DNSSEC which employs only one key pair KSK (Key Sign Key) to generate DNSKEY and RRSIG records for the zone (NSEC is not supported). The supported algorithm and key size are only RSASHA512 and 2048 bits. Note that Multihoming's DNSSEC is not supported for Relay Mode.

Remember that you have to configure DS records with your domain registrar after you complete configurations for DNSSEC. Please contact your domain registrar for further details about managing DS records.

## Relay Mode

For the case that a DNS server already exists in your network, Relay Mode is the way to combine the existing DNS servers with Multihoming's inbound load balance and fault tolerance. With Relay Mode enabled, FortiWAN will forward all the DNS requests it receives to the specified name servers, instead of processing the requests directly. Answer of the DNS request will be responded to FortiWAN from the name server. FortiWAN's Multihoming then reprocess the answer with appropriate IP address according to the AAAA/A records and AAAA/A policies (load balancing algorithm). The DNS answer that contains appropriate IP address will finally be responded to client, so that the inbound access could connect via the appropriate WAN link.

## Enable Backup

FortiWAN Multihoming employs Backup mechanism to provide disaster recovery approach for network across various regions. Under this mechanism, the same backup service is set up across different regions. Therefore, when master site is down, backup site will immediately take over to resume the service.

To deploy Multihoming Backup between two FortiWAN units for one domain, at least one of the WAN links' localhost IPv4 addresses of each FortiWAN unit must be registered with the parent domain (so that a DNS request for the domain can be delivered to the two FortiWAN units). Check "Enable Backup" on the Slave FortiWAN Web UI and specify the IPv4 addresses (which are registered with parent domain) of the Master FortiWAN in "Remote Master Servers". Configurations for Multihoming Backup deployment is only necessary on the Slave unit, please do not check "Enable Backup" on the Master unit.

Then the Slave unit will detect the state of the Master unit periodically with its built-in Dig tool. The detect packets will be delivered to Master unit via the IP addresses specified on the Slave unit. When the Master's Multihoming works properly, the Slave's Multihoming will get into non-active mode (Unit that is in non-active mode will not answer to any DNS request); when the Master's Multihoming is down, the Slave will get into active mode and take over to resume Multihoming. After takeover, the Slave will continuously detect Master's state. Once the Master recovers, the Slave will return Multihoming service back to Master and get into non-active mode. This is how the Backup mechanism offers disaster recovery function. DNS database synchronization is not provided for Multihoming Backup deployment, so that DNS database can be maintained individually on the two units for local and remote-backup services. In case that multiple IP addresses of FortiWAN are registered with parent domain (to avoid single WAN links failure), those IP addresses should be configured into the "Server IPv4 Address" field on the Slave unit.

## Configurations

[Auto-routing](#) is a trunking technology that provides load balancing and fault tolerance for all outbound requests, but it does not apply to inbound requests. These are handled by a unique technology called SwiftDNS, a

multihoming service which includes load balancing and fault tolerance for inbound requests. The minimum requirements for multihoming are networks must have multiple WAN links and registered domain names for publicly accessible servers. Note that a DNS request from client is delivered to FortiWAN via a fixed WAN link, whose the IP address is registered with parent domain. It would be better to have multiple IP addresses registered to avoid single WAN link failure.

When FortiWAN receives a DNS query, it replies with a public IP assigned to one of the WAN links based on the settings of the answering policies. Therefore, subsequent requests to server will be sent to a public IP of the WAN link based on FortiWAN's previous response. The policies are based on weight for each WAN link and are definable. Multihoming is also capable of automatically detecting the best links by "[Optimum Route](#)", and if WAN link failure occurs, the public IP assigned to that failed link will not be returned even though the servers are still reachable via other links.

FortiWAN offers two options for Multihoming: Non Relay Mode and Relay Mode. The details of will be explained in this section.

The section explains how to configure Multihoming. First, check the box to enable Multihoming in "Enable Multihoming". Multihoming supports Backup mechanism. To enable this function, check "Enable Backup" and enter the IP addresses of the backup server.

FortiWAN provides mechanisms to record, notify and analysis on events refer to the Multihoming service, see "[Log](#)", "[Statistics: Traffic](#)", "[Statistics: Bandwidth](#)" and "[Reports](#)".

## Non-Relay Mode

To enable Multihoming in non-relay mode, go to **Service > Multihoming** on the Web UI, check the box **Enable Multihoming**, and uncheck the box **Enable Relay**. FortiWAN will performs DNS analysis on local host if the relay mode is disabled. It contains three blocks to get non-relay mode Multihoming configured: Global Settings, Policy Settings and Domain Name Settings.

### Global Settings: IPv4/IPv6 PTR Record

PTR (Pointer Record) is used to resolve the IPv4/IPv6 address to a domain or hostname.

| TTL |                                                                                                                                                                                                                     |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | Set the TTL for the PTR record. TTL (Time To Live) Specifies the amount of time that the record will stay in cache on systems requesting the record (other resolving nameservers, applications, browsers and etc.). |

**Reverse Lookup Zone**

Set the reverse lookup zone (domain) of the hosts for the PTR record. Click the add button to create new tables for configuring other zones.

**Zone Name** The reverse lookup zone name. For hosts in IPv4 subnet 1.2.3.0/24 (such as 1.2.3.4, 1.2.3.5 and etc.), the reverse lookup zone for its PTR records is 3.2.1.in-addr.arpa. Thus, this field should be filled in with "3.2.1". For host with IPv6 2001:470:0:64::2 (/64), the reverse lookup zone is 4.6.0.0.0.0.0.0.7.4.0.1.0.0.2.ip6.arpa and this field should be filled in with "4.6.0.0.0.0.0.0.7.4.0.1.0.0.2".

Click **Hide Details** / **Show Details** to collapse or expand the SOA configurations of the reverse lookup zone.

|                |                                                                                               |                                                                                                                                                                                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SOA</b>     | SOA (Start of Authority) record of the reverse lookup zone.                                   |                                                                                                                                                                                                                                                                                                                     |
|                | <b>Primary Name Server</b>                                                                    | The primary name server for the reverse lookup zone or the first name server in the name server list below.                                                                                                                                                                                                         |
|                | <b>Host Email</b>                                                                             | The responsible party for the reverse lookup zone.                                                                                                                                                                                                                                                                  |
|                | <b>Serial Number</b>                                                                          | A timestamp that changes whenever you update the reverse lookup zone.                                                                                                                                                                                                                                               |
|                | <b>Refresh Time</b>                                                                           | The number of seconds before the reverse lookup zone should be refreshed.                                                                                                                                                                                                                                           |
|                | <b>Retry Time</b>                                                                             | The number of seconds before a failed refresh should be retried.                                                                                                                                                                                                                                                    |
|                | <b>Expire Time</b>                                                                            | The upper limit in seconds before the reverse lookup zone is considered no longer authoritative.                                                                                                                                                                                                                    |
|                | <b>Minimum TTL</b>                                                                            | The negative result TTL.                                                                                                                                                                                                                                                                                            |
| <b>NS1</b>     | NS record. The primary name server for the reverse lookup zone.                               |                                                                                                                                                                                                                                                                                                                     |
| <b>NS2</b>     | NS record. The secondary name server for the reverse lookup zone.                             |                                                                                                                                                                                                                                                                                                                     |
| <b>Entries</b> | Set the PTR entries in the reverse lookup zone. Click the add button to create multiple PTRs. |                                                                                                                                                                                                                                                                                                                     |
|                | <b>IP Number</b>                                                                              | The last octet of the host IP address for resolving in the reverse lookup zone. For a IPv4 host 1.2.3.4 in the reverse lookup zone "3.2.1.in-addr.arpa", this field should be filled in with "4". For host with IPv6 2001:470:0:64::2 (/64), this field should be filled in with "2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0". |
|                | <b>Host Name</b>                                                                              | The FQDN of the host that that Multihoming will response to the request for resolving IPv4 address 1.2.3.4 or IPv6 address 2001:470:0:64::2, such as "www.example.com".                                                                                                                                             |

### Policy Settings: A/AAAA Record Policy

An A/AAAA record policy defines how to dynamically answer to the requests for an A/AAAA record according to traffic loading of WAN links, which achieve the inbound load balancing. The basic items to define a policy are the



load balancing algorithm and the related WAN parameters. By associating an A/AAAA record with a policy, Multihoming can determine a good WAN link among the candidates and answer the WAN port IP to the requests for the A/AAAA record. Click the add button to create a new policy and get the following settings configured.

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Policy Name</b> | Enter a name to the A/AAAA record policy. The policy name will be listed in the <b>To Policy</b> drop-menu of an A/AAAA configuration for assigning a policy to an A/AAAA record.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>T</b>           | <p>Check to enable threshold function to the policy.</p> <p>Administrators can configure the downstream and upstream threshold of each WAN link on the configuration page of WAN Setting (See "<a href="#">Configuring your WAN</a>"). WAN links with traffic that exceeds the threshold values will be considered as failed to Multihoming, and the other WAN links will be replied according to the configured A / AAAA Record Policy.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Algorithm</b>   | <p>Select an load balancing algorithm from the drop-down menu for this A/AAAA policy. Multihoming determines a WAN link among the candidates according to the selected algorithm and replies its IP to requests for a A/AAAA record. The algorithms for options are:</p> <ul style="list-style-type: none"> <li>• <b>By Weight:</b> selects a WAN link by weighted round-robin. See <a href="#">Round Robin (weighted)</a> for the details.</li> <li>• <b>By Downstream:</b> selects a WAN link with the lightest downstream traffic load. See <a href="#">By Downstream Traffic</a> for the details.</li> <li>• <b>By Upstream:</b> selects a WAN link with the lightest upstream traffic load. See <a href="#">By Upstream Traffic</a> for the details.</li> <li>• <b>By Total Traffic:</b> selects a WAN link with the lightest total traffic load. See <a href="#">By Total Traffic</a> for the details.</li> <li>• <b>By Optimum Route:</b> selects the best WAN link according to "Optimum Route Detection". See <a href="#">By Optimum Route for the details</a> for the details.</li> <li>• <b>By Static:</b> answers to queries with the specified static IP addresses. See <a href="#">By Static</a> for the details.</li> <li>• <b>Fail-Over:</b> answers to the queries with the IP address of the first-available WAN link specified in the <b>Policy Advanced Setting</b>. See <a href="#">Fail-Over</a> for the details.</li> </ul> |

**Policy Advanced Setting**

Set the WAN parameters to the selected algorithm for this policy. By clicking the add button aside the WAN Link field, you add one or more WAN links to the policy for the select algorithm. The algorithm selects one of them for Multihoming to reply a DNS query. For algorithm By Static, only the IP addresses are required, no WAN link is involved. Click the add button to add one or more static IPs for it. The followings are the WAN parameters need to be configured.

**Show/Hide Details**

Click to expand or collapse the settings.

**E**

Click to enable/disable the WAN link in the policy. A disabled WAN link will not be a candidate in the algorithm evaluation.

Note that Multihoming will always answer the IP of the first available WAN link you specify here if all the configured WAN link here are set to disabled.

**WAN Link**

Select the WAN link to be a candidate for the selected algorithm.

This field is not available for algorithm By Static, since Multihoming answers the static IPs to requests without evaluating traffic loading of WAN links.

**IPv4/IPv6 Address**

Specify an IP address for Multihoming to answer to resolving requests when the defined WAN link is chosen by the algorithm.

By default, the first IP deployed on the localhost of the selected WAN link (see [Configuring your WAN](#)) is listed on the drop-down menu for an option, or you can specify another IP manually if multiple IPs are deployed on the WAN link. If the host is deployed in LAN (see [Virtual Server](#)), the IP address that Multihoming replies to requests of resolving the host must be an IP deployed on the WAN's localhost. If the host is deployed in DMZ of a WAN link, then you can directly specify the IP (an IP of the DMZ subnet) of the host here.

For algorithm By Static, there is no default IP listed for options. Specify it manually.

**Weight**

Specify the weight to the WAN link. This is only available for algorithm By Weight. Weighted round-robin determines a WAN link from the candidates according to the weight of each WAN link.

## Domain Settings

Non-relay mode Multihoming not only performs the inbound load balancing, but also manages domains and resolves hostnames. Thus, Multihoming supports the resource records, NS, A/AAAA, CName, DName, SRV, MX and TXT, for a managed domain. Among the records, A/AAAA records are required to associate with predefined policies to achieve the idea of inbound load balancing. It contains the following settings to get a domain configured to Multihoming: basic domain information, DNSSEC, related resource records and external sub-domain of the domain.

The table below configures Domain Settings: multihoming domain names, DNS servers names (for querying domain), and answering policies to be applied when being given a prefix of the domain name.

### Basic domain information

It usually requires to assign a DNS/Host Server Name and the corresponding IP address to a domain when you register it to a domain name registrar. It tells the registrar that the domain is delegated to the specific name server. Let's assume that a domain *example.com* is registered to a registrar with specifying "DNS Server Name=ns1.example.com" and "IP address=10.10.10.10". *ns1.example.com* is the name server responsible (authoritative) for the domain *example.com* and its IP is 10.10.10.10. This is what for the TLD authorities to place NS records in the TLD name servers to point to the domain, and so that the recursive name servers can work out who is really in charge of this domain. For non-relay mode Multihoming, the FortiWAN device would be the name server authoritative for this domain. The DNS Server Name (name server) you used to register the domain can be named without restrictions (such as *ns1* in the example), but the IP address (10.10.10.10) must be an IP that is deployed on one of the WAN links of the FortiWAN, so that requests for the domain can be finally delivered to FortiWAN's Multihoming.

The following settings is actually for the SOA record of the domain in Multihoming.

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Domain Name</b>         | Enter the registered domain name, such as <i>example.com</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>TTL</b>                 | Set the TTL (Time to Live) for the domain information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Responsible Mail</b>    | Enter an administrator's email for this domain. Note that the @ symbol is not acceptable to Multihoming. You are required to replace the symbol @ of the email address with a dot ".", such as <i>admin.mail.example.com</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Primary Name Server</b> | <p>Enter the hostname of name server authoritative for this domain. Usually, it is the prefix of DNS Server Name that you specified for registering the domain, such as <i>ns1</i> for <i>ns1.example.com</i>. Dot characters within a hostname is acceptable, such as <i>abc.ns1</i> for <i>abc.ns1.example.com</i> or <i>abc.d.ns1</i> for <i>abc.d.ns1.example.com</i>. The domain name specified above is appended automatically to this hostname in Multihoming system backend. A hostname ends with a dot character, such as <i>ns1.</i> is not acceptable.</p> <p>Note that after applying the configurations, this primary name server and the corresponding IP addresses (set in the following fields) for the domain will be automatically added to the NS and A/AAAA records.</p> |
| <b>IPv4 Address</b>        | The IPv4 address that you specified for registering the domain, such as 10.10.10.10 in the above example.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>IPv6 Address</b>        | The IPv6 address that you specified for registering the domain if it is necessary.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## DNSSEC

As the previous descriptions, Multihoming supposes the DNSSEC to protect the DNS resource records in the domain. To enable it, the followings are the settings need to get configured.

|                        |                                                                                                                                                                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable</b>          | Check to enable DNSSEC.                                                                                                                                                                                                                                                  |
| <b>Private Key</b>     | Click the [+] button to generate DNSSEC private key used to sign the domain. This private key information will be listed. DNSKEY record and RRSIG record set for this domain are generated while applying the domain configuration. (For multiple keys, use the [+] key) |
| <b>Signing</b>         | States for the key, Active or Standby for options. Keys in the active state are those that are in use. Keys in standby state are not introduced into the zone.                                                                                                           |
| <b>Algorithm</b>       | Only RSASHA512 is supported. This field is visible only for Administrator permission.                                                                                                                                                                                    |
| <b>Key Size</b>        | Only 2048 bits is supported. This field is visible only for Administrator permission.                                                                                                                                                                                    |
| <b>Key Tag</b>         | Key ID.                                                                                                                                                                                                                                                                  |
| <b>Hash</b>            | Hash of the public key. Send the hash value to parent zone to generate a DS record.                                                                                                                                                                                      |
| <b>Modulus</b>         | Public modulus for the keypair. This field is visible only for Administrator permission.                                                                                                                                                                                 |
| <b>PublicExponent</b>  | Exponent for the public key. This field is visible for only Administrator permission.                                                                                                                                                                                    |
| <b>PrivateExponent</b> | Exponent for the private key. This field is visible for only Administrator permission.                                                                                                                                                                                   |
| <b>Prime1</b>          | Prime number 1 for the keypair. This field is visible for only Administrator permission.                                                                                                                                                                                 |
| <b>Prime2</b>          | Prime number 2 for the keypair. This field is visible for only Administrator permission.                                                                                                                                                                                 |

Notice:

1. You can generate multiple key pairs in batches from the configuration panel. Generally one key pair is in Active state for using while the other key pairs are in Standby state for manually key rollover at the appropriate time as determined by your key management policy.
2. In case of replacement keys, it is strongly suggested to keep both new and old keys in Active state for at least one TTL value. When the caching of records using the old keys in external name servers has expired, the old keys can be deleted.
3. Before deleting DNSSEC keys from your domain, you have to delete the corresponded DS record from the parent zone. Be careful that any mistake in the process of key replacement or delete might cause DNS queries to your domain failure.

## NS Record

Name Server (NS) records identify the name servers that are authoritative for a DNS domain. It requires at least one NS record for a domain to tell other name servers who to ask for resolving the domain name. For Multihoming, after the previous settings Domain Name, Primary Name Server and IPv4 Address are configured, the values will be automatically set to a NS record and an A/AAAA record for the domain. For example:

```
example.com. 86400 IN NS ns1.example.com
```

```
ns1.example.com 86400 IN A 10.10.10.10
```

You do not need to manually add a NS record and an A/AAAA record for the primary name server through the Web UI.

You can have multiple NS records in a domain, if there are multiple name servers authoritative for the domain for redundancy purpose. So that if the primary name server is unavailable, the domain will still be accessible. Configure the following settings to add the redundant NS records.

#### Name Server

The other name server authoritative for the domain, except the primary name server. This field can be configured in two formats: a hostname (prefix) or a FQDN.

##### Hostname (prefix)

Text string (dot characters within is acceptable) specified here that does not end with a dot character is regarded as a hostname (prefix) of the name server, and the base domain specified previously will be appended automatically to this hostname in Multihoming system backend. For example entering "ns2", "abc.ns2" or "abc.d.ns2" here, if the name server's FQDN is *ns2.example.com*, *abc.ns2.example.com* or *abc.d.ns2.example.com*. The corresponding NS record in backend will be:

```
example.com. 86400 IN NS ns2.example.com
```

or

```
example.com. 86400 IN NS abc.ns2.example.com
```

or

```
example.com. 86400 IN NS abc.d.ns2.example.com
```

##### FQDN

On the contrary, text string (dot characters within is acceptable) specified here that ends with a dot character is regarded as a FQDN of the name server, and the base domain specified previously will not be appended to it in backend. For example entering "ns2.example.com.", "abc.ns2.example.com." or "ns.otherdomain.com." here, if the name server's FQDN is *ns2.example.com*, *abc.ns2.example.com* or *ns.otherdomain.com*. The corresponding NS record in backend will be:

```
example.com. 86400 IN NS ns2.example.com
```

or

```
example.com. 86400 IN NS abc.ns2.example.com
```

or

```
example.com. 86400 IN NS ns.otherdomain.com
```

#### IPv4 Address

IPv4 address of the name server.

#### IPv6 Address

IPv6 address of the name server.

A NA record configuration entry implies a NS record and an A/AAAA record in the domain. For example:

```
example.com. 86400 IN NS ns2.example.com
ns2.example.com 86400 IN A 20.20.20.20
```

You do not need to manually add an A/AAAA record for the NS record through the Web UI.

### A/AAAA Record

A/AAAA record (Address Record) points a FQDN (fully qualified domain name) to an IP address, so that a host (such as `www.example.com`) can be found. A traditional A/AAAA record is configured with a specific host and a fixed IP for connecting to the host. However, Multihoming dynamically determines the IP according predefined policies. Thus, the settings of an A/AAAA record will associate a host with a policy (please get the A/AAAA record policies configured first).

|                  |                                                                                                                                                                                                                                                                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Host Name</b> | Hostname (prefix) of a computer or server within the domain. Enter "www" if the FQDN to be resolved is <code>www.example.com</code> , or enter the wildcard character * (see <a href="#">Support wildcard in A/AAAA records</a> ). Dot characters within the hostname here is not acceptable.                                    |
| <b>When</b>      | Select a time period for this filter term to evaluate the DNS queries by the receiving time, or leave it as All-Time. See <a href="#">Busyhour Settings</a> for details.                                                                                                                                                         |
| <b>Source</b>    | Define the source IPv6/IPv4 address for this filter term to evaluate DNS queries by where they come from, or leave it as Any Address. This could be a single IP, a range of IPs or an IP subnet.                                                                                                                                 |
| <b>To Policy</b> | Select a predefined A/AAAA record policy used for the domain settings. Specify an A/AAAA policy for DNS queries that match filter items: Host Name, When and Source. According to the policy, Multihoming determines an IP for answering the matched query. All the predefined A/AAAA record policies are list here for options. |
| <b>TTL</b>       | Set the TTL (Time to Live) for the A/AAAA record.                                                                                                                                                                                                                                                                                |

You can associate a hostname with multiple policy by the filter items When and Source. Multihoming resolves the same domain name with different policies by the receiving time and source of the DNS queries. For example:

```
Host Name=www, When=Idle, Source=Any Address, To Policy=Policy_A
Host Name=www, When=Busy, Source=8.8.8.8, To Policy=Policy_B
```

### Support wildcard in A/AAAA records

A wildcard character is supported in Multihoming's A records and AAAA records for resolving domain names. However, the wildcard character \* can only be used standalone. Mixture of a wildcard character and other ASCII characters, such as `"*abc"`, `"abc*"`, `"a*bc"` and `"*.abc"`, will not be accepted by Multihoming. A wildcard character matches the DNS queries for any hostname that is not stated in any NS record, primary name server, external subdomains and other A/AAAA records of a domain, and so that the specified A/AAAA policy matches.

For example, we have a domain `example.com` and its resource records as followings:

```
Primary name server=ns1, IPv4 Address=10.10.10.1
NS Record: Name Server=ns2, IPv4 Address=10.10.10.2
A Record: Host Name=www, To Policy=policy_www
A Record: Host Name=ftp, To Policy=policy_ftp
```

A Record: Host Name=\*, To Policy=policy\_wildcard  
 External Sudomain Record: Subdomain Name=subdomain1  
 NS Record of the subdomain: Name Server=ns3, IPv4 Address=20.20.20.1

Any DNS query for hostnames and subdomain excepting "www", "ftp", "ns1", "ns2", "subdomain1" and "ns3.subdomain1" will match the wildcard A record and be answered according to the wildcard policy *policy\_wildcard*.

- Request for *ns1.example.com* will be answered with *10.10.10.1*.
- Request for *ns2.example.com* will be answered with *10.10.10.2*.
- Request for *ns3.subdomain1.example.com* will be answered with *20.20.20.1*.
- Request for *ftp.example.com* will be answered by *policy\_ftp*.
- Request for *www.example.com* will be answered by *policy\_www*.
- Requests for FQDNs such as *abc.example.com*, *abc.d.example.com* and *abc.d.e.example* will be answered by *policy\_wildcard*.

Note that wildcard character is only supported for A/AAAA and CName records.

## CName Record

CName (Canonical Name) records are used to alias one hostname to another, so that a host can be known by more than one hostname. The hostname of a host that is stated in an A/AAAA record is called the canonical name of the host. It always require an A/AAAA record for the host first to point an alias to the canonical name in a CName record then. An host can have multiple alias name, but an alias can only be assigned to one host.

### Alias

Alias name for a host. This field can be configured in two formats: a hostname (prefix) or a FQDN.

#### Hostname (prefix)

Text string (dot characters within is acceptable) specified here that does not end with a dot character is regarded as a prefix of the alias name, and the base domain specified previously will be appended automatically to this prefix in Multihoming system backend. For example entering "www" or "www.abc" here, if you want to alias a target *host1.example.com* to *www.example.com* or *www.abc.example*.

#### FQDN

On the contrary, text string (dot characters within is acceptable) specified here that ends with a dot character is regarded as a FQDN of the alias name, and the base domain specified previously will not be appended to it in backend. For example entering "www.example.com." or "www.abc.example.com." here, if you want to alias a target *host1.example.com* to *www.example.com* or *www.abc.example*.

The possible sub-domains in an alias name here can be represented as a wildcard character, such as *\*.abc.example* and *\*.example.com* (see [Support wildcard in CName records](#)).

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Target</b> | <p>Canonical name (the real name) of the host that you want to alias. This field can be configured in two formats: a hostname (prefix) or a FQDN.</p> <p><b>Hostname (prefix)</b></p> <p>Text string specified here that does not contain a dot character is regarded as a hostname (prefix) of the target, and the base domain specified previously will be appended automatically to this hostname in Multihoming system backend. For example entering "host1" here if you want to alias <i>host1.example.com</i> to <i>www.example.com</i>. In this case, this name must be stated in an A/AAAA record first.</p> <p><b>FQDN</b></p> <p>Text string specified here that contains dot characters is regarded as a FQDN of the target (but text string that ends with a dot character is not acceptable), and the base domain specified previously will not be appended automatically to it in backend. For example entering "host1.example.com" here if you want to alias <i>host1.example.com</i> to <i>www.example.com</i>, or entering "host.otherdomain.com" here if you want to alias an external target <i>host.otherdomain.com</i> to <i>www.example.com</i>. This can be used to configure a CName record for DKIM signing.</p> |
| <b>TTL</b>    | Set the TTL (Time to Live) for the CName record.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

CName record is a better way to manage alias for a real host than creating multiple A/AAAA records for it, but all the name resolving via CName records will be redirected to the only one A/AAAA record, which is applied to the one A/AAAA record policy. If a host is aliased through multiple A/AAAA records, different A/AAAA records might be applied to each of them.

### Support wildcard in CName records

A wildcard character is supported for Multihoming's CName record to represent all the possible subdomain name in an alias name. For example if the alias name of a CName record is configured as *\*.example.com*, queries for such as

- *www.example.com*
- *ftp.example.com*
- *123.example.com*
- *www.a.example.com*
- *www.a.b.example.com*
- *www.a.b.c.example.com*

will match this CName record and be pointed to a A/AAAA record according to the target name in the CName record. To use the wildcard character in an alias name, it must start with *"\*."*. Combinations such as *"\*abc"*, *"abc\*"*, *"a\*bc"* and *"abc.\*"*, and standalone *"\*"* and *"\*."* are not be acceptable. You can use *\*.example.com*. (do not miss the dot in the end) to cover all the possible subdomain names of *example.com*. The following example describes how it works:

We have a domain *example.com* and its resource records as followings:

```
A Record: Host Name=host1, When=All-Time, Source=Any, To Policy=policy_host1
A Record: Host Name=wildcard1, When=All-Time, Source=Any, To Policy=policy_wildcard1
```



```
A Record: Host Name=wildcard2, When=All-Time, Source=Any, To Policy=policy_wildcard2
CName Record: Alias=www, Target=host1
CName Record: Alias=*.abc, Target=wildcard1
CName Record: Alias=*.example.com., Target=wildcard2
```

Requests are answered as following:

- Request for **www.example.com**:

It matches the alias name `www` and then refers to the A record with the host name `host1` (according to the target name). If the time and source of the request matches this A record, the request will be answered according to the corresponding A record policy: `policy_host1`.

- Request for **www.abc.example.com**:

It matches the alias name `*.abc` and then refers to the A record with the host name `wildcard1` (according to the target name). If the time and source of the request matches this A record, the request will be answered according to the corresponding A record policy: `policy_wildcard1`.

- Request for **123.abc.example.com**:

It matches the alias name `*.abc` and then refers to the A record with the host name `wildcard1` (according to the target name). If the time and source of the request matches this A record, the request will be answered according to the corresponding A record policy: `policy_wildcard1`.

- Request for **www.123.abc.example.com**:

It matches the alias name `*.abc` and then refers to the A record with the host name `wildcard1` (according to the target name). If the time and source of the request matches this A record, the request will be answered according to the corresponding A record policy: `policy_wildcard1`.

- Request for **abc.example.com**:

It matches the alias name `*.example.com.` and then refers to the A record with the host name `wildcard2` (according to the target name). If the time and source of the request matches this A record, the request will be answered according to the corresponding A record policy: `policy_wildcard2`.

- Request for **abc.123.example.com**:

It matches the alias name `*.example.com.` and then refers to the A record with the host name `wildcard2` (according to the target name). If the time and source of the request matches this A record, the request will be answered according to the corresponding A record policy: `policy_wildcard2`.

- Request for **cde.abc.123.example.com**:

It matches the alias name `*.example.com.` and then refers to the A record with the host name `wildcard2` (according to the target name). If the time and source of the request matches this A record, the request will be answered according to the corresponding A record policy: `policy_wildcard2`.

Note that wildcard character is only supported for A/AAAA and CName records.

## DName Record

DName (Delegation Name) records are used to alias an entire subtree of a domain to another. An domain can have multiple alias, but an alias can only be assigned to one domain.

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Alias</b>  | Alias name for a domain. Note that domain name of the domain you are setting for will be appended to the value you specify here, to become the final alias name. For example, specifying the Alias field here with "another" in base domain <i>example.com</i> means you alias a domain (the domain you are required to set in Target field) to <i>another.example.com</i> .                                                                                                                                                                                                   |
| <b>Target</b> | Target domain that you want to alias.<br><br>For in-zone redirection, you should enter "example.com" for the target if you are setting the DName records in the base domain <i>example.com</i> . For example, queries for <i>www.another.example.com</i> will be redirected to <i>www.example.com</i> .<br><br>For out-zone redirection, you could enter another domain name here such as "another.com" or others. Queries for <i>www.another.example.com</i> will be redirected to <i>www.another.com</i> then. Of course, domain <i>another.com</i> must be delegated first. |
| <b>TTL</b>    | Set the TTL (Time to Live) for the DName record.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

### SRV Record

|                 |                                                                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Service</b>  | Specify the symbolic name prepended with an underscore, for example, <i>_http</i> , <i>_ftp</i> or <i>_imap</i> .                                                                                     |
| <b>Protocol</b> | Specify the protocol name prepended with an underscore, for example, <i>_tcp</i> or <i>_udp</i> .                                                                                                     |
| <b>Priority</b> | Specify the relative priority of this service (0 - 65535). Lowest is highest priority.                                                                                                                |
| <b>Weight</b>   | Specify the weight of this service. Weight is used when more than one service has the same priority. The highest is most frequently delivered. Leave is blank or zero if no weight should be applied. |
| <b>Port</b>     | Specify the port number of the service.                                                                                                                                                               |
| <b>Target</b>   | The hostname of the machine providing this service.                                                                                                                                                   |
| <b>TTL</b>      | Set the TTL (Time to Live) for the SRV record.                                                                                                                                                        |

### MX Record

MX (Mail Exchanger) record specifies a mail server responsible for accepting recipient email messages for your domain.

|            |                                               |
|------------|-----------------------------------------------|
| <b>TTL</b> | Set the TTL (Time to Live) for the MX record. |
|------------|-----------------------------------------------|

**Host Name**

The domain name that the mail servers are responsible for. This field can be configured in two formats: a hostname (prefix) or a FQDN.

**Hostname (prefix)**

Text string (dot characters within is acceptable) specified here that does not end with a dot character is regarded as a prefix of the domain, and the base domain specified previously will be appended automatically to this prefix in Multihoming system backend. For example, if a mail server is responsible for the recipient emails such as *user@mail.example.com*, enter "mail" here. If the mail server is responsible for the recipient emails such as *user@example.com*, leave this field blank.

**FQDN**

Text string (dot characters within is acceptable) specified here that ends with a dot character is regarded as a FQDN of the domain, and the base domain specified previously will not be appended to it in backend. For example, if a mail server is responsible for the recipient emails such as *user@mail.example.com*, enter "mail.example.com." here. If the mail server is responsible for the recipient emails such as *user@example.com*, enter "example.com." here.

**Priority**

The priority of the mail servers. This value is used to prioritize mail delivery if multiple mail servers for a domain are available (Note that each mail server requires a corresponding MX record). The higher the priority is, the lower the number is.

**Mail Server**

The host name of the mail server responsible for the domain specify in Host Name field. The host must be manually predefined in an A/AAAA record or a CName record. This field can be configured in two formats: a hostname (prefix) or a FQDN.

**Hostname (prefix)**

Text string specified here that does not contain a dot character is regarded as a hostname (prefix) of the mail server, and the base domain specified previously will be appended automatically to this hostname in Multihoming system backend. For example entering "ms1" here if *ms1.example.com* is the mail sever responsible for domain *mail.example.com* or *example.com*. In this case, this name must be stated in an A/AAAA record first.

**FQDN**

Text string specified here that contains dot characters is regarded as a FQDN of the mail server (but text string that ends with a dot character is not acceptable), and the base domain specified previously will not be appended automatically to it in backend. For example entering "ms1.example.com." here if *ms1.example.com* is the mail sever responsible for domain *mail.example.com* or *example.com*, or entering an external mail server "ms.otherdomain.com" here if it is responsible for domain *mail.example.com* or *example.com*.

For example, to route emails for recipient *user@mail.example.com* to a mail server *mail1.example.com*, it requires the following A/AAAA record and MX record:

- **A/AAAA record:** Host Name=mail1, When=All-Time, Source IP=Any Address, To Policy=Policy\_A
- **MX record:** Host Name=mail, Priority=10, Mail Server=mail1

If you want to route emails for recipient *user@example.com* to mail servers *mail1.example.com* and *mail2.example.com*, it requires the following A/AAAA record and MX record:

- **A/AAAA record:** Host Name=mail1, When=All-Time, Source IP=Any Address, To Policy=Policy\_A
- **A/AAAA record:** Host Name=mail2, When=All-Time, Source IP=Any Address, To Policy=Policy\_B
- **MX record:** Host Name=[blank], Priority=10, Mail Server=mail1
- **MX record:** Host Name=[blank], Priority=20, Mail Server=mail2

Mail server *mail1.example.com* has higher priority and is the more preferred for recipient emails *user@example.com*.

### TXT Record (multiple TXT records on one hostname is allowed)

TXT (Text) record provides text information a host. The text can be used for a variety of purposes depending on what you're using the TXT record for. For example, Sender Policy Framework (SPF) is one of the most common uses for TXT records. TXT records can also be used to describe a server, network, data center, and other accounting information by containing human readable information.

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>TTL</b>       | Set the TTL (Time to Live) for the TXT record.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Host Name</b> | <p>The prefix of a domain name that the TXT record is used for. This field can be configured in two formats: a hostname (prefix) or a FQDN.</p> <p><b>Hostname (prefix)</b></p> <p>Text string specified here that does not contain a dot character is regarded as a hostname (prefix) of the domain, and the base domain will be appended automatically to this hostname in Multihoming system backend. For example, if this TXT record is used for a domain <i>mail.example.com</i>, enter "mail" here. If the TXT record is used for base domain <i>example.com</i>, leave this field blank.</p> <p><b>FQDN</b></p> <p>Text string specified here that contains dot characters is regarded as a FQDN of the domain, and the base domain will not be appended automatically to this it in backend. For example, if this TXT record is used for a domain <i>mail.example.com</i>, enter "mail.example.com" here. If the TXT record is used for base domain <i>example.com</i>, enter "example.com" here.</p> |
| <b>TXT</b>       | Free form text data of any type or information in format <attribute name>=<attribute value> for specific purposes. For example using a TXT record for SPF to fight spam, you could specify "v=spf1 a:mail ip4:10.16.130.2/24 ~all" here, which means emails sent from domain IP 10.16.130.2/24 are effective, while emails sent from other IPs are assumed as spams.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

### External Subdomain Record (available only in non-relay mode)

External subdomain records are used to delegate the responsibility for subdomains to other name servers, which means the responsibility for the administration of a subdomain (such as *child*) of the base domain (such as *example.com*) will be delegated to another management group (such as *child.example.com*). Multihoming (the name server of base domain *example.com*) is responsible for redirecting all the queries which end with *child.example.com* to the subdomain name servers.

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Subdomain Name</b> | The prefix of the delegated subdomain. For example, if the delegated subdomain is <i>child.example.com</i> , enter <i>child</i> here. Note that this name can not be a duplicate of what is specified to the A/AAAA, NS, CName, DName or MX record in the base domain.                                                                                                                                                                                                                                                                                        |
| <b>NS Record</b>      | Specify the external name servers that the subdomain is delegated to. The NS records here will point the subdomain to the responsible name servers. Note that Multihoming only answers the IP addresses of external name servers authoritative for the subdomain to the queries for anything in the subdomain. So please have the external name servers (another machines) configured and online first. If the name servers authoritative for the subdomain is not a FortiWAN running Multihoming, inbound load balancing is not available for the subdomain. |
| <b>Name Server</b>    | Hostname (prefix) or FQDN of the external name server authoritative for the subdomain. Enter "ns1" or "ns1.child.example.com.", if the name server's FQDN is "ns1.child.example.com" for example. See section NS Record above for details.                                                                                                                                                                                                                                                                                                                    |
| <b>IPv4 Address</b>   | IPv4 address of the name server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>IPv6 Address</b>   | IPv6 address of the name server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

### Relay Mode

To enable Multihoming in relay mode, go to **Service > Multihoming** on the Web UI, check the boxes **Enable Multihoming** and **Enable Relay**.

When Relay is enabled, FortiWAN will relay the DNS requests it receives to a specified name servers, and reprocess the answer with appropriate IP address according to the AAAA/A record policies. The necessary configurations for Multihoming in Relay Mode are AAAA/A Record Policy and Domain Settings. The name server the Multihoming Relay Mode forward a DNS request to must be configured in field "Domain Settings". Only if the AAAA/A record of the request answer that the name server responds to FortiWAN matches Multihoming's AAAA/A Record, the request answer will be reprocessed with appropriate IP address according to the AAAA/A record policies, otherwise, Multihoming will simply forward the DNS answer to client without any changing. **Please make sure the same configuration of AAAA/A record on both FortiWAN Multihoming and the specified name server working with Multihoming Relay Mode.**

Note that it's necessary to update the registrations on your parent domain with FortiWAN's localhost IP addresses, so that a request for your domain can be delivered to FortiWAN and forwarded to the specified name server.

For other query type such as MX and TXT, Multihoming's Relay Mode will simply forward the answer from the specified name server to clients.

## Policy Settings: A/AAAA Record Policy

Please refer to **Policy Settings: A/AAAA Record Policy** in Non-relay mode.

### Domain Settings

#### Domain Name

|                    |                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------|
| <b>Domain Name</b> | The registered domain name that Multihoming relays the queries for, such as <i>example.com</i> . |
|--------------------|--------------------------------------------------------------------------------------------------|

#### Name Server

|                     |                                                                                                                    |
|---------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>IPv4 Address</b> | Specify the IPv4 addresses of the name servers authoritative for the domain and Multihoming relays the queries to. |
| <b>IPv6 Address</b> | Specify the IPv6 addresses of the name servers authoritative for the domain and Multihoming relays the queries to. |

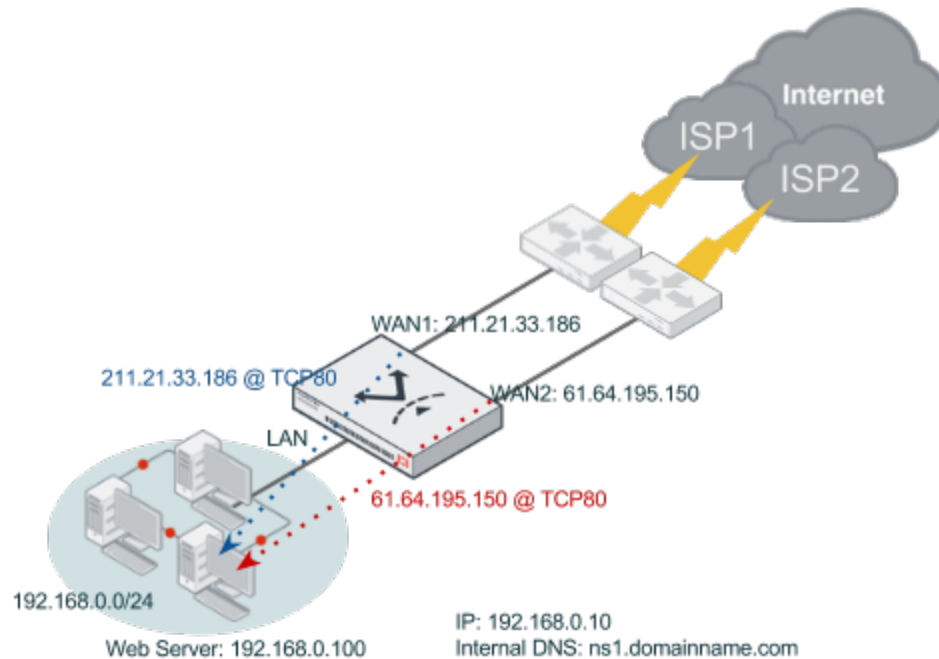
#### A/AAAA Record

Please refer to **A/AAAA Record** in Non-relay mode.

## Scenarios

### Example 1

Here is a typical usage to balance inbound traffic load by Multihoming (non-relay mode). Thinking about the inbound traffic to access a virtual server on FortiWAN, Multihoming distributes the accesses over Multiple WAN links by dynamically answering the best WAN link IP to DNS queries for *www.domainname.com* (domain name of the virtual server). The followings are the related configurations.



An internal web server (192.168.0.100 on HTTP 80) is installed in LAN and virtual server on FortiWAN is associated with it by the following settings on Web UI: Service > Virtual Server (See [Virtual Server](#) for details):

| WAN IP        | Service   | Algorithm   | Server Pool   |          |
|---------------|-----------|-------------|---------------|----------|
|               |           |             | Server IP     | Service  |
| 211.21.33.186 | HTTP (80) | Round-Robin | 192.168.0.100 | HTTP(80) |
| 61.64.195.150 | HTTP (80) | Round-Robin | 192.168.0.100 | HTTP(80) |

This web server is bound to the two WAN ports. Accesses on 211.21.33.186 and 61.64.195.150 for HTTP 80 will be translated to the real server 192.168.0.100 in LAN. To get details about WAN configurations, see [Configuring your WAN](#).

To make accesses distributed among the two WAN links according to their upstream load, you need to have Multihoming configured as follows. Go to Service > Multihoming on Web UI, enable Multihoming (disable Relay) and have the following basic settings configured.

### A Record Policy Settings

| Policy Name | Algorithm   | Policy Advance Setting |               |
|-------------|-------------|------------------------|---------------|
|             |             | WAN Link               | IPv4 Address  |
| web         | By Upstream | 1                      | 211.21.33.186 |
|             |             | 2                      | 61.64.195.150 |

## Domain Settings

You need to register the domain *domainname.com*, the responsible name server *ns1.domainname.com* and its IP address 211.21.33.186 to a registrar.

| Domain Name    | TTL | Responsible Mail     | Primary Name Server | IPv4 Address  |
|----------------|-----|----------------------|---------------------|---------------|
| domainname.com | 30  | admin.domainname.com | ns1                 | 211.21.33.186 |

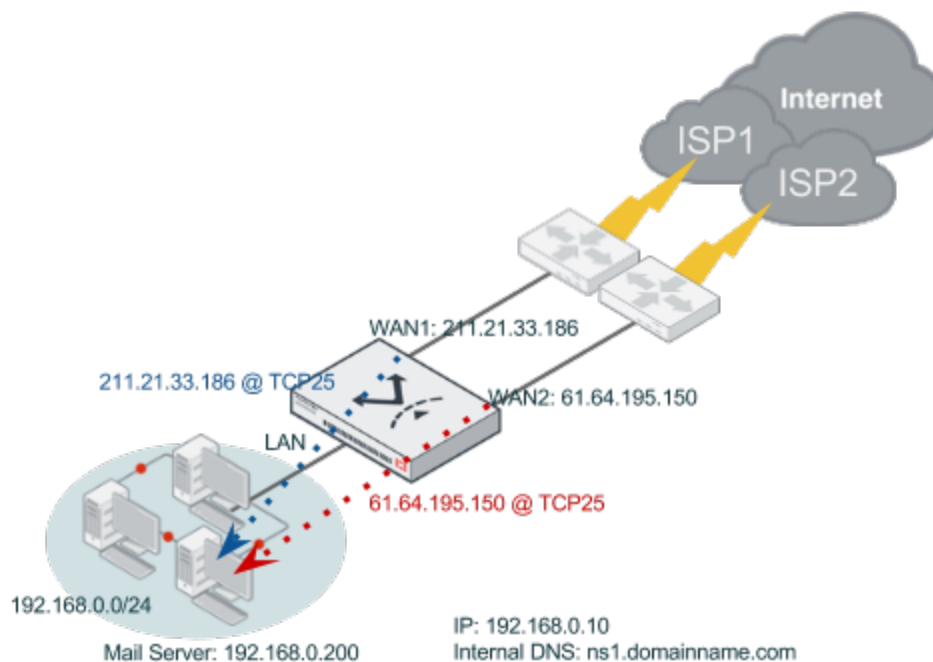
## A/AAAA Record

| Host Name | When     | Source IP | To Policy | TTL |
|-----------|----------|-----------|-----------|-----|
| www       | All-Time | Any       | web       | 30  |

Multihoming answers to queries for *www.domainname.com* with IP address (211.21.33.186 or 61.64.195.150) of the better one of the two WAN links according to their upstream load, so that external users can always access the virtual server through an efficient WAN link.

## Example 2

Here is another similar usage for Multihoming and an internal SMTP server. Multiple will answer the mail server responsible for accepting recipient email for domain *domainname.com*, for example *user@domainname.com*.



An internal mail server (192.168.0.200 on SMTP 25) is installed in LAN and virtual server on FortiWAN is associated with it by the following settings on Web UI: Service > Virtual Server (See [Virtual Server](#) for details):



| WAN IP        | Service  | Algorithm   | Server Pool   |          |
|---------------|----------|-------------|---------------|----------|
|               |          |             | Server IP     | Service  |
| 211.21.33.186 | SMTP(25) | Round-Robin | 192.168.0.200 | SMTP(25) |
| 61.64.195.150 | SMTP(25) | Round-Robin | 192.168.0.200 | SMTP(25) |

To make accesses distributed among the two WAN links by weighted round-robin, you need to have Multihoming configured as followings. Go to Service > Multihoming on Web UI, enable Multihoming (disable Relay) and have the following basic settings configured.

### A Record Policy Settings

| Policy Name | Algorithm | Policy Advance Setting |               |        |
|-------------|-----------|------------------------|---------------|--------|
|             |           | WAN Link               | IPv4 Address  | Weight |
| smtp        | By Weight | 1                      | 211.21.33.186 | 1      |
|             |           | 2                      | 61.64.195.150 | 1      |

### Domain Settings

You need to register the domain *domainname.com*, the responsible name server *ns1.domainname.com* and its IP address 211.21.33.186 to a registrar.

| Domain Name    | TTL | Responsible Mail     | Primary Name Server | IPv4 Address  |
|----------------|-----|----------------------|---------------------|---------------|
| domainname.com | 30  | admin.domainname.com | ns1                 | 211.21.33.186 |

### A/AAAA Record

| Host Name | When     | Source IP | To Policy | TTL |
|-----------|----------|-----------|-----------|-----|
| mail1     | All-Time | Any       | smtp      | 30  |

### MX Record

| TTL | Host Name        | Priority | Mail Server |
|-----|------------------|----------|-------------|
| 30  | [Leave it blank] | 1        | mail1       |

## Tunnel Routing

**Tunneling** is a technique to perform data transmission for a foreign protocol over a incompatible network; such as running IPv6 over IPv4, and the transmission of data for use within a private, corporate network through a public network. Tunneling is done by encapsulating and decapsulating data and information of the particular protocol within the incompatible transmission units symmetrically.

Traditional tunneling is established over single WAN link which is a lack of load balancing and fault tolerance. FortiWAN's Tunnel Routing (TR) is a technique that builds a special connection between two FortiWAN units to deliver **link aggregation** and **fault tolerance** over multiple WAN links ideally tailored for multinational intranet systems. Different to Auto Routing distributing sessions over WAN links, Tunnel Routing breaks further a session down to packets over multiple WAN links and allows data to be prioritized during transfer while boosting the performance of critical services such as VPN and live video streaming while avoiding delays and data loss.

Basically, FortiWAN's Tunnel Routing implies routing packets of a session over tunnels (WAN links), which contains the two elements - **Tunnels** and **Routing**.

### GRE Tunnel

FortiWAN's Tunnel Routing sets up proprietary tunnels between symmetric FortiWAN sites (local and remote) with GRE (Generic Routing Encapsulation) protocol. GRE (Generic Routing Encapsulation) Protocol packs the Payload (Original Packet) with Delivery Header and GRE Encapsulation Header. Physically, a point-to-point GRE tunnel for Tunnel Routing is the transimission of GRE packets via a pair of WAN links predefined on the symmetric FortiWAN sites (a WAN link on the local FortiWAN, and another one on the remote FortiWAN) (See "Tunnel Group" and "Group Tunnel" in "[Tunnel Routing - Setting](#)").

### Routing

With the multiple WAN links on each FortiWAN, Tunnel Routing distributes (routes) GRE packets of a session over the GRE tunnels (a tunnel group) according the balancing algorithms and tunnel status detection. This is what the load balancing and fault tolerance Tunnel Routing provides for tunneling. Moreover, with proper policy setting, Tunnel Routing can route GRE packets over multiple sites (more than two sites) without full-mesh connections between the sites (See "Default Rule", "Routing Rule" and "Persistent Rules" in "[How to set up routing rules for Tunnel Routing](#)"). Briefly, it performs routing of GRE packets over multiple tunnels and multiple sites.

### Next we introduce Tunnel Routing in the following topics:

[How the Tunnel Routing Works](#)

[Tunnel Routing - Setting](#)

[How to set up routing rules for Tunnel Routing](#)

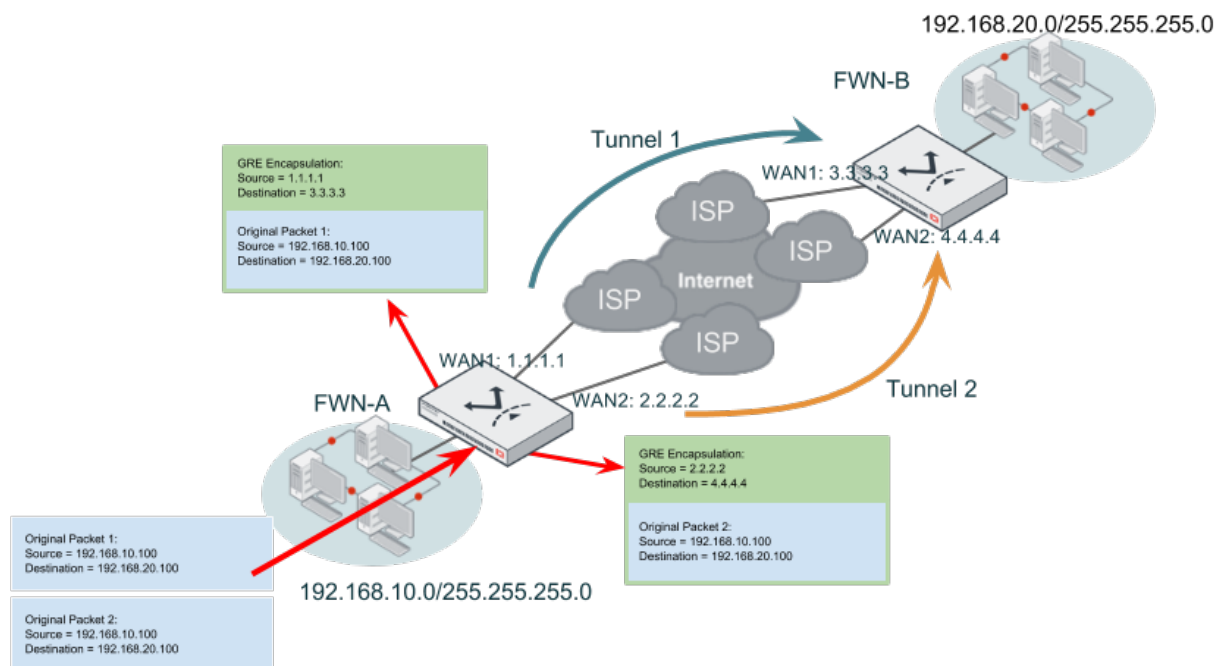
[Tunnel Routing - Benchmark](#)

[Scenarios](#)

## How the Tunnel Routing Works

Here is an example to explain the processes that how Tunnel Routing delivers packets to remote private internal network via Internet. Here are two FortiWAN sites (FWN-A and FWN-B) connected to Internet with two WAN links respectively. Two private LAN networks: 192.168.10.0/255.255.255.0 and 192.168.20.0/255.255.255.0 are connected to FWN-A and FWN-B respectively. Now host 192.168.10.100 would like to communicate with host 192.168.20.100 which is located at remote private LAN. Here are the steps:

1. Host 192.168.10.100 sends the first original packet to FWN-A, source IP and destination IP of the packet are indicated as 192.168.10.100 and 192.168.20.100.
2. FWN-A's Tunnel Routing takes charge of transferring the packet because it matches a tunnel routing rule (A routing rule is predefined for packets from 192.168.10.0/255.255.255.0 to 192.168.20.0/255.255.255.0).
3. According the specified balancing algorithm (determining a WAN link for transferring), FWN-A encapsulates the original packet with GRE and Delivery headers which the source IP and destination IP are indicated as public addresses 1.1.1.1 (FWN-A's WAN 1) and 3.3.3.3 (FWN-B's WAN 1) respectively.
4. The GRE packet is then transferred via Tunnel 1 (from FWN-A's WAN 1 to FWN-B's WAN 1 via Internet).
5. FWN-B receives this GRE packet and decapsulates it to recover the original packet.
6. The original packet then is forwarded to host 192.168.20.100 in the private LAN network.
7. The subsequent packets (for example the packet 2 in the figure below) of the session from host 192.168.10.100 are transferred in the same way except the different tunnels that balancing algorithm determines.



After the basic concept how Tunnel Routing transfers packets, several topics related to Tunnel Routing are explained in detail.

## Priority over Auto Routing and NAT

Tunnel Routing rules are in higher priority than Auto Routing rules and NAT rules for FortiWAN matching packets with. Predefine a Tunnel Routing rule, a Auto Routing rule (See ["Auto Routing"](#)) and a NAT rule (See ["NAT"](#)) with

the same source and destination, packets that are indicated the source and destination will be first matched to the Tunnel Routing rule and transferred by Tunnel Routing, without be processed by FortiWAN's Auto Routing and NAT.

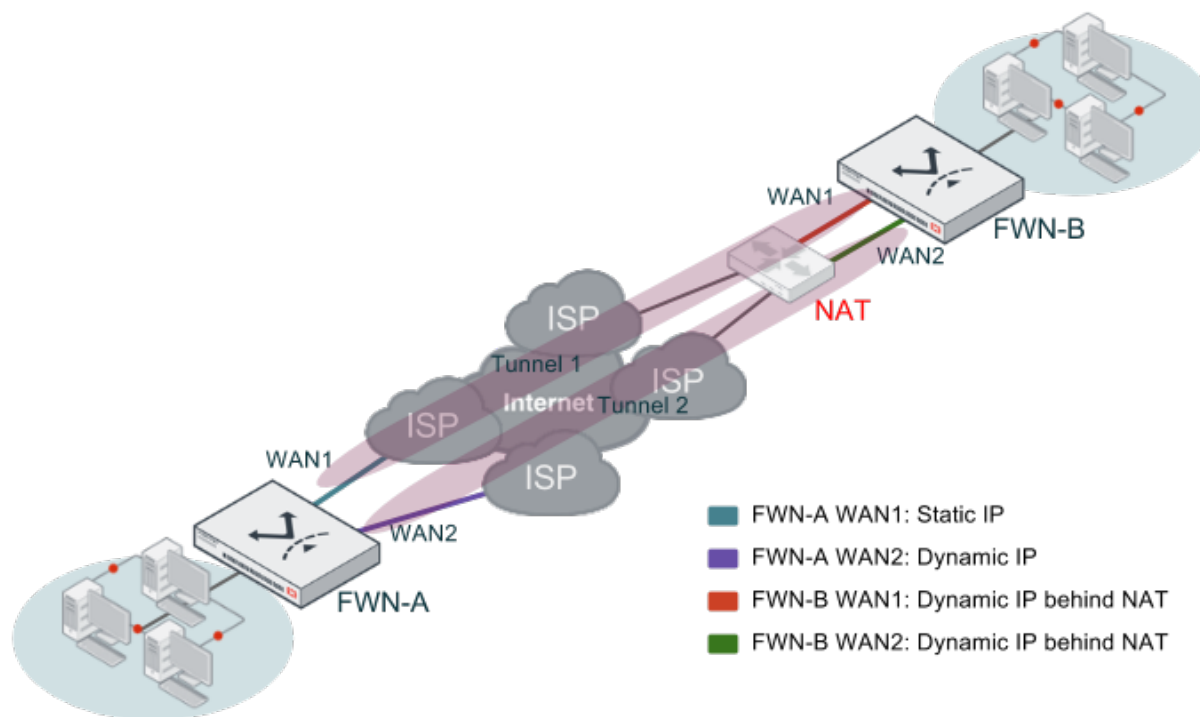
### Tunnel healthy detection

Tunnel Routing maintains a unique mechanism of healthy detection for tunnels, which is different from FortiWAN's WLHD (See "[WAN Link Health Detection](#)"). Symmetric FortiWAN sites continue sending GRE encapsulated detection packets to each other via the defined tunnels. The detection receiver on each FortiWAN site decides the status of a tunnel (OK or Fails) by monitoring if the detection packets arrive continuously. Tunnel Routing's balancing algorithms distribute packets only over those healthy tunnels, so that the network connection and the data transfer reliability are guaranteed. Tunnel Routing's healthy detection contains the whole connection between two FortiWAN sites (from the WAN link one side to the WAN link another side via Internet), while WLHD only detects the status of connections to Internet. Therefore, the two mechanisms might show different detection result. For example, the Web UI reports a WAN link is OK but a tunnel established with the WAN link is failed. This might be the failed WAN link on the opposite site of the tunnel. For another example, the Web UI reports a WAN link is failed but a tunnel established with the WAN link is OK. This might because a incorrect configuration to WLHD results in incorrect detection.

See [Configuring the parameters for tunnel health detection](#) for the setting details.

### Dynamic IP addresses and NAT pass through

FortiWAN's Tunnel Routing supports dynamic IP addresses and NAT pass through. Only one **static public IP address** (No NAT employed to the static IP address) is required for tunnel routing deployment between the symmetric FortiWAN sites. A negotiation will be dynamically performed via the only one static public IP address to synchronize the dynamic IP addresses and the IP addresses of NAT device to each other. Therefore, changes on dynamic IP addresses or IP addresses NAT device causes no damage to tunnel connections. Note that NAT pass through for Tunnel Routing here is not the NAT function of FortiWAN, FortiWAN will never perform NAT translation for tunnel packets. The NAT pass through here is for the application that another NAT device in front of FortiWAN. Usually, this happens when a ISP provides WAN links with private IP addresses and does NAT translation for the private WAN links on the ISP side.



## IPSec Support

Although Tunnel Routing provides itself a simple data protection by encrypting the data payload of original packets, it is not secure enough as standard IPSec's protection. IPSec defines rigorous procedures on security parameters negotiation, key exchange and authentication to prevent any compromise. Various encryption and authentication algorithms, and key strengths are contained in IPSec, so that various security levels are provided. With IPSec protection, a standard virtual private network (VPN) can be implemented.

Although Tunnel Routing connects two incompatible networks (private networks) by tunneling through Internet, it is seriously not a standard VPN since it is short on security. FortiWAN IPSec (Transport mode) is capable of protecting Tunnel Routing tunnels, so that Tunnel Routing becomes qualified to the standard VPN. With IPSec protection, Tunnel Routing not only functions in a securer way, but also keeps the advantage of bandwidth aggregation and fault tolerance between tunnels. The only sacrifice is dynamic IP addresses and NAT pass through are not supported for Tunnel Routing over IPSec. Besides, deployments of Tunnel Routing over IPSec is limited. For more information about Tunnel Routing over IPSec, please refer to "[IPSec - About FortiWAN IPSec VPN](#)", "[Limitation in the IPSec deployment](#)" and "[IPSec - Define routing policies for an IPSec VPN](#)".

## How to reach to a maximum of aggregated throughput

Tunnel Routing spreads packets of a session over multiple tunnels and arranges the packets in correct order at the opposite site, then forwards the well-ordered packets to the destinations. Different quality of tunnels (Round Trip Time between the two ends of a tunnel) causes different latency to packets arriving, which is the major factor for data transmission performance. Bad quality of a tunnel or greatly difference of quality between tunnels will cause packet loss and retransmission in higher possibility, which results in terrible decrease in Tunnel Routing transmission performance.

## Throughput of a tunnel

As the previous description, a logical tunnel is established by two FortiWAN units via two physical WAN links (such as WAN1 of FWN-A and WAN2 of FWN-B in the above diagram). Throughput of the tunnel is bounded by one of the two WAN links with the worst throughput. For example, if throughput of the two WAN links are 30Mbps and 50Mbps respectively, packets can not be transferred via the tunnel at speed higher than 30Mbps. We can roughly say that throughput of the tunnel is 30Mbps.

## Latency that a tunnel group

Ideally, we expect data transmission over tunnels can reach to the summary of the maximum throughput of the tunnels. For example, you might expect a speed close to 100 Mbps if both the two tunnels are 50Mbps. However, realistic network latency and transport layer protocols make it impossible to aggregate the bandwidth in such perfect way. We tried to figure out the factors affecting Tunnel Routing performance, and network latency is surely the major one. If packets of a session is transferred via a group of tunnels (packets are distributed among the tunnels, the concept of tunnel group will be introduced in [Tunnel Routing - Setting](#)), performance of the transmission will be mainly influenced by the highest latency of the participating tunnels. For example, if connection latency of two tunnels (such as Tunnel1 and Tunnel2 in above diagram) are 10ms and 30ms respectively, a transmission via the two tunnels will suffer from 30ms delays. We can roughly say that the latency that the tunnel group is experiencing is 30ms.

## Evaluation of your tunnels

The throughput and quality of WAN links so that are the important factors in your plan for deploying a Tunnel Routing network. Basically, WAN links with better quality (lower latency) bring better performance for Tunnel Routing transmission. Measuring the latency of all the pairs of WAN links between two FortiWAN units in advance helps you to determine the WAN links for the Tunnel Routing network. For example, two FortiWAN units have three WAN links individually, and the latency of all the pairs of WAN links between the two units is as followings:

|                   | <b>FWN-A-WAN1</b> | <b>FWN-A-WAN2</b> | <b>FWN-A-WAN3</b> |
|-------------------|-------------------|-------------------|-------------------|
| <b>FWN-B-WAN1</b> | 45ms              | 50ms              | <b>15ms</b>       |
| <b>FWN-B-WAN2</b> | <b>30ms</b>       | 55ms              | 65ms              |
| <b>FWN-B-WAN3</b> | 55ms              | <b>20ms</b>       | 52ms              |

According the above measure, pairs of FWN-A's WAN1 and FWN-B's WAN2, FWN-A's WAN2 and FWN-B's WAN3, and FWN-A's WAN3 and FWN-B's WAN1 are the better connections among all the pairs. It seems that the three WAN link pairs are qualified to be used for establishing tunnels in your Tunnel Routing network. You can pick two or three of them and combine them into a tunnel group. FortiWAN provides a benchmark (See "[Tunnel Routing - Benchmark](#)") to measure the latency (RTT) and evaluate the tunnels , which is helpful to plan a Tunnel Routing network.

Now let's see how the latency influence Tunnel Routing performance. If the WAN link pairs of FWN-A's WAN1 and FWN-B's WAN2, and FWN-A's WAN3 and FWN-B's WAN1 are used to establish tunnels for a tunnel group, the throughput of the WAN links and the two tunnels are as following:

|                            | Tunnel 1      |            | Tunnel 2      |               |
|----------------------------|---------------|------------|---------------|---------------|
|                            | FWN-A-WAN1    | FWN-B-WAN2 | FWN-A-WAN3    | FWN-B-WAN1    |
| <b>Throughput/WAN link</b> | <b>50Mbps</b> | 60Mbps     | 100Mbps       | <b>50Mbps</b> |
| <b>Throughput/tunnel</b>   | <b>50Mbps</b> |            | <b>50Mbps</b> |               |

As the previous discussion that throughput of a tunnel is bounded to the worse WAN link, throughput of the two tunnels is bounded to 50Mbps. Similar according previous definition, transmission through the tunnel group consisting of the two tunnels suffers from 30ms delay, which is the higher latency of the two tunnels. However, according to measure, this Tunnel Routing deployment (two 50Mbps tunnels with 30ms latency) results in 69Mbps performance, which is 69% usages of the two tunnels (69Mbps/50Mbps+50Mbps). In the measurement of tunnel performance and latency, bandwidth of the participating WAN links is wholly available for the Tunnel Routing transmission; there is no other traffic occupied the bandwidth.

|                                | Tunnel Group |          |
|--------------------------------|--------------|----------|
|                                | Tunnel 1     | Tunnel 2 |
| <b>Latency/tunnel</b>          | 30ms         | 15ms     |
| <b>Latency/tunnel group</b>    | 30ms         |          |
| <b>Throughput/tunnel</b>       | 50Mbps       | 50Mbps   |
| <b>Throughput/tunnel group</b> | 69Mbps       |          |
| <b>Bandwidth Usage</b>         | 69%          |          |

With the same latency of a tunnel group, the higher throughput of each the participating tunnel brings lower aggregation percentage, which means the higher throughput the tunnels the lower latency is required to remain the aggregation percentage at the same level. For example, the following measurement shows how the aggregation percentage of tunnels performance is varied by single tunnel's throughput under the same latency.

|                                | Tunnel Group |          | Tunnel Group |          | Tunnel Group |          |
|--------------------------------|--------------|----------|--------------|----------|--------------|----------|
|                                | Tunnel 1     | Tunnel 2 | Tunnel 1     | Tunnel 2 | Tunnel 1     | Tunnel 2 |
| <b>Latency/tunnel group</b>    | 30ms         |          |              |          |              |          |
| <b>Throughput/tunnel</b>       | 50Mbps       | 50Mbps   | 100Mbps      | 100Mbps  | 250Mbps      | 250Mbps  |
| <b>Throughput/tunnel group</b> | 69Mbps       |          | 70Mbps       |          | 92Mbps       |          |
| <b>Bandwidth Usage</b>         | 69%          |          | 35%          |          | 18%          |          |

With the same conditions, packets of a session are transferred through the tunnel group consisting of two 100Mbps tunnels at a maximum of 70Mbps. Bandwidth usages of the two tunnels is down to 35%. It might require latency less than 5ms to bring bandwidth usage of the two 100Mbps tunnels close to 60%.

The above measurement gives basic concept that how the performance of a Tunnel Routing transmission is influenced. Both the throughput (bandwidth) of single WAN link and its connection latency deeply influence the performance, and these factors greatly concern the plan you deploy the Tunnel Routing network. The above data is for your reference, some variations in details are possible.

### Throughput of bidirectional TR transmission

For one-way TR transmission, although either download or upload bandwidth of tunnels is consumed by the transferred data packets, bandwidth (in the opposite direction) is available to get relative TCP control packets responded in acceptable latency and correct order. Both the download and upload bandwidth will be consumed if the tunnels are loaded with bidirectional connections. Respondent TCP control packets of a connection and data packets of another connection will scramble for limited bandwidth. In the meantime, distributing TCP control packets of a connection over tunnels must bring higher latency and out-of-order delivery and result in poor transmission performance. To guarantee expected throughput for bidirectional TR transmission, FortiWAN Tunnel Routing fixes TCP control packets (packets without data payloads) of all connections running on a TR group to a single tunnel (rather than distributing them over tunnels), which will significantly reduce latency and out-of-order delivery. This specific tunnel is not reserved for only TCP control packets, parts of data packets of connections will also be assigned to this tunnel according to the specified balancing algorithm. Therefore, this specific tunnel is supposed to be the most stable (largest bandwidth, best quality) one in the tunnel (refer to the above description for how to evaluate a tunnel). This mechanism requires no extra configurations, but needs posit the tunnels on the configuration GUI in a appropriate ordering , see [Tunnel Routing - Setting](#).

### Persistent Route in Tunnel Routing

As the above description, Tunnel Routing could hardly 100% aggregate bandwidth of multiple tunnels for TCP connections. TCP is intrinsically such sensitive to factors, such as latency, packet out-of-order delivery, TCP window size, quality of the links and etc., so that there will always be a bottleneck to the transmission performance, as long as packets of each connection are distributed over multiple tunnels. However, on the other hand, higher bandwidth usage (almost 100%) of multiple tunnels could be achieved if Tunnel Routing just persistently transfers packets of each connection via a single tunnel rather than distributing them over multiple tunnels. Like the cooperation of Persistent Routing and Auto Routing (see [Outbound Load Balancing and Failover \(Auto Routing\)](#) and [Persistent Routing](#)), Tunnel Routing supposes the Persistent Routing as well. Although a persistently-routed TR connection will be bounded in performance by the maximum throughput of the tunnel that TR fixes it to (conversely, a packet-distributed TR connection can use aggregated bandwidth of tunnels, even if it is about a maximum of 70% aggregation), in real practice, Tunnel Routing will not serve only one connection at a time; there will always be various connections existing concurrently between two sites and tunnels are full of their traffic. In that case, each connection need compete with others for available bandwidth and it is hard to tell whether a packet-distributed connection or a persistently-routed connection runs in better throughput, but it certainly gives higher usage of overall bandwidth if all the connection in tunnels are persistently-routed.

Here is the comparison between packet-distributed TR connection and persistently-routed TR connection.

#### Packet-distributed TR connection

- Bandwidth of multiple tunnels are aggregated for a connection.
- There is no impact to a connection when single tunnel fails.
- A connection is sensitive to TCP parameters of all the participating tunnels.
- A connection can hardly use more that 70% aggregated bandwidth.
- The overall connections running on the tunnels can hardly use more that 70% aggregated bandwidth.



### Persistently-routed TR connection

- Bandwidth aggregation is not available for a connection.
- Single tunnel failure impacts the connection.
- Only TCP parameters of the specified tunnel effects the connection.
- Performance of a connection is bounded by throughput of the specified tunnel.
- The overall connections running on the tunnels can use almost 100% aggregated bandwidth (number of connections must be larger than number of participating tunnels).

You might have various non-critical traffic and critical applications between sites in the Tunnel Routing (intranet) network. Packet-distributed Tunnel Routing is suggested for critical application requiring higher level of load-balancing and fault-tolerance, such as remote database backup, while persistently-routing Tunnel Routing might be more suitable to non-critical traffic for better overall TR transmission performance. Tunnel Routing performance is a complex topic, so that you need to take a deliberation on this before configuration. See section Persistent Rules in [How to set up routing rules for Tunnel Routing](#) for configuring it.

### Default rule

If your TR network deployment requires more than 100 TR routing rules, replacing the TR routing rules with TR default rules will be suggested for better performance (see [How to set up routing rules for Tunnel Routing](#)).

### Monitoring quality of a tunnel

Transmission quality of tunnels is one of the important factors determines the transmission performance of Tunnel Routing. A tunnel with poor quality becomes a encumbrance seriously decreasing the entire throughput of a tunnel group. However this kind of impact can be mitigated by stopping packets for the poor-quality tunnel in the tunnel group.

For example, a tunnel group consists of three tunnels, and each of them has 50Mbps throughput. When all of the tunnels are in good quality the entire TR transmission (packets are distributed over the three tunnels) maybe reach 100Mbps, which is a best case. Once one of the tunnels becomes extreme low-throughput because of unexpected delay, the entire throughput of the tunnel group could very well be lower than 69Mbps (maybe 60Mbps or worse); which means a three-tunnels group is worse than a two-tunnels group in this case. Removing this bad tunnel from the group or stopping distributing packets to the tunnel can recover the entire throughput back to what a two-tunnels group is supposed to be.

As the previous discussion we suggest the tunnels of a tunnel group are equal in quality for having a reasonable and stable TR performance. It is expected that a tunnel that is always in bad quality will not be used in the tunnel group. However in physical network unexpected communication problem, such as packet loss and increased delay, causing temporary poor quality is unavoidable. FortiWAN provides a mechanism to monitor the quality of each tunnel in a tunnel group. According to a predefined quality policy, FortiWAN dynamically determines whether a tunnel is having low quality. Once it is identified, FortiWAN will trigger the process to stop distributing packets to this tunnel until this tunnel backs to normal.

Packet RTT (round-trip time) and jitter (the variation in the latency on a packet flow) between the two endpoints of a tunnel are used to evaluate the quality of tunnels. By specify the RTT and jitter thresholds and time durations in a policy, FortiWAN can identify quality of a tunnel, stop distributing packets to the tunnel when it is in poor quality and join the tunnel in the packet distribution when its quality backs to normal.

See [Configuring tunnel quality policies](#) for the setting details.

## Bandwidth Management

Tunnel Routing is designed to be transparent to FortiWAN's Bandwidth Management (See "[Bandwidth Management](#)"). The way to allocate or limit bandwidth to traffic of Tunnel Routing is to drill it down to the original packets, control the traffic by individual service, source or destination. In other words, traffic of each service processed by Tunnel Routing can be controlled individually. Guaranteeing proper bandwidth to individual traffic helps for the performance of Tunnel Routing transmission. Packets encapsulated by Tunnel Routing becomes invisible to Bandwidth Management; controlling the overall Tunnel Routing traffic by service GRE will go to failure.

## Scale

For large-scale Tunnel Routing network deployment, FortiWAN supports up to 100 tunnel groups for FWN-200B, 400 tunnel groups for FWN-1000B and 1000 tunnel groups for FWN-3000B. All of the three models have a default maximum total allowed enable amount of 2500 GRE tunnels (total amount of enabled GRE tunnels of all the tunnel groups).

FortiWAN provides mechanisms to record, notify and analysis on events refer to the Tunnel Routing service, see "[Log](#)", "[Statistics: Tunnel Status](#)", "[Statistics: Tunnel Traffic](#)", "[Report: TR Status](#)" and "[Report: TR Reliability](#)".

## See also

[Tunnel Routing](#)

[Tunnel Routing - Setting](#)

[How to set up routing rules for Tunnel Routing](#)

[Tunnel Routing - Benchmark](#)

[Scenarios](#)

## Tunnel Routing - Setting

There are two major steps to set up Tunnel Routing, **define the association of tunnels** (see the tables: **Basic Setting** and **Tunnel Group**) and **set up the routing rules** (see the tables: **Default Rules**, **Routing Rules** and **Persistent Rules**). Tunnel Routing works in symmetric FortiWAN sites, when the unit we are talking about or configuring to is called **local host** (or local site), the opposite unit is then called **remote host** (or remote site).

### Basic Setting

The basic settings are located here: enabling or disabling Tunnel Route logging, define names and entering tunnel routing activation key (if the encryption function is enabled for a tunnel group).

#### Tunnel Route Log

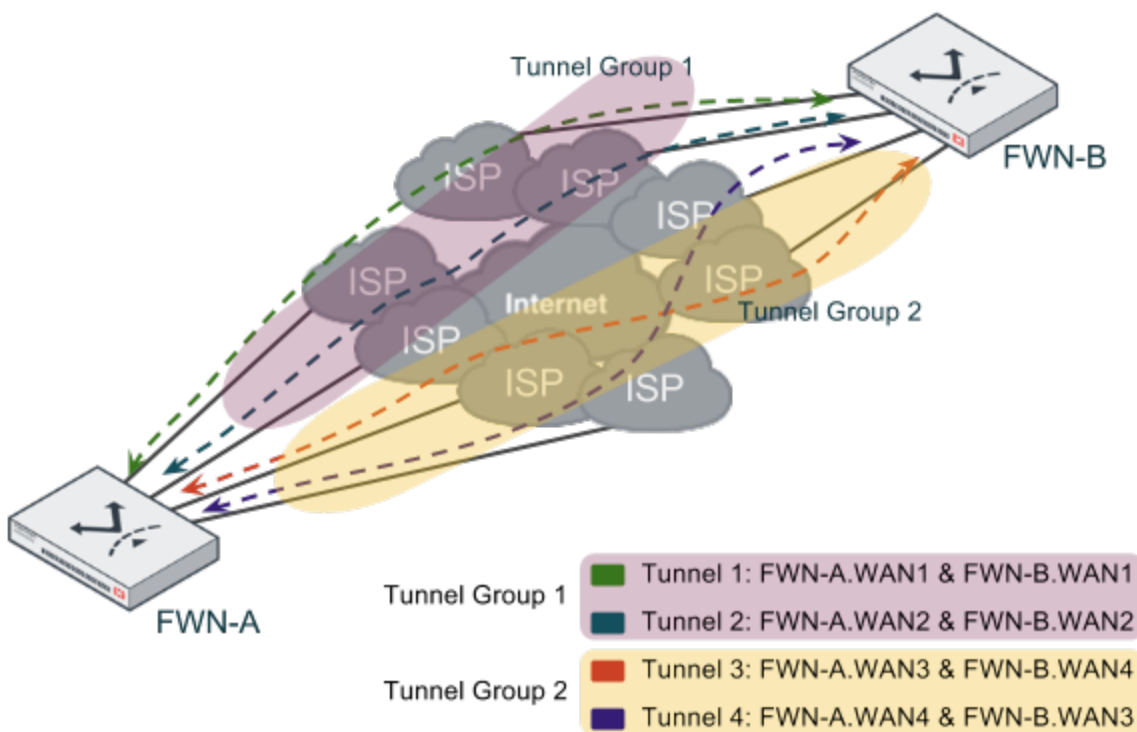
Enable or disable logging. FortiWAN provides mechanisms to record, notify and analysis on events refer to the Tunnel Routing service, see "[Log](#)", "[Statistics: Tunnel Status](#)", "[Statistics: Tunnel Traffic](#)", "[Report: TR Status](#)" and "[Report: TR Reliability](#)".

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Local Host ID</b> | Assign a <b>unique</b> host name for this unit. Tunnels are established between two FortiWAN units. Host ID is used for Tunnel Routing to recognize the units running TR transmission. Symmetrically, this field is required to the opposite unit.                                                                                                                                                                                                   |
| <b>Key</b>           | Decide a secret key for tunnel encryption and enter it here, if the encryption function is enabled for a tunnel group. Tunnel Routing encryption employs only one secret key for all tunnel transmissions, therefore, please set the decided key to all the tunnel routing hosts. This key is used for the data encryption built in Tunnel Routing, not for encryption of IPSec. For an IPSec protection on Tunnel Routing, please refer to "IPSec". |
| <b>Confirm</b>       | Confirm the key above.                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Tunnel Group

Consider the symmetric FortiWAN sites with multiple WAN links on each side, a **tunnel** between the two units are the connection with one WAN link of local unit and one WAN link of remote unit. A **tunnel group** contains multiple tunnels which might be various combinations of WAN links between the two FortiWAN units. A tunnel group is the basic unit to be used for a Tunnel Routing transmission. Packets of a session transferred via tunnel routing between units would be distributed (according to the balancing algorithms) to the multiple tunnels defined in the tunnel group. Therefore, a tunnel group is logically a big tunnel that multiple WAN links are integrated to.

The figure below is an example to illustrate tunnels and tunnel groups. Tunnel Group 1 contains two tunnels which tunnel 1 is established with FWN-A's WAN 1 and FWN-B's WAN 1, and tunnel 2 is established with FWN-A's WAN 2 and FWN-B's WAN 2. A transmission via Tunnel Group 1 will be distributed over tunnel 1 and tunnel 2. Tunnel Group 2 also contains two tunnels which tunnel 3 is established with FWN-A's WAN 3 and FWN-B's WAN 4, and tunnel 4 is established with FWN-A's WAN 4 and FWN-B's WAN 3. Containing only one tunnel in a tunnel group, which is a degenerate case, is allowed.



Tunnel group is the basic unit to be employed for tunnel routing transmission. Therefore, balancing algorithms, encryption, the opposite site, tunnels in the group and even quality of the WAN links are the necessary associations for a tunnel group transmission. To set up a tunnel group, here is the necessary information:

- Which opposite FortiWAN unit the tunnel group is established with: Remote host ID
- What are the tunnels included in the tunnel group: Local IP and Remote IP for a tunnel
- How to distribute packets over the tunnels: Algorithm
- Does the transmission keep in secret: Encryption

**Note that every tunnel group must contain at least one tunnel which is configured with one static public IP address.** FortiWAN supports up to 100 tunnel groups for FWN-200B, 400 tunnel groups for FWN-1000B and 1000 tunnel groups for FWN-3000B. All of the three models have a default maximum total allowed enable amount of 2500 GRE tunnels.

In this configuration table, tunnels are configured for a tunnel group with IP addresses of WAN links of local and remote FortiWAN units and the routing algorithm used to rout packets over tunnels.

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Add</b>            | Click the Add button to add a new Tunnel Group setting panel.<br><br><b>Note</b> that the default maximum allowed to add is: <ul style="list-style-type: none"> <li>• <b>100</b> tunnel groups for FortiWAN 200B</li> <li>• <b>400</b> tunnel groups for FortiWAN 1000B</li> <li>• <b>1000</b> tunnel groups for FortiWAN 3000B</li> </ul>                                                                            |
| <b>Group Name</b>     | Assign a group name to the tunnel group.                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Remote Host ID</b> | Enter the Host ID of the Remote unit the Tunnel Group connects to.                                                                                                                                                                                                                                                                                                                                                    |
| <b>Algorithm</b>      | <ul style="list-style-type: none"> <li>• Round-Robin: Route the connections in every tunnel by weight. Note: Please specify the weight value of “Group Tunnels” when selecting “Round-Robin” (See <a href="#">Load Balancing Algorithms</a>).</li> <li>• By Upstream Traffic: Route the connections to the tunnel with the lightest upstream traffic flow (See <a href="#">Load Balancing Algorithms</a>).</li> </ul> |

## Group Tunnels

Click the add button on the Group Tunnels panel, then a configuration block pops up for adding a GRE tunnel in the tunnel group. Move the cursor over an existing tunnel (it will be highlighted) and click it, the configuration block pops up also for editing it.

|               |                                                                                                                                                                                                                                                          |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable</b> | Check to enable/disable this GRE tunnel.<br><br><b>Note</b> that the default maximum allowed to enable for a tunnel group is <b>16</b> GRE tunnels. For all the configured tunnel groups, a maximum total of <b>2500</b> enabled GRE tunnels is allowed. |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Local IP**

Configure local IP address for tunnels in the tunnel group. The local IP addresses here are the localhost IP defined on the WAN links of local FortiWAN. According to the WAN type defined on WAN links, here are several types of Local IP for options.

- **Static-IP WAN link without NAT on local side:** If the WAN link of local FortiWAN you want to employ for the tunnel is configured with a static public IP address and there will be no NAT translation to this IP address, please select "IPv4 Address" and configure it with the static public IP address of the WAN link.
- **Static-IP WAN link with NAT on local side:** If the WAN link of local FortiWAN you want to employ for the tunnel is configured with a static IP address and there is a NAT translation to this IP address, please select "(NAT) IP Address" and configure it with the static IP address of the WAN link.
- **Dynamic-IP WAN link without NAT on local side:** If the WAN link of local FortiWAN you want to employ for the tunnel is configured with a dynamic IP address (Bridge Mode: PPPoE or DHCP for the WAN type) and there will be no NAT translation to the dynamic IP address, please select "Dynamic WANx" for the configuration.
- **Dynamic-IP WAN link with NAT on local side:** If the WAN link of local FortiWAN you want to employ for the tunnel is configured with a dynamic IP address (Bridge Mode: PPPoE or DHCP for the WAN type) and there is a NAT translation to the dynamic IP address, please select "(NAT) Dynamic WANx" for the configuration.

According your WAN Setting, "Dynamic WAN x" and "(NAT) Dynamic WAN x" are listed in pair in the drop-down menu to correspond all the dynamic WAN links (Bridge Mode: PPPoE and Bridge Mode: DHCP). To avoid a TR transmission failure, please select corresponding types for the deployments which involve NAT translating within.

If the IP addresses that ISP provides is private IP addresses (no matter they are static or dynamic), the ISP might perform NAT translations to the private IP addresses. Please contact with the ISP for further information.

For options "Static-IP WAN link without NAT" and "Static-IP WAN link with NAT", if a change on the IP address of the WAN link is made (from Network Setting) on the local FortiWAN unit, a corresponding update to the setting here is necessary (manually).

For deployment of Tunnel Routing over IPSec, make sure Local IP here is equal to the Local IP configured to correspondent IPSec Phase 1 (See ["IPSec - Define routing policies for an IPSec VPN"](#)).

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Remote IP</b>               | <p>Configure remote IP address for tunnels in the tunnel group. The remote IP addresses here are the localhost IP defined on the WAN links of remote FortiWAN. According to the WAN type defined on WAN links, here are several types of Remote IP for options.</p> <ul style="list-style-type: none"> <li>• <b>Static-IP WAN link without NAT on remote side:</b> If the WAN link of remote FortiWAN you want to employ for the tunnel is configured with a static IP and there will be no NAT translation to the IP address, please select "IPv4 Address" and configure it with the static IP address of the WAN link.</li> <li>• <b>Dynamic-IP WAN link without NAT on remote side:</b> If the WAN link of remote FortiWAN you want to employ for the tunnel is configured with a dynamic IP and there will be no NAT translation to the IP address, please select "Dynamic IP" for the configuration.</li> <li>• <b>WAN link with NAT on remote side:</b> No matter the WAN link of remote FortiWAN you want to employ for the tunnel is configured with a static or dynamic IP address, please select "(NAT) Dynamic IP" for the configuration if there is a NAT translation to the IP address.</li> </ul> <p>To avoid a TR transmission failure, please select corresponding types for the deployments which involve NAT translating within.</p> <p>For option "Static-IP WAN link without NAT", if a change on the IP address of the WAN link is made (from Network Setting) on the remote FortiWAN unit, a corresponding update to the setting here is necessary (manually).</p> <p>For deployment of Tunnel Routing over IPSec, make sure Remote IP here is equal to the Remote IP configured to correspondent IPSec Phase 1 (See <a href="#">"IPSec - Define routing policies for an IPSec VPN"</a>).</p> |
| <b>Weight</b>                  | The weight/priority of the tunnel for the Round-Robin balancing algorithm. This field is displayed only if Round-Robin is selected for Algorithm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Encrypt</b>                 | Check to enable/disable encryption for packets transferred via this tunnel. Remember to set the secret key for encryption. This is a simple encryption built in Tunnel Routing, which employs AES in ECB mode. If a higher and stricter security is required, please perform Tunnel Routing under protection of IPSec Transport mode (See <a href="#">"IPSec"</a> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>DSCP</b>                    | DSCP(Differentiated Services Code Point) provides simple mechanism for quality of service (QoS) on IP networks. DSCP uses the differentiated services code in IP header to indicated different traffic QoS classification. If your ISP provides DSCP service, please contact them for the values. In the field, specify the value to the tunnel. Leave it blank if you do not apply DSCP to the tunnel. Note that only the tunnels established with static local and remote IP addresses support DSCP. This will primarily be used for tunnels over MPLS networks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Health Detection Policy</b> | Select a predefined health detection policy (see <a href="#">Configuring the parameters for tunnel health detection</a> ) from the list. FortiWAN monitors this tunnel according to the policy (see <a href="#">Tunnel healthy detection</a> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Add (button)</b>            | Click to add configuration of the tunnel into Group Tunnels panel. After clicking, this tunnel is listed on the panel. <b>Note</b> that clicking the Apply button is still required to save the whole configurations to system back-end for Tunnel Routing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**Save (button)** This button appears while you are editing an existing tunnel. Click to save the editing back to Group Tunnels panel. **Note** that clicking the Apply button is still required to save the whole configurations to system back-end for Tunnel Routing.

**Cancel (button)** Click to close the configuration block.

As previous description, for the performance of bidirectional transmission, Tunnel Routing will automatically fix any TCP control packet (packet without data payload) to the first available tunnel listed on the Group Tunnel block in bottom-up order. Not only the control packets but also data packets will be assigned to this specific tunnel, therefore, the more bandwidth this tunnel is capable of, the more smoothly the control packets can be delivered. You are suggested to arrange the tunnels (by clicking the Move Down and Move Up buttons) in a order that the higher throughput the lower position on the list.

Note that one group tunnel configuration cannot be duplicates (group tunnels with the same configuration on fields Local IP and Remote IP) for multiple tunnel groups. One group tunnel configured with a static local IP address and a static remote IP address can only be used for one tunnel group between one pair of local host and remote host. One group tunnel configured with a static IP address and a dynamic WAN link can be duplicates in the tunnel groups which is used with different remote host, but cannot be duplicates in the tunnel groups which is used with the same remote host.

Beside the GRE tunnels, configuration of a tunnel group includes setting for Default Rule, which is an option. If your TR network deployment requires more than 100 TR routing rules, replacing the TR routing rules with TR default rules will be suggested for better performance. Default Rule is introduced in [How to set up routing rules for Tunnel Routing](#).

## Configuring the parameters for tunnel health detection

A tunnel health detection (see [Tunnel healthy detection](#)) policy tells how FortiWAN behaves when detecting tunnel health. A policy contains the following parameters:

| Fields                                 | Description                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                            | Policy name                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Detection Period</b>                | <p>The time interval (in milliseconds) between detection packets sending. A shorter detection interval can detect tunnel failure more real-time, but it consumes more bandwidth resource.</p> <p><b>Note</b> that the tunnel health detection requires the same detection period at two endpoints of the tunnels. Please make sure you set the same period to the two FortiWAN appliances.</p> |
| <b>Number of Retries</b>               | The times that FortiWAN will retry for confirming that a tunnel is failed. Every time when FortiWAN does not receive response to a detection packet, it continues sending detection packets for the specified times. A tunnel will be declared as failed only if all of the retries are not responded.                                                                                         |
| <b>Number of Successful Detections</b> | The number of continuously successful detections that is required for declaring a tunnel is available.                                                                                                                                                                                                                                                                                         |

The three parameters decides how much time that FortiWAN can detect a state switch on a tunnel. For example, if the Number of Successful Detections field is set to 5 and the Detection Period field is set to 3000 (milliseconds), it will take 15 seconds to detect a recovery from failure. On the other hand, if Number of Retries or Number of Successful Detections is set as a small value, the detection becomes sensitive to subtle changes, which may cause wild shifts of tunnel state.

## Configuring tunnel quality policies

As the descriptions in [How to reach to a maximum of aggregated throughput](#) and [Monitoring quality of a tunnel](#), data transmission over TR tunnels is extremely sensitive to unexpected packet delay since the packets of sessions are distributed over the tunnels. This is especially required by some delay-sensitive applications such as streaming. They have high standard for the equal quality between tunnels. The entire data transmission of a tunnel group contains traffic of multiple applications, each of them has different standard for tunnel quality. Applying tunnel quality policies to applications avoid them from the worst case that mentioned in [Monitoring quality of a tunnel](#).

To create a quality policy, go to **Service > Tunnel Routing** and create a **Routing Quality Rule Policy** configuration. It contains the following fields:

| Fields           |                   | Description                                                                                                                                                                                                                                     |
|------------------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>      |                   | Policy name                                                                                                                                                                                                                                     |
| <b>Threshold</b> | <b>RTT</b>        | Specify a RTT threshold (in milliseconds) used to evaluate tunnels.                                                                                                                                                                             |
|                  | <b>Jitter</b>     | Specify a jitter threshold (in milliseconds) used to evaluate tunnels.                                                                                                                                                                          |
| <b>Duration</b>  | <b>Under time</b> | Specify a time period (in seconds). If <b>both</b> the RTT and jitter between the endpoints of a tunnel are consistently lower the specified thresholds for a period longer than this value, the tunnel will be declared as in normal quality.  |
|                  | <b>Over time</b>  | Specify a time period (in seconds). If <b>any</b> of the RTT and jitter between the endpoints of a tunnel are consistently higher the specified thresholds for a period longer than this value, the tunnel will be declared as in poor quality. |



The period that FortiWAN uses for updating the real RTT and jitter values of a tunnel is relative to the [detection period](#) of tunnel health detection (see [Configuring the parameters for tunnel health detection](#)). The RTT is updated every two detection periods, and the jitter is updated every the detection period (but it costs two detection period to get the first jitter value at the beginning). For example, if the detection period of tunnel health detection is 500ms, then FortiWAN will update the RTT of a tunnel every 1000ms, and update the jitter every 500ms (the first jitter will costs 1000ms).

See [Configuring a routing rule](#) to apply quality policies to TR routing rules and [Example for using quality policies](#) for how to use quality policies.



## See also

[Tunnel Routing](#)

[How the Tunnel Routing Works](#)

[How to set up routing rules for Tunnel Routing](#)

[Tunnel Routing - Benchmark](#)

[Scenarios](#)

## How to set up routing rules for Tunnel Routing

To perform Tunnel Routing, symmetric FortiWAN deployment is a basic requirement. Therefore, symmetric routing rules are also required for two-way data transmission. A routing rule here contains three basic elements that are

**What is the traffic to be transferred by Tunnel Routing?** Tunnel Routing filter traffic by **Source**, **Destination** and **Service**.

**Which Tunnel Group is employed to transfer the traffic?** Apply a predefined tunnel group to the specified traffic, then it will be transferred according to the how the tunnel group is defined; the balancing algorithm, the tunnels, the weight, the encryption and DSCP.

**What to do if the Tunnel Group fails?** A failed tunnel group means all the tunnels defined in the tunnel group are disconnected (detected by Tunnel Routing's tunnel healthy detection mechanism). Therefore, it is necessary to specify another way for the traffic. Note that as long as one tunnel in a tunnel group remains connected, Tunnel Routing keeps employing the tunnel group for transmission.

Next we introduce the two ways, **Routing Rule** and **Default Rule**, to establish the routing rules for Tunnel Routing.

## Configuring routing rules for tunnel routing

This is the general way to set routing rules for Tunnel Routing. A routing rule contains the three basic elements above, which evaluates traffic by Source, Destination, Service, (Tunnel) Group and Fail-Over. Note that a routing rule sat on a FortiWAN site is required symmetrically for the opposite FortiWAN site, so that the bidirectional transmission is achieved.

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Add</b>    | Click the Add button to add a new rule.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Source</b> | <p>The source of the connection (See "<a href="#">Using the web UI</a>").</p> <p><b>IPv4 Address, IPv4 Range and IPv4 Subnet:</b> To filter out the traffic coming from the specified IPv4 Address, IPv4 Range or IPv4 Subnet.</p> <p><b>LAN:</b> To filter out the traffic coming from LAN area.</p> <p><b>DMZ:</b> To filter out the traffic coming from DMZ area.</p> <p><b>Any Address:</b> To filter out the traffic coming from any IP address</p> |

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Destination</b>    | <p>The destination of the connection (See <a href="#">"Using the web UI"</a>).</p> <p><b>IPv4 Address, IPv4 Range and IPv4 Subnet:</b> To filter out the traffic going to the specified IPv4 Address, IPv4 Range or IPv4 Subnet.</p> <p><b>WAN:</b> To filter out the traffic going to WAN area.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Service</b>        | <p>The TCP/UDP service type to be matched. The default is "Any". Administrators can select from the publicly known service types (e.g. FTP), or can choose the port number in TCP/UDP packet. To specify a range of port numbers, type starting port number plus hyphen "-" and then end port number. e.g. "TCP@123-234" (See <a href="#">"Using the web UI"</a>).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Group</b>          | <p>The <b>tunnel group</b> used to transfer the specified traffic (filtered by Source, Destination and Service). The balancing algorithm and tunnels for distributing the traffic are defined in the tunnel group.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Quality Policy</b> | <p>Select a predefined quality policy (see <a href="#">Configuring quality policies</a>) from the list.</p> <p>When a quality policy is selected, FortiWAN monitors the quality of tunnels of the specified tunnel group for the specified traffic (source, destination and service) according this policy, and reacts if a poor tunnel is identified (see <a href="#">Monitoring quality of a tunnel</a>).</p> <p>See <a href="#">Example for using quality policies</a> for how to use quality policies.</p>                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Fail-Over</b>      | <p>This field defines the fail-over policy for situation that all the WAN links (tunnels) of the specified tunnel group in the routing rule fail. Possible options are:</p> <p><b>NO-ACTION:</b> Traffic will not be diverted when the tunnel group get failed, and transmission will get failed.</p> <p><b>Auto Routing:</b> Traffic will be re-evaluated against Auto Routing's rules and transferred according to the Auto Routing policies. Transmission gets failed if there is no rule matches.</p> <p><b>Tunnel: [Group Name]:</b> All the defined tunnel groups are listed for options. Traffic will be diverted to the specified tunnel group here, however, the diverted traffic will not be diverted again if the back-up tunnel group is also failed. Note: it takes the same action as "NO-ACTION" if a tunnel group that is the same as what specified in field "Group" is selected as back-up for fail-over here.</p> |

If your TR network deployment requires more than 100 TR routing rules, replacing the TR routing rules with TR default rules will be suggested for better performance.

### Example for using quality policies

Here are two quality policies:

```
Name=strict, Threshold-RTT=250ms, Threshold-Jitter=20ms, Duration-Under time=5, Duration-Over time=5
Name=loose, Threshold-RTT=400ms, Threshold-Jitter=40ms, Duration-Under time=10, Duration-Over time=10
```

#### One tunnel group:

```
Group name=tr-group1, Algorithm=Round-Robin
Local IP=1.1.1.1, Remote IP=4.4.4.4, Weight=1
```

```
Local IP=2.2.2.2, Remote IP=5.5.5.5, Weight=1
Local IP=3.3.3.3, Remote IP=6.6.6.6, Weight=1
```

### Two routing rules:

```
Source=Any, Destination=Any, Service=TCP@5060, Group=tr-group1, Quality Policy=strict
Source=Any, Destination=Any, Service=Any, Group=tr-group1, Quality Policy=loose
```

According to the configurations, FortiWAN monitors the three tunnels of tr-group1. Normally when the RTT and jitter of the three tunnels are lower than the specified thresholds, various traffic packets are distributed over the three tunnels, including TCP@5060 traffic. The following cases describe how Tunnel Routing behaves when the latency varies:

#### Case 1:

FortiWAN detects the RTT and jitter between 1.1.1.1 and 4.4.4.4 remain higher than 250ms and 20ms (lower than 400ms and 40ms) for over 5 seconds. Traffic of TCP@5060 is only distributed over the 2.2.2.2-5.5.5.5 tunnel and the 3.3.3.3-6.6.6.6 tunnel. Other traffic is still distributed over the three tunnels.

#### Case 2:

FortiWAN detects the RTT and jitter between 1.1.1.1 and 4.4.4.4 remain higher than 250ms and 20ms (lower than 400ms and 40ms), and RTT and jitter between 3.3.3.3 and 6.6.6.6 remain higher than 400ms and 40ms for over 10 seconds. Traffic of TCP@5060 is only assigned to the 2.2.2.2-5.5.5.5 tunnel. Other traffic is only distributed over the 1.1.1.1-4.4.4.4 tunnel and the 2.2.2.2-5.5.5.5 tunnel.

#### Case 3:

FortiWAN detects the RTT and jitter between 1.1.1.1 and 4.4.4.4 remain lower than 250ms and 20ms for over 5 seconds, but RTT and jitter between 3.3.3.3 and 6.6.6.6 remain higher than 400ms and 40ms. Traffic of TCP@5060 is only distributed over the 1.1.1.1-4.4.4.4 tunnel and the 2.2.2.2-5.5.5.5 tunnel. Other traffic is only distributed over the 1.1.1.1-4.4.4.4 tunnel and the 2.2.2.2-5.5.5.5 tunnel.

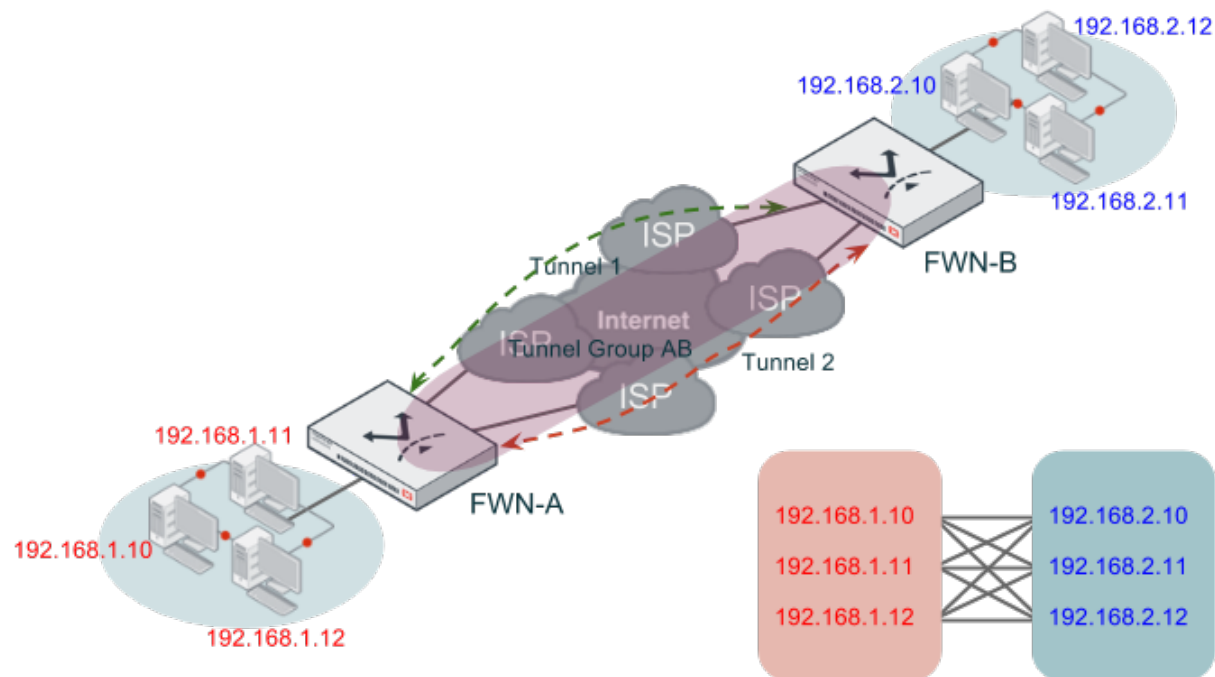
## Configuring default rules for tunnel groups

Default Rule provides a semiautomatic way to establish symmetric routing rules, while Routing Rule is a fully-manual way. Default Rule is a simple and efficient way to configure symmetric routing rules for tunnel transmission between FortiWANs. Although Default Rule is a simplified way to set routing rules up, it still contains the three basic elements that we introduced above. Default Rule filters traffic by Source and Destination while ignoring the Service (Service = Any). To set the default rules up, only the source IP addresses need to be specified on both FortiWAN units that a tunnel group connects. Then the symmetric FortiWAN units **automatically negotiate** for the destinations; One's source in a default rule will become to the destination in the default rule on the opposite unit. In other words, Default Rule is the fully-connected association established by specified sources on local and remote units.

A Default Rule is attached to a Tunnel Group. The configurations of a tunnel group contains items for its default rules, so that traffic filtered out by the default rule would be transferred via this tunnel group, which is the second element for a tunnel routing rule we introduced above. Every default rule contains fail-over policy for transmission when the tunnel group fails; this is the third element for a tunnel routing rule.

|            |                                         |
|------------|-----------------------------------------|
| <b>Add</b> | Click the Add button to add a new rule. |
| <b>E</b>   | Check to enable the rule.               |

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Source</b>    | <p>The source of the connection (See "Using the web UI").</p> <p><b>IPv4 Address, IPv4 Range and IPv4 Subnet:</b> Specify the IPv4 Address, IPv4 Range or IPv4 Subnet that the traffic comes from to be filtered by this rule.</p> <p><b>LAN:</b> To filter out the traffic that comes from LAN area.</p> <p><b>DMZ:</b> To filter out the traffic that comes from DMZ area.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Fail-Over</b> | <p>Select a policy from the list. Once the tunnel group get failed (every single tunnel in the tunnel group fails), traffic will be diverted based on Fail-Over policies.</p> <p><b>NO-ACTION:</b> Traffic will not be diverted when the tunnel group get failed, and transmission will get failed.</p> <p><b>Auto Routing:</b> Traffic will be re-evaluated against Auto Routing's rules and transferred according to the Auto Routing policies. Transmission gets failed if there is no rule matches.</p> <p><b>Tunnel: [Group Name]:</b> All the defined tunnel groups are listed for options. Traffic will be diverted to the specified tunnel group here, however, the diverted traffic will not be diverted again if the back-up tunnel group is also failed. Note that it takes the same action as "NO-ACTION" if a tunnel group that is the same as what this default rule attached to is selected as back-up for fail-over here.</p> |



Considering the illustration above, a tunnel group (Tunnel Group AB) containing two tunnels (Tunnel 1 and Tunnel 2) connects two FortiWAN units (FWN-A and FWN-B) that two internal networks connect respectively to. Configurations of default rules on two sites are as follow:

#### Default rules sat on FWN-A

| Source       | Fail-Over           |
|--------------|---------------------|
| 192.168.1.10 | NO-ACTION           |
| 192.168.1.11 | Auto Routing        |
| 192.168.1.12 | Tunnel: BackupGroup |

**Default rules sat on FWN-B**

| Source       | Fail-Over           |
|--------------|---------------------|
| 192.168.2.10 | Tunnel: BackupGroup |
| 192.168.2.11 | NO-ACTION           |
| 192.168.2.12 | Auto Routing        |

The sources sat on FWN-B's default rules, which are treated as destinations for FWN-A, are sent to FWN-A via the automatic negotiation. FWN-A then generates logically the following routing rules in system back-end.

| Source       | Destination  | Service | Group           | Fail-Over              |
|--------------|--------------|---------|-----------------|------------------------|
| 192.168.1.10 | 192.168.2.10 | Any     | Tunnel Group AB | NO-ACTION              |
| 192.168.1.10 | 192.168.2.11 | Any     | Tunnel Group AB | NO-ACTION              |
| 192.168.1.10 | 192.168.2.12 | Any     | Tunnel Group AB | NO-ACTION              |
| 192.168.1.11 | 192.168.2.10 | Any     | Tunnel Group AB | Auto Routing           |
| 192.168.1.11 | 192.168.2.11 | Any     | Tunnel Group AB | Auto Routing           |
| 192.168.1.11 | 192.168.2.12 | Any     | Tunnel Group AB | Auto Routing           |
| 192.168.1.12 | 192.168.2.10 | Any     | Tunnel Group AB | Tunnel:<br>BackupGroup |
| 192.168.1.12 | 192.168.2.11 | Any     | Tunnel Group AB | Tunnel:<br>BackupGroup |
| 192.168.1.12 | 192.168.2.12 | Any     | Tunnel Group AB | Tunnel:<br>BackupGroup |

The sources sat on FWN-A's default rules, which are treated as destinations for FWN-B, are sent to FWN-B via the automatic negotiation. FWN-B then generates logically the following routing rules in system back-end.

| Source       | Destination  | Service | Group           | Fail-Over              |
|--------------|--------------|---------|-----------------|------------------------|
| 192.168.2.10 | 192.168.1.10 | Any     | Tunnel Group AB | Tunnel:<br>BackupGroup |
| 192.168.2.10 | 192.168.1.11 | Any     | Tunnel Group AB | Tunnel:<br>BackupGroup |
| 192.168.2.10 | 192.168.1.12 | Any     | Tunnel Group AB | Tunnel:<br>BackupGroup |
| 192.168.2.11 | 192.168.1.10 | Any     | Tunnel Group AB | NO-ACTION              |
| 192.168.2.11 | 192.168.1.11 | Any     | Tunnel Group AB | NO-ACTION              |
| 192.168.2.11 | 192.168.1.12 | Any     | Tunnel Group AB | NO-ACTION              |
| 192.168.2.12 | 192.168.1.10 | Any     | Tunnel Group AB | Auto Routing           |
| 192.168.2.12 | 192.168.1.11 | Any     | Tunnel Group AB | Auto Routing           |
| 192.168.2.12 | 192.168.1.12 | Any     | Tunnel Group AB | Auto Routing           |

In the example above, Source of every default rule is specified with single IPv4 address. It is a easier way that set up default rules by specifying Source with a IPv4 range, IPv4 subnet, LAN or DMZ.

Default Rule gives a great help to establish fully-connected routing rules while constructing an Intranet on many branch sites via Tunnel Routing. Consider an Intranet deployment over three branch sites, only three default rules (each one on a branch site) are required to establish the fully connection over the three sites, which requires six routing rules without using Default Rule.

Default Rule refers the configurations of LAN and DMZ in Network Setting to negotiate the routing rules if the Source is specified as LAN or DMZ for a default rule. It is necessary to re-apply the configurations of Default Rule to trigger the negotiation and update the default rules if any change to LAN or DMZ networks setting.

### Configuring persistent rules for tunnel routing

Traffic that a persistent rule matches is transferred via a fixed tunnel (WAN link). Tunnel Routing transfers the first packet of a session through a tunnel according to the specified balancing algorithm. Persistent routing then marks this tunnel for the session, so that the subsequent packets of the session will be transferred directly via the same tunnel (GRE encapsulated directly with the source and destination of the tunnel) without evaluation against routing rules and balancing algorithms until this session disconnects or timeout. For any new session that a persistent rule matches, only the first packet of the session will be processed with routing rules and balancing algorithms. Persistent routing makes Tunnel Routing degenerate into traditional tunnel transmission (transfer every single session via one WAN link), which provides no load balancing and fault tolerance to single session; even so, multiple sessions (not packets) are still distributed over multiple WAN links (similar concept as Auto Routing).

#### Source

The source of the connection (See "[Using the web UI](#)").

|                    |                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Destination</b> | The destination of the connection (See <a href="#">"Using the web UI"</a> ).                                                                                                                                                                                                                                                                                     |
| <b>Service</b>     | The TCP/UDP service type to be matched. The default is "Any". Administrators can select from the publicly known service types (e.g. FTP), or can choose the port number in TCP/UDP packet. To specify a range of port numbers, type starting port number plus hyphen "-" and then end port number. e.g. "TCP@123-234" (See <a href="#">"Using the web UI"</a> ). |

So far, Routing Rules, Default Rule and Persistent Rules are introduced. Any packet for Tunnel Routing will be first evaluated against Persistent Rules. Once a persistent rule matches and a tunnel that the previous packet are transferred through is marked for the session, this packet will be transferred directly via the tunnel without evaluation against Default Rule and Routing Rules. Packets that no persistent rules match or no tunnel is marked for transferring directly will be evaluated against Routing Rules first and Default Rule then, the rule that matches first is applied.

## See also

[Tunnel Routing](#)

[How the Tunnel Routing Works](#)

[Tunnel Routing - Setting](#)

[Tunnel Routing - Benchmark](#)

[Scenarios](#)

## Tunnel Routing - Benchmark

To guarantee a performance aggregation transferring TR packets, FortiWAN requires equal quality for the WAN links employed in a tunnel group. The Benchmark here provides evaluation of WAN link quality for every single tunnel. Tunnels are judged in run trip time, packet loss and bandwidth. It is not suggested to employ a WAN link that is worse than others in a tunnel group.

Tunnel Routing's Benchmark works as **Client/Server mode**. Test traffic is sent from the client site to the server site via every single configured tunnel, and then the benchmark results are reported at client site. Two steps to start Tunnel Routing's Benchmark between two FortiWAN appliances (make sure the Tunnel Routing network is established between the two FortiWANs),

1. Specify one of the FortiWANs to be the benchmark server.
2. Start benchmark traffic from the benchmark client, the FortiWAN opposite to the benchmark server.

### Start a benchmark server

From the Web UI, the Tunnel Routing page, all the configured tunnel groups are listed in the Benchmark panel. To start the benchmark server on a FortiWAN for a tunnel group, you need:

1. Specify the port number on the **Test Port** field for sending/receiving the testing traffic. Note that the port number on both benchmark sites (Client/Server) must be identical. It will fail to receive testing packets if unequal port numbers are used by the two sites.

2. Click the button **Start Test Server** of the tunnel group that you want to test from the list (in **Test Client Status** block). This button will be switched to **Stop Test Server** while benchmark server is running; click it to stop the server.

While the benchmark server is running, a message *Test server is running. Please do not change to another page or close browser* will display and occupy the main page of Web UI. For all the administrator accounts, it become unable to apply new configurations to Tunnel Routing (the Apply button on Web UI becomes ineffective) during benchmark server is running. Web UI will allow apply configurations to other functions during benchmark server is running, but we suggest not to do this since changes to some functions such as Network Setting, Firewall or IPSec might interrupt benchmark server. During benchmark server running, you can switch Web UI main page to other functions, but a message *Test server is running. Please stop it first* displays when you turn the main page back to Tunnel Routing. This message reminds you the benchmark server is still running, and the Apply button of Tunnel Routing remains ineffective until you stop the server. **Note** that the benchmark server can work for only one tunnel group anytime; stop the server on one tunnel group to start it for another.

### Start testing traffic from the benchmark client

For the symmetric FortiWAN sites of a tunnel routing network, benchmark client, the site that is opposite to the benchmark server, triggers the testing traffic. Similarly, all the configured tunnel groups are listed in Benchmark panel. To start benchmark traffic on the site you need:

1. Specify the port number on the **Test Port** field for sending/receiving the test traffic. Note that the port number on both benchmark sites (Client/Server) must be identical. It will fail to receive testing packets if unequal port numbers are used by the two sites.
2. Click the button **Test** of the same tunnel group that the opposite benchmark server is working for. You will be direct to a management panel to start benchmark testing. For a disable tunnel group, a error message *This group is not enabled* displays.
3. In the testing management panel, you see all the tunnels of the tunnel group listed (IP addresses of the two endpoints of a tunnel), and two test cases provided:
  1. **Single tunnel test:** Click the **Test** button of a tunnel, testing traffic will be generated and sent to the opposite (the server side) of the tunnel. All the packets of the testing session will be sent through only the specified tunnel. This will bring out a testing result for evaluating performance of the specified tunnel.
  2. **Tunnel group test:** Click the **Test** button of the last item **All Tunnels in Group** (at the bottom of the table), testing traffic will be generated and sent to the opposite (the server side) of the tunnel group. All the packets of the testing session will be distributed over the tunnels of the tunnel group according to the configured algorithm of the tunnel group. This will bring out a testing result for evaluating performance of the tunnel group.
4. On the upper right corner of the table, there is a button **Test All** used to perform every Single Tunnel Testing and the Tunnel Group Testing one by one in a top-down order.
5. You can click **Close** to stop and leave the benchmark management panel.

### Tunnel group information

In **Test Client Status** panel, all the configured tunnel groups are listed in the table. Information of tunnel groups is also listed in the table, it includes the group name, remote host ID, algorithm, enable and the group tunnels of a tunnel group. Click **Show/Hide Details** to expand or collapse information of the tunnel group. Note that information of tunnel groups listed in the table cannot be changed for benchmark, and testing cannot be performed for a disable (the checkbox "Enable" is unchecked) tunnel group. Buttons to trigger benchmark testing and display test result are also listed together with every tunnel group in the table.



## Measurement

All the benchmark testing cases (single tunnel testing and tunnel group testing) contain two parts, testing **without traffic** and testing **with traffic**. In the first 20 seconds, benchmark client continues to send ping ICMP echo requests to the benchmark server without sending other testing traffic together. In the next 20 seconds then, benchmark client continues to create TCP data streams together with ping ICMP echo requests to measure the throughput of the tunnel (WAN links). The testing traffic between benchmark client and server is encapsulated with GRE header, so that it simulates real tunnel transmission for performance measurement. Benchmark server responds client for the testing traffic via the same tunnel, and the measurement result can be generated by benchmark client and displays in the table. The measurement result contains

|                                      |                                                                                                   |
|--------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>Tunnel</b>                        | WAN links employed by the tunnel between the symmetric sites.                                     |
| <b>Without Traffic - RTT</b>         | Round-Trip Time of the ping ICMP packets in average (without other tunnel traffic).               |
| <b>Without Traffic - Packet Loss</b> | Packet loss of the ping ICMP packets in percentage (without other tunnel traffic).                |
| <b>With Traffic - Bandwidth</b>      | Throughput of the tunnel.                                                                         |
| <b>With Traffic - RTT</b>            | Round-Trip Time of the ping ICMP packets in average (with the traffic of throughput measurement). |
| <b>With Traffic - Packet Loss</b>    | Packet loss of the ping ICMP packets in percentage (with the traffic of throughput measurement).  |

To evaluate the quality of a tunnel (two WAN links) exactly, we suggest to stop any general-purpose traffic passing through the WAN links while a measurement is running on a tunnel.

## See also

[Tunnel Routing](#)

[How the Tunnel Routing Works](#)

[Tunnel Routing - Setting](#)

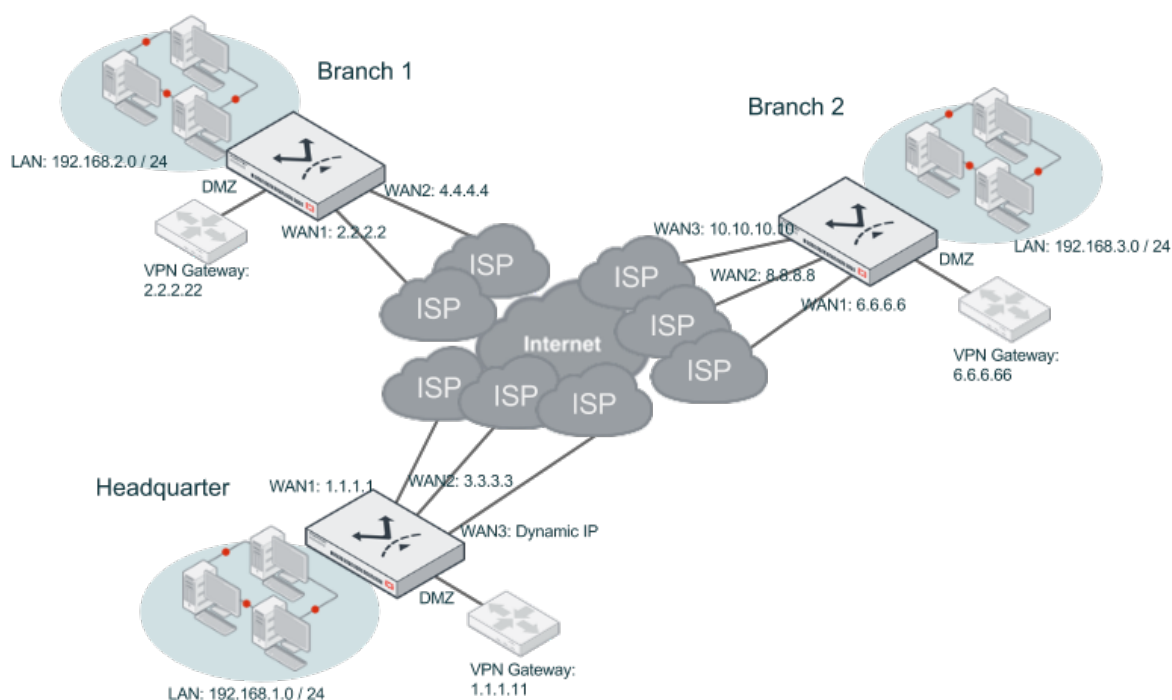
[How to set up routing rules for Tunnel Routing](#)

[Scenarios](#)

## Scenarios

### Example 1

A company's headquarters and two branch offices are located in different cities. Each office has a LAN, multiple WAN links and a DMZ with VPN gateway:



|      | Headquarters   | Branch 1       | Branch 2       |
|------|----------------|----------------|----------------|
| WAN1 | 1.1.1.1        | 2.2.2.2        | 6.6.6.6        |
| WAN2 | 3.3.3.3        | 4.4.4.4        | 8.8.8.8        |
| WAN3 | Dynamic IP     | N/A            | 10.10.10.10    |
| LAN  | 192.168.1.0/24 | 192.168.2.0/24 | 192.168.3.0/24 |

### The settings for the headquarters:

Set the field Local Host ID as HQ.

**Local Host ID:** HQ

### Tunnel Group

| Group Name | Remote Host ID | Algorithm   | Tunnels  |           |        |
|------------|----------------|-------------|----------|-----------|--------|
|            |                |             | Local IP | Remote IP | Weight |
| HQ-Branch1 | B1             | Round-Robin | 1.1.1.1  | 2.2.2.2   | 1      |
|            |                |             | 1.1.1.1  | 4.4.4.4   | 1      |

| Group Name        | Remote Host ID | Algorithm   | Tunnels     |             |        |
|-------------------|----------------|-------------|-------------|-------------|--------|
|                   |                |             | Local IP    | Remote IP   | Weight |
| HQ-Branch1 Backup | B1             | Round-Robin | 3.3.3.3     | 2.2.2.2     | 1      |
|                   |                |             | 3.3.3.3     | 4.4.4.4     | 1      |
| HQ-Branch2        | B2             | Round-Robin | 1.1.1.1     | 6.6.6.6     | 1      |
|                   |                |             | 3.3.3.3     | 8.8.8.8     | 1      |
| HQ-Branch2 Backup | B2             | Round-Robin | Dynamic WAN | 10.10.10.10 | 1      |

### Routing Rules

| Source                   | Destination              | Service | Group      | Fail-Over         |
|--------------------------|--------------------------|---------|------------|-------------------|
| 192.168.1.1-192.168.1.10 | 192.168.2.1-192.168.2.10 | Any     | HQ-Branch1 | HQ-Branch1 Backup |
| 192.168.1.1-192.168.1.10 | 192.168.3.1-192.168.3.10 | Any     | HQ-Branch2 | HQ-Branch2 Backup |
| 1.1.1.11                 | 2.2.2.22                 | Any     | HQ-Branch1 | AR                |
| 1.1.1.11                 | 6.6.6.66                 | Any     | HQ-Branch2 | No-Action         |

### The settings for the branch1

Set the field Local Host ID as B1

**Local Host ID:** B1

### Tunnel Group

| Group Name | Remote Host ID | Algorithm   | Tunnels  |           |        |
|------------|----------------|-------------|----------|-----------|--------|
|            |                |             | Local IP | Remote IP | Weight |
| Branch1-HQ | HQ             | Round-Robin | 2.2.2.2  | 1.1.1.1   | 1      |
|            |                |             | 2.2.2.2  | 3.3.3.3   | 1      |
|            |                |             | 4.4.4.4  | 1.1.1.1   | 1      |
|            |                |             | 4.4.4.4  | 3.3.3.3   | 1      |

**Routing Rules**

| Source                   | Destination              | Service | Group       | Fail-Over |
|--------------------------|--------------------------|---------|-------------|-----------|
| 192.168.2.1-192.168.2.10 | 192.168.1.1-192.168.1.10 | Any     | Branch1- HQ | No-Action |
| 2.2.2.22                 | 1.1.1.11                 | Any     | Branch1- HQ | AR        |

**The settings for the branch2**

Set the field Local Host ID as B2

**Local Host ID:** B2

**Tunnel Group**

| Group Name | Remote Host ID | Algorithm   | Tunnels     |            |        |
|------------|----------------|-------------|-------------|------------|--------|
|            |                |             | Local IP    | Remote IP  | Weight |
| Branch2-HQ | HQ             | Round-Robin | 6.6.6.6     | 1.1.1.1    | 1      |
|            |                |             | 6.6.6.6     | 3.3.3.3    | 1      |
|            |                |             | 8.8.8.8     | 1.1.1.1    | 1      |
|            |                |             | 8.8.8.8     | 3.3.3.3    | 1      |
|            |                |             | 10.10.10.10 | Dynamic IP | 1      |

**Routing Rules**

| Source                   | Destination              | Service | Group       | Fail-Over |
|--------------------------|--------------------------|---------|-------------|-----------|
| 192.168.3.1-192.168.3.10 | 192.168.1.1-192.168.1.10 | Any     | Branch2- HQ | No-Action |
| 6.6.6.66                 | 1.1.1.11                 | Any     | Branch2- HQ | AR        |

According to example 1, any data sent from 1.1.1.11 (or 192.168.1.1-192.168.1.10) to 2.2.2.22 will be wrapped and sent as a GRE packet. If 1.1.1.1 experiences a WAN link failure, the packet will still be sent from 3.3.3.3 to continue the transfer.

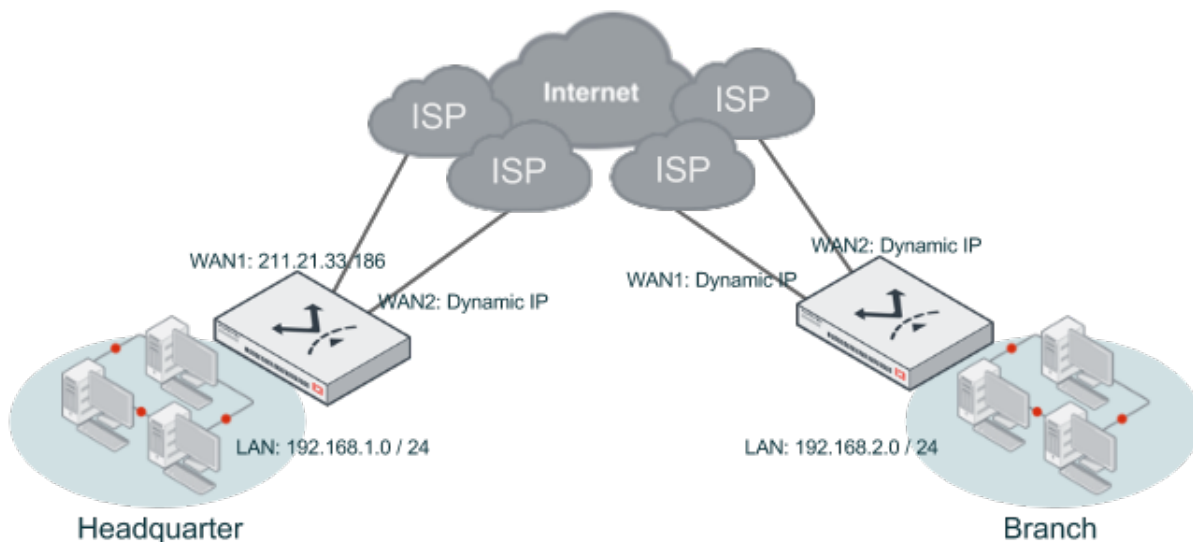
**NOTE:** When using tunnel routing in FortiWAN, the settings must correspond to each other or else tunnel routing will not perform its function. For example, if FortiWAN in Taipei has removed the values 2.2.2.2 to 3.3.3.3 in their routing rule settings, then the FortiWAN in Taichung will not be operational.

## Example 2: Tunnel Routing with Dynamic IP

A company operates a branch office overseas. In the headquarters, two WAN links are deployed: a fixed IP WAN and a dynamic IP WAN; in the branch, two dynamic IP WAN.

### Requirements

As illustrated in the diagram below, a tunnel is established between LAN1 and LAN2. Packets are transferred via two WAN links evenly.



### Summary of the Network

|      | Headquarters   | Branch         |
|------|----------------|----------------|
| WAN1 | 211.21.33.186  | Dynamic IP     |
| WAN2 | Dynamic IP     | Dynamic IP     |
| LAN  | 192.168.1.0/24 | 192.168.2.0/24 |

### The settings for the headquarters:

Set the field Local Host ID as "HQ".

**Local Host ID:** HQ

**Tunnel Group**

| Group Name | Remote Host ID | Algorithm   | Tunnels            |                    |        |
|------------|----------------|-------------|--------------------|--------------------|--------|
|            |                |             | Local IP           | Remote IP          | Weight |
| HQ-Branch  | Branch         | Round-Robin | 211.21.33.186      | Dynamic IP at WAN1 | 1      |
|            |                |             | Dynamic IP at WAN2 | Dynamic IP at WAN2 | 1      |

**Routing Rules**

| Source                    | Destination               | Service | Group     | Fail-Over |
|---------------------------|---------------------------|---------|-----------|-----------|
| 192.168.1.0/255.255.255.0 | 192.168.2.0/255.255.255.0 | Any     | HQ-Branch | No-Action |

**The settings for the branch1**

Set the field Local Host ID as Branch

**Local Host ID:** Branch

**Tunnel Group**

| Group Name | Remote Host ID | Algorithm   | Tunnels            |                    |        |
|------------|----------------|-------------|--------------------|--------------------|--------|
|            |                |             | Local IP           | Remote IP          | Weight |
| Branch-HQ  | HQ             | Round-Robin | Dynamic IP at WAN1 | 211.21.33.186      | 1      |
|            |                |             | Dynamic IP at WAN2 | Dynamic IP at WAN2 | 1      |

**Routing Rules**

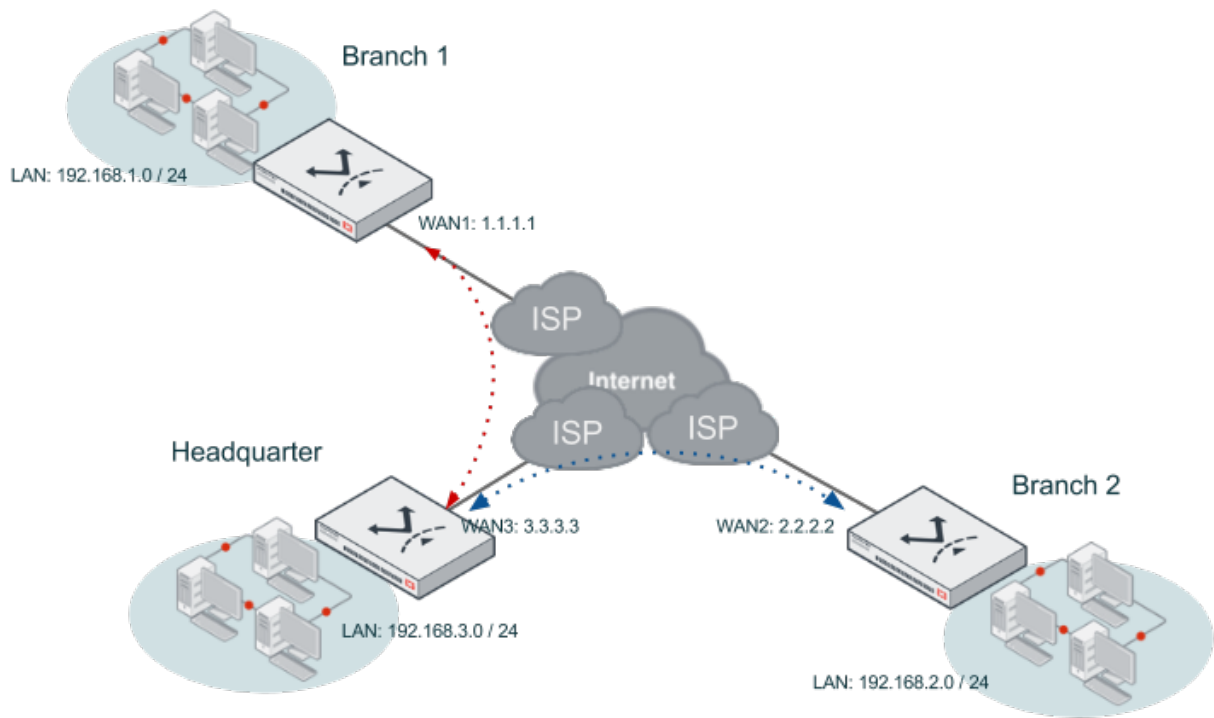
| Source                    | Destination               | Service | Group     | Fail-Over |
|---------------------------|---------------------------|---------|-----------|-----------|
| 192.168.2.0/255.255.255.0 | 192.168.1.0/255.255.255.0 | Any     | Branch-HQ | No-Action |

**Example 3 Forwarding of Tunnel Routing**

A company operates two branch offices overseas. Each office deploys a public line to access Internet. Each branch office sets up an individual tunnel with the headquarters to access the corporate Intranet.

Requirements

The LAN links in branch 1 and branch 2 can communicate with each other via the tunnel established with the headquarter.



Summary of the Network

|       | Headquarters   | Branch 1       | Branch 2       |
|-------|----------------|----------------|----------------|
| WAN 1 | No             | 1.1.1.1        | No             |
| WAN 2 | No             | No             | 2.2.2.2        |
| WAN 3 | 3.3.3.3        | No             | No             |
| LAN   | 192.168.3.0/24 | 192.168.1.0/24 | 192.168.2.0/24 |

The settings for the headquarters:

Set the field Local Host ID as "HQ".

Local Host ID: HQ

**Tunnel Group**

| Group Name | Remote Host ID | Algorithm   | Tunnels  |           |        |
|------------|----------------|-------------|----------|-----------|--------|
|            |                |             | Local IP | Remote IP | Weight |
| HQ-Branch1 | Branch1        | Round-Robin | 3.3.3.3  | 1.1.1.1   | 1      |
| HQ-Branch2 | Branch2        | Round-Robin | 3.3.3.3  | 2.2.2.2   | 1      |

**Routing Rules**

| Source                    | Destination               | Service | Group      | Fail-Over |
|---------------------------|---------------------------|---------|------------|-----------|
| 192.168.1.0/255.255.255.0 | 192.168.2.0/255.255.255.0 | Any     | HQ-Branch2 | No-Action |
| 192.168.2.0/255.255.255.0 | 192.168.1.0/255.255.255.0 | Any     | HQ-Branch1 | No-Action |

The settings for the branch1

Set the field Local Host ID as Branch1

**Local Host ID:** Branch1

**Tunnel Group**

| Group Name | Remote Host ID | Algorithm   | Tunnels  |           |        |
|------------|----------------|-------------|----------|-----------|--------|
|            |                |             | Local IP | Remote IP | Weight |
| Branch1-HQ | HQ             | Round-Robin | 1.1.1.1  | 3.3.3.3   | 1      |

**Routing Rules**

| Source                    | Destination               | Service | Group      | Fail-Over |
|---------------------------|---------------------------|---------|------------|-----------|
| 192.168.1.0/255.255.255.0 | 192.168.2.0/255.255.255.0 | Any     | Branch1-HQ | No-Action |

The settings for the branch2

Set the field Local Host ID as Branch2

**Local Host ID:** Branch2

**Tunnel Group**

| Group Name | Remote Host ID | Algorithm   | Tunnels  |           |        |
|------------|----------------|-------------|----------|-----------|--------|
|            |                |             | Local IP | Remote IP | Weight |
| Branch2-HQ | HQ             | Round-Robin | 2.2.2.2  | 3.3.3.3   | 1      |

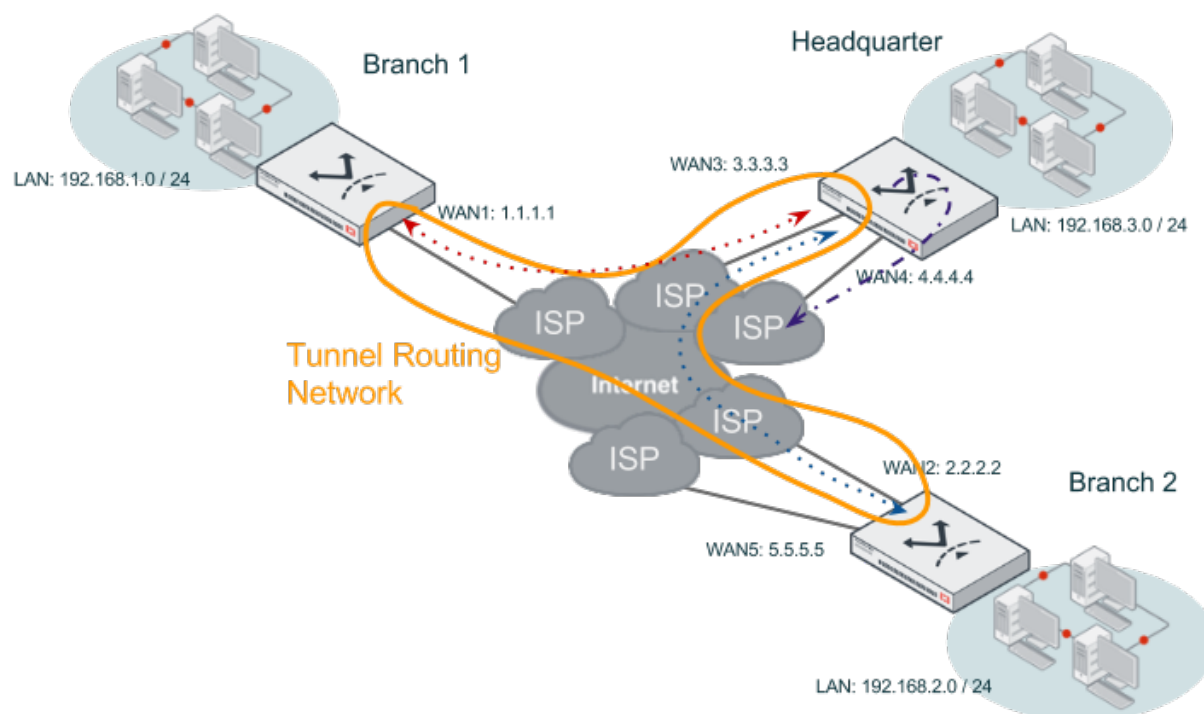


## Routing Rules

| Source                    | Destination               | Service | Group      | Fail-Over |
|---------------------------|---------------------------|---------|------------|-----------|
| 192.168.2.0/255.255.255.0 | 192.168.1.0/255.255.255.0 | Any     | Branch2-HQ | No-Action |

## Example 4: Central Routing of Tunnel Routing

A company operates two branch offices overseas. Intranet is established throughout the three locations, but the branch 1 does not have any public links to the internet and uses tunnel routing to connect to the internet via the WAN in the headquarters. The branch 2 uses a public WAN link for internet. In the event of WAN link failure, the tunnel between branch 2 and headquarters office will be the backup line for internet connection.



## Summary of the Network

|       | Headquarters | Branch 1 | Branch 2 |
|-------|--------------|----------|----------|
| WAN 1 | No           | 1.1.1.1  | No       |
| WAN 2 | No           | No       | 2.2.2.2  |
| WAN 3 | 3.3.3.3      | No       | No       |
| WAN 4 | 4.4.4.4      | No       | No       |

|       | Headquarters | Branch 1       | Branch 2       |
|-------|--------------|----------------|----------------|
| WAN 5 | No           | No             | 5.5.5.5        |
| LAN   | No           | 192.168.1.0/24 | 192.168.2.0/24 |

### The settings for the headquarters:

Set the field Local Host ID as "HQ".

**Local Host ID:** HQ

### Tunnel Group

| Group Name | Remote Host ID | Algorithm   | Tunnels  |           |        |
|------------|----------------|-------------|----------|-----------|--------|
|            |                |             | Local IP | Remote IP | Weight |
| HQ-Branch1 | Branch1        | Round-Robin | 3.3.3.3  | 1.1.1.1   | 1      |
| HQ-Branch2 | Branch2        | Round-Robin | 3.3.3.3  | 2.2.2.2   | 1      |

### Routing Rules

| Source      | Destination               | Service | Group      | Fail-Over |
|-------------|---------------------------|---------|------------|-----------|
| Any Address | 192.168.2.0/255.255.255.0 | Any     | HQ-Branch2 | No-Action |
| Any Address | 192.168.1.0/255.255.255.0 | Any     | HQ-Branch1 | No-Action |

### Auto Routing Settings

#### Policies

| Label          | Algorithm             | Parameter                                   |
|----------------|-----------------------|---------------------------------------------|
| WAN4           | Fixed                 | Tick the check box "4"                      |
| Default Policy | By Downstream Traffic | Tick the check boxes "1", "2", "3", "4" ... |

#### Filters

| Source      | Destination | Service | Routing Policy | Fail-Over |
|-------------|-------------|---------|----------------|-----------|
| Tunnel      | WAN         | Any     | WAN4           | No-Action |
| Any Address | WAN         | Any     | Default Policy | No-Action |

## The settings for the branch1

Set the field Local Host ID as Branch1

**Local Host ID:** Branch1

### Tunnel Group

| Group Name | Remote Host ID | Algorithm   | Tunnels  |           |        |
|------------|----------------|-------------|----------|-----------|--------|
|            |                |             | Local IP | Remote IP | Weight |
| Branch1-HQ | HQ             | Round-Robin | 1.1.1.1  | 3.3.3.3   | 1      |

### Routing Rules

| Source      | Destination | Service | Group      | Fail-Over |
|-------------|-------------|---------|------------|-----------|
| Any Address | WAN         | Any     | Branch1-HQ | No-Action |

## The settings for the branch2

Set the field Local Host ID as Branch2

**Local Host ID:** Branch2

### Tunnel Group

| Group Name | Remote Host ID | Algorithm   | Tunnels  |           |        |
|------------|----------------|-------------|----------|-----------|--------|
|            |                |             | Local IP | Remote IP | Weight |
| Branch2-HQ | HQ             | Round-Robin | 2.2.2.2  | 3.3.3.3   | 1      |

### Routing Rules

| Source                    | Destination               | Service | Group      | Fail-Over |
|---------------------------|---------------------------|---------|------------|-----------|
| 192.168.2.0/255.255.255.0 | 192.168.1.0/255.255.255.0 | Any     | Branch2-HQ | No-Action |

## Auto Routing Settings

### Policies

| Label          | Algorithm             | Parameter                                   |
|----------------|-----------------------|---------------------------------------------|
| WAN5           | Fixed                 | Tick the check box "5"                      |
| Default Policy | By Downstream Traffic | Tick the check boxes "1", "2", "3", "4" ... |

**Filters**

| Source      | Destination | Service | Routing Policy | Fail-Over             |
|-------------|-------------|---------|----------------|-----------------------|
| Any Address | WAN         | Any     | WAN5           | Tunnel:<br>Branch2-HQ |
| Any Address | WAN         | Any     | Default Policy | No-Action             |

**See also**[Tunnel Routing](#)[How the Tunnel Routing Works](#)[Tunnel Routing - Setting](#)[How to set up routing rules for Tunnel Routing](#)[Tunnel Routing - Benchmark](#)

## Virtual Server & Server Load Balancing

Virtual Server is a method for single gateway machine to act as multiple servers while the real servers sit inside corporate network to process requests passed in from the gateway machine. Inbound traffic does not have to know where the real servers are, or whether there are just one or many servers. This method prevents direct access by users and therefore increases security and flexibility.

FortiWAN has built in virtual server and is capable of supporting various virtual server mapping methods. For example, different public IP addresses can be mapped to various real servers in LAN or DMZ. Or ports can be mapped to public IP address on different servers.

Virtual server are configured by designating and adjusting virtual server rules. Each rule specifies a mapping condition. It maps WAN IP address and a service (port or ports) to an internal server IP. The order of virtual server rules is like any other rule tables in FortiWAN as it also uses the “first match scheme”, viz. the first rule of request matched is the rule to take effect.

For example, a public IP address 211.21.48.196 and wants a web server on 192.168.123.16 to handle all the web page requests coming to this public IP address. To do this, a virtual server rule must be created with 211.21.48.196 to be its WAN IP, 192.168.123.16 to be its Server IP, and HTTP(80) to be its Service.

Virtual Server makes intranet (LAN) servers accessible for the internet (WAN). The private IP addresses assigned to intranet servers will become invisible to the external environment, making services accessible for users outside the network. Then FortiWAN is available to redirect these external requests to the servers in LAN or DMZ. Whenever an external request arrives, FortiWAN will consult the Virtual Server table and redirect the packet to the corresponding server in LAN or DMZ. The rules of Virtual Server tables are prioritized top down. If one rule is similar to another in the table, only the higher ranked one will be applied, and the rest will be ignored. In addition, Virtual Server enables to balance load on multiple servers, which is to distribute traffic over a group of servers (server cluster), making services highly accessible.

FortiWAN provides mechanisms to record, notify and analysis on events refer to the Virtual Server service, see ["Log"](#), ["Statistics: Virtual Server Status"](#) and ["Report: Virtual Server"](#).

## Server Pool

| Fields                      | Descriptions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Server Pool Name</b>     | Name for the server pool                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hind Details</b>         | Click to collapse or expand the settings.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Server Pool Settings</b> | A server pool can contain multiple backend server settings. Click the add button to create a new setting and complete the following fields.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Enable</b>               | Check the box to enable/disable the backend server in the server pool. A virtual server will only distribute received requests over the enabled backend servers of the server pool that it associates to.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Server IP</b>            | The real IP (IPv4) of the backend server, most likely in LAN or DMZ.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Detect</b>               | <p>Choose the protocol for detecting server status:</p> <ul style="list-style-type: none"> <li>• ICMP: Detect health status of the server through ICMP.</li> <li>• HTTP(80): Detect health status of the server through HTTP(80).</li> <li>• FTP(21): Detect health status of the server through FTP(21).</li> <li>• SMTP(25): Detect health status of the server through SMTP(25).</li> <li>• POP3(110): Detect health status of the server through POP3(110).</li> <li>• TCP@: Detect health status of the server through specified TCP port. Note that you must specify the port number for this option.</li> <li>• No-Detect: Do not perform health detection.</li> </ul> <p>Please make sure that the service that you specify for health detection is running correctly on the server so that it can reply the detection packets. If a detection method is selected, only the available servers (health status is OK) in the server pool will be the candidates to serve the incoming requests. If No-Detect is selected, virtual server will distribute the incoming requests over all the servers in the pool whether they are alive or not.</p> |
| <b>Service</b>              | <p>Specify the type of TCP/UDP service for service port translation. Virtual server translates the service port of an incoming request into the specified service before sending the packet to this backend server.</p> <p>You can select matching criteria from publicly known service types (e.g. FTP), or choose port number from TCP/UDP packet. To specify a range of port numbers, enter starting port number plus hyphen "-" and ending port number, e.g. "TCP@123-234" (see <a href="#">"Using the web UI"</a>).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Weight</b>               | <p>Weight for the Round-Robin algorithm to determine which backend server responds to the incoming requests. The higher the weight, the greater the chance is for the corresponding server to be used.</p> <p>Leave this blank if the algorithm applied to the server pool is not Round-Robin.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |



A physical backend server can be involved in multiple server pools for multiple virtual servers. The backend server can be disabled in some of the server pools while others are enabled.

## IPv4 Virtual Server Rules

| Fields           | Descriptions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>E</b>         | Click to enable/disable the rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>When</b>      | <p>Specified the time period to be matched. The time that FortiWAN receives the incoming request will be evaluated against this time period.</p> <ul style="list-style-type: none"> <li>• Busy hour</li> <li>• Idle hour</li> <li>• All-Time</li> </ul> <p>See <a href="#">Busyhour Settings</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>WAN IP</b>    | <p>Specified an WAN IP to the virtual server. Destination IP address of an incoming request will be evaluated against this WAN IP. All the WAN links are listed in the drop-down menu for options:</p> <ul style="list-style-type: none"> <li>• <b>WAN#:IP_address</b>: For a static-IP-based (routing mode and bridge mode) WAN link, the first IP that is deployed on the WAN port (hosthost of the WAN link) will be an option here, such as <b>WAN1:10.12.102.4</b>.</li> <li>• <b>Dynamic IP at WAN#</b>: For a dynamic-IP-based (PPPoE and DHCP) WAN link, its WAN IP is represented as <b>Dynamic IP at WAN#</b>.</li> <li>• <b>IPv4 Address</b>: In case that you deployed multiple IPs on a WAN port, and you want to use one of them except the first one for the virtual server, you can select <b>IPv4 Address</b> to enter the IP you want. However please make sure that you enter an IP that is deployed on any of the WAN port.</li> </ul> |
| <b>Service</b>   | <p>Specified the TCP/UDP service to be matched. Service of an incoming request will be evaluated against this service.</p> <p>You can select matching criteria from publicly known service types, or choose port number from TCP/UDP packets. To specify a range of port numbers, type starting port number plus hyphen "-" and ending port number, e.g. "TCP@123-234" (see "<a href="#">Using the web UI</a>").</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Algorithm</b> | <p>Specify the algorithm to distribute the incoming requests over the server candidates in the specified server pool. (See <a href="#">Load Balancing Algorithms</a>)</p> <ul style="list-style-type: none"> <li>• Round-Robin</li> <li>• By Connection</li> <li>• By Response Time</li> <li>• Hash</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Fields              | Descriptions                                                                                                                                                                                                                                           |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Keep Session</b> | Check the box to keep session after a connection has been established. If the session is to be stored, then enter a time period. Default value is 30s                                                                                                  |
| <b>Server Pool</b>  | Specified a server pool to the virtual server. A incoming request will be assigned to a server of the server pool if the arriving time, destination IP and service of the request matches the virtual server rule (When, WAN IP and Service settings). |
| <b>L</b>            | Check to enable logging: Whenever the rule is matched, system will record the event to log file.                                                                                                                                                       |

After an incoming request matches a virtual server rule (the When, WAN IP and Service fields), the procedure to process the request is:

1. Deciding a backend sever from the specified server pool (the Server Pool field) according to the specified algorithm (the Algorithm field).
2. Translating the destination service of the request into the specified service of the backend server (the Service field of the backend server).
3. Pushing the request to the backend server.

### IPv6 Virtual Server Rules

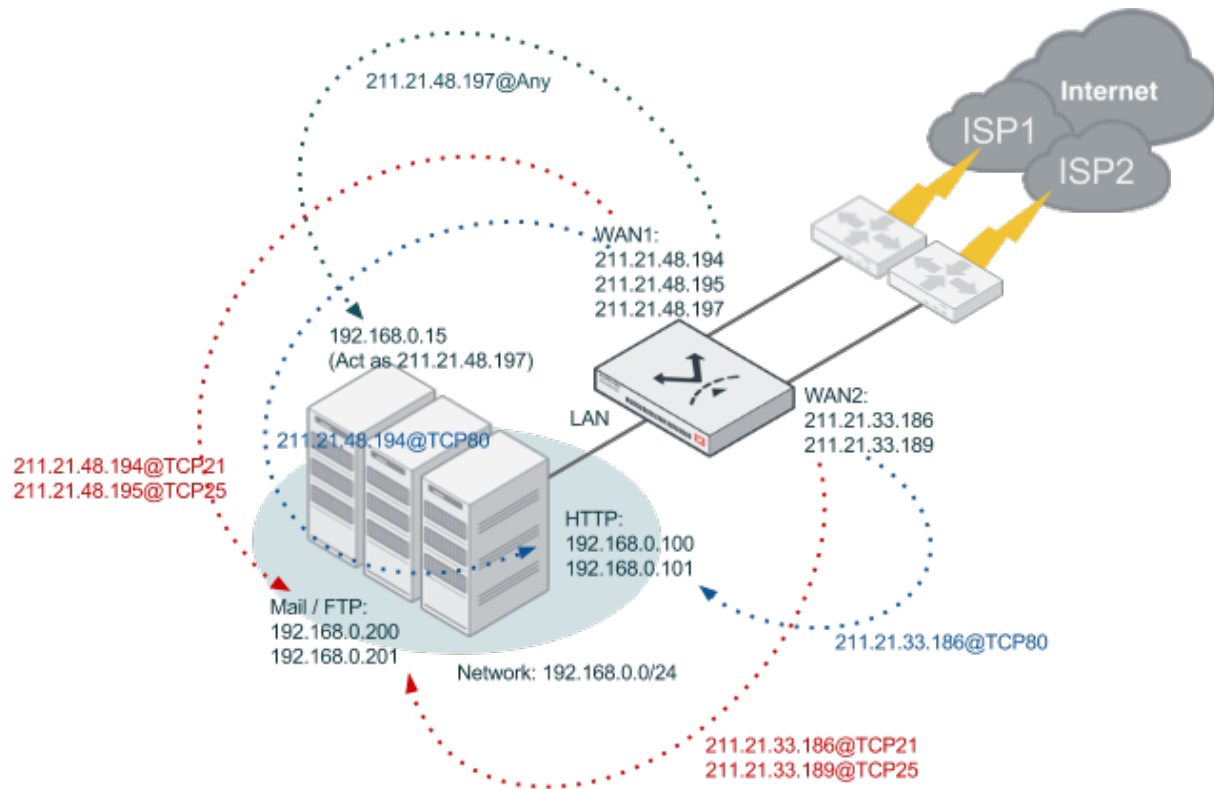
| Fields           | Descriptions                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>E</b>         | Check the box to enable the rule.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>When</b>      | Options: Busy hour, Idle hour, and All-Time (See " <a href="#">Busyhour Settings</a> ").                                                                                                                                                                                                                                                                                                                                                            |
| <b>WAN IP</b>    | For external internet users, the virtual server is presented as a public IP (IPv6) on WAN port. This WAN IP is the "visible" IP for the virtual server in external environment. Select a public IP, and in "Routing Mode", either enter the IP manually or select the IP obtained from WAN link; In "Bridge Mode One Static IP", insert WAN IP and the public IP assigned by ISP; Or choose "dynamic IP at WAN#", if WAN type is none of the above. |
| <b>Service</b>   | The type of TCP/UDP service to be matched. Select matching criteria from publicly known service types, or choose port number from TCP/UDP packets. To specify a range of port numbers, type starting port number plus hyphen "-" and ending port number, e.g. "TCP@123-234" (See " <a href="#">Using the web UI</a> ").                                                                                                                             |
| <b>Server IP</b> | The real IP (IPv6) of the server, most likely in LAN or DMZ.                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>L</b>         | Check to enable logging: Whenever the rule is matched, system will record the event to log file.                                                                                                                                                                                                                                                                                                                                                    |



You can monitor health status (OK or Failed) of the configured virtual servers in the GUI page Statistics > Virtual Server Status (see [Virtual Server Status](#)). Note that the disabled virtual servers and backend servers will not be listed in Virtual Server Status.

## Example 1

The settings for virtual servers look like:



- Assign IP address 211.21.48.194 to WAN1. Refer to [System] -> [Network Settings] -> [WAN Settings] for more regarding WAN IP configurations.
- Assign IP address 211.21.33.186 to WAN2.
- Forward all HTTP requests (port 80) through WAN1 or WAN2 to the two HTTP servers 192.168.0.100 and 192.168.0.101 in LAN.
- Forward all FTP requests (port 21) through WAN1 or WAN2 to two FTP servers 192.168.0.200 and 192.168.0.201 in LAN.
- Assign 211.21.48.195 and 211.21.33.189 to WAN 1 and WAN2. Forward all requests to 211.21.48.195 or 211.21.33.189 to two SMTP servers 192.168.0.200 and 192.168.0.201 in LAN.
- Forward all requests from 211.21.48.197 to 192.168.0.15 in LAN.

Note:

1. FortiWAN can auto-detect both active and passive FTP servers.
2. All public IPs must be assigned to WAN 1. To configure these IPs, go to "IP(s) on Localhost of the Basic Subnet" table in [System] -> [Network Settings] -> [WAN Settings] -> [WAN Link 1].
3. 211.21.48.197 does not belong to any physical host, and it must be assigned to WAN port.

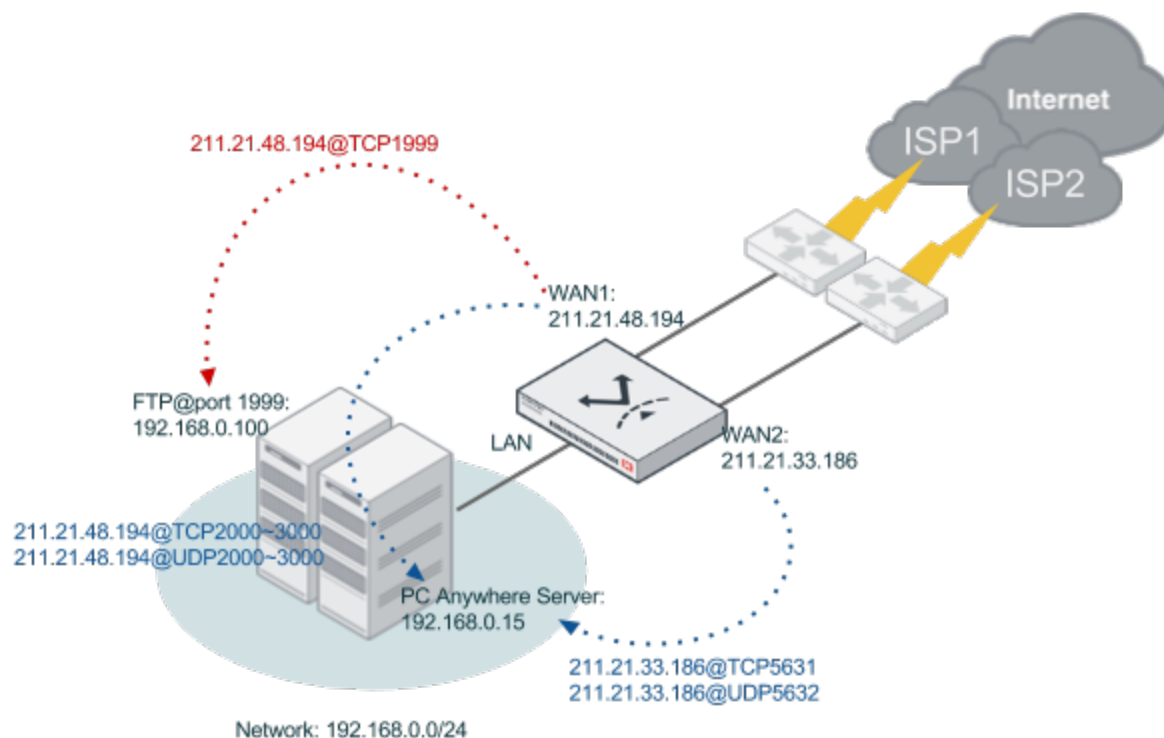
Virtual server table for the above settings:



| Server Pool Name |           | Server IP     | Detect | Service   | Weight |
|------------------|-----------|---------------|--------|-----------|--------|
| 211.21.48.194    | HTTP (80) | 192.168.0.100 | ICMP   | HTTP (80) | 1      |
|                  |           | 192.168.0.101 | TCP@80 | HTTP (80) | 1      |

| WAN IP        | Service   | Server Pool   |        | Service   | Weight |
|---------------|-----------|---------------|--------|-----------|--------|
|               |           | Server IP     | Detect |           |        |
| 211.21.48.194 | HTTP (80) | 192.168.0.100 | ICMP   | HTTP (80) | 1      |
|               |           | 192.168.0.101 | TCP@80 | HTTP (80) | 1      |
| 211.21.33.186 | HTTP (80) | 192.168.0.100 | ICMP   | HTTP (80) | 1      |
|               |           | 192.168.0.101 | TCP@80 | HTTP (80) | 1      |
| 211.21.48.194 | FTP (21)  | 192.168.0.200 | ICMP   | FTP (21)  | 1      |
|               |           | 192.168.0.201 | TCP@21 | FTP (21)  | 1      |
| 211.21.33.186 | FTP (21)  | 192.168.0.200 | ICMP   | FTP (21)  | 1      |
|               |           | 192.168.0.201 | TCP@21 | FTP (21)  | 1      |
| 211.21.48.195 | SMTP (25) | 192.168.0.200 | ICMP   | SMTP (25) | 1      |
|               |           | 192.168.0.201 | TCP@25 | SMTP (25) | 1      |
| 211.21.33.189 | SMTP (25) | 192.168.0.200 | ICMP   | SMTP (25) | 1      |
|               |           | 192.168.0.201 | TCP@25 | SMTP (25) | 1      |
| 211.21.48.197 | Any       | 192.168.0.15  | ICMP   | Any       | 1      |

## Example 2



The settings for virtual servers look like:

- Forward all the TCP port 1999 requests established between external network and public IP 211.21.48.194 to FTP Server@ TCP port 1999 at 192.168.0.100 in LAN.
- Note: Due to the nature of ftp protocol, in port style ftp-data connection, when ftp-control is used in port 1999, port 1998 will be taken by ftp-data.
- Enable external users to access WAN IP 211.21.33.186, and connect PcAnywhere to .LAN hosts.
- Note: PcAnywhere uses TCP port 5631 and UDP port 5632. Refer to PcAnywhere software manual for more details.
- Enable external users to access WAN IP 211.21.48.194, and forward packets of TCP/UDP range 2000-3000 to host 192.168.0.15.

Note: Port range redirecting is supported as well.

Virtual server table for the settings above:

| WAN IP        | Service  | Server Pool   |          |          |        |
|---------------|----------|---------------|----------|----------|--------|
|               |          | Server IP     | Detect   | Service  | Weight |
| 211.21.48.194 | TCP@1999 | 192.168.0.100 | ICMP     | TCP@1999 | 1      |
|               |          | 192.168.0.101 | TCP@1999 | TCP@1999 | 1      |

| WAN IP        | Service       | Server Pool  |          | Service       | Weight |
|---------------|---------------|--------------|----------|---------------|--------|
|               |               | Server IP    | Detect   |               |        |
| 211.21.33.186 | TCP@5631      | 192.168.0.15 | ICMP     | TCP@5631      |        |
| 211.21.33.186 | TCP@5632      | 192.168.0.15 | TCP@5632 | TCP@5632      |        |
| 211.21.48.194 | TCP@2000-3000 | 192.168.0.15 | ICMP     | TCP@2000-3000 |        |
| 211.21.48.194 | UDP@2000-3000 | 192.168.0.15 | ICMP     | UDP@2000-3000 |        |

## WAN Link Health Detection

[WAN Link Health Detection] offers you insight into the health status of WAN links. It allows you to set up specific health detection criteria against each individual WAN link in network of multiple links. FortiWAN detects the connection status of the WAN link by sending out ICMP and TCP packets to targets, and determines the connection quality with data that reports back. [WAN Link Detection] lists a few fields to fulfill. Concerning about detection packets flooding, FortiWAN determines a WAN link alive without sending detection packets if inbound traffic on the WAN link is detected. The ICMP and TCP detection packets are sent only if no inbound traffic is detected.

For a single detection via ICMP / TCP packets, FortiWAN sends a ICMP or TCP packet (defined in "Detection Protocol") individually to multiple targets (defined in "Ping List / TCP Connect List" and "Number of Hosts Picked out per Detection") via a WAN link (defined in "WAN Link"). FortiWAN determines the WAN link alive if receiving response from at least one of those targets in a time period (defined in "Detection timeout in milliseconds"), otherwise this detection is consider failed (FortiWAN will not judge whether a WAN link is down by just one detection failure). No matter whether a single detection succeed, FortiWAN continues the detection after seconds (defined in "Detection Period in Second"). The WAN link is determined as down only if multiple detections fail continually (defined in "Number of Retries"). WAN link health detection monitors the WAN links status which FortiWAN's Summary, Auto Routing, Multihoming and Statistics will refer to.

|                                          |                                                                                                                                                                                                                                                                                                          |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Ignore Inbound Traffic</b>            | Enable [Ignore Inbound Traffic], FortiWAN will determine WAN link status only by sending ICMP and TCP packets to targets, regardless of inbound traffic on the WAN link. Disable [Ignore Inbound Traffic], FortiWAN monitors WAN links status via the mixture of inbound traffic and ICMP / TCP packets. |
| <b>Detection timeout in milliseconds</b> | This indicates the timeout period for every single detection in milliseconds. If no response packets are detected during this period, the system will consider the detection failed.                                                                                                                     |
| <b>WAN Link</b>                          | The WAN link to be configured health detection criteria to. Configure the WAN links individually by selecting them from the list.                                                                                                                                                                        |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Detection Protocol</b>                   | Two protocols used to perform WAN link detection are available: ICMP and TCP.                                                                                                                                                                                                                                                                                                                        |
| <b>Detection period, in seconds</b>         | The time interval between ICMP or TCP packets sending for detection. The unit is second. A shorter interval configuration can detect connection condition earlier, but it consumes more bandwidth resource.                                                                                                                                                                                          |
| <b>Number of hosts picked per detection</b> | The number of hosts that is picked out from Ping List or TCP Connection List for detection. When FortiWAN starts checking the link health, it will send out ICMP and TCP packets to the IP address of the hosts that has been picked out. Detection will not be performed if setting the value to zero.                                                                                              |
| <b>Number of retries</b>                    | The number of times FortiWAN retries if a detection being indicated failed. Once all the retries in the number of times fail, FortiWAN claims the WAN connection fails.                                                                                                                                                                                                                              |
| <b>Number of successful detection</b>       | <p>The number of continuously successful detections that is required for declaring a WAN link indeed available.</p> <p>If this field is set to 5 and detection period is set to 3 seconds, it will require at least 15 seconds to detect an available WAN link. If Ignore Inbound Traffic is disabled, inbound traffic being detected on a WAN link will be counted to one successful detection.</p> |

#### In ICMP packet detection, the optional list is:

**Ping List:** Lists the data of hosts (Destination IP: IPv4 or IPv6) available to ping detection. Each detection sends one ping packet to the IP address of a host that has been picked out randomly from the list. The TTL (Time to Live) of the ping packet is determined by Hops and generally defined as "3". FortiWAN takes the TTL expired message as a legal response for a ICMP detection, even the detection packet is not delivered to the destination.

Note that always employ real external IP addresses (hosts in Internet) for the Ping List, gateway and hosts in near WAN are not appropriate destinations for the detection.

#### In TCP packet detection, the optional list is:

**TCP Connect List:** Lists the data of hosts (Destination IP: IPv4 or IPv6) available to TCP connect detection. Each detection performs TCP connect test for a host that has been picked out randomly from the list, and assigns a value to the TCP port.

A WAN link is determined alive if:

- A single detection succeeds.
- Value of field "Number of hosts picked per detection" is set to zero or "Ping List / TCP Connect List" is left blank.
- "Ignore Inbound Traffic" is disabled and inbound traffic on the WAN link is detected.

A WAN link is determined down if:

- All the detection retries fail.
- No carrier signal detected (failures on cables or physical ports).

- The WAN link is disabled or a sleeping backup line.
- A PPPoE or DHCP WAN link which fails to get a dynamic IP address.

FortiWAN provides statistics to the WAN Link Health Detection service, see "[Statistics: WAN Link Health Detection](#)".

# IPSec

FortiWAN's IPSec VPN is based on the standard two-phase Internet Key Exchange (IKE) protocol, and two communication modes: tunnel mode and transport mode. IPSec is one of the popular standards for establishing a site-to-site VPN network. It contains the tunneling technology and strict security mechanisms. Different from the tunneling of IPSec VPN, FortiWAN's Tunnel Routing has the advantages of bandwidth aggregation and fault tolerance. By integrating IPSec and Tunnel Routing, FortiWAN is fit for the requirement that an IPSec VPN with ability of bandwidth aggregation and fault tolerance.

We start the topic with [IPSec VPN Concepts](#), which includes the descriptions of IPSec VPN overview, IPSec key exchange and How IPSec VPN works. The next topic describes how to set up FortiWAN IPSec VPN, see [IPSec set up](#). IPSec VPN installation is divided into the stages as follows:

- The specifications of FortiWAN IPSec, see [About FortiWAN IPSec VPN](#).
- Concern of planning a VPN deployment, see [Planning your VPN](#).
- Operations and configurations on Web UI, see [IPSec VPN in the Web UI](#).
- Necessary routing policies for the VPN (with scenarios), see [Define routing policies for an IPSec VPN](#).
- Basic setting for establishing IPSec VPN with FortiGate, see [Establish IPSec VPN with FortiGate](#).

If you already have Tunnel Routing running and desire IPSec protection (IPSec Transport mode) on it, you could refer to the descriptions in [IPSec VPN in the Web UI](#) and the examples in [Define routing policies for an IPSec VPN](#) directly.

## IPSec VPN Concepts

As we know, a private network (deployment of private IP addresses) is invisible, closed to public network (usually the Internet). Two private networks in geographically different location can not directly access each other through Internet. Virtual Private Network (VPN) is a concept that connects local and remote private networks over Internet to logically become one private network. An user in a local private network is capable to have accesses to resource in remote private network in a secure way through Internet, such as the access to remote private network of the headquarters office from (branch) local private network. Users of the two private networks access to each other without being aware of the VPN transmissions, just like they are physically in the same network.

The VPN concept implies two critical elements, a tunnel connecting two private networks over an intermediate network and a secure way transferring data through the tunnel (over an untrusted network), which make the virtual private network matches the properties of a physical private network, accesses among private IP address and invisibility to public network (data privacy). IPSec is just the technology designed to implement the two properties of VPN concept. A VPN network established by IPSec can be called IPSec VPN. It not only gives the tunneling implementation for connectivity of two incompatible networks, but also put emphasis on the strict security definitions.

## IPSec VPN overview

### VPN Tunnels

Tunneling is a technique to perform data transmission for a foreign protocol over a incompatible network; such as running IPv6 over IPv4, and the transmission of data for use within a private, corporate network through a public network. Tunneling is done by encapsulating and decapsulating data and information of the particular protocol within the incompatible transmission units symmetrically. IPSec protocol sets define the processes, which is the Tunnel Mode we will introduce later (See [Modes of IPSec VPN data transmission](#)), to deliver encryption protected data between incompatible networks by tunneling through an intermediate network. IPSec offers another option to deliver protected data end-to-end without tunneling, which is called Transport Mode (See [Modes of IPSec VPN data transmission](#)). It provides the flexibility to integrate other tunneling protocols with IPSec to establish a VPN network.

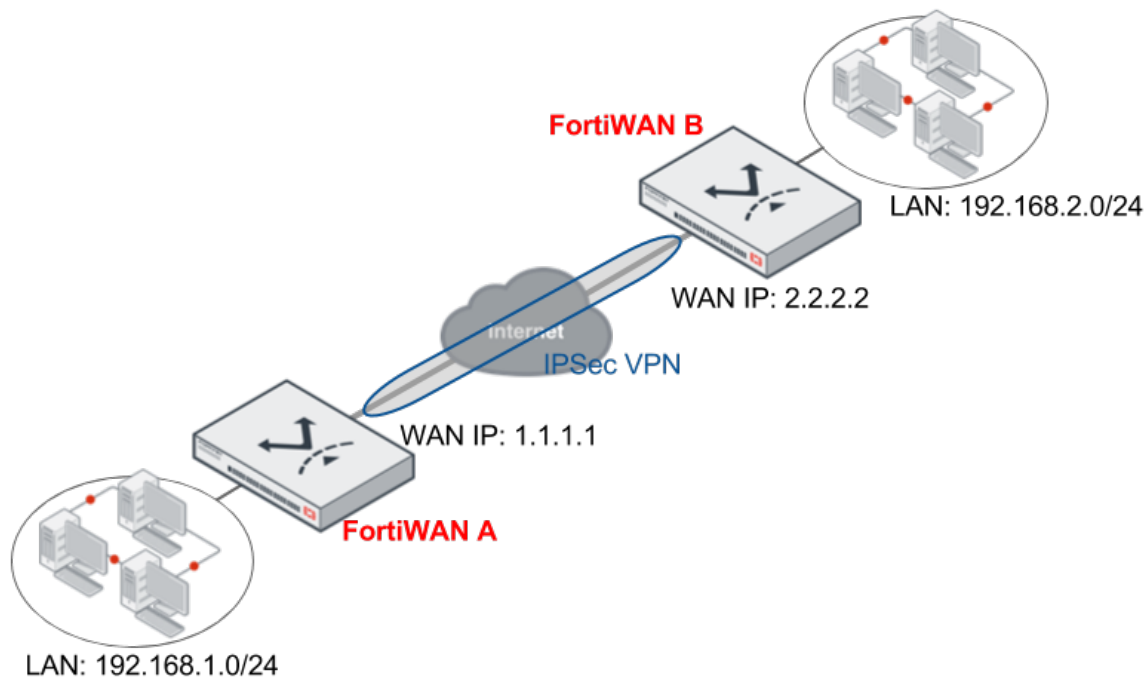
### Secure data transmission

IPSec employs encryption and authentication of data packets for VPN transmission to ensure that any third-party from public network who intercepts the packets can not access the data and impersonate each endpoint. It protects the communications between two endpoints against malicious attacks from intermediate, untrusted network, so that privacy and authenticity are guaranteed to the communications. However, it is concerned that how the two endpoints securely share the encryption and authentication methods, and the correspondent secret key without compromising them to others. This is the major object that IPSec functions for. Once these security parameters are shared securely between the two entities, which is called a establishment of Security Association (See [IPSec key exchange](#)), the privacy and authentication of data transmission are guaranteed.

### Basic IPSec VPN scenario

To connect two incompatible networks within an IPSec VPN network over an intermediate network, an IPSec VPN device is required to be deployed in front of each the network. The IPSec VPN devices (the FortiWAN units) establish an IPSec VPN tunnel with each other. Each of the IPSec VPN devices performs the processes to encrypt and encapsulate, or decapsulate and decrypt the incoming packets (from the network behind it or the opposite IPSec VPN device), and then forwards the packets to the destination (the opposite IPSec VPN device or the network behind it). The two incompatible networks, therefore, have the secure access to each other through the two IPSec VPN devices (the IPSec VPN tunnel established between the two devices). A host in the network communicates with a opposite host (in the opposite network) without running any IPSec VPN software; what they do is like performing a communication in the same network as usual. All the processes and details for a IPSec VPN communication are taken by the two IPSec VPN devices; hosts are not aware of this. The IPSec VPN devices are so-called IPSec VPN gateways, and this is the typical site-to-site VPN.

### VPN tunnel between two private networks



The above diagram shows an IPSec VPN connection between two private networks, which two FortiWAN units (two endpoints of the VPN tunnel) functions as the IPSec VPN gateways for. The IPSec VPN tunnel is established through public IP addresses (for example 1.1.1.1 and 2.2.2.2) of FortiWAN's WAN interfaces. FortiWAN A receives packets from site A network (192.168.1.0/24) with source IP 192.168.1.10 and destination IP 192.168.2.10 (site B network), and then performs:

- encrypt packets with shared security parameters (algorithms and secret keys)
- encapsulate packets with a new IP header that source IP is 1.1.1.1 and destination IP is 2.2.2.2.
- forward packets to the site B network (FortiWAN B)

FortiWAN B receives the packets and performs:

- recover the encrypted packets by decapsulation
- recover the original data and IP header by decryption
- forward packets to host 192.168.2.10

Processes for traffic in the opposite direction are the same. From the standpoint of FortiWAN A, FortiWAN A is local unit and FortiWAN B is the remote unit, vice versa.

## IPSec key exchange

After the basic concept of IPSec VPN introduced above, here comes the details of IPSec's key exchange processes which is the major part to configure an IPSec VPN. As the previous discussion, IPSec performs data encryption and authentication for the VPN communications. The way to securely distribute a common secret key to each endpoint is essential to make the secure data transmission complete. After all, a encrypted data is no



longer secure if its secret key is not safe or compromised. Before we take look into IPSec's key exchange, a basic concept of encryption and authentication is introduced first.

## Encryption

Encryption mathematically transforms data to meaningless random numbers. The original data is called plaintext and the encrypted data is called ciphertext. The opposite process, called decryption, performs the inverse operation to recover the original plaintext from the ciphertext. The process by which the plaintext is transformed to ciphertext and back again is called an algorithm. All algorithms use a small piece of information, a key, in the arithmetic process of converted plaintext to ciphertext, or vice-versa. IPSec uses symmetrical algorithms, which the same key is used for both encrypt and decrypt the data. The length of the key is one of the factors determining the security of an encryption algorithm. FortiWAN IPsec VPNs offer the following encryption algorithms, in descending order of security:

|        |                                                                               |
|--------|-------------------------------------------------------------------------------|
| AES256 | A 128-bit block algorithm that uses a 256-bit key.                            |
| AES192 | A 128-bit block algorithm that uses a 192-bit key.                            |
| AES128 | A 128-bit block algorithm that uses a 128-bit key.                            |
| 3DES   | Triple-DES, in which plain text is DES-encrypted three times by three keys.   |
| DES    | Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. |

## Authentication

In Information Security (or Cryptography), Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In authentication, one has to prove its identity to the remote one, and the identity will be verified by the remote one. A typical providing proof can be a certificate or username and password. In cryptography, a message authentication code (MAC) is a short piece of information used to authenticate a message—in other words, to provide integrity and authenticity assurances on the message. Integrity assurances detect accidental and intentional message changes, while authenticity assurances affirm the message's origin. A MAC algorithm, sometimes called a keyed (cryptographic) hash function (however, cryptographic hash function is only one of the possible ways to generate MACs), accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a tag). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content. As with any MAC, it may be used to simultaneously verify both the data integrity and the authentication of a message. FortiWAN IPsec VPNs offer the following MAC algorithms, in descending order of security:

|             |                                                        |
|-------------|--------------------------------------------------------|
| hmac-sha512 | A SHA512-based MAC algorithm with 512-bit hash output. |
| hmac-sha384 | A SHA384-based MAC algorithm with 384-bit hash output. |
| hmac-sha256 | A SHA256-based MAC algorithm with 256-bit hash output. |
| hmac-sha1   | A SHA1-based MAC algorithm with 160-bit hash output.   |
| hmac-md5    | A MD5-based MAC algorithm with 128-bit hash output.    |

## Security Association

To support secure communications (data encryption and authentication) between two VPN gateways, the common security attributes must be shared in advance, which are the cryptographic and authentication algorithms, encryption secret key and other necessary parameters. A common set of the security attributes maintained by two IPSec VPN gateways for an IPSec VPN tunnel is what called Security Association (SA), which is used to provide a secure channel and protect the communications between the two site networks. Each of the two IPSec VPN gateways encrypts/decrypts data according to the established Security Association. The process to establish a Security Association involves sharing and negotiation of the security attributes.

## IKE key exchange

Internet Key Exchange (IKE) is the protocol used to establish a Security Association (SA), which is included in the IPSec protocol suite. The purposes of IKE are to

- Negotiate an encrypt algorithm and an authentication algorithm
- Generate a shared secret key to encrypt/decrypt IPSec VPN communications (data transmission).

Both are used by IPSec VPN to provide secure communications between two endpoints.

IKE consists of two phases, Phase 1 and Phase 2. The purpose of IKE Phase 1 is to establish a secure and authenticated channel, which is actually a Security Association (called ISAKMP SA as well), between two entities for further IKE Phase 2 negotiations. With the protection of ISAKMP SA, Phase 2 will then be performed to establish the final Security Association (called IPSec SA as well) used to protect the VPN communications (data transmission) between two sites. In other words, before users' VPN communication starts (data packet being transferred to each other), the corresponding IKE Phase 1 and Phase 2 must be done to establish the SAs between the two VPN gateways. With the established SA between two VPN gateways, privacy and authenticity are so that guaranteed to the VPN communications (by encryption and authentication). Basically, IKE Phase 1 authenticates a remote peer and sets up a secure channel for going forward Phase 2 negotiations to establish the IPSec SA.

## IKE Phase 1

Before we talk about the details of IKE Phase 1, let us have an overview on Phase 1's Identity Verification (Authentication). The endpoint who begins the IKE Phase1 negotiation makes a declaration of who it is to the opposite endpoint, and the opposite endpoint verifies the identity. FortiWAN's IPSec employs a **pre-shared key** to achieve the identity verification. The pre-shared key is a common key (similar to a password) pre-shared between the two entities who join in the Phase 1 negotiations. This pre-shared key is used for verification of the declared identity in a cryptographic system (MAC calculation of the identity). This mechanism is on the premise that the pre-shared key is never compromised to the third-party. Although it looks like a password, the pre-shared key, also known as a shared secret, is never sent by either endpoint during the processes of authentication. Actually, the pre-shared key is involved in the calculations of encryption keys, which is actually used for the authentication, at each endpoint. Unmatched pre-shared keys result in unmatched encryption keys, and indirectly cause the authentication in IKE Phase 1 failed.

Now back to the IKE Phase 1. Phase 1 achieves the following objectives to establish ISAKMP Security Association:

## IKE Proposals negotiation

An IKE proposal is a set of necessary parameters for negotiations to establish a Security Association. The negotiation initiator offers opposite endpoint the proposals of the suggested encryption and authentication algorithms, the time-period that keys should remain active, and the strength of the keys used in Diffie-Hellman

key exchange process. The opposite endpoint chooses an appropriate proposal and responds it to the initiator, so that the algorithms and other parameters used to protect data transmission between two endpoints are determined.

### **Generate the secret key for encryption**

A secret key is necessary for the established ISAKMP Security Association to work with the determined encryption and authentication protocols. Therefore, except the negotiations of IKE proposals, a secret key must be determined and shared between the two entities during IKE Phase 1 negotiations. However, it is insecure to send a secret key directly to the opposite endpoint over the public network (no SA protection is offered during Phase 1 negotiations). Diffie-Hellman key exchange, which is a method used to securely exchange cryptographic keys over a public channel, is introduced to IKE to generate the secret key. The two entities running a Diffie-Hellman key exchange will start by exchanging key materials, which are public to third-party, via the public network. With the key materials, calculation of Diffie-Hellman key exchange performed on each of the endpoints derives a common value, which is a seed to generate the secret key we need. With the private and common seed, the two endpoints further calculate the common secret key, and so that the secret key is securely shared. Actually, the pre-shared key used for identity authentication is involved in the final calculations generating the secret key.

## **Authentication**

### **Identity protection**

The two endpoints running the Phase 1 processes declare its identity to each other. A pre-shared key between the two entities is used to verify the declared identity and thus prevent malicious attacks from counterfeit identity. With cryptographic method and the pre-shared key, one can prove its identity to the opposite end. Although it looks like a password, the pre-shared key, also known as a shared secret, is never sent by either gateway. Actually, it is involved in the generation of encryption secret key.

### **Message integrity**

A message authentication code (MAC) not only verifies identity but also provides integrity and authenticity assurances on the exchanged messages. The MAC value protects both a message's data integrity as well as its authenticity against man-in-the-middle attacks or tampering.

## **Main mode and Aggressive mode**

Phase 1 parameters are exchanged in either Main mode or Aggressive mode:

In Main mode, the processes of IKE Phase 1 consists of six message exchanges. An IKE Phase 1 session begins with IKE proposals negotiations between initiator and responder (as the previous description). In the next two message exchanges, the necessary keying materials are exchanged to calculate the common secret key at both ends. For the last two exchanges, encrypted authentication information is exchanged to verify the identity and message integrity on each end.

In Aggressive mode, the processes of IKE Phase 1 is squeezed into three message exchanges. All data required for IKE proposal negotiation and Diffie-Hellman key exchange passed by the initiator and responder in the first two message exchanges. Unencrypted authentication information for sessions passed in the second and third message exchanges. Comparing with main mode, aggressive mode might not be such secure (weak identity protection and risk of pre-shared key crack), the advantage to aggressive mode is that it is faster than Main mode however. FortiWAN's IPSec, however, does not support IKE Phase 1 in Aggressive mode, only Main mode is available.

The successful outcome of Phase 1 negotiations (either aggressive mode or main mode) establishes the ISAKMP Security Association, and the Phase 2 negotiation begins immediately. Phase 2 negotiations will be protected (encryption) within the ISAKMP Security Association.

## IKE Phase 2

Under the protection of ISAKMP Security Association, IKE Phase 2 performs parameters negotiations to establish the IPsec Security Association which protects the subsequent IPsec VPN communications. IKE Phase 2 is processed in one mode called Quick Mode (New Group Mode is not supported by FortiWAN). Similar to Phase 1, in IKE Phase 2, another proposal of encryption and authentication algorithms is negotiated, shared secret keys are derived, and the negotiation sessions are authenticated. The negotiated encryption and authentication algorithms, derived secret keys and other necessary parameters, which are the successful outcome of IKE Phase 2, constitute the IPsec Security Association. So that the security association between two IPsec VPN gateways is established, and the VPN communications are so that protected.

## Perfect Forward Secrecy, PFS

Perfect Forward Secrecy is a property of communication security that past session keys can not be compromised by the compromise of long-term keys if a session key is associated to the long-term key in some way. Actually, the shared secret key we introduced in IKE Phase 2 is derived by calculation with the secret key derived in IKE Phase 1 and some insecure (is public to any third-party) parameters (a Diffie-Hellman exchange is not involved in the calculation), if PFS is not enabled for IKE Phase 2. Once the secret key of IKE Phase 1 is compromised to an attacker, all the secret session keys derived in IKE Phase 2 might become compromised. With enabling PFS, the calculation of secret keys involves a new Diffie-Hellman exchange. The private key material of Diffie-Hellman exchange protects the session secret keys of IKE Phase 2 from the compromise of IKE Phase 1's keys. However, system performance might be concerned if Diffie-Hellman exchange is performed twice (Phase 1 and Phase 2 individually) for a establishment of IPsec Security Association.

## How IPSec VPN Works

So far we have a overview of IPSec concept and how the Security Associations are established. Before a further discussion, here is the IPSec VPN's operation broken down into five main steps:

1. The initial packet matching correspondent IPSec VPN policies and attempting to pass through the IPSec VPN gateway triggers the IKE processes to establish Security Associations.
2. During IKE Phase 1, IKE proposals are negotiated, secret keys are shared and the two IPSec endpoints are authenticated. The ISAKMP SA is established for IKE Phase 2.
3. IKE Phase 2 negotiates new parameters and calculates new secret keys. The IPsec SA is established for VPN communications.
4. Communications over the two IPSec VPN gateways are protected according on the security parameters and keys stored in Security Association database. Data packets are encapsulated with ESP header and new IP header, and transferred over the IPSec VPN tunnel.
5. IPsec SAs terminate by timing out.

## Modes of IPSec VPN data transmission

IPSec transfers the encrypted or authenticated IP packets (ESP or AH encapsulated packets) in a host-to-host transport mode, as well as in a tunneling mode. Packet exchanges during IKE Phase 1 and Phase 2 are nothing about the two modes.

### Tunnel mode

IPSec Tunnel mode is commonly used for site-to-site communications by tunneling through incompatible networks. For example, it delivers protected communications between two private networks through Internet, which is a typical IPSec VPN. In IPSec tunnel mode, the original IP packet is entirely encrypted (not only the payload data but also the routing information are encrypted), and is encapsulated with a new IP header. With the new IP header encapsulation and decapsulation, two incompatible networks deliver encrypted packets to each other by tunneling through Internet.

### Transport mode

IPSec Transport mode is used for communications between two end-stations (host-to-host). An end-station can be a IPSec gateway or just a host running IPSec server/client. Both are actually the destination to each other while communicating. The basic concept of IPSec Transport mode is that the original IP header is intact; the routing is neither modified nor encrypted. Transport mode only provides protection of the payload of the original IP packet by encryption. The two endpoints are supposed to be accessible to each other originally. Usually, Transport mode is applied to other tunneling protocols to provide protection of GRE/L2TP encapsulated IP data packets ( GRE/L2TP transmission over IPSec protection). FortiWAN IPSec Transport mode is only available for Tunnel Routing.

## IPSec set up

After basic concept of IPSec introduced previously, this section focus on the introduction of FortiWAN's IPSec and the configurations to set up FortiWAN's IPSec. FortiWAN provides a complete VPN solution through the cooperation of Tunnel Routing and IPSec. FortiWAN's Tunnel Routing is used to build a site-to-site VPN with bandwidth aggregation and fault tolerance over multiple WAN links. Moreover, with FortiWAN's IPSec protection, Tunnel Routing delivers packets over secure channels.

## About FortiWAN IPSec VPN

### Specifications of FortiWAN's IPsec VPN

Since FortiWAN's IPSec is designed for applications of site-to-site VPN, it is functionally-limited comparing with standard IPSec protocol suite. However, FortiWAN's IPSec still provides basic protections for tunneling communications. The specifications is listed as following:

|            |                                                                                                                                                                   |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IKE</b> | Support IKE v1 and IKE v2<br><br>(A specific procedure is required to switch the version, see <a href="#">IKE Phase 1 Web UI fields - Internet Key Exchange</a> ) |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                 |                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authentication method</b>    | Support pre-shared key only                                                                                                                                                                                                                           |
| <b>IKE Phase 1 modes</b>        | Support Main mode only                                                                                                                                                                                                                                |
| <b>Encryption algorithm</b>     | DES, 3DES, AES128, AES192, AES256                                                                                                                                                                                                                     |
| <b>Authentication algorithm</b> | MD5, SHA1, SHA256, SHA384, SHA512                                                                                                                                                                                                                     |
| <b>DH group</b>                 | 1 (modp768), 2 (modp1024), 5 (modp1536), 14 (modp2048)                                                                                                                                                                                                |
| <b>Transmission mode</b>        | Tunnel mode and limited Transport mode. Transport mode is only available for Tunnel Routing.                                                                                                                                                          |
| <b>Security protocol</b>        | Support Encapsulating Security Payload (ESP) only                                                                                                                                                                                                     |
| <b>NAT traversal</b>            | Not Support                                                                                                                                                                                                                                           |
| <b>DPD</b>                      | Support                                                                                                                                                                                                                                               |
| <b>PFS</b>                      | Support                                                                                                                                                                                                                                               |
| <b>IP deployment</b>            | Support static IPv4 only, the supported WAN link types (See <a href="#">Configuring your WAN</a> ): <ul style="list-style-type: none"> <li>• Routing mode</li> <li>• Bridge Mode: One Static IP</li> <li>• Bridge Mode: Multiple Static IP</li> </ul> |
| <b>IPv6</b>                     | Not Support                                                                                                                                                                                                                                           |
| <b>Peer device</b>              | Support FortiWAN/FortiGate                                                                                                                                                                                                                            |
| <b>Fail over</b>                | Not Support (Both IPSec Tunnel mode and Transport mode themselves have no ability to do fail over, only Tunnel Routing over IPSec Transport mode supports fail over)                                                                                  |

## Tunnel mode, Transport mode and Tunnel Routing

FortiWAN provides standard Tunnel mode to build IPSec VPN as the previous descriptions. By encapsulating the encrypted packet with a new IP header, a tunnel is established between two FortiWAN units so that IPSec packets can be delivered to the private networks deployed behind the two units through Internet (the public and untrusted network). This is what called IPSec VPN typically. Compare with FortiWAN's Tunnel Routing, IPSec Tunnel mode can also establish multiple tunnels through different WAN ports (WAN interfaces) between two FortiWAN units, but bandwidth aggregation and fault tolerance are not available for the IPSec VPN transmission. It is unable to distribute the IPSec packets of a connection or the connections of a specified group over multiple IPSec tunnels; they are delivered through one of the tunnels fixedly.

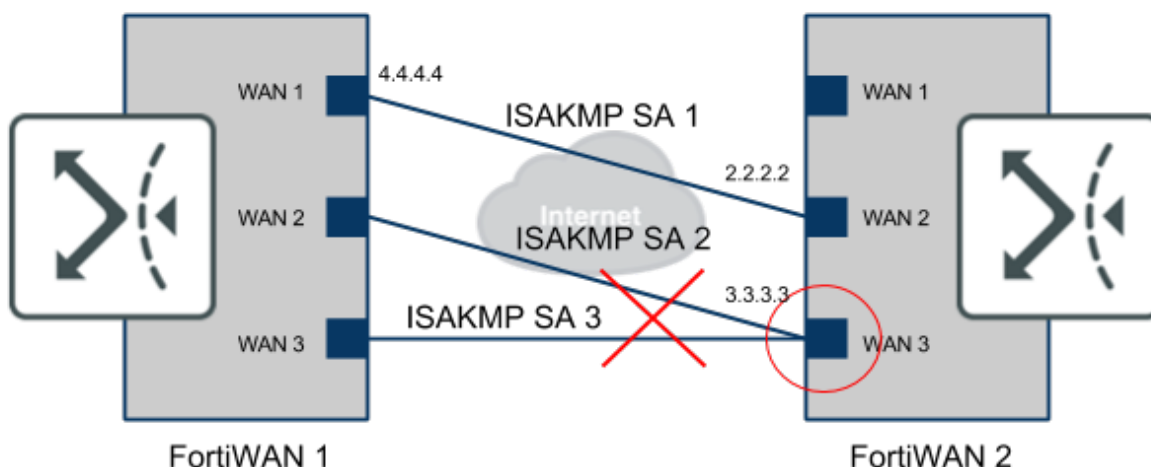
Although FortiWAN's Tunnel Routing (See "[Tunnel Routing](#)") is the technology to distribute packets of one tunneling connection over multiple tunnels (bandwidth aggregation and fault tolerance are so that supported), it does not provide strict protection to the tunneling communications (the encryption function built-in Tunnel Routing is very simple and low security). For this reason, the major purpose of FortiWAN's IPSec Transport mode is to provide Tunnel Routing transmissions an IPSec protection. Actually, the FortiWAN's IPSec Transport mode is designed for Tunnel Routing only; an Transport mode IPSec SA can not be applied to the traffic except Tunnel Routing. By establishing an IPSec SA on every TR tunnel, Tunnel Routing's GRE packets will be encrypted (ESP encapsulated) and be transferred through the specified interface (according to the specified TR algorithm) in IPSec Transport mode (the original routing of the GRE packet remains intact as the previous description). The ESP packets are decrypted on the opposite FortiWAN unit to recover the original GRE packets, and the subsequence is the normal Tunnel Routing processes, packet decapsulation, reassembly and forwarding (to the hosts behind the FortiWAN). The way for IPSec Transport mode to protect Tunnel Routing transmission is very flexible. For every TR tunnel of a tunnel group, it is your options to establish a IPSec SA protecting the TR tunnel or not. Tunnel Routing works normally under full and partial IPSec protection (full protection: each TR tunnel of a tunnel group is protected by a IPSec SA; partial protection: parts of the TR tunnels of a tunnel group are protected by IPSec SAs).

In conclusion, FortiWAN provides three methods to build a VPN network, which are **Tunnel Routing**, **IPSec Tunnel mode** and **Tunnel Routing over IPSec Transport mode**. Note that Tunnel Routing can not support dynamic IP and NAT pass-through (one of the features of Tunnel Routing, see "Dynamic IP addresses and NAT pass through" in "Tunnel Routing > How the Tunnel Routing Works"), if it is protected by IPSec.

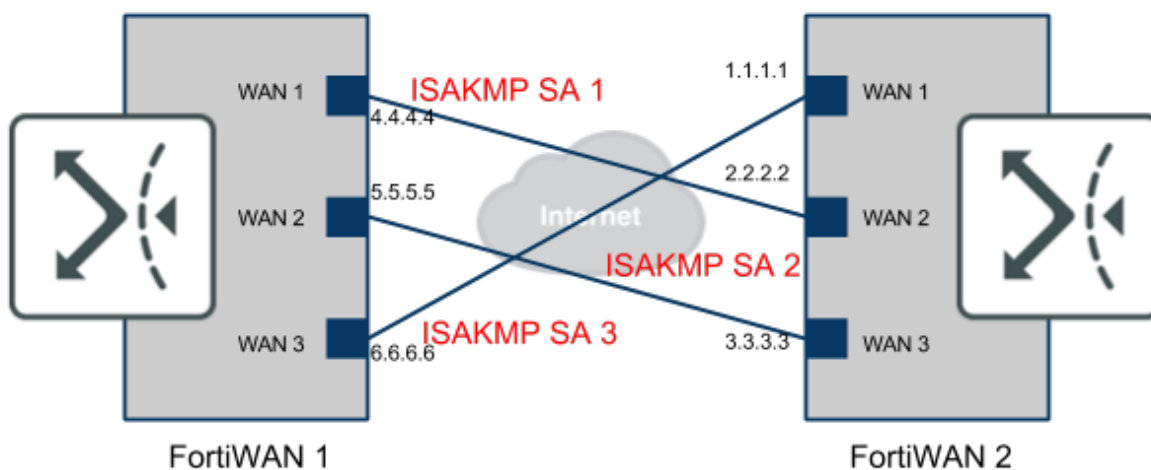
| Type                                            | IPSec protection | Tunneling | Bandwidth Aggregation & Fault Tolerance | Peer device                           |
|-------------------------------------------------|------------------|-----------|-----------------------------------------|---------------------------------------|
| <b>IPSec Tunnel mode</b>                        | Yes              | Yes       | No                                      | Peer can be a FortiWAN or a FortiGate |
| <b>Tunnel Routing</b>                           | No               | Yes       | Yes                                     | Peer must be a FortiWAN               |
| <b>Tunnel Routing over IPSec Transport mode</b> | Yes              | Yes       | Yes                                     | Peer must be a FortiWAN               |

## Limitation in the IPSec deployment

FortiWAN IPsec has an intrinsic limitation in establishing ISAKMP Security Associations. For the establishment of ISAKMP SA between **any two devices, one IP address of a WAN link of a FortiWAN device is restricted to participate in only one ISAKMP SA**. The mapping of WAN link IP addresses for establishing ISAKMP SAs between any two devices must be **one-to-one**. The negotiations of ISAKMP SAs go to failure (the subsequent negotiations of IPSec SAs abort so that) if those Phase 1 configurations on any two FortiWAN devices contain a common WAN link IP address, no matter on the local side or remote side. The following diagrams give the clear explanation of this in details.



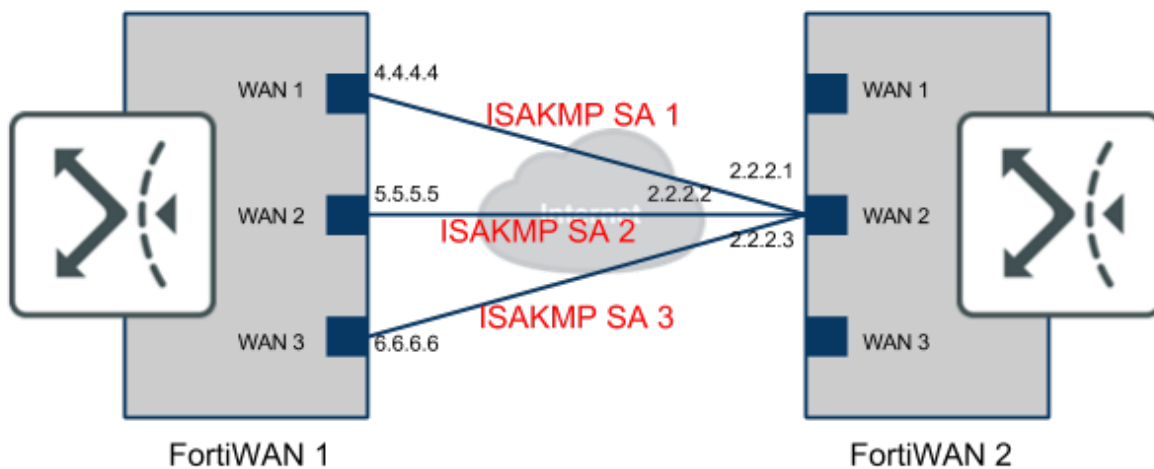
In the example above, the WAN link IP address mapping of ISAKMP SA 1 between FortiWAN 1 and FortiWAN 2 is typical and correct. Both the WAN link IP addresses, 2.2.2.2 and 4.4.4.4, participate in only one ISAKMP SA, the ISAKMP SA 1. As for WAN link 3 on FortiWAN 2, its IP address 3.3.3.3 participates in ISAKMP SA 2 and ISAKMP SA 3 (more than one ISAKMP SA), which causes failure to establish ISAKMP SA 2 and ISAKMP SA 3. IPSec connections thus can not be established.



The above example indicates a **valid** IPSec deployment. The mapping of WAN link IP address for all the ISAKMP SAs between the two devices are in one-to-one relationship:

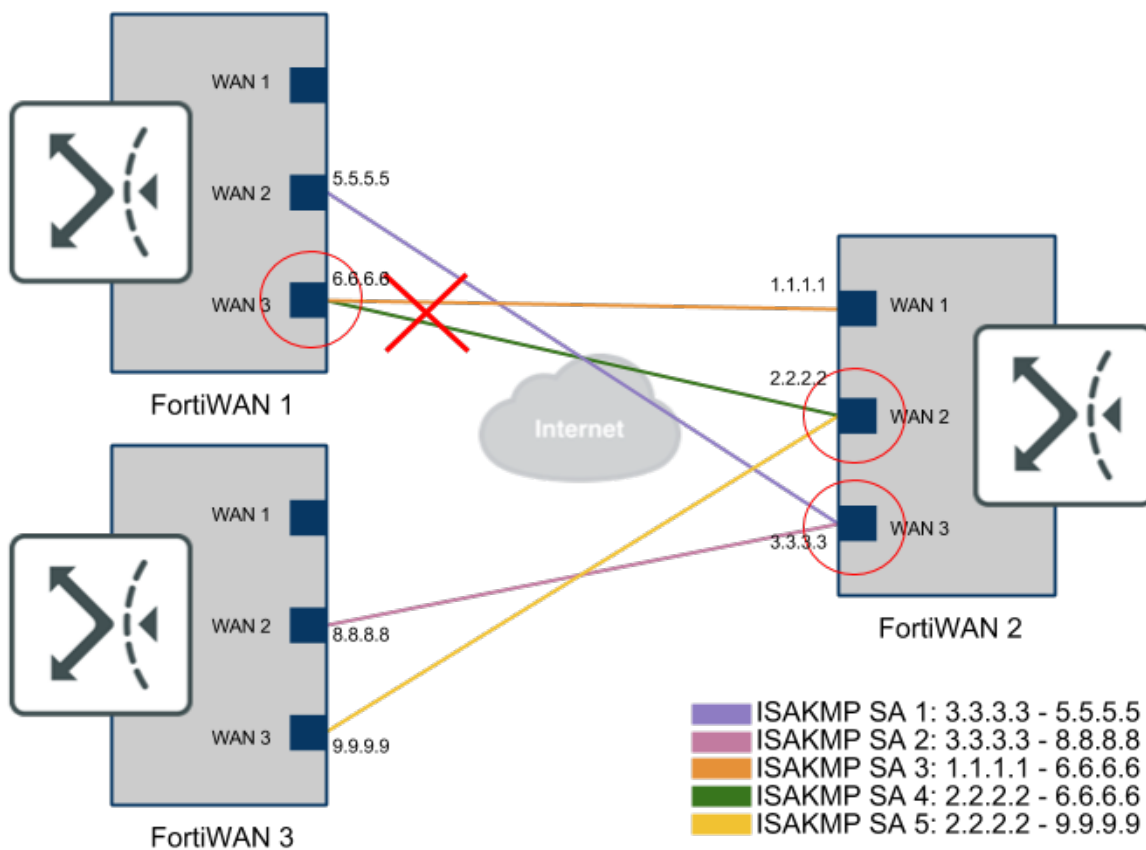
- ISAKMP SA 1: 2.2.2.2 - 4.4.4.4
- ISAKMP SA 2: 3.3.3.3 - 5.5.5.5
- ISAKMP SA 3: 1.1.1.1 - 6.6.6.6





The above diagram is another example of **valid** IPSec deployment. There are three IPs deployed on FortiWAN 2's WAN link 2 (See "[Configuring your WAN](#)"), and each IP address participates in only one ISAKMP SA.

- ISAKMP SA 1: 2.2.2.1 - 4.4.4.4
- ISAKMP SA 2: 2.2.2.2 - 5.5.5.5
- ISAKMP SA 3: 2.2.2.3 - 6.6.6.6



Considering the IPSec deployment among more than two FortiWAN devices as the above example.

| ISAKMP SA   | State       | Reason                                                                                                                                                                                                                                                                                                                                                                    |
|-------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISAKMP SA 1 | established | For the two FortiWAN devices (FortiWAN1 and FortiWAN 2), the two WAN link IP addresses, 3.3.3.3 and 5.5.5.5, participate in only ISAKMP SA 1. Although 3.3.3.3 also participates in ISAKMP SA 2, it takes no influence on ISAKMP SA 1 since it is the thing about another device, FortiWAN 3. The deployment limitation is about any two devices, others can be ignored.  |
| ISAKMP SA 2 | established | For the two FortiWAN devices (FortiWAN 2 and FortiWAN 3), the two WAN link IP addresses, 3.3.3.3 and 8.8.8.8, participate in only ISAKMP SA 2.                                                                                                                                                                                                                            |
| ISAKMP SA 3 | failed      | For the two FortiWAN devices (FortiWAN 1 and FortiWAN 2), the WAN link IP addresses 6.6.6.6 participates in not only ISAKMP SA 3 but also ISAKMP SA 4.                                                                                                                                                                                                                    |
| ISAKMP SA 4 | failed      | For the two FortiWAN devices (FortiWAN 1 and FortiWAN 2), the WAN link IP addresses 6.6.6.6 participates in not only ISAKMP SA 3 but also ISAKMP SA 4.                                                                                                                                                                                                                    |
| ISAKMP SA 5 | established | For the two FortiWAN devices (FortiWAN 2 and FortiWAN 3), the two WAN link IP addresses, 2.2.2.2 and 9.9.9.9, participate in only ISAKMP SA 5. Although 2.2.2.2 also participates in ISAKMP SA 4, it takes no influence on ISAKMP SA 5 since it is the thing about another device, FortiWAN 1. The deployment limitation is about any two devices, others can be ignored. |

Between any two FortiWANs, we cannot terminate traffic through multiple IPSec connections on the same local or remote IP address. This limitation exists in both of the IPSec types: IPSec Tunnel mode and IPSec Transport mode, so that **Tunnel Routing over IPSec Transport mode** is involved indirectly. You have to give careful consideration to the issue when planning how to deploy the IPSec VPN (and Tunnel Routing) between multiple FortiWANs.

## Planning your VPN

Building a VPN between sites might involve complex association with sites and confusing configurations. Beginning hastily to configure settings without a comprehensive plan usually causes failure. Making a plan in advance for your VPN topology is a great help to the next VPN configurations. The following considerations help you determine the VPN topology and necessary information for configurations.

### The locations of the sites that the site-to-site traffic originates from and needs to be delivered to

- Choose the network sites that they need to communicate to each other through the VPN and define what kind of communication it is (what kind of services provided in a network site and what kind of services that users in a network site need to access).

### The networks, individual hosts or server frames participating in the VPN communications

- A network site consists of hosts, servers, and/or networks (private IP addresses deployment). You need to determine the participating private IP addresses (the source and destination of traffic) and make policies to permit traffic to pass through the VPN.

### The VPN devices used to build the VPN

- A site-to-site VPN (tunnels) between two FortiWAN units, or a FortiWAN unit and a FortiGate unit.

### **The network interfaces that two VPN devices communicate through**

- For any VPN tunnel between two VPN devices, you need to determine the participating network interface for each end-point. This implies the public IP addresses (local IP and remote IP) used to establish a VPN tunnel through Internet. Note that only static IP addresses are supported.
- One WAN interface cannot serve for more than one IPSec connectivity between any two FortiWAN devices. You need to take this for consideration when you determine the topology. See "[Limitation in the IPSec deployment](#)" for the details.

### **The VPN device interfaces that a private network accesses the VPN through**

- The private IP addresses associated with the VPN device interfaces to the private networks. Hosts in the private network behind the VPN device access VPN through these interface. Traffic is forwarded between the VPN tunnels and the private networks on each site.

### **The types used to build the VPN**

- IPSec protected VPN without bandwidth aggregation and fault tolerance: IPSec Tunnel mode.
- IPSec protected VPN with bandwidth aggregation and fault tolerance: Tunnel Routing over IPSec Transport mode.
- VPN with bandwidth aggregation and fault tolerance: Tunnel Routing (See "[Tunnel Routing](#)").

## **IPSec VPN in the Web UI**

The configurations introduced in this section are based on the deployment of FortiWAN-to-FortiWAN. For the IPSec VPN established between a FortiWAN unit and a FortiGate unit, see "[Establish IPSec VPN with FortiGate](#)". This section focus on the configurations of IPSec protected VPN, IPSec Tunnel mode and Tunnel Routing over IPSec Transport mode. For configurations of Tunnel Routing, see "[Tunnel Routing](#)".

To set up the IPSec VPN between two FortiWAN units, the following steps are necessary for each of the endpoints.

1. Define IKE Phase 1 parameters for establishment of ISAKMP Security Association with authenticated a remote peer.
2. Define IKE Phase 2 parameters for establishment of IPSec Security Association with authenticated a remote peer.
3. Create correspondent policies of NAT, Auto Routing (AR) and Tunnel Routing (TR) to correctly route the packets of IKE negotiations and IPSec VPN communications (will be discussed in next section, see "[Define routing policies for an IPSec VPN](#)").

### **Configurations of IKE Phase 1**

An IPSec VPN tunnel involves the connection of two FortiWAN units. Most of the settings used to establish an IPSec VPN tunnel are required to be corresponding on the both endpoints. Therefore, it is better to collect enough information in preparation for the configurations of an IPSec VPN tunnel.

Here are the items and information that you need to determine for IKE Phase 1 settings:

### **Defining the remote and local ends of the IPSec VPN tunnel**

Basically, this is to specify the public IP addresses for the two ends (a local FortiWAN unit and a remote FortiWAN unit) of the IPSec VPN tunnel. The IPSec VPN tunnel is established through connection of the two public IP

addresses. You need to determine the WAN link of a FortiWAN unit to connect with each other for an IPSec VPN tunnel; and the IP addresses deployed on the two WAN ports are actually the two ends (local IP and remote IP) of the IPSec VPN tunnel. FortiWAN's IPSec VPN does not support dynamic IP addresses; it is only available for the WAN links that are deployed as **Routing Mode, Bridge Mode: One Static IP** or **Bridge Mode: Multiple Static IP** (see "[Configuring your WAN](#)" for details). For the settings of a IPSec VPN tunnel configured on the two endpoints, the Local IP of a FortiWAN unit becomes the Remote IP of the opposite FortiWAN unit and vice versa. An IPSec VPN tunnel consists of the IKE negotiations (for the security associations, SAs) and the data transmission tunnel; both are established through the two public IP addresses. You also have to give consideration to the limitation that we cannot deploy multiple IPSec connections between any two FortiWANs on the same local or remote IP address. See "[Limitation in the IPSec deployment](#)" for details.

### **A pre-shared key used to authenticate the FortiWAN unit to the remote unit**

During the IKE Phase 1 negotiations, a FortiWAN unit need to authenticate itself to the remote unit by a pre-shared key. The two endpoints of an IPSec VPN tunnel share a common key in advance, so that they can authenticate itself to each other with the common key, like a password. You need to distribute the pre-shared key in a secure way. The pre-shared key configured on the two endpoints of a IPSec VPN tunnel must be equal, or the establishment of IPSec Security Association goes to failure (failed authentication results in failure of IKE Phase 1 and Phase 2).

### **The modes for parameters exchanging, Main mode and Aggressive mode, used for IKE Phase 1 negotiations**

A FortiWAN unit exchange Phase 1 parameters with the remote unit in only Main mode. In Main mode, the Phase 1 parameters are exchanged in six messages with encrypted authentication information. As the previous introductions, Main mode gives securer authentication by a encryption with the negotiated secret key. By comparison, Aggressive mode is weak in authentication since the lack of encryption. However, with the simplified exchanging process, Aggressive mode is faster than Main mode indeed. Security and efficiency are the considerations you need to evaluate for IKE Phase 1 negotiations. Once it is determined, both the two endpoints must be configured with the same mode.

### **Enable Dead Peer Detection (DPD) or not**

The connectivity between two endpoints communicating through IPSec may goes down unexpectedly due to routing problems, hardware broken, host rebooting, etc. In the situation, however, the IPSec entities are not aware of the loss of peer connectivity (availability of peer), and the security associations (SAs) of each peer remains. Packets of communication will continue being sent to oblivion, and reestablishment goes to failure. Dead Peer Detection (DPD) is such a method, by sending periodic HELLO/ACK messages, to confirm the availability of an IPSec endpoint, recognize a disconnection, reclaim the lost resources (SAs) and reestablish IKE negotiations automatically. When a disconnection is detected, the active ISAKMP SA and the correspondent IPSec SAs are removed and renegotiated immediately whether the secret keys expire or not. FortiWAN's IPSec DPD is performed in the Always Send mode, which the detection messages are sent at configured intervals regardless of traffic activity between the peers (some products probe for a idle tunnel before sending DPD detection messages, but FortiWAN does not). Related SAs would be removed once a disconnection is recognized by FortiWAN's IPSec DPD, but FortiWAN would not automatically perform the reestablishment (new establishment of the SAs is triggered only if an outgoing packets of the IPSec communication arrive at the FortiWAN unit).

## The IKE Phase 1 proposals for negotiating security parameters

The main object of IKE Phase 1 is to negotiate the encryption and authentication algorithms, and the correspondent keys between two FortiWAN units so that they can authenticate the identity to each other during the Phase 1 process, and protect the subsequent IKE Phase 2 negotiations.

IKE Phase 1 negotiations determine:

- Which encryption algorithms may be applied for converting messages into a form that only the intended recipient can read
- Which authentication hash may be used for creating a keyed hash from a pre-shared or private key
- Which Diffie-Hellman group (DH Group) will be used to generate a secret session key

The initiator of IKE Phase 1 proposes a list of potential cryptographic parameters that are supported (this is what the Proposal fields supposed to be configured on Web UI, algorithms and DH Group) to remote FortiWAN. The remote FortiWAN compares the received proposals with its own list of Phase 1 Proposal and responds with the choice of matching parameters to use for authenticating and encrypting packets. According the determined proposal, the two peers handle the subsequent exchanges to generate encryption keys between them, and authenticate the exchanges through a pre-shared key. The negotiated encryption algorithm, authentication algorithm and secret session key, which are the outcome of successful IKE Phase 1, will be used to protect the subsequent IKE Phase 2 negotiations.

To guarantee a successful IKE proposal negotiation, the configurations of proposals on both endpoints must be partially matched. However, FortiWAN's IKE Phase 1 does not support multiple proposals, which means the IKE Phase 1 proposal must contain only one encryption algorithm, one authentication algorithm and one DH group. Therefore, you need to make sure that the IKE Phase 1 proposals on the two FortiWAN units are exactly the same, or Phase 1 negotiation goes to failure.

## IKE Phase 1 Web UI fields

Go to **Service > IPSec**, select the **Tunnel Mode** or **Transport Mode** and click the add button to add a new configuration panel of Phase 1. The Phase 1 configuration defines the endpoints of the IPSec VPN tunnel, and the necessary parameters used to negotiate with the opposite unit to establish ISAKMP Security Association.

### Add / Delete / Move-Up / Move-Down

The buttons for:

- Adding a new configuration panel below current Phase 1 configuration
- Deleting the current Phase 1 configuration (all the Phase 2 configurations belong to the Phase 1 configuration will be deleted as well)
- Moving the current Phase 1 configuration up a row
- Moving the current Phase 1 configuration down a row

Packets that matching a Phase 2's Quick Mode selector or Phase 1's [Local IP, Remote IP] are allowed to pass through the correspondent IPSec VPN. However, both the two filters are required to be incompatible with the others, Phase 1 configurations moving-up or moving-down is nothing about rule first-match.

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                        | A "unique" description name for the Phase 1 definition. The name is not a parameter exchanged with the opposite unit during Phase 1 negotiations. This name can contain a piece of information used for simple management, such as it can reflect where the correspondent remote unit is or what the purpose it is. It is also the index used in IPSec Statistics (See " <a href="#">Statistics &gt; IPSec</a> ").                                                                                                                                                                               |
| <b>Hide Details / Show Details</b> | Click to expand or collapse the configuration details.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Local IP</b>                    | <p>Type the IP address of local FortiWAN's WAN port used to establish the IPSec VPN tunnel with remote FortiWAN unit. Packets of IKE negotiations (Both Phase 1 and Phase 2) and IPSec VPN communications are transferred through the WAN port on the local side. Note that only static IP address is supported, please make sure the WAN link type is <b>Routing Mode</b>, <b>Bridge Mode: One Static IP</b> or <b>Bridge Mode: Multiple Static IP</b>.</p> <p>The local IP address must equal to the Remote IP on the opposite unit that the local unit establish the IPSec VPN with.</p>      |
| <b>Remote IP</b>                   | <p>Type the IP address of remote FortiWAN's WAN port used to establish the IPSec VPN tunnel with the local FortiWAN unit. Packets of IKE negotiations (Both Phase 1 and Phase 2) and IPSec VPN communications are transferred through the WAN port on the remote side. Note that only static IP address is supported, please make sure the WAN link type is <b>Routing Mode</b>, <b>Bridge Mode: One Static IP</b> or <b>Bridge Mode: Multiple Static IP</b>.</p> <p>The remote IP address must equal to the Local IP on the opposite unit that the local unit establish the IPSec VPN with.</p> |

Please make sure the entered IP address is equal to the IP address of the WAN port that you would like to employ to establish the IPSec VPN, system will not run error checking on this. Incorrect IP address causes the negotiations to go to failure.

A duplicate of **Remote IP (or pair of Local IP and Remote IP)** of a Phase 1 configuration is not acceptable to other Phase 1 configurations. Please make sure each Phase 1 configuration is incompatible with others on the Remote IP. See "[Limitation in the IPSec deployment](#)" for details.

In Transport mode, the Local IP and Remote IP of a Phase 1 configuration must be equal to the Local IP and Remote IP of a TR tunnel that IPSec provides protection to, so that TR packets match the ISAKMP SA and are protected by ESP encapsulation. See "[Tunnel Routing](#)".

Additional routing policies are necessary for system to route the packets of IKE negotiations and IPSec VPN communications to the IP address (WAN port) you defined here (See "[Define routing policies for an IPSec VPN](#)").

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authentication Method</b> | <p>Only Pre-Shared Key is supported. Enter the pre-shared key in the field "Input key" next to the drop-down menu. The pre-shared key is used to authenticate the identity to each other, the local and remote FortiWAN units, during IKE Phase 1 negotiations. Make sure both the local and remote units are defined an equal key. For stronger protection against currently known attacks, a key consisting of a minimum of 16 randomly chosen alphanumeric characters is suggested.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Internet Key Exchange</b> | <p>Select either IKE v1 or IKE v2.</p> <p><b>Note 1:</b> It requires the two endpoints of an IPSec VPN connectivity running the same IKE protocol. Unequal IKE version fails the establishment of ISAKMP SA for an IPSec VPN connectivity.</p> <p><b>Note 2:</b> To change the IKE version for an existing IPSec VPN connectivity, we strongly recommend to following steps:</p> <ol style="list-style-type: none"> <li>1. Stop the traffic passing through the connectivity.</li> <li>2. Click the Delete button to remove the whole IKE configuration and click the Apply button.</li> <li>3. Click the Add button to create a new IKE configuration with the specified IKE version, and click the Apply button.</li> <li>4. Make sure the same change is done to both the two endpoint.</li> </ol> <p>System might fail to reestablish the connectivity if you change the IKE version by simply editing the configuration field.</p> |
| <b>Mode</b>                  | <p>Main mode: the Phase 1 parameters are exchanged in six messages with securer authentication by a encryption with the negotiated secret key.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Dead Peer Detection</b>   | <p>Check to enable the monitoring of current existence and availability of the remote unit. PDP sends a detection message periodically to remote unit every specified time interval. The IPSec tunnel will be considered down if local unit sends the detection message without a response from the remote unit for five consecutive times. When a disconnection is recognized, the active ISAKMP SA (and the correspondent IPSec SAs) are removed immediately whether the secret keys expire or not (a renegotiation would not be performed automatically).</p> <p>Delay: Set the time interval that PDP sends periodically the detection message.</p>                                                                                                                                                                                                                                                                                 |

**Proposal**

An IKE Phase 1 proposal is a combination of one encryption algorithm, one authentication algorithm, one strength of DH key exchange, and the key lifetime. Select the encryption and authentication algorithms, strength of DH key exchange, and enter the key lifetime for the IKE Phase 1 proposal that will be used in the IKE Phase 1 negotiations. The remote unit must be configured to use the same proposal that you define here. Make sure the Phase 1 proposals of the both units are exactly the same. Unmatched proposals result in failure of negotiations.



|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Encryption</b>     | <p>Select one of the following symmetric-key encryption algorithms:</p> <ul style="list-style-type: none"> <li>• <b>DES:</b> Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.</li> <li>• <b>3DES:</b> Triple-DES; plain text is encrypted three times by three keys.</li> <li>• <b>AES128:</b> A 128-bit block algorithm that uses a 128-bit key.</li> <li>• <b>AES192:</b> A 128-bit block algorithm that uses a 192-bit key.</li> <li>• <b>AES256:</b> A 128-bit block algorithm that uses a 256-bit key.</li> </ul> <p>Note that AES128, AES192 and AES256 will be suggested for better performance.</p> |
| <b>Authentication</b> | <p>Select one of the following authentication algorithms:</p> <ul style="list-style-type: none"> <li>• <b>MD5:</b> A MD5-based MAC algorithm (hmac-md5) with 128-bit message digest.</li> <li>• <b>SHA1:</b> A SHA1-based MAC algorithm (hmac-sha1) with 160-bit message digest.</li> <li>• <b>SHA256:</b> A SHA256-based MAC algorithm (hmac-sha256) with 256-bit message digest.</li> <li>• <b>SHA384:</b> A SHA384-based MAC algorithm (hmac-sha384) with 384-bit message digest.</li> <li>• <b>SHA512:</b> A SHA512-based MAC algorithm (hmac-sha512) with 512-bit message digest.</li> </ul>                                        |
| <b>DH Group</b>       | <p>Select one Diffie-Hellman group from the DH groups 1, 2, 5, and 14. Diffie-Hellman (DH) groups determine the strength of the private key material used in the Diffie-Hellman key exchange process. A higher group number implies a securer key against private key recover attacks, but additional processing time to calculate the key is required.</p> <ul style="list-style-type: none"> <li>• <b>DH Group 1:</b> 768-bit group</li> <li>• <b>DH Group 2:</b> 1024-bit group</li> <li>• <b>DH Group 5:</b> 1536-bit group</li> <li>• <b>DH Group 14:</b> 2048-bit group</li> </ul>                                                 |
| <b>Keylife</b>        | <p>Enter the time interval (in seconds) that the negotiated secret key (used for ISAKMP SA) is valid during. For the expiration of a key, IKE Phase 1 is performed automatically to negotiate a new key without interrupting normal IPSec VPN communications.</p>                                                                                                                                                                                                                                                                                                                                                                        |

## Configurations of IKE Phase 2

After IKE Phase 1 negotiations complete successfully, Phase 2 negotiation begins. Configurations of Phase 2 defines the parameters that are required to establish the IPSec Security Association. The basic parameters of IKE

Phase 2 settings are associated with a Phase 1 configuration for an establishment of IPSec VPN (IPSec SA). This section we describe the configurations of IKE Phase 2.

Here are the items and information that you need to determine for IKE Phase 2 settings:

## The IKE Phase 2 proposals for negotiating security parameters

Similar to Phase 1 negotiations, the purpose of IKE Phase 2 is to negotiate another set of encryption and authentication algorithms, and the correspondent secret keys, so that the established IPSec SA provides protection to subsequent IPSec VPN communications.

IKE Phase 2 negotiations determine:

- Which encryption algorithms may be applied to provide data confidentiality for IP Encapsulating Security Payload (ESP)
- Which authentication hash may be used for data integrity, authentication and anti-replay creating in IP Encapsulating Security Payload (ESP)
- Whether PFS is applied to generate a secret session key or not
- Which Diffie-Hellman group (DH Group) will be used to generate a secret session key if PFS is applied

FortiWAN IKE Phase 2 supports multiple proposals of encryption and authentication algorithms. However, a successful IKE Phase 2 proposal negotiation requires partially matched proposals on the both units. Incompatible IKE proposals fails the IKE Phase 2 negotiations. Please make sure on this while configuring.

Similar to the processes in Phase 1, two FortiWAN units handle the negotiations of encryption and authentication algorithms according to their IKE proposals. The only thing that is different from Phase 1 is Perfect Forward Secrecy (PFS).

### Perfect Forward Secrecy (PFS)

By default, the standard IKE Phase 2 derives the secret session key (for IPSec Security Association) based on the secret session key of ISAKMP Security Association (outcome of Phase 1 negotiations) without additional private materials. The secret session keys of IPSec SA might become vulnerable (to be recovered) if the keys of ISAKMP SA are broken or compromised. Perfect Forward Secrecy (PFS) is the option for IKE Phase 2 to force a new Diffie-Hellman exchange (it implies a new private key material) involved in the calculations of secret session keys, so that they are unrelated to only the Phase 1 keys (can not be recovered with only the compromised ISAKMP SA secret key). Therefore, a DH Group has to be specified for a IKE Phase 2 proposal if the PFS is applied to it. Certainly, PFS gives securer IPSec SA secret key, but more time is spent on the calculations.

### Quick mode selector

Quick mode selector is a rule to determine which packet is transferred through IPSec VPN, according to the source IP address, source port, destination IP address, destination port and protocol of a packet. For Tunnel Mode, it usually implies the hosts (or a network) behind the two FortiWAN units trying to communicate to each other through the IPSec VPN tunnel established between the two FortiWAN. Make sure the Quick mode selector of one endpoint is correspondent to the opposite endpoint. A source IP address defined in the selector in one peer must be defined as the destination IP address of the selector of the opposite peer, and vice versa. FortiWAN supports only Tunnel Routing (TR) traffic to be transferred through IPSec VPN in Transport Mode, therefore, the quick mode selector is not required for Phase 2 configurations of Transport Mode.

## IKE Phase 2 Web UI fields:

IKE Phase 1 and Phase 2 are both the necessities to establish an IPSec VPN, thus configurations of an IPSec VPN must contain configurations of the two Phases. Choosing a set of Phase 1 parameters that you would like to define the correspondent Phase 2 parameters for. The Phase 2 configuration panel is below the Phase 1 panel on the Web UI. Click the add button on the header of Phase 2 or the add button of an existing Phase 2 configuration to add a new Phase 2 configuration panel.

For IPSec Tunnel mode, you can define multiple sets of Phase 2 parameters within one Phase 1 configuration for different Phase 2 Quick Mode selectors. A Phase 2 configuration contains only one quick mode selector used to filter packets matching the only one pair of packet source, destination and protocol. To allow different traffic (for example, traffic of different protocol) to be transferred through the same IPSec VPN tunnel (through the same Local and Remote IPs), it requires multiple Phase 2 configurations (different quick mode selectors) to associate with the same Phase 1. Moreover, you can deliver different IKE Phase 2 proposals (different encryption, authentication algorithms and DH groups) to the multiple quick mode selectors, if multiple security levels are necessary.

For IPSec Transport mode, the Phase 2 configuration does not require a Quick Mode selector. FortiWAN's IPSec Transport mode is designed to protect only communications of Tunnel Routing. Tunnel Routing takes the part to evaluate packets for TR transmission (TR rules) and distributes packets over TR tunnels (TR algorithms), then IPSec Transport mode established on a TR tunnel (Local IP and Remote IP) protects all the passing TR packets. Therefore, multiple Phase 2 sets within a Phase 1 is not required for Transport mode. Remember that FortiWAN supports only two kinds of site-to-site IPSec VPN, "IPSec Tunnel mode" and "Tunnel Routing over IPSec Transport mode".

### Add / Delete / Move-Up / Move-Down

The buttons for:

- Adding a new configuration panel below current Phase 2 configuration
- Deleting the current Phase 2 configuration
- Moving the current Phase 2 configuration up a row
- Moving the current Phase 2 configuration down a row

The buttons for Phase 2 configurations are only available for IPSec Tunnel mode. Each Phase 1 configuration of Transport mode contains one and only one Phase 2 configuration.

Packets that matching a Quick Mode selector are allowed to pass through the correspondent IPSec VPN. However, each Quick Mode selector is required to be incompatible with the others, Phase 2 configurations moving-up or moving-down is nothing about rule first-match.

### Name

A "unique" description name for the Phase 2 definition. The maximum length is "?" characters. The name is not a parameter exchanged with the opposite unit during Phase 2 negotiations. This name can contain a piece of information used for simple management, such as it can reflect where the correspondent remote unit is or what the purpose it is. It is also the index used in IPSec Statistics (See "[Statistics > IPSec](#)").

**Hide Details / Show Details**

Click to expand or collapse the configuration details.

**Proposal**

An IKE phase 2 proposal is a combination of one or multiple encryption algorithms, one or multiple authentication algorithms, one strength of DH key exchange if PFS is enabled, and the key lifetime.

Select the encryption and authentication algorithms, strength of DH key exchange, and the key lifetime for the IKE phase 2 proposal that will be used in the IKE Phase 2 negotiations.

Make sure the Phase 2 proposals of the both units performing the Phase 2 negotiations are compatible. Incompatible proposals cause Phase 2 negotiations going to failure.

**Encryption**

Select one or multiple of the following symmetric-key encryption algorithms:

- **NULL:** NULL means perform an integrity check only; packets are not encrypted. It is invalid to set both Encryption and Authentication to null.
- **DES:** Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- **3DES:** Triple-DES; plain text is encrypted three times by three keys.
- **AES128:** A 128-bit block algorithm that uses a 128-bit key.
- **AES192:** A 128-bit block algorithm that uses a 192-bit key.
- **AES256:** A 128-bit block algorithm that uses a 256-bit key.

The remote peer or client must be configured to use at least one of the encryption proposals that you define.

Note that AES128, AES192 and AES256 will be suggested for better performance.

**Authentication** Select one multiple of the following authentication algorithms:

- **NULL:** NULL means perform an message encryption only; ESP Auth is not calculated. It is invalid to set both Encryption and Authentication to null.
- **MD5:** A MD5-based MAC algorithm (hmac-md5) with 128-bit message digest.
- **SHA1:** A SHA1-based MAC algorithm (hmac-sha1) with 160-bit message digest.
- **SHA256:** A SHA256-based MAC algorithm (hmac-sha256) with 256-bit message digest.
- **SHA384:** A SHA384-based MAC algorithm (hmac-sha384) with 384-bit message digest.
- **SHA512:** A SHA512-based MAC algorithm (hmac-sha512) with 512-bit message digest.

The remote peer or client must be configured to use at least one of the authentication proposals that you define.

**PFS Group**

As the previous descriptions, PFS is an option to involve a new Diffie-Hellman exchange in the calculation of secret session key during Phase 2. Thus, you have to specify the Diffie-Hellman group for the new Diffie-Hellman exchange if PFS is enable.

To apply PFS to the Phase 2 key calculation, you just need to select one of the PFS groups 1, 2, 5, and 14 for Diffie-Hellman group. A PFS group implies a Diffie-Hellman (DH) group actually, which determines the strength of the private key material used in the Diffie-Hellman key exchange process. A higher group number implies a securer key against private key recover attacks, but additional processing time for the key calculation is required. To apply no PFS to the Phase 2 key calculation, just make all the PFS Group options unchecked.

- **PFS Group 1:** Enable PFS with DH Group 1, 768-bit group
- **PFS Group 2:** Enable PFS with DH Group 2, 1024-bit group
- **PFS Group 5:** Enable PFS with DH Group 5, 1536-bit group
- **PFS Group 14:** Enable PFS with DH Group 14, 2048-bit group



|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Keylife</b>    | Enter the time interval (in seconds) that the negotiated secret keys (used for IPSec SA) are valid during. For the expiration of keys, IKE Phase 2 is performed automatically to negotiate new keys without interrupting normal IPSec VPN communications. Keylife of IPSec SA's secret keys is suggested to be shorter than the keylife of ISAKMP SA's secret keys.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Quick Mode</b> | <p>Configurations of Quick Mode is required only for IPSec Tunnel Mode. A Quick Mode selector determines the acceptance or rejection of transmission through the IPSec VPN tunnel for packets. It usually implies the IPSec VPN communications between private networks (hosts) behind the two FortiWANs unit (IPsec VPN gateways). Packets coming from the networks behind the local FortiWAN and going to another network behind the remote FortiWAN are evaluated by Quick Mode selectors at the local FortiWAN unit. Only packets matching the selector are allowed to be transferred via the IPSec VPN tunnel. A Quick Mode selector consists of the following five filters:</p> <ul style="list-style-type: none"> <li>• <b>Source:</b> the source of a packet that is allowed to be transferred via the IPSec VPN tunnel. It can be an IPv4 address or an IPv4 subnet behind the local FortiWAN.</li> <li>• <b>Source Port:</b> the source port of a packet that is allowed to be transferred via the IPSec VPN tunnel.</li> <li>• <b>Destination :</b> the destination of a packet that is allowed to be transferred via the IPSec VPN tunnel. It can be an IPv4 address or an IPv4 subnet behind the remote FortiWAN.</li> <li>• <b>Destination Port:</b> the destination port of a packet that is allowed to be transferred via the IPSec VPN tunnel.</li> <li>• <b>Protocol:</b> the protocol of a packet that is allowed to be transferred via the IPSec VPN tunnel.</li> </ul> <p>Note that one pair of source and destination is not allowed to be set to multiple Quick Mode selectors, neither a subset of the pair is. Make sure the pair of source and destination defined in a Quick Mode selector is absolutely incompatible to other Quick Mode selectors (no matter which Phase 1 configuration they belong to, current one or others).</p> <p>It's necessary to have an Auto Routing (AR) filter that is correspondent with the Quick Mode selector you made, see the following section "<a href="#">Define routing policies for an IPSec VPN</a>".</p> |

So far, we have introduced the concept of IPSec VPN and how to configure the settings of FortiWAN's IPSec. However, the success of the IPSec VPN establishment and communications actually requires the cooperation between FortiWAN' IPSec and other functions, Auto Routing, NAT and Tunnel Routing. In other words, besides the configurations of IPSec, correspondent policies of Auto Routing, NAT or Tunnel Routing are required to set up an IPSec VPN. See "[Define routing policies for IPSec VPN](#)".

## Define routing policies for an IPSec VPN

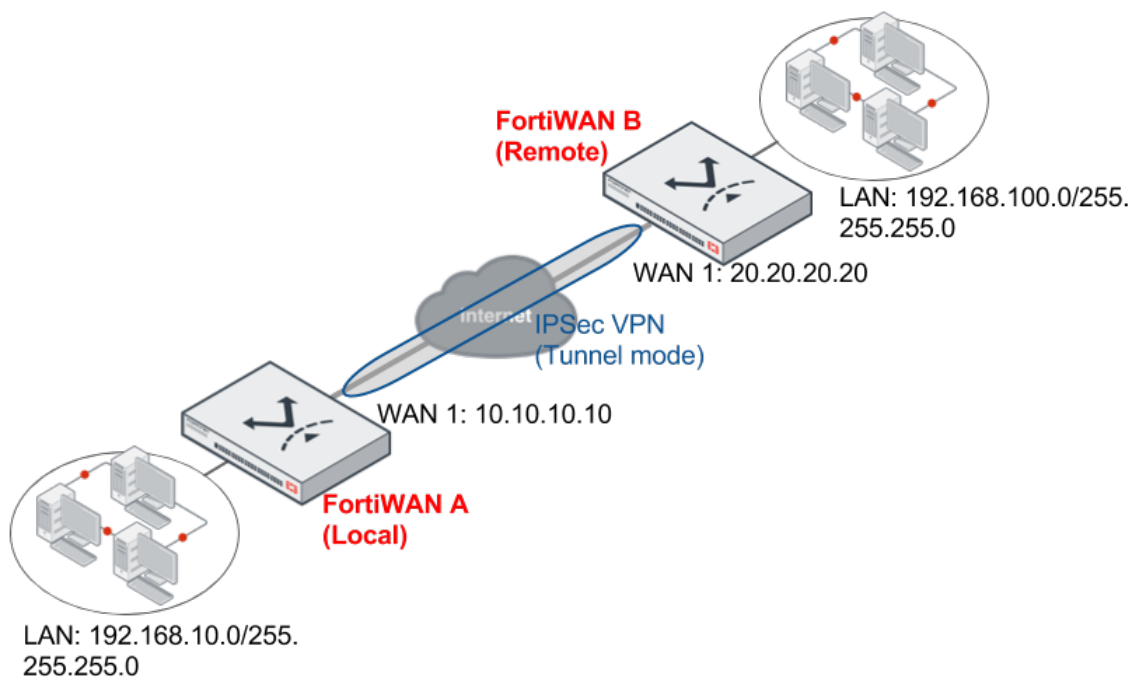
FortiWAN's intelligent routing function (Auto Routing and Tunnel Routing) transferred all packets, including packets of IPSec, outward over multiple WAN links. Although an IPSec configuration specifies the IP addresses of the WAN ports (Phase 1: Local IP and Remote IP) used to establish the IPSec VPN and the IP addresses that Quick Mode selectors evaluate for, it does not imply the correspondent routing for the IPSec packets. You are required to have extra rules of Auto Routing or Tunnel Routing setting manually to fixedly route the IPSec packets to correct WAN port.

The IPSec packets we are talking about consist of the packets of 2 phases IKE negotiations (called "IKE packets" here) and the packets of IPSec VPN communications (called "ESP packets" here). An IKE packet comes from the local FortiWAN unit and its source IP address is just the configured Local IP (a WAN port); an ESP packet comes from a private network behind the local FortiWAN and its source IP address is a private IP address. The followings describe the procedures defining related policies for "IPSec Tunnel mode" and "Tunnel Routing over IPSec Transport mode".

### Define Auto Routing and NAT policies for an IPSec Tunnel-mode VPN

For IPSec Tunnel Mode, you need to make sure connections of both IKE and ESP packets are fixedly routed by Auto Routing to the WAN port that is configured as the Local IP of the IPSec VPN tunnel.

#### Example topology for the following policies



For this example topology, we need to have configurations of **Network Setting**, **Auto Routing**, **NAT** and **IPSec** as follows:

## Network Setting

Network Settings on the both sides:

### WAN settings

Go to **System > Network Setting > WAN Setting**

| WAN Setting          | Local endpoint (Site A) | Remote endpoint (Site B) |
|----------------------|-------------------------|--------------------------|
| WAN Link             | 1                       | 1                        |
| WAN Type             | Routing Mode            | Routing Mode             |
| WAN Port             | Port1                   | Port1                    |
| IPv4 Localhost IP    | 10.10.10.10             | 20.20.20.20              |
| IPv4 Netmask         | 255.255.255.0           | 255.255.255.0            |
| IPv4 Default Gateway | 10.10.10.254            | 20.20.20.254             |

For the details of WAN link setting, see "[Configurations for a WAN link in Routing Mode](#)", "[Configurations for a WAN link in Bridge Mode: One Static IP](#)" and "[Configurations for a WAN link in Bridge Mode: Multiple Static IP](#)".

### LAN private subnets

Go to **System > Network Setting > LAN Private Subnet**

| LAN Private Subnet | Local endpoint (Site A) | Remote endpoint (Site B) |
|--------------------|-------------------------|--------------------------|
| IP(s) on Localhost | 192.168.10.254          | 192.168.100.254          |
| Netmask            | 255.255.255.0           | 255.255.255.0            |
| LAN Port           | Port3                   | Port3                    |

For the details of LAN private subnet setting, see "[LAN Private Subnet](#)".

## Define Auto Routing policies for IKE negotiation and IPSec communication packets

### For IKE negotiation packets

Packets of IKE negotiation are generated by FortiWAN itself (source and destination IP address of the packets is respectively the Local IP and Remote IP of Phase 1 configuration), therefore the Source and Destination of the Auto Routing filter for IKE negotiation must be configured with the Local IP and Remote IP (the IP address of WAN port of two FortiWAN units). Remember that the IPSec SAs are established on the WAN port of both the two FortiWANs.

Go to **Service > Auto Routing**

You need add a new policy to Policies of Auto Routing like:.

| Auto Routing Policy | Local endpoint (Site A)          | Remote endpoint (Site B)         |
|---------------------|----------------------------------|----------------------------------|
| <b>Label</b>        | IPSec_WAN1 (Any name you desire) | IPSec_WAN1 (Any name you desire) |
| <b>T</b>            | Enable Threshold or not          | Enable Threshold or not          |
| <b>Algorithm</b>    | Fixed                            | Fixed                            |
| <b>Parameter</b>    | Only 1 is checked                | Only 1 is checked                |

Then you add a filter to IPv4 Filters like:

| Auto Routing Filter     | Local endpoint (Site A)  | Remote endpoint (Site B) |
|-------------------------|--------------------------|--------------------------|
| <b>When</b>             | All-Time                 | All-Time                 |
| <b>Input Port</b>       | Any Port                 | Any Port                 |
| <b>Source</b>           | 10.10.10.10 or Localhost | 20.20.20.20 or Localhost |
| <b>Destination</b>      | 20.20.20.20              | 10.10.10.10              |
| <b>Service</b>          | Any or IKE(500)          | Any or IKE(500)          |
| <b>Routing Policy</b>   | IPSec_WAN1               | IPSec_WAN1               |
| <b>Fail-Over Policy</b> | NO-ACTION                | NO-ACTION                |

**Note that packets of IKE negotiations are generated from FortiWAN's localhost, the Source field of an AR filter must be configured to "Localhost" to match the negotiation traffic and direct it to correct WAN link.**

#### For IPSec communication packets

Routing of packets that are going to be transferred through IPsec VPN between the private networks (LANs) behind the two sites (local and remote) is also controlled by FortiWAN's Auto Routing. It is necessary to route packets to the WAN link that the IPSec SA is established on, so that the packets can be processed (evaluated by Quick Mode selector and ESP encapsulated) by IPSec on the WAN port.

With the existing policy "For IPsec", you only need to add the filters like:

| Auto Routing Filter | Local endpoint (Site A)           | Remote endpoint (Site B)          |
|---------------------|-----------------------------------|-----------------------------------|
| <b>When</b>         | All-Time                          | All-Time                          |
| <b>Input Port</b>   | Any Port (or the LAN port, PortX) | Any Port (or the LAN port, PortX) |
| <b>Source</b>       | 192.168.10.0/255.255.255.0        | 192.168.100.0/255.255.255.0       |

| Auto Routing Filter     | Local endpoint (Site A)     | Remote endpoint (Site B)   |
|-------------------------|-----------------------------|----------------------------|
| <b>Destination</b>      | 192.168.100.0/255.255.255.0 | 192.168.10.0/255.255.255.0 |
| <b>Service</b>          | Any                         | Any                        |
| <b>Routing Policy</b>   | IPSec_WAN1                  | IPSec_WAN1                 |
| <b>Fail-Over Policy</b> | NO-ACTION                   | NO-ACTION                  |

IPSec Phase 2 Quick Mode selector controls the IPSec availability to specified users (the source, destination and service of packets); before that, it requires the Auto Routing filter to direct the packets to the correct WAN link (Routing Policy). Make sure the Auto Routing filter and Phase 2 Quick Mode selector are equal on Source, Destination and Service. For the details of Auto Routing, see ["Auto Routing"](#). Although Auto Routing provides fail-over policy to redirect packets to another WAN link when a failure occurs, it is unable to achieve the fail-over for IPSec Tunnel mode since the same Quick Mode selector cannot be applied to different IPSec SAs.

### Define NAT policies for IKE negotiation and IPSec communication packets

NAT default rules translate the source addresses of packets come from the private subnet (LAN) behind FortiWAN after Auto Routing determines a WAN link for them. In IPSec VPN Tunnel mode, Packets of communications usually come from LAN subnet of FortiWAN and are evaluated with NAT rule before Phase 2 Quick Mode selector. If the source address of a IPSec packet is translated to another by NAT, the packet fails in matching the Quick Mode selector and the IPSec communication goes to failure.

#### For IKE negotiation packets

IKE negotiation packets are generated on FortiWAN's localhost. The source of a IKE packet is the Local IP (IP address on the WAN port) of the Phase 1, which will not be translated by NAT. Therefore, a NAT policy is not required for IKE negotiations.

#### For IPSec communication packets

By default, all the packets will be processed by NAT once Auto Routing determines a WAN link to the packets. However, IPSec VPN communication will go to failure if source IP address of the packets are translated (mismatching the Quick Mode selectors). To disable NAT for the packets:

1. Go to **Service > NAT**
2. From the drop down menu WAN, select the WAN link used as the local interface of the IPsec VPN tunnel.
3. Add a rule to NAT Rules to disable NAT translation for the packetsdefinition of the Quick Mode selector:

| NAT Rule           | Local endpoint (Site A)     | Remote endpoint (Site B)    |
|--------------------|-----------------------------|-----------------------------|
| <b>When</b>        | All-Time                    | All-Time                    |
| <b>Source</b>      | 192.168.10.0/255.255.255.0  | 192.168.100.0/255.255.255.0 |
| <b>Destination</b> | 192.168.100.0/255.255.255.0 | 192.168.10.0/255.255.255.0  |

| NAT Rule          | Local endpoint (Site A) | Remote endpoint (Site B) |
|-------------------|-------------------------|--------------------------|
| <b>Service</b>    | Any                     | Any                      |
| <b>Translated</b> | No NAT                  | No NAT                   |

Make sure the NAT rule and Phase 2 Quick Mode selector are equal on Source, Destination and Service. For the details of NAT, see ["NAT"](#).

## Define IPSec parameters

Go to **Service > IPSec**

Add Phase 1 configurations for the IPSec tunnel mode VPN between site A's WAN 1 (10.10.10.10) and site B's WAN 1 (20.20.20.20). The other parameters are not listed here.

| Phase 1          | Local endpoint (Site A) | Remote endpoint (Site B) |
|------------------|-------------------------|--------------------------|
| <b>Name</b>      | WAN1_WAN1_Phase1        | WAN1_WAN1_Phase1         |
| <b>Local IP</b>  | 10.10.10.10             | 20.20.20.20              |
| <b>Remote IP</b> | 20.20.20.20             | 10.10.10.10              |

Add Phase 2 configurations for the IPSec tunnel mode VPN between site A's WAN 1 (10.10.10.10) and site B's WAN 1 (20.20.20.20). The other parameters are not listed here.

| Phase 2                 | Local endpoint (Site A)     | Remote endpoint (Site B)    |
|-------------------------|-----------------------------|-----------------------------|
| <b>Name</b>             | WAN1_WAN1_Phase2            | WAN1_WAN1_Phase2            |
| <b>Quick Mode</b>       |                             |                             |
| <b>Source</b>           | 192.168.10.0/255.255.255.0  | 192.168.100.0/255.255.255.0 |
| <b>Source Port</b>      | Any                         | Any                         |
| <b>Destination</b>      | 192.168.100.0/255.255.255.0 | 192.168.10.0/255.255.255.0  |
| <b>Destination Port</b> | Any                         | Any                         |
| <b>Protocol</b>         | Any                         | Any                         |

For the details of IPSec configuration, see ["IPSec VPN in the Web UI"](#).

## Procedures to set up a IPSec Tunnel-mode VPN

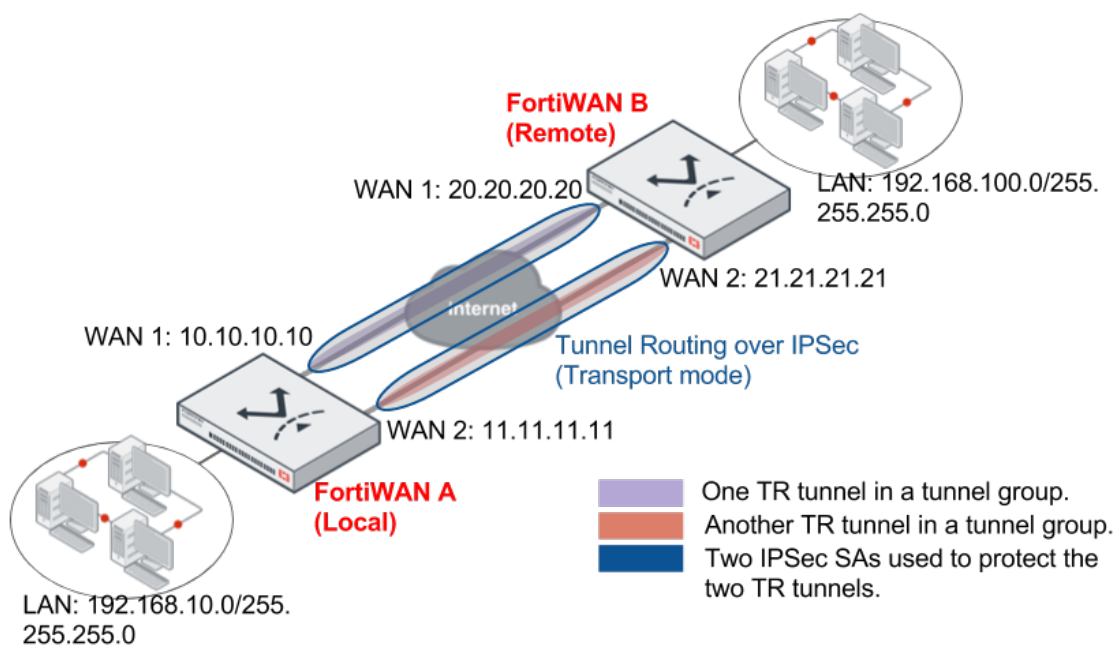
To set up a IPSec Tunnel-mode VPN, we suggest the steps to follow as below:

1. Configure Network Settings on both units.
2. Define correspondent Auto Routing and NAT policies on both units.
3. Configure the settings of IPSec Tunnel mode Phase 1 and Phase 2 on both units.

## Define Auto Routing and Tunnel Routing policies for an Tunnel Routing over IPSec Transport mode VPN

As previous descriptions, IPSec Transport mode provides secure data transmission without IP tunneling (IP encapsulation). However, IPSec Transport mode can give protections to FortiWAN's Tunnel Routing, which brings a securer (compare to the original TR) and more efficient (compare to the "IPsec Tunnel mode VPN" on load balancing and fault tolerance) VPN application. Tunnel Routing distributes the encapsulated (GRE) packets over multiple tunnels (pairs of local WAN port and remote WAN port). With the IPSec SAs established on these TR tunnels, GRE packets will be protected (encrypted/decrypted) by correspondent SA when they pass through a TR tunnel (the local and remote WAN ports). Transport-mode IPSec SAs are required for each of Tunnel Routing's GRE tunnels to associate Tunnel Routing with IPSec.

### Example topology for the following policies



IPSec Transport mode protects the communications between private networks behind two FortiWAN units through two TR tunnels. For this example topology, we need to have configurations of Network Setting, Auto Routing, IPSec and Tunnel Routing as follows:

### Network Setting

Network Setting on the local side:

## WAN settings

Go to **System > Network Setting > WAN Setting**

| WAN Setting                 | Local endpoint (Site A) | Local endpoint (Site A) | Remote endpoint (Site B) | Remote endpoint (Site B) |
|-----------------------------|-------------------------|-------------------------|--------------------------|--------------------------|
| <b>WAN Link</b>             | 1                       | 2                       | 1                        | 2                        |
| <b>WAN Type</b>             | Routing Mode            | Routing Mode            | Routing Mode             | Routing Mode             |
| <b>WAN Port</b>             | Port1                   | Port2                   | Port1                    | Port2                    |
| <b>IPv4 Localhost IP</b>    | 10.10.10.10             | 11.11.11.11             | 20.20.20.20              | 21.21.21.21              |
| <b>IPv4 Netmask</b>         | 255.255.255.0           | 255.255.255.0           | 255.255.255.0            | 255.255.255.0            |
| <b>IPv4 Default Gateway</b> | 10.10.10.254            | 11.11.11.254            | 20.20.20.254             | 21.21.21.254             |

For the details of WAN link setting, see "[Configurations for a WAN link in Routing Mode](#)", "[Configurations for a WAN link in Bridge Mode: One Static IP](#)" and "[Configurations for a WAN link in Bridge Mode: Multiple Static IP](#)".

## LAN private subnets

Go to **System > Network Setting > LAN Private Subnet**

| LAN Private Subnet        | Local endpoint (Site A) | Remote endpoint (Site B) |
|---------------------------|-------------------------|--------------------------|
| <b>IP(s) on Localhost</b> | 192.168.10.254          | 192.168.100.254          |
| <b>Netmask</b>            | 255.255.255.0           | 255.255.255.0            |
| <b>LAN Port</b>           | Port3                   | Port3                    |

For the details of LAN private subnet setting, see "[LAN Private Subnet](#)".

## Define Auto Routing policies for IKE negotiation

Our goal is two establish IPSec protected VPN based on Tunnel Routing (See "[Tunnel Routing](#)") through two TR tunnels, which implies two IPSec SAs being established on the two TR tunnels. Therefore, it requires routing policies to route the IKE negotiation packets for establishing the two IPSec SAs.

Packets of IKE negotiation are generated by FortiWAN itself (source and destination IP address of the packets is respectively the Local IP and Remote IP of Phase 1 configuration), therefor the Source and Destination of the Auto Routing filter for IKE negotiation must be configured with the Local IP and Remote IP (the IP address of WAN port of two FortiWAN units). Remember that the IPSec SAs are established on the WAN port of both the two FortiWANs.

Go to **Service > Auto Routing**



Add two Auto Routing policies on the both endpoints like:

| Auto Routing Policy | Local endpoint (Site A)          | Local endpoint (Site A)          | Remote endpoint (Site B)         | Remote endpoint (Site B)         |
|---------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|
| <b>Label</b>        | IPSec_WAN1 (Any name you desire) | IPSec_WAN2 (Any name you desire) | IPSec_WAN1 (Any name you desire) | IPSec_WAN2 (Any name you desire) |
| <b>T</b>            | Enable Threshold or not          | Enable Threshold or not          | Enable Threshold or not          | Enable Threshold or not          |
| <b>Algorithm</b>    | Fixed                            | Fixed                            | Fixed                            | Fixed                            |
| <b>Parameter</b>    | Only 1 is checked                | Only 2 is checked                | Only 1 is checked                | Only 2 is checked                |

Then you add two IPv4 filters like:

| Auto Routing Filter     | Local endpoint (Site A)  | Local endpoint (Site A)  | Remote endpoint (Site B) | Remote endpoint (Site B) |
|-------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <b>When</b>             | All-Time                 | All-Time                 | All-Time                 | All-Time                 |
| <b>Input Port</b>       | Any Port                 | Any Port                 | Any Port                 | Any Port                 |
| <b>Source</b>           | 10.10.10.10 or Localhost | 11.11.11.11 or Localhost | 20.20.20.20 or Localhost | 21.21.21.21 or Localhost |
| <b>Destination</b>      | 20.20.20.20              | 21.21.21.21              | 10.10.10.10              | 11.11.11.11              |
| <b>Service</b>          | Any or IKE(500)          | Any or IKE(500)          | Any or IKE(500)          | Any or IKE(500)          |
| <b>Routing Policy</b>   | IPSec_WAN1               | IPSec_WAN2               | IPSec_WAN1               | IPSec_WAN2               |
| <b>Fail-Over Policy</b> | NO-ACTION                | NO-ACTION                | NO-ACTION                | NO-ACTION                |

Tunnel Routing itself takes the responsibility to route packets over multiple tunnels, therefore Auto Routing policies are not required for packets of IPSec communication. For the details of Auto Routing, see "[Auto Routing](#)".

**Note that packets of IKE negotiations are generated from FortiWAN's localhost, the Source field of an AR filter must be configured to "Localhost" to match the negotiation traffic and direct it to correct WAN link.**

## Define IPSec parameters

Next is the Phase 1 configurations for two IPSec SAs in Transport mode. To associate an IPSec SA with a TR tunnel, make sure the Phase 1 configuration and the TR tunnel are equal on the Local IP and Remote IP.

Go to **Services > IPSec**

Add Phase 1 configurations for IPSec Transport mode SAs between site A's WAN 1 (10.10.10.10) and site B's WAN 1 (20.20.20.20), and site A's WAN 1 (11.11.11.11) and site B's WAN 1 (21.21.21.21). The other parameters are not listed here.

| Phase 1          | Local endpoint (Site A) | Local endpoint (Site A) | Remote endpoint (Site B) | Remote endpoint (Site B) |
|------------------|-------------------------|-------------------------|--------------------------|--------------------------|
| <b>Name</b>      | peers_AB_1              | peers_AB_2              | peers_BA_1               | peers_BA_2               |
| <b>Local IP</b>  | 10.10.10.10             | 11.11.11.11             | 20.20.20.20              | 21.21.21.21              |
| <b>Remote IP</b> | 20.20.20.20             | 21.21.21.21             | 10.10.10.10              | 11.11.11.11              |

Next you need to configure the settings to Phase 2 for the four Phase 1 configurations above. Phase 2 of Transport mode does not require specifying a Quick Mode selector, only a name and IKE proposal are required. For the details of IPSec configuration, see "[IPSec VPN in the Web UI](#)".

### Define Tunnel Routing policies for IPSec communications

As for the communication packets between networks behind the two FortiWAN units, Tunnel Routing controls the routing of them. You need the configurations to set up the two TR tunnels, and the policies to route GRE packets over the TR tunnels.

To establish the TR tunnels, go to **Service > Tunnel Routing** > add a new Tunnel Group with two Group Tunnels and appropriate balancing algorithm:

| Tunnel Group          | Local endpoint (Site A)   | Remote endpoint (Site B)  |
|-----------------------|---------------------------|---------------------------|
| <b>Name</b>           | Tunnel_Group_AB           | Tunnel_Group_BA           |
| <b>Algorithm</b>      | Round-Robin (for example) | Round-Robin (for example) |
| <b>Group Tunnel 1</b> |                           |                           |
| <b>E</b>              | Checked                   | Checked                   |
| <b>Local IP</b>       | 10.10.10.10               | 20.20.20.20               |
| <b>Remote IP</b>      | 20.20.20.20               | 10.10.10.10               |
| <b>Weight</b>         | 1 (for example)           | 1 (for example)           |
| <b>Group Tunnel 2</b> |                           |                           |
| <b>E</b>              | Checked                   | Checked                   |
| <b>Local IP</b>       | 11.11.11.11               | 21.21.21.21               |
| <b>Remote IP</b>      | 21.21.21.21               | 11.11.11.11               |
| <b>Weight</b>         | 1 (for example)           | 1 (for example)           |

Next, you need a new rule to Routing Rules, like this:

| Routing Rule       | Local endpoint (Site A)     | Remote endpoint (Site B)    |
|--------------------|-----------------------------|-----------------------------|
| <b>Source</b>      | 192.168.10.0/255.255.255.0  | 192.168.100.0/255.255.255.0 |
| <b>Destination</b> | 192.168.100.0/255.255.255.0 | 192.168.10.0/255.255.255.0  |
| <b>Service</b>     | Any                         | Any                         |
| <b>Group</b>       | Tunnel_Group_AB             | Tunnel_Group_BA             |
| <b>Fail-Over</b>   | NO-ACTION                   | NO-ACTION                   |

A packet matching the rule will be delivered to appropriate tunnel according the Tunnel Routing algorithm (or you can say a packet matching the rule will be GRE encapsulated and delivered to appropriate WAN port). The IPSec SAs established on the tunnels guarantee the privacy to transmission on the tunnels by encrypting the packets before they are transferred outward.

The pair of Local IP and Remote IP is the link to associated a GRE tunnel with an IPSec Transport mode SA, please make sure the configurations are equal on this. Note that please do not configure an Tunnel mode Phase 1 with the Local IP and Remote IP of a TR tunnel and configure the Phase 2 Quick Mode selector being equal to a TR routing rule, or Tunnel Routing goes to failure.

For the details of Tunnel Routing, see "[Tunnel Routing](#)".

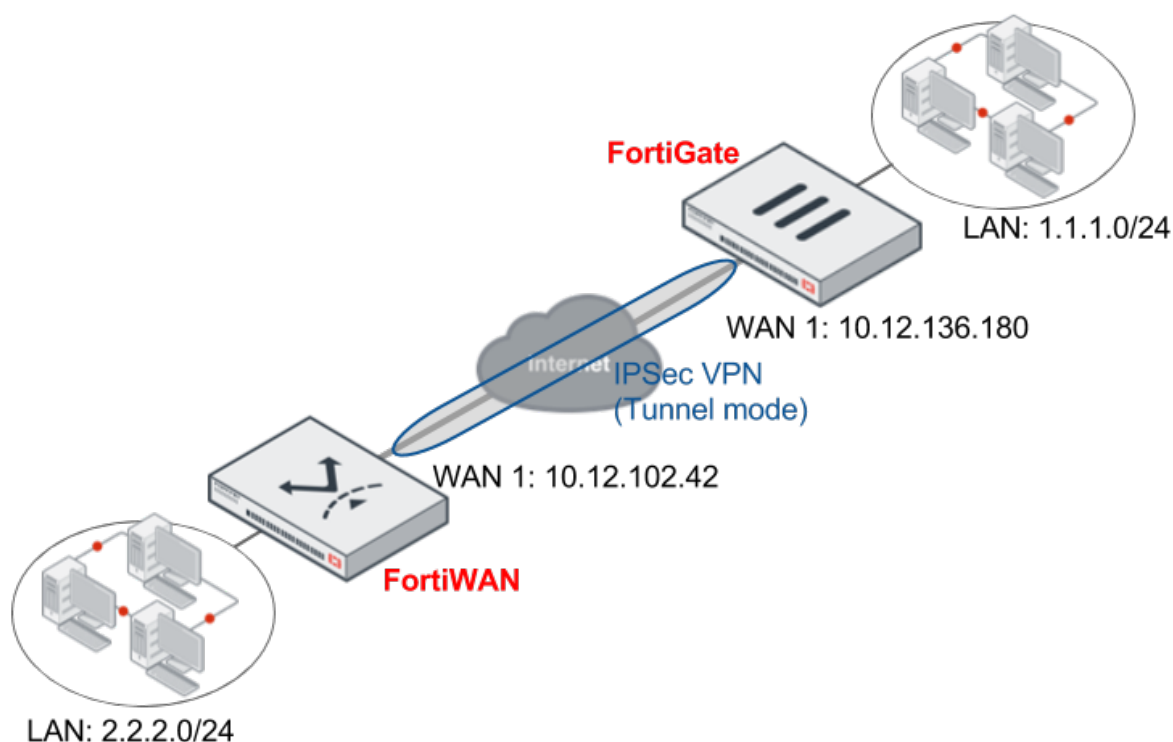
## Procedures to set up a Tunnel Routing over IPSec Transport mode

To set up a Tunnel Routing over IPSec Transport mode, we suggest the steps to follow as below:

1. Configure Network Settings on both units.
2. Define correspondent Auto Routing policies on both units.
3. Configure the settings of IPSec Transport mode Phase 1 and Phase 2 on both units.
4. Define Tunnel Routing policies and routing rules on both units.

## Establish IPSec VPN with FortiGate

FortiWAN supports the IPSec VPN established with a FortiGate unit. However, the deployment of IPSec VPN established between FortiWAN and FortiGate is limited by the Spec. of FortiWAN's IPSec (See "[About FortiWAN IPSec VPN](#)"). For example, IPSec Transport mode, IKE v2, authentication with certificates, IKE phase 1 aggressive mode, NAT traversal, dynamic IP address, and some algorithms are not supported for this deployment. An example for explaining how to set up a simple IPSec VPN (Tunnel mode) between a FortiWAN and a FortiGate is introduced below:



In this example, the common parameters for establishing IPSec SAs between the two units are as follows:

- Authentication Method: Pre-shared Key
- Phase 1 Mode: Main (ID protection)
- Dead Peer Detection: disable
- Phase 1 Encryption: DES
- Phase 1 Authentication: MD5
- Phase 1 DH Group: 5
- Phase 1 Keylife: 1200 Secs
- Phase 2 Encryption: DES
- Phase 2 Authentication: MD5
- Perfect Forward Secrecy (PFS): enable
- Phase 2 DH Group: 5
- Phase 2 Keylife: 120 Secs

## Configurations on FortiWAN

To set up the IPSec VPN, configurations of **Network Setting**, **Auto Routing**, **NAT** and **IPSec** are required on FortiWAN (See "[Define routing policies for an IPSec VPN](#)").

### Network Setting

#### WAN settings

Go to **System > Network Setting > WAN Setting**, and create a WAN link configuration:

|                             |               |
|-----------------------------|---------------|
| <b>WAN Link</b>             | 1             |
| <b>WAN Type</b>             | Routing Mode  |
| <b>WAN Port</b>             | Port1         |
| <b>IPv4 Localhost IP</b>    | 10.12.102.42  |
| <b>IPv4 Netmask</b>         | 255.255.255.0 |
| <b>IPv4 Default Gateway</b> | 10.12.102.254 |

For the details of WAN link setting, see "[Configurations for a WAN link in Routing Mode](#)", "[Configurations for a WAN link in Bridge Mode: One Static IP](#)" and "[Configurations for a WAN link in Bridge Mode: Multiple Static IP](#)".

### LAN private subnets

Go to **System > Network Setting > LAN Private Subnet**, and create a LAN subnet configuration:

|                           |               |
|---------------------------|---------------|
| <b>IP(s) on Localhost</b> | 2.2.2.254     |
| <b>Netmask</b>            | 255.255.255.0 |
| <b>LAN Port</b>           | Port3         |

For the details of LAN private subnet setting, see "[LAN Private Subnet](#)".

### Auto Routing

Go to **Service > Auto Routing**, and create a policy and two IPv4 filters for IKE negotiations and IPSec communication.

#### Policy

|                  |                                  |
|------------------|----------------------------------|
| <b>Label</b>     | IPSec_WAN1 (Any name you desire) |
| <b>T</b>         | Enable Threshold or not          |
| <b>Algorithm</b> | Fixed                            |
| <b>Parameter</b> | Only 1 is checked                |

#### IPv4 Filter

Two IPv4 filters: one for IKE negotiations, and another for general IPSec communication.

|             |          |          |
|-------------|----------|----------|
| <b>When</b> | All-Time | All-Time |
|-------------|----------|----------|

|                         |                 |                                   |
|-------------------------|-----------------|-----------------------------------|
| <b>Input Port</b>       | Any Port        | Any Port (or the LAN port, PortX) |
| <b>Source</b>           | Localhost       | 2.2.2.0/255.255.255.0             |
| <b>Destination</b>      | 10.12.136.180   | 1.1.1.0/255.255.255.0             |
| <b>Service</b>          | Any or IKE(500) | Any                               |
| <b>Routing Policy</b>   | IPSec_WAN1      | IPSec_WAN1                        |
| <b>Fail-Over Policy</b> | NO-ACTION       | NO-ACTION                         |

For the details of Auto Routing, see "[Auto Routing](#)".

## NAT

Go to **Service > NAT**, and create a NAT rule:

|                    |                       |
|--------------------|-----------------------|
| <b>When</b>        | All-Time              |
| <b>Source</b>      | 2.2.2.0/255.255.255.0 |
| <b>Destination</b> | 1.1.1.0/255.255.255.0 |
| <b>Service</b>     | Any                   |
| <b>Translated</b>  | No NAT                |

For the details of NAT, see "[NAT](#)".

## IPSec

Go to Service > IPSec, and create a Tunnel Mode:

### Phase 1

|                              |                       |
|------------------------------|-----------------------|
| <b>Name</b>                  | IPSec_FGT_P1          |
| <b>Local IP</b>              | 10.12.102.42          |
| <b>Remote IP</b>             | 10.12.136.180         |
| <b>Authentication Method</b> | Pre-shared Key: 12345 |
| <b>Internet Key Exchange</b> | v1                    |
| <b>Mode</b>                  | Main (ID protection)  |

|                            |           |
|----------------------------|-----------|
| <b>Dead Peer Detection</b> | Disable   |
| <b>Proposal</b>            |           |
| <b>Encryption</b>          | DES       |
| <b>Authentication</b>      | MD5       |
| <b>DH Group</b>            | 5         |
| <b>Keylife</b>             | 1200 Secs |

## Phase 2

|                       |                       |
|-----------------------|-----------------------|
| <b>Name</b>           | IPSec_FGT_P2          |
| <b>Proposal</b>       |                       |
| <b>Encryption</b>     | DES                   |
| <b>Authentication</b> | MD5                   |
| <b>PFS Group</b>      | 5                     |
| <b>Keylife</b>        | 120 Secs              |
| <b>Quick Mode</b>     |                       |
| <b>Source</b>         | 2.2.2.0/255.255.255.0 |
| <b>Port</b>           | Any                   |
| <b>Destination</b>    | 1.1.1.0/255.255.255.0 |
| <b>Port</b>           | Any                   |
| <b>Protocol</b>       | Any                   |

So far, it is complete to set up the IPSec VPN on the FortiWAN side, configurations on the FortiGate side are introduced next. For the details of IPSec parameters, see "[IPSec VPN in the Web UI](#)".

## Configurations on FortiGate

To set up the IPSec VPN, configurations of **Network**, **Router** and **VPN** are required on FortiGate. For further information of FortiGate configurations, see FortiOS Handbook on [Fortinet document site](#).

## Network

Go to **System > Network > Interface**. Configure the setting for WAN 1 with IP address 10.12.136.180 on a physical interface.

|                 |                             |
|-----------------|-----------------------------|
| Interface Name  | wan1                        |
| Type            | Physical Interface          |
| Addressing mode | Manual                      |
| IP/Network Mask | 10.12.136.180/255.255.255.0 |

## VPN

Go to **VPN > IPsec > Tunnels** and click **Create New**.

|      |                 |
|------|-----------------|
| Name | IPSec_to_FWN_P1 |
|------|-----------------|

Select "**Custom VPN Tunnel (No Template)**" and click **Next** to configure the settings as follows:

### Network

|                     |                   |
|---------------------|-------------------|
| IP Version          | IPv4              |
| Remote Gateway      | Static IP Address |
| IP Address          | 10.12.102.42      |
| Interface           | WAN1              |
| Mode Config         | Disable           |
| NAT Traversal       | Disable           |
| Dead Peer Detection | Disable           |

### Authentication

|                |                |
|----------------|----------------|
| Method         | Pre-shared key |
| Pre-shared key | 12345          |

### IKE

|         |                      |
|---------|----------------------|
| Version | V1                   |
| Mode    | Main (ID protection) |



**Phase 1 Proposal**

|                               |               |
|-------------------------------|---------------|
| <b>Encryption</b>             | DES           |
| <b>Authentication</b>         | MD5           |
| <b>Diffie-Hellman Group</b>   | 5             |
| <b>Key Lifetime (seconds)</b> | 1200          |
| <b>Local ID</b>               | Keep it blank |

**XAUTH**

|             |         |
|-------------|---------|
| <b>Type</b> | Disable |
|-------------|---------|

**Phase 2 Selectors**

|                       |                               |
|-----------------------|-------------------------------|
| <b>Name</b>           | IPSec_to_FWN_P2               |
| <b>Local Address</b>  | Subnet: 1.1.1.0/255.255.255.0 |
| <b>Remote Address</b> | Subnet: 2.2.2.0/255.255.255.0 |

**Phase 2 Proposal**

|                                             |           |
|---------------------------------------------|-----------|
| <b>Encryption</b>                           | DES       |
| <b>Authentication</b>                       | MD5       |
| <b>Enable Replay Detection</b>              | disable   |
| <b>Enable Perfect Forward Secrecy (PFS)</b> | enable    |
| <b>Diffie-Hellman Group</b>                 | 5         |
| <b>Local Port</b>                           | All check |
| <b>Remote Port</b>                          | All check |
| <b>Protocol All</b>                         | All check |
| <b>Autokey keep Alive</b>                   | disable   |
| <b>Auto-negotiate</b>                       | disable   |

|                     |         |
|---------------------|---------|
| <b>Key Lifetime</b> | Seconds |
| <b>Seconds</b>      | 120     |

## Router

Go to **Router > Static > Static Routes**, and click **Create New** to create two rules for WAN1 and the IPSec tunnel - IPSec\_to\_FWN\_P1:

|                            |                 |                       |
|----------------------------|-----------------|-----------------------|
| <b>Destination IP/Mask</b> | 0.0.0.0/0.0.0.0 | 2.2.2.0/255.255.255.0 |
| <b>Device</b>              | wan1            | IPSec_to_FWN_P1       |
| <b>Gateway</b>             | 10.12.136.254   | N/A                   |

## Optional Services

As an edge device, FortiWAN provides other functions except the major traffic load balancing and fault tolerance. These optional functions are helpful to manage the network in all the ways.

### Firewall

This section introduces how to set up the firewall. Unlimited number of rules can be added to the firewall rule list. The rules are prioritized from top to bottom that is rules at the top of the table will be given higher precedence over lower ranked ones. [IPv4 Rules] and [IPv6 Rules] are for configurations of IPv4 and IPv6 respectively.

FortiWAN provides mechanisms to record, notify and analysis on events refer to the Firewall service, see "[Log](#)" and "[Reports: Firewall](#)".

|                    |                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>E</b>           | Check the box to enable the rule                                                                                                                                                                                                                                                                                                    |
| <b>When</b>        | Three options available: Busy hour, Idle hour and All-Time (See " <a href="#">Busyhour Settings</a> ").                                                                                                                                                                                                                             |
| <b>Source</b>      | Packets sent from specified source will be matched (See " <a href="#">Using the web UI</a> ").                                                                                                                                                                                                                                      |
| <b>Destination</b> | Packets sent to a specific destination will be matched. This field is the same as the "Source" field, except that packets are matched with specified destination (See " <a href="#">Using the web UI</a> ").                                                                                                                        |
| <b>Service</b>     | The TCP/UDP service type to be matched. Select the matching criteria from publicly known service types (e.g. FTP), or enter the port number in TCP/UDP packets and specify the range. Type the starting port number plus hyphen "-" and then the ending port number. e.g. "TCP@123-234" (See " <a href="#">Using the web UI</a> "). |
| <b>Action</b>      | Choose the actions when the rule is matched: Accept: The firewall will let the matched packets pass. Deny: The firewall will drop the matched packets.                                                                                                                                                                              |
| <b>L</b>           | Check to enable logging. Whenever the rule is matched, the system will record the event to the log file.                                                                                                                                                                                                                            |

#### Default rules

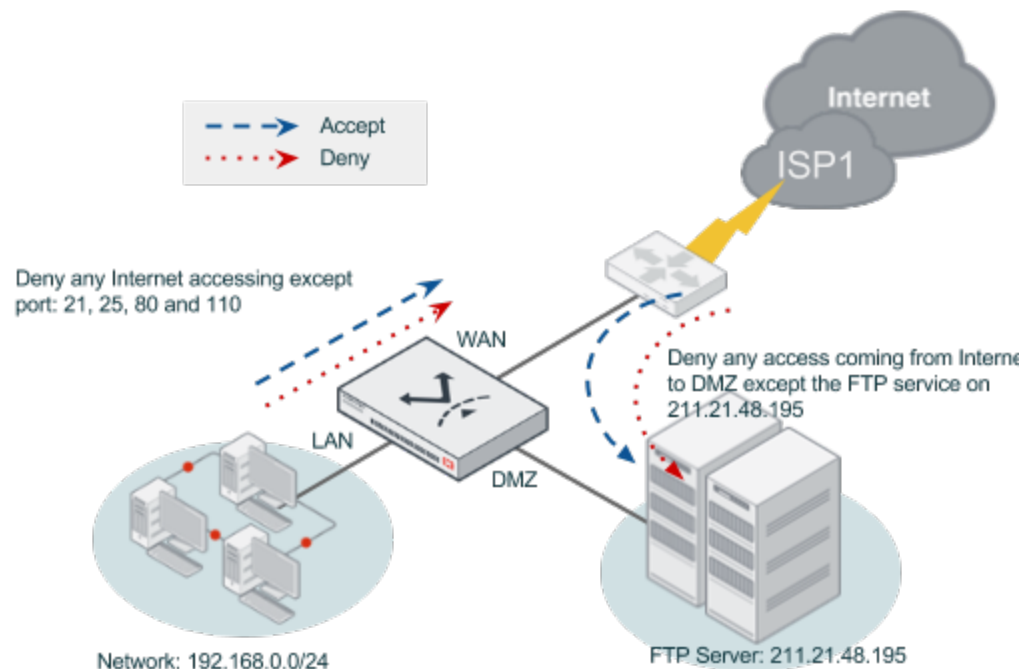
By default, FortiWAN's firewall enables the following IPv4/IPv6 rules to deny some accesses coming from the Internet, which might cause general security issues:

1. When=All-Time & Source=WAN & Destination=Localhost & Service=HTTP(80) & Action=Deny
2. When=All-Time & Source=WAN & Destination=Localhost & Service=HTTPS(443) & Action=Deny
3. When=All-Time & Source=WAN & Destination=Localhost & Service=SSH(22) & Action=Deny
4. When=All-Time & Source=WAN & Destination=Localhost & Service=SNMP(61) & Action=Deny

5. When=All-Time & Source=WAN & Destination=Localhost & Service=RIP(520) & Action=Deny
6. When=All-Time & Source=WAN & Destination=Any Address & Service=TCP@139 & Action=Deny
7. When=All-Time & Source=WAN & Destination=Any Address & Service=TCP@445 & Action=Deny
8. When=All-Time & Source=WAN & Destination=Localhost & Service=TCP@5432 & Action=Deny
9. When=All-Time & Source=Any Address & Destination=Any Address & Service=Any & Action=Accept

The ninth rule is fixed to be the last rule at the bottom for evaluation. Packets that do not match any other rule will match this rule and be accepted. This rule is unmodifiable. The second rule denies any HTTPS access to FortiWAN's localhost from the Internet, which means it is unable to access to the Web UI through any WAN port. You can disable this rule or change Action to Accept to allow Web UI accessing through WAN ports if no security issues are concerned. The sixth, seventh and eighth rules deny any access (coming from the Internet) of NetBIOS, Microsoft-DS Active Directory, Windows shares and Microsoft-DS SMB file sharing, and the Postgre SQL database system that FortiWAN uses for Reports.

### Example 1



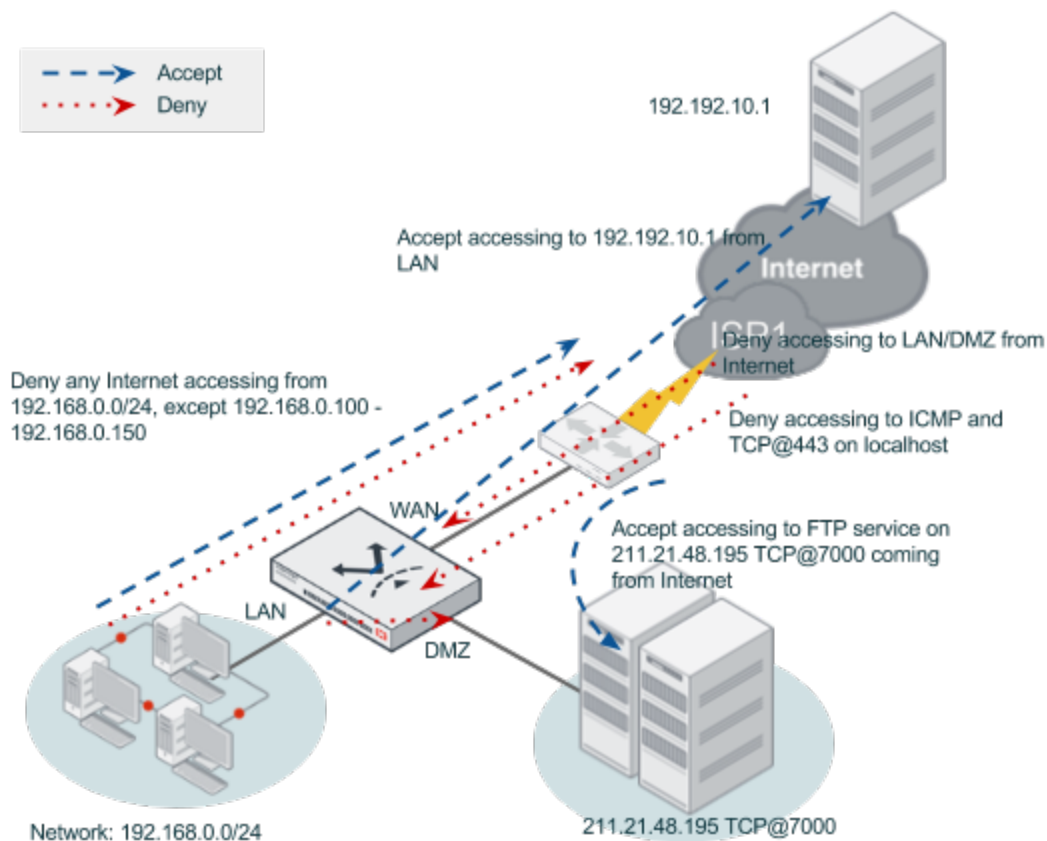
#### Rules for Filtering Packets

- The users from the internet (WAN) can only access FTP Server 211.21.48.195 through port 21.
- The users from LAN can access all servers and hosts on the internet (WAN) through port 25 (SMTP), port 80 (HTTP), port 21 (FTP), and port 110 (POP3).
- All other packets are blocked.

The rules table for the example will look like this:

| Source | Destination   | Service    | Action |
|--------|---------------|------------|--------|
| WAN    | 211.21.48.195 | FTP (21)   | Accept |
| WAN    | DMZ           | Any        | Deny   |
| LAN    | WAN           | HTTP (80)  | Accept |
| LAN    | WAN           | SMTP (25)  | Accept |
| LAN    | WAN           | FTP (21)   | Accept |
| LAN    | WAN           | POP3 (110) | Accept |
| LAN    | WAN           | Any        | Deny   |

### Example 2



### Rules for Filtering Packets

- The users from the internet (WAN) can access server 211.21.48.195 inside DMZ through TCP port 7000.
- The hosts 192.168.0.100 – 192.168.0.150 in the LAN can access the Internet (WAN) but the others cannot.

- Users from the Internet (WAN) cannot connect to the port 443 on FortiWAN (i.e. Web Administration on FortiWAN).  
Note: "Localhost" represents the address of FortiWAN host machine.
- Users from LAN can access FTP server 192.192.10.1 through port 21.
- Users from the internet cannot ping FortiWAN . Note: To intercept ping messages, users can deny "ICMP" protocol in service type because ping is a type of "ICMP".
- Users from the LAN cannot access DMZ.
- Users from the internet (WAN) cannot access LAN and DMZ.

The rules table for the example will look like this:

| Source                          | Destination   | Service  | Action |
|---------------------------------|---------------|----------|--------|
| WAN                             | 211.21.48.195 | TCP@7000 | Accept |
| 192.168.0.100-<br>192.168.0.150 | WAN           | Any      | Accept |
| WAN                             | Localhost     | TCP@443  | Deny   |
| LAN                             | 192.192.10.1  | FTP (21) | Accept |
| WAN                             | Localhost     | ICMP     | Deny   |
| LAN                             | DMZ           | Any      | Deny   |
| WAN                             | DMZ           | Any      | Deny   |
| WAN                             | LAN           | Any      | Deny   |

#### See also

- [Busyhour Settings](#)
- [Using the web UI](#)
- [Reports: Firewall](#)

## NAT

FortiWAN is an edge server that is usually placed on the boundary between WAN and LAN. When a connection is established from a private IP address (in LAN or DMZ) to the internet (WAN), it is necessary to translate the private IP address into one of the public IP addresses assigned to the FortiWAN's WAN link. This process is called NAT (Network Address Translation). FortiWAN provides the typical NAT (called S-NAT also) for sessions established from internal area. Once the private source IP address of outgoing packet of a session is translated to a public IP address, the mapping is kept in translation table and therefore the inbound traffic (from public area) of the session can be accepted and forwarded to the internal host who established the session.

With the typical NAT, two-way data transmission between an internal host and an external host is achieved, only if the internal host starts the sessions. An external host is unable to starts a session with an internal host via the

typical NAT. FortiWAN's 1-to-1 NAT gives the availability of two-way transmission between an internal host and an external host not only for sessions starting from the internal host but also for sessions starting from the external host.

FortiWAN provides log mechanism to the NAT service, see "[Log](#)".

## Default Rules

FortiWAN's NAT Default Rules are the NAT rules (and IPv6 NAT rules) generated automatically by system according to the Network Setting of WAN links. Once a WAN link is set up (See "[Configuring your WAN](#)"), the default rules are generated at the same time so that FortiWAN performs NAT automatically to packets coming from anywhere (except subnets in WAN or/and DMZ and static routing subnets of the WAN link) and going to be transferred via the WAN link. NAT default rules are varied according to how the WAN link is deployed. For example,

**WAN link 1:** Routing mode with a basic subnet (125.227.251.0/255.255.255.0) in WAN and DMZ, and the IP(s) on localhost are 128.227.251.80 and 128.227.251.81. System adds the default rules to WAN link 1 as following:

```
When = All-Time, Source = 125.227.251.0/255.255.255.0, Destination = Any Address, Service = Any, Translated = No NAT
```

```
When = All-Time, Source = Any Address, Destination = Any Address, Service = Any, Translated = 128.227.251.80
```

**WAN link 2:** Bridge mode: One Static IP, the IP on localhost is 125.227.250.10. System adds the default rules to WAN link 2 as following:

```
When = All-Time, Source = 125.227.250.10, Destination = Any Address, Service = Any, Translated = No NAT
```

```
When = All-Time, Source = Any Address, Destination = Any Address, Service = Any, Translated = 128.227.250.10
```

**WAN link 3:** Bridge mode: Multiple Static IP, 125.227.252.100-125.227.252.101 are deployed on localhost, 125.227.252.102-125.227.252.103 are deployed in WAN, 125.227.252.104-125.227.252.105 are deployed in DMZ. System adds the default rules to WAN link 3 as following:

```
When = All-Time, Source = 125.227.252.100-125.227.252.101, Destination = Any Address, Service = Any, Translated = No NAT
```

```
When = All-Time, Source = 125.227.252.104-125.227.252.105, Destination = Any Address, Service = Any, Translated = No NAT
```

```
When = All-Time, Source = Any Address, Destination = Any Address, Service = Any, Translated = 128.227.252.100
```

**WAN link 4:** Bridge mode: PPPoE, system adds the default rule to WAN link 4 as following:

```
When = All-Time, Source = Any Address, Destination = Any Address, Service = Any, Translated = DynamicIP(DHCP/PPPoE)
```

The last rule translates source IP address of all packets into an IP address (localhost) of the WAN link. The second (or third) rule from the bottom ignores NAT to packets coming from subnets of the WAN link. Those default rules are added as the bottom rules to the top-down rule table. They are unable to be deleted and edited, unless the correspondent deployment of the WAN link changes. The default rules will translate source IP address of a matched packet into the first of the IP addresses that are assigned to localhost of the WAN link, which normally is a public IPv4 address or global IPv6 address. Therefore, packets with private source address (IPv4) or Link-Local source address (IPv6) are acceptable to Internet after the NAT process. However, even a packet comes with public source address (IPv4) or Global source address (IPv6), NAT is also performed if it matches the last rule. NAT default rules are based on deployment of a WAN link, deployment of LAN is regardless. Set NAT rules manually for advanced applications.

Similarly, system generates default rules for IPv6/IPv4 dual stack WAN links. Take the WAN link 1 above as example, if a IPv6 basic subnet 2001::/64 is deployed on WAN link 1 and the localhost is 2001::1, system adds the IPv6 default rules to WAN link 1 as following:

```
When = All-Time, Source = 2001::/64, Destination = Any Address, Service = Any,
Translated = No NAT
```

```
When = All-Time, Source = Any Address, Destination = Any Address, Service =
Any, Translated = 2001::1
```

**Note that for FortiWAN V4.0.x, system does not generate IPv6 default rules for IPv6/IPv4 dual stack WAN link. It is necessary to add IPv6 default rules manually, or the IPv6 transmission might fail if its source IP address is a Link-Local address. Please refer to the examples above for this.**

## Non-NAT

Non-NAT is used for Private Network and MPLS Network where the host in WAN can directly access the host in DMZ, and where FortiWAN is used to balance VPN load and backup lines.

FortiWAN's inbound and outbound load balancing (Auto Routing and Multihoming) distribute session over multiple WAN links. It's necessary to make sure the correct NAT rules are applied to every enabled WAN link.

- Enable NAT** : Enable the function, and NAT will translate any private IP to a fixed public IP assigned to a given WAN link. Disable the function; FortiWAN will act as a general router for the host in WAN to directly access the host in DMZ.
- WAN** : Enabled WAN links are listed in the menu. Select the WAN link to set and apply NAT rules to.

## NAT Rules

As the previous description, FortiWAN provides typical NAT for out-going session (established from internal host to external host). Here we describe the NAT rules which specified how to translate source IP address of a out-going packet into specified IP address of the WAN link. Incoming packets from a external host can be accepted and forwarded to the correct internal host only if a out-going packet has already be translated and transferred to the same external host. NAT rules are separated into IPv4 NAT rules and IPv6 NAT rules, which are used to translate a IPv4 address to another IPv4 address and translate a IPv6 address to another IPv6 address respectively. You will see the default rules at the bottom of the two rule tables, if IPv4 and/or IPv6 addresses are deployed on localhost of the WAN link.



## IPv4 NAT Rules

Customized rules for IPv4-to-IPv4 NAT on a specified WAN link (select from the drop-down menu WAN above).

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>E</b>           | Enable the NAT rule or not.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>When</b>        | The predefined time periods during which the rules will apply. Options are Busy, Idle, All-Times (See " <a href="#">Busyhour Settings</a> ").                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Source</b>      | The packets sent from the source will be matched. Note: The source IPv4 to be translated must be the IPv4 address assigned to the LAN or DMZ (See " <a href="#">Using the web UI</a> ").                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Destination</b> | The packets sent to the destination will be matched (See " <a href="#">Using the web UI</a> ").                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Service</b>     | The packets with the service port number to which users would like NAT to apply. It can be the TCP/UDP port, or Predefined service groups from [System]->[Service Grouping] (See " <a href="#">Using the web UI</a> ").                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Translated</b>  | <p>Specify manually the IPv4 address or a range of IPv4 addresses that is assigned to the localhost of the specified WAN link. Source IP address of the packets that match the rule would be translated to the IP address specified here.</p> <p>The first IPv4 address assigned to the localhost of the WAN link automatically displays in the drop-down menu for options. If multiple IPv4 addresses are assigned to the WAN link's localhost, you can set any of them manually by selecting the options "IPv4 Address" and "IPv4 Range".</p> <p>Select No NAT if no translation is needed.</p> <p>The option [Dynamic IP] will be available while a Dynamic WAN link (Bridge Mode: PPPoE and Bridge Mode: DHCP) is applied.</p> |
| <b>L</b>           | Check to enable logging. Whenever the rule is matched, the system will record the event to the log file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## IPv6 NAT Rules

Customized rules for IPv6-to-IPv6 NAT on a specified WAN link (select from the drop-down menu WAN above).

|                    |                                                                                                                                                                                          |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>E</b>           | Enable the NAT rule or not.                                                                                                                                                              |
| <b>When</b>        | The predefined time periods during which the rules will apply. Options are Busy, Idle, All-Times (See " <a href="#">Busyhour Settings</a> ").                                            |
| <b>Source</b>      | The packets sent from the source will be matched (See " <a href="#">Using the web UI</a> "). Note: The source IPv6 to be translated must be the IPv6 address assigned to the LAN or DMZ. |
| <b>Destination</b> | The packets sent to the destination will be matched (See " <a href="#">Using the web UI</a> ").                                                                                          |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Service</b>    | The packets with the service port number to which users would like NAT to apply. It can be the TCP/UDP port, or Predefined service groups from [System]->[Service Grouping] (See <a href="#">"Using the web UI"</a> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Translated</b> | <p>Specify manually the IPv6 address or a range of IPv6 addresses that is assigned to the localhost of the specified WAN link. Source IP address of the packets that match the rule would be translated to the IP address specified here.</p> <p>The first IPv6 address assigned to the localhost of the WAN link automatically displays in the drop-down menu for options. If multiple IPv6 addresses are assigned to the WAN link's localhost, you can set any of them manually by selecting the options "IPv6 Address" and "IPv6 Range".</p> <p>Select No NAT if no translation is needed.</p> <p>The option [Dynamic IP] will be available while a Dynamic WAN link (Bridge Mode: PPPoE) is applied. Bridge Mode: DHCP does not support IPv6/IPv4 dual stack.</p> <p>Note that this field must be an IPv6 address obtained upon public DMZ subnet and with 64-bit or lower prefix length.</p> |
| <b>L</b>          | Check to enable logging. Whenever the rule is matched, the system will record the event to the log file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

### 1-to-1 NAT Rules

1-to-1 NAT maintains a fixed 1-to-1 mapping (binding) between internal IP addresses and the IP addresses of a WAN link's localhost (also called external addresses here), which requires the same amount of IP addresses on both sides. Therefore, both a internal host and external host can launch sessions to each other. 1-to-1 NAT supports translation for IPv4 only.

|                         |                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>E</b>                | Enable the 1-to-1 NAT rule or not.                                                                                                                                                                                                                                                                                                                                 |
| <b>When</b>             | Select the time when to apply the 1-to-1 NAT rule, including three options: Busy, Idle and All-Time (See <a href="#">"Busyhour Settings"</a> ).                                                                                                                                                                                                                    |
| <b>Internal Address</b> | Select the internal IPv4 address, IPv4 range or IPv4 subnet that the 1-to-1 NAT rule should be applied to (See <a href="#">"Using the web UI"</a> ). For a 1-to-1 NAT rule, the amount of internal IP address here must be the same as amount of external IP address below. (Note: Internal IP Address must be an IP address of the internal network or DMZ port.) |
| <b>Service</b>          | Select a service port where the 1-to-1 NAT rule should be applied to, such as TCP, UDP, ICMP or any of the predefined network service groups (See <a href="#">"Using the web UI"</a> ).                                                                                                                                                                            |
| <b>External Address</b> | Select the external IPv4 address, IPv4 range or IPv4 subnet that the 1-to-1 NAT rule should be applied to (See <a href="#">"Using the web UI"</a> ). For a 1-to-1 NAT rule, the amount of external IP address here must be the same as amount of internal IP address above. (Note: External IP Address must be an IP address obtained upon WAN link connection.)   |
| <b>L</b>                | Check to enable logging. Whenever the rule is matched, the system will record the event to the log file.                                                                                                                                                                                                                                                           |

For any out-going packet (no matter a internal or a external host launch the session), if the packet matches a 1-to-1 NAT rule on When, Internal Address (Source) and Service, source IP address of the packet will be translate to correspondent external address specified in the rule. For any in-coming packet (no matter a internal or a external host launch the session), if the packet matches a 1-to-1 NAT rule on When, External Address (Destination) and Service, destination IP address of the packet will be translate to correspondent internal address specified in the rule.

### Enable NAT

Example: To translate packets from local machine 192.168.123.100 to public IP address 172.31.5.51, check “Enable NAT”, and select WAN #1, then check “Enable”. The NAT rule settings look like:

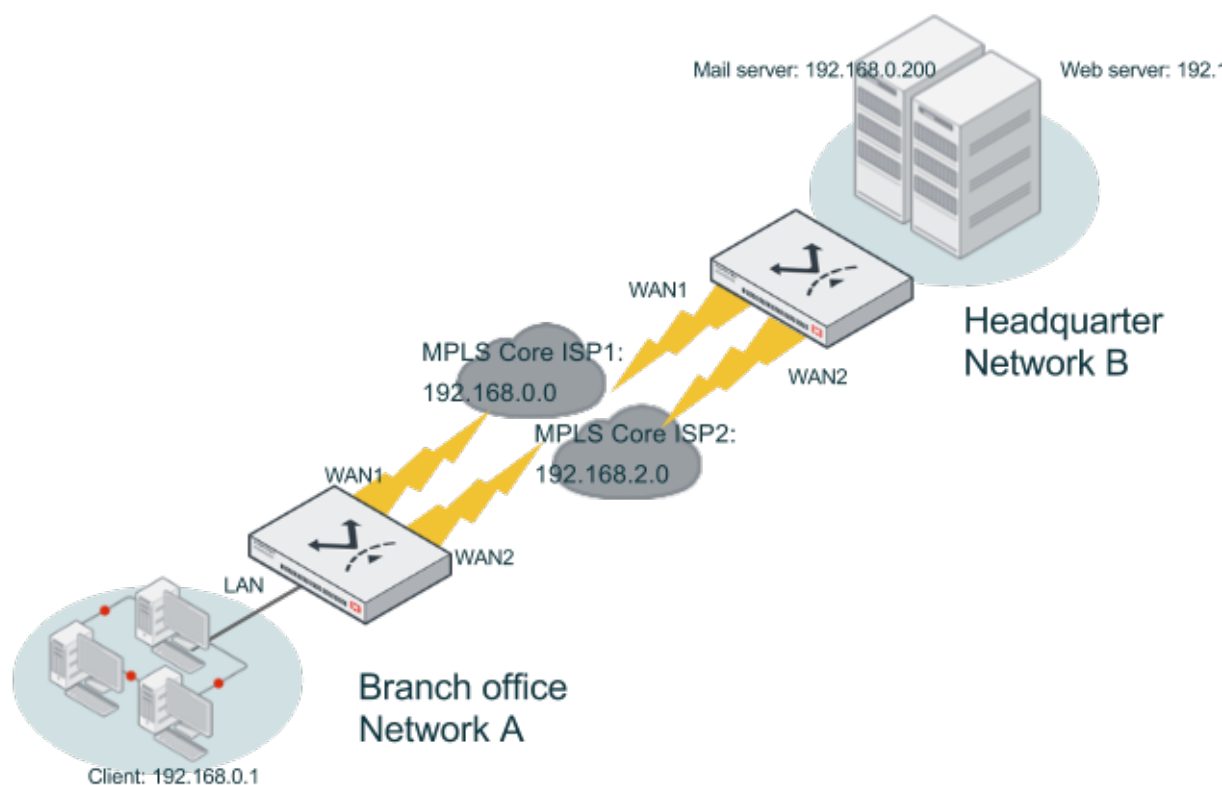
| Source          | Destination | Service | Translated  |
|-----------------|-------------|---------|-------------|
| 192.168.123.100 | Any Address | Any     | 172.31.5.51 |

### Disable NAT

Disable NAT sets FortiWAN to Non-NAT mode whereby all the WAN hosts can access DMZ hosts directly with proper routing setup. In this mode, FortiWAN acts as a router connecting multiple subnets.

Note: Once NAT is disabled, it is disabled on all the WAN Links.

Example: Non-NAT Settings



Non-NAT is commonly used on Private Network and MPLS network, which makes possible for the hosts of the branch office to directly access the headquarters. In case that ISP 1 is down, FortiWAN will automatically route the link to ISP 2, and, accordingly, serve as VPN load balancer based on the status of each link.

## Persistent Routing

Persistent routing is used to secure subsequent connections of source and destination pairs that are first determined by Auto-Routing in FortiWAN. It is useful for applications require secure connection between the server and client whereby client connection will be dropped if server detects different source IP addresses for the same client during an authenticated and certified session. PR ensures that the source IP address remains unchanged in the same session.

**Timeout:** For every session (pair of source and destination), if there is no packets occurred during the timeout period, records of persistent route of the session will be cleared. That means the next coming connection of the session will be routed by the auto-routing rules first.

FortiWAN provides mechanisms to record, notify and analysis on events refer to the Persistent Routing service, see "[Log](#)" and "[Statistics: Persistent Routing](#)".

### IPv4/IPv6 Web Service Rules

Sets persistent routing rules on Web services. Enable this function, and all the http and https connections established from source IP specified below to destination port 80 and port 443 are governed by Web Service Rules.

- E** : Check the box to enable the rule.
- When** : Options: Busy hour, Idle hour, and All-Time (See "[Busyhour Settings](#)").
- Source** : Established connections from the specified source will be matched (See "[Using the web UI](#)").
- Action** :
  - Do PR: the matched connections will be routed persistently.
  - No PR: the matched connections will NOT be routed persistently. (The Default)
- L** : Check to enable logging: Whenever the rule is matched, system will record the event to log file.

### IPv4/IPv6 IP Pair Rules

Sets persistent routing rules on IPv4/IPv6 addresses. Enable this function, and all connections established from the source IPv4/IPv6 to destination IPv4/IPv6 specified below are governed by IPv4/IPv6 IP Pair Rules.

- E** : Check the box to enable the rule.
- When** : Options: Busy hour, Idle hour, and All-Time (See "[Busyhour Settings](#)").
- Source** : Established connections from the specified source will be matched (See "[Using the web UI](#)").

**Destination** : The connections to the specified destination will be matched. This field is the same as the "Source" field, except it matches packets with the specified destination (See ["Using the web UI"](#)).

**Action** : Do PR: the matched connections will be routed persistently. (The Default)  
No PR: the matched connections will NOT be routed persistently.

**L** : Check to enable logging: Whenever the rule is matched, system will record the event to log file.

Persistent routing is often used when destination servers check source IP. The function is performed on most secure connections (e.g. HTTPS and SSH). To prevent the connections from being dispatched over a diverse range of WAN links, persistent routing serves the best solution for maintaining connections over a fixed WAN link.

See below for how auto-routing is related to persistent-routing:

Once a connection is established, auto-routing rules are applied to determine the WAN link to be used.

Subsequent connections with the same destination and source pair obey the rules formulated in the persistent routing table. Note that the device will consult the rule table whenever established connections are to be sent to new destinations.

Auto-routing will be reactivated once in persistent routing the interval between two successive connections are longer than timeout period. A second connection will be considered as a "new" one. Then auto-routing will secure the connection to go through a different WAN link.

### Example 1

The persistent routing policies to be established accordingly:

- In LAN, established connections from IP address 192.168.0.100 to 192.168.10.100 are NOT to be routed persistently.
- Established connections from DMZ to LAN are NOT to be routed persistently.
- Established connections from LAN to the host IP ranging from 10.10.1.1 ~ 10.10.1.10 are NOT to be routed persistently.
- Since the default action by IP Pair rules is Do PR, if no rule is added, all connections will use persistent routing.

Then persistent routing table will look like:

| Source        | Destination          | Action |
|---------------|----------------------|--------|
| 192.168.0.100 | 192.192.10.100       | No PR  |
| DMZ           | WAN                  | No PR  |
| LAN           | 10.10.1.1-10.10.1.10 | No PR  |

### Example 2

The persistent routing policies to be established accordingly:

HTTP and HTTPs connections from the subnet 192.168.0.0/24 in LAN use persistent routing.

HTTP and HTTPs connections from WAN use persistent routing.

As there is no default action set by Web Service Rules, if no rule is added, all connections will be based on IP Pair Rules to determine whether to use persistent routing.

The persistent routing table should look like:

| Source                    | Action |
|---------------------------|--------|
| 192.168.0.0/255.255.255.0 | Do PR  |
| WAN                       | Do PR  |

### Example 3

The persistent routing policies to be established accordingly:

HTTP and HTTPs connections from LAN hosts with IP range 192.168.0.10~192.168.0.20 use persistent routing, but this does not apply to other services except IP address 192.168.0.15.

HTTP and HTTPs connections from subnet 192.168.10.0/24 to 192.192.10.100 use persistent routing. But this does not apply to other connections.

Connections from IP address 211.21.48.196 in DMZ to the WAN subnet 10.10.1.0/24 in WAN do NOT use persistent routing.

Since the default action by IP Pair Rules is Do PR, if no rule is added, all connections will use persistent routing.

Then persistent routing table will look like:

| Source                     | Action |
|----------------------------|--------|
| 192.168.0.10-192.168.0.20  | Do PR  |
| 192.168.10.0/255.255.255.0 | Do PR  |

| Source                     | Destination             | Action |
|----------------------------|-------------------------|--------|
| 192.168.0.15               | WAN                     | Do PR  |
| 192.168.0.10-192.168.0.20  | WAN                     | No PR  |
| 192.168.10.0/255.255.255.0 | ANY                     | No PR  |
| 211.21.48.196              | 10.10.1.0/255.255.255.0 | No PR  |

Note: Rules are matched top down. Once one rule is matched, the rest will be ignored. In this case, the connections from 192.168.0.15 may meet the criteria of the first and second IP Pair rules, only the first rule will be applied. Hence the rules will not perform NoPR on 192.168.0.15 even though it matches the second rule. It shall be noted that Web Service Rules are prioritized over IP Pair Rules. As 192.168.10.0/255.255.255.0 is configured to be NoPR in IP Pair Rules, but DoPR in Web Service Rules, HTTP connections will still apply persistent routing.

## Bandwidth Management

Bandwidth Management (BM) allocates bandwidth to applications. To secure the bandwidth of critical applications, FortiWAN Bandwidth Management (BM) defines inbound and outbound bandwidth based on traffic direction, i.e. take FortiWAN as the center, traffic flows from WAN to LAN is inbound traffic, otherwise, it is outbound traffic. No matter which direction a connection is established in, a connection must contain inbound traffic and outbound traffic. The section will mainly explain how to guarantee bandwidth based on priority settings, and how to manage inbound and outbound traffic by configuring busy/idle hours, data source/destination, and service type, etc.

Bandwidth Management consists of Classes and Filters (IPv4/IPv6). Click "Expand Link Settings" or "Collapse Link Settings" to show or hide configuration details of links and bandwidth limit.

FortiWAN provides mechanisms to record, notify and analysis on events refer to the Bandwidth Management service, see "[Log](#)", "[Statistics: Bandwidth](#)" and "[Report: Bandwidth Usage](#)".

### Inbound BM and Outbound BM

Bandwidth Management is divided into inbound BM and outbound BM, which are used to control the inbound traffic and outbound traffic respectively on each WAN port. Packets (network streams) that are transferred inward (from WAN to LAN, DMZ or localhost) on a WAN port are counted to inbound traffic; packets that are transferred outward (from LAN, DMZ or localhost to WAN) on a WAN port are counted to outbound traffic. Therefore, both inbound BM and outbound BM are required if you would like to control a connection in the two ways (Bandwidth Management ignores the direction of a connection, the initiator of the connection). BM policy consists of BM classes and filters. A BM class defines the bandwidth to allocate applications on each WAN port, while a BM filter defines the associated application by source, destination and service of the packets. According to the associated inbound/outbound classes, bandwidth is allocated to the inbound/outbound traffic that is defined in an inbound/outbound filter.

### Inbound & Outbound Classes

An inbound/outbound class defines how to allocate bandwidth to the specified traffic. Specified traffic associated with the class can be controlled according to the WAN link it passes through and the time it is generated, and bandwidth is allocated according to settings of Guarantee, Max and Priority.

|                  |                                                                                                                                                                                                                                         |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable BM</b> | Tick the check box to enable Bandwidth Management.                                                                                                                                                                                      |
| <b>Name</b>      | Assign a name to bandwidth class. Better use simple names to avoid confusion, e.g. "HTTP" to manage the bandwidth of HTTP service.                                                                                                      |
| <b>Link</b>      | The WAN link number which bandwidth limitation will be applied to. Traffic of specified applications (defined in inbound and outbound filters) passing through the WAN link will be shaped according to the bandwidth limitation below. |

**Busy Hour Settings**

This is the bandwidth allocation on a WAN link during defined busy hour (see System > Busyhour Settings for more details, "[Busyhour Settings](#)"). Associated traffic passing through the WAN link during the time period will be shaped according to the following settings.

**Guaranteed Kbps** The guaranteed bandwidth for this class. This secures bandwidth allocated as defined for WAN link in peak hours. This is significant to guarantee the service quality especially for critical applications like VoIP.

**Max Kbps** The maximum bandwidth for WAN link. Maximum bandwidth is often allocated to services like WWW and SMTP that consume large bandwidth. Note that traffic of the WAN link would be blocked if value of the field is zero.

**Priority** Sessions matching the BM class and being distributed to the WAN link will get the amount of guaranteed traffic (set in the Guaranteed Kbps field) no matter how. Priority is responsible for distribution of remaining bandwidth to the sessions so that they can probably reach the maximum bandwidth (set in the Max Kbps field). Queue with higher priority will reach the maximum bandwidth before the queue with lower priority. FortiWAN provides eight levels that 7 is the lowest priority and 0 is the highest.

**Idle Hour Settings**

This is the bandwidth allocation on a WAN link during defined idle hour (see System > Busyhour Settings for more details, "[Busyhour Settings](#)"). Associated traffic passing through the WAN link during the time period will be shaped according to the following settings.

**Guaranteed Kbps** The guaranteed bandwidth for this class. This secures bandwidth allocated as defined for WAN link in peak hours. This is significant to guarantee the service quality especially for critical applications like VoIP.

**Max Kbps** The maximum bandwidth for WAN link. Maximum bandwidth is often allocated to services like WWW and SMTP that consume large bandwidth. Note that traffic of the WAN link would be blocked if value of the field is zero.

**Priority** Sessions matching the BM class and being distributed to the WAN link will get the amount of guaranteed traffic (set in the Guaranteed Kbps field) no matter how. Priority is responsible for distribution of remaining bandwidth to the sessions so that they can probably reach the maximum bandwidth (set in the Max Kbps field). Queue with higher priority will reach the maximum bandwidth before the queue with lower priority. FortiWAN provides eight levels that 7 is the lowest priority and 0 is the highest.



## Inbound & Outbound IPv4/IPv6 Filter

A filter is used to evaluate the traffic passing through FortiWAN by its source, destination and service. Traffic matches the filter will be associated to the corresponding BM class, so that the traffic is shaped according to the bandwidth allocation of the class. The source and destination here mean the actual initiator and terminator of the inbound/outbound traffic, no matter whether the traffic is processed by NAT or Virtual Server.

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>E</b>           | Check the box to enable the rule.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Input Port</b>  | Select a interface that packets are received on for this filter term to evaluate the outbound traffic, or leave it as Any Port. See <a href="#">Using the web UI</a> for details. This field is only available for Outbound IPv4/IPv6 filters.                                                                                                                                                                                                         |
| <b>Source</b>      | The source used to evaluate traffic (original packets) by where it comes from (See <a href="#">"Using the web UI"</a> ).                                                                                                                                                                                                                                                                                                                               |
| <b>Destination</b> | The destination used to evaluate traffic (original packets) by where it goes to (See <a href="#">"Using the web UI"</a> ).                                                                                                                                                                                                                                                                                                                             |
| <b>Service</b>     | <p>The service used to evaluate traffic (original packets) by what the source port and destination port they are. Service matches as long as source port or destination port matches (See <a href="#">"Using the web UI"</a>).</p> <p>The options GRE and ESP in the Service drop-down menu is for the GRE and ESP packets coming from other VPN devices. GRE and ESP packets generated by FortiWAN are invisible to Bandwidth Management filters.</p> |
| <b>Classes</b>     | The BM class that traffic matching the filter (Source, Destination and Service) is associated with.                                                                                                                                                                                                                                                                                                                                                    |
| <b>L</b>           | Check to enable logging: Whenever the rule is matched, system will record the event to log file.                                                                                                                                                                                                                                                                                                                                                       |



While system is applying the bandwidth management settings, traffic passing through FortiWAN will be blocked for a while.

## Managing Bandwidth for Tunnel Routing and IPsec

Bandwidth Management is capable to control the original traffic that is encapsulated by Tunnel Routing or IPsec VPN. Traffic that is going to be transferred outward through Tunnel Routing or IPsec VPN will be processed by Bandwidth Management before encapsulating, and traffic that is transferred inward through Tunnel Routing or IPsec VPN is controlled by Bandwidth Management after decapsulating. In other words, FortiWAN's Tunnel Routing and IPsec are transparent to Bandwidth Management (and the corresponding BM log and statistics). Bandwidth Management can only recognize the original applications (by matching a filter on the Service) that is going to be encapsulated or has been decapsulated by Tunnel Routing or IPsec. The GRE and ESP packets generated by FortiWAN are invisible to Bandwidth Management.

To control Tunnel Routing or IPSec transmission by Bandwidth Management, please make sure a Bandwidth Management filter is defined correctly (on the source, destination and service) to match its original packets. If you would like to control the overall Tunnel Routing or IPSec transmission no matter what the original services it is, try to classify the traffic by its Source and Destination; the Source and Destination of the Routing Rules of Tunnel Routing, or the Source and Destination of the Quick Mode selectors of IPSec Tunnel mode (See "[How to set up routing rules for Tunnel Routing](#)" and "[IPSec VPN in the Web UI](#)").

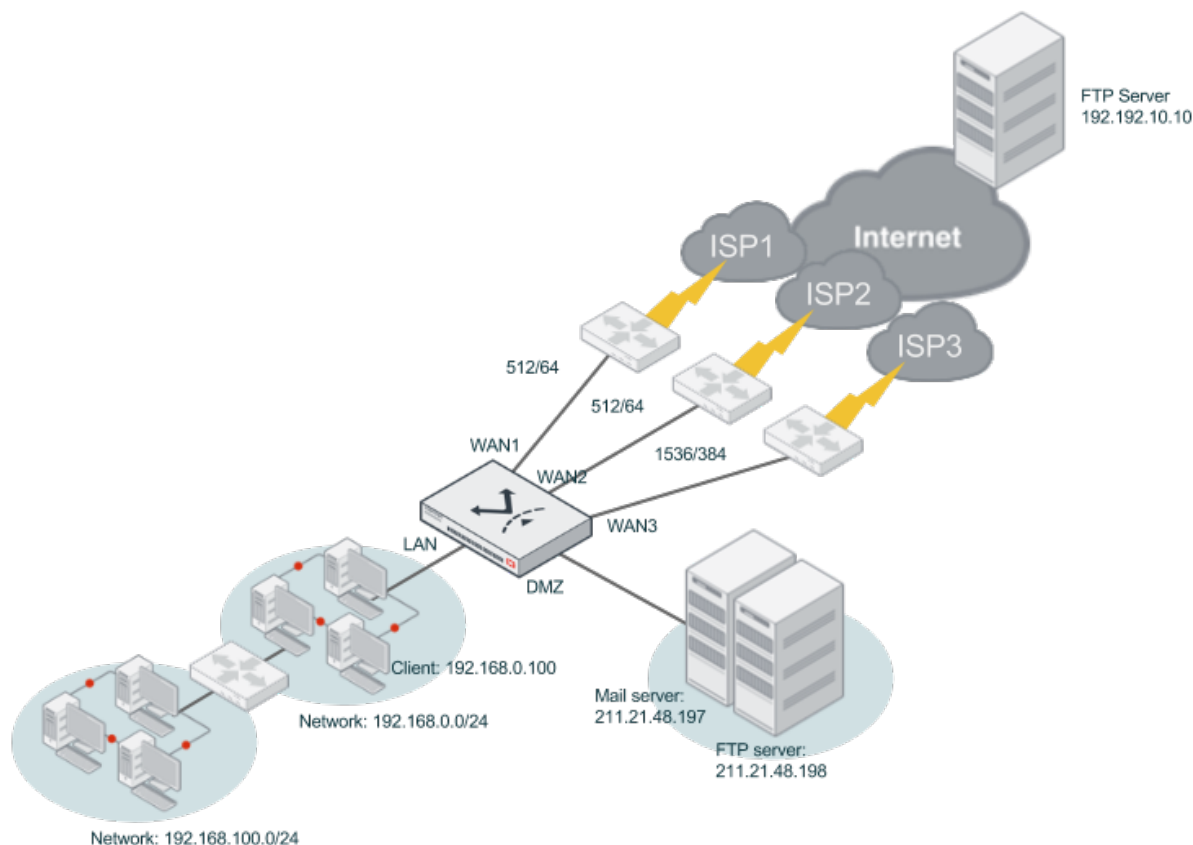
Traffic shaping by Bandwidth Manage takes place before Tunnel Routing and IPSec encapsulations. Traffic of an application is counted together in BM logs no matter whether it is transferred through Tunnel Routing and IPSec, thus you cannot identify whether the traffic is processed by FortiWAN's Tunnel Routing (includes Tunnel Routing over IPSec Transport mode) and FortiWAN's IPSec (Tunnel mode) according to the `PROTO` field of BM logs (see "[Log > View](#)") and the Service report of FortiWAN Reports. All the traffic processed by TR and IPSec is marked as its original application name in BM logs and Reports. The only case that you see the traffic identified as GRE or ESP in BM logs and Reports is because other devices generate the GRE or ESP traffic (encapsulated by other devices, not FortiWAN) and pass it through the FortiWAN. See "[Traffic Statistics for Tunnel Routing and IPSec](#)" for the details.



To recognize the traffic processed by Tunnel Routing and IPSec from the Reports, you can manage this kind of traffic with exclusive BM classes by matching its input port, source or destination IP addresses, so that you can get the statistics and bandwidth usage of Tunnel Routing and IPSec from the In Class and Out Class reports.

## Scenarios

### Example 1 Inbound BM



The maximum bandwidth limited for internet users to transfer emails to mail server 211.21.48.197 in DMZ during both busy and idle periods is 128K on WAN1, 64K on WAN2, and 128K on WAN3. The guaranteed bandwidth on WAN1, WAN2 and WAN3 is zero.

The maximum bandwidth limited for hosts in LAN zone to download data from internet web servers during both busy and idle periods is 128K on WAN1, 64K on WAN2, and 64K on WAN3. The guaranteed bandwidth on WAN1, WAN2 and WAN3 is zero.

During the busy period, the maximum bandwidth limited for 192.168.0.100 to download data from internet FTP servers is 50K on WAN1, 30K on WAN2 and WAN3. The guaranteed bandwidth on WAN1 is 20K, and zero on WAN2 and WAN3. During the idle period, the maximum bandwidth limited for 192.168.0.100 to download data from internet FTP servers is 50K on WAN1, 200K on WAN2 and WAN3. The guaranteed bandwidth is 20K on WAN1, 100K on WAN2 and WAN3. The bandwidth is prioritized as "High" during both busy and idle periods.

During the busy period, the maximum bandwidth limited for internet users to upload data to FTP server 211.21.48.198 in DMZ is 500K on WAN1, 256K on WAN2 and WAN3. The guaranteed bandwidth on WAN1 is 200K, and zero on WAN2 and WAN3. During the idle period, the maximum bandwidth limited for internet users to upload data to FTP server 211.21.48.198 in DMZ is 500K on WAN1, 300K on WAN2 and WAN3. The guaranteed bandwidth is 200K on WAN1, WAN2 and WAN3. The bandwidth is prioritized as "Low" during both busy and idle periods.

| Name              | Link | Busy Hour Settings |          |          | Idle Hour Settings |          |          |
|-------------------|------|--------------------|----------|----------|--------------------|----------|----------|
|                   |      | Guaranteed Kbps    | Max Kbps | Priority | Guaranteed Kbps    | Max Kbps | Priority |
| Mail Server       | WAN1 | 0                  | 128      | Normal   | 0                  | 128      | Normal   |
|                   | WAN2 | 0                  | 64       | Normal   | 0                  | 64       | Normal   |
|                   | WAN3 | 0                  | 128      | Normal   | 0                  | 128      | Normal   |
| For LAN Zone      | WAN1 | 0                  | 128      | Normal   | 0                  | 128      | Normal   |
|                   | WAN2 | 0                  | 64       | Normal   | 0                  | 64       | Normal   |
|                   | WAN3 | 0                  | 64       | Normal   | 0                  | 64       | Normal   |
| For 192.168.0.100 | WAN1 | 20                 | 50       | High     | 20                 | 50       | High     |
|                   | WAN2 | 0                  | 30       | High     | 100                | 200      | High     |
|                   | WAN3 | 0                  | 30       | High     | 100                | 200      | High     |
| FTP Server        | WAN1 | 200                | 5000     | Low      | 200                | 500      | Low      |
|                   | WAN2 | 0                  | 256      | Low      | 200                | 300      | Low      |
|                   | WAN3 | 0                  | 256      | Low      | 200                | 300      | Low      |

### Filter Settings

| Source | Destination   | Service  | Classes           |
|--------|---------------|----------|-------------------|
| WAN    | 211.21.48.197 | SMTP(25) | Mail Server       |
| WAN    | LAN           | HTTP(80) | For LAN Zone      |
| WAN    | 192.168.0.100 | FTP(21)  | For 192.168.0.100 |
| WAN    | 211.21.48.198 | FTP(21)  | FTP Server        |

There are two possible scenarios for inbound data. One is local host downloading data from a remote FTP server in WAN, the other is a remote user in WAN uploading data to FTP in LAN. In both two scenarios data are sent from WAN to LAN. Thus it is necessary to configure BM rules for the scenarios on the Inbound BM page.

## Example 2 Inbound BM

During the busy period, the maximum bandwidth limited for hosts in LAN zone to download data from FTP server 192.192.10.10 is 128K on WAN1, 128K on WAN2, and 64K on WAN3. During the idle period, the maximum bandwidth limited for hosts in LAN zone to download data from FTP server 192.192.10.10 is 512K on WAN1, WAN2 and WAN3. The guaranteed bandwidth on WAN1, WAN2 and WAN3 is zero during both busy and idle periods.

During the busy period, the maximum bandwidth limited for hosts 192.168.0.10 ~ 192.168.0.50 in LAN zone to download data from internet web servers is 128K on WAN1, 256K on WAN2 and WAN3. The guaranteed bandwidth is zero on WAN1, 128K on WAN2 and 64K on WAN3. During the idle period, the maximum bandwidth limited for hosts 192.168.0.10 ~ 192.168.0.50 in LAN zone to download data from internet web servers is 128K on WAN1, 512K on WAN2 and WAN3. The guaranteed bandwidth is zero on WAN1, WAN2 and WAN3. The bandwidth is prioritized as "Low" on WAN2 and WAN3 during both busy and idle periods.

During the busy period, the maximum bandwidth limited for hosts in a subnet 192.168.100.0/24 in LAN to download data from internet FTP servers is 50K on WAN1, 64K on WAN2 and WAN3. The guaranteed bandwidth on WAN1 is 20K, and zero on WAN2 and WAN3. During the idle period, the maximum bandwidth limited for hosts in a subnet 192.168.100.0/24 in LAN to download data from internet FTP servers is 20K on WAN1, 128K on WAN2 and WAN3. The guaranteed bandwidth is 20K on WAN1, 32K on WAN2 and WAN3. The bandwidth is prioritized as "High" during both busy and idle periods.

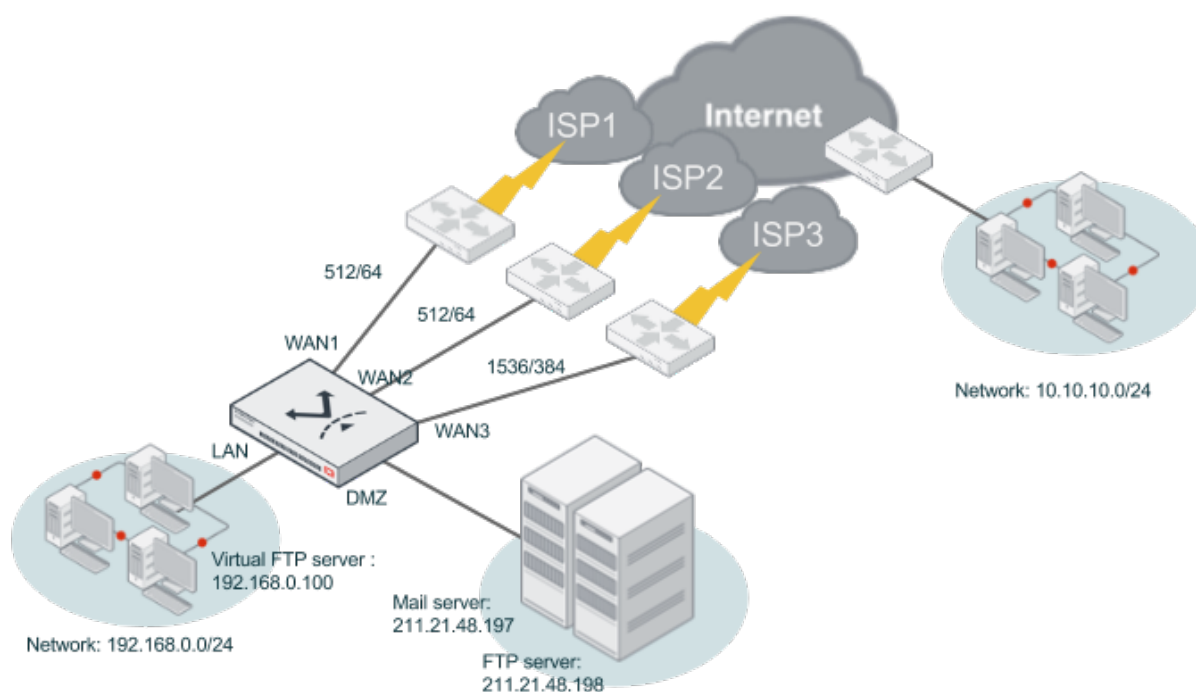
### Configuring inbound BM class table

| Name                 | Link | Busy Hour Settings |          |          | Idle Hour Settings |          |          |
|----------------------|------|--------------------|----------|----------|--------------------|----------|----------|
|                      |      | Guaranteed Kbps    | Max Kbps | Priority | Guaranteed Kbps    | Max Kbps | Priority |
| For LAN Zone         | WAN1 | 0                  | 128      | Normal   | 0                  | 512      | Normal   |
|                      | WAN2 | 0                  | 128      | Normal   | 0                  | 512      | Normal   |
|                      | WAN3 | 0                  | 64       | Normal   | 0                  | 512      | Normal   |
| For 192.168.0.10-50  | WAN1 | 0                  | 128      | Normal   | 0                  | 128      | Normal   |
|                      | WAN2 | 128                | 256      | Low      | 0                  | 512      | Low      |
|                      | WAN3 | 64                 | 256      | Low      | 0                  | 512      | Low      |
| For 192.168.100.0/24 | WAN1 | 20                 | 50       | High     | 20                 | 50       | High     |
|                      | WAN2 | 0                  | 64       | High     | 32                 | 128      | High     |
|                      | WAN3 | 0                  | 64       | High     | 32                 | 128      | High     |

## Filter Settings

| Source        | Destination                 | Service  | Classes                 |
|---------------|-----------------------------|----------|-------------------------|
| 192.192.10.10 | LAN                         | SMTP(25) | For LAN Zone            |
| WAN           | 192.168.0.10-192.168.0.50   | HTTP(80) | For<br>192.168.0.10-50  |
| WAN           | 192.168.100.0/255.255.255.0 | FTP(21)  | For<br>192.168.100.0/24 |

## Example 3 Outbound BM



During the busy period, the maximum bandwidth limited for internet users to download data from FTP server 211.21.48.198 in DMZ is 128K on WAN1 and WAN2, and 64K on WAN3. During the idle period, the maximum bandwidth limited for internet users to download data from FTP server 211.21.48.198 in DMZ is 512K on WAN1, WAN2 and WAN3. The guaranteed bandwidth on WAN1, WAN2 and WAN3 is zero during both busy and idle period.

During the busy period, the maximum bandwidth limited for internet users to receive emails from mail server 211.21.48.197 in DMZ is 128K on WAN1 and WAN2, and 256K on WAN3. During the idle period, the maximum bandwidth limited for internet users to receive emails from mail server 211.21.48.197 in DMZ is 128K on WAN1 and WAN2, and 512K on WAN3. The guaranteed bandwidth on WAN1, WAN2 and WAN3 is zero. The bandwidth is prioritized as "Low" during both busy and idle periods.

During the busy period, the maximum bandwidth limited for internet users to download data from a virtual FTP server 192.168.0.100 in LAN is 200K on WAN1, 100K on WAN2 and WAN3. The guaranteed bandwidth on WAN1 is 100K, and 50K on WAN2 and WAN3. During the idle period, the maximum bandwidth limited for internet users

to download data from a virtual FTP server 192.168.0.100 in LAN is 512K on WAN1, WAN2 and WAN3. The guaranteed bandwidth is on WAN1, WAN2 and WAN3 is zero. Note: When configuring filters on virtual servers, specify the private IP assigned to the virtual server and not the translated public IP.

During the busy period, the maximum bandwidth limited for hosts in a remote subnet 10.10.10.0/24 to download data from FTP server 211.21.48.198 in DMZ is 128K on WAN1 and WAN2 and 256K on WAN3. During the idle period, the maximum bandwidth limited for hosts in a remote subnet 10.10.10.0/24 to download data from FTP server 211.21.48.198 in DMZ is 256K on WAN1 and WAN2, and 512K on WAN3. The guaranteed bandwidth is zero on WAN1, WAN2 and WAN3, and the bandwidth is prioritized as "Low" during both busy and idle periods.

### Settings for BM classes above

| Name              | Link | Busy Hour Settings |          |          | Idle Hour Settings |          |          |
|-------------------|------|--------------------|----------|----------|--------------------|----------|----------|
|                   |      | Guaranteed Kbps    | Max Kbps | Priority | Guaranteed Kbps    | Max Kbps | Priority |
| Mail Server       | WAN1 | 0                  | 128      | Normal   | 0                  | 512      | Normal   |
|                   | WAN2 | 0                  | 128      | Normal   | 0                  | 512      | Normal   |
|                   | WAN3 | 0                  | 64       | Normal   | 0                  | 512      | Normal   |
| For LAN Zone      | WAN1 | 0                  | 128      | Low      | 0                  | 128      | Low      |
|                   | WAN2 | 0                  | 128      | Low      | 0                  | 128      | Low      |
|                   | WAN3 | 0                  | 256      | Low      | 0                  | 512      | Low      |
| For 192.168.0.100 | WAN1 | 100                | 200      | Normal   | 0                  | 512      | Normal   |
|                   | WAN2 | 50                 | 100      | Normal   | 0                  | 512      | Normal   |
|                   | WAN3 | 50                 | 100      | Normal   | 0                  | 512      | Normal   |
| FTP Server        | WAN1 | 0                  | 128      | Low      | 0                  | 256      | Low      |
|                   | WAN2 | 0                  | 128      | Low      | 0                  | 256      | Low      |
|                   | WAN3 | 0                  | 256      | Low      | 0                  | 512      | Low      |

### Filter Settings

| Source        | Destination | Service  | Classes            |
|---------------|-------------|----------|--------------------|
| 211.21.48.198 | WAN         | FTP(21)  | FTP Server         |
| 211.21.48.197 | WAN         | POP(110) | Mail Server (POP3) |

| Source        | Destination              | Service | Classes           |
|---------------|--------------------------|---------|-------------------|
| 192.168.0.100 | WAN                      | FTP(21) | For 192.168.0.100 |
| 211.21.48.198 | 10.10.10.0/255.255.255.0 | Any     | For 10.10.10.0    |

Two possible scenarios for upstream data: e.g. FTP (scenario 1), is that local host uploads data from a remote FTP server in the WAN. The other scenario is a remote user in WAN downloads data from a FTP server in the LAN. Both of these scenarios are sending data from LAN to WAN. Thus configuring BM rules for these two scenarios on the inbound BM page is necessary.

#### See also:

- [Busyhour Settings](#)
- [Using the web UI](#)
- [Log](#)
- [Statistics: Bandwidth](#)
- [Report: Bandwidth Usage](#)

## Connection Limit

Connection Limit is a feature that restricts the number of connections to remain below a certain specified limit. When the number of connections exceeds that limit, the system will automatically log the event (if logging is enabled). Connection limit can detect exceptionally high volumes of traffic caused by malicious attacks. FortiWAN protects the network by rejecting connections above the threshold.

Configurations of Connection Limit are divided into two sections: Count Limit and Rate Limit.

Count Limit is aimed to limit the number of concurrent connections issued by a source. That is to say at anytime FortiWAN will deny a new connection request coming from the source if the count of current established connections requested by the source reaches the threshold, no matter what the destinations and services of the connections are.

Rate Limit is aimed to restrict the rate that the specified connections are establishing at. FortiWAN recognizes the connections according to the source, destination, service and issue time that you specified, and monitors the number of the connection establishments every second. FortiWAN will deny a new connection that matches the specified rule if the number of matched connections established in recent second has reached to the value of the specified rate.

FortiWAN provides mechanisms to record, notify and analysis on events refer to the Connection Limit service, see "[Log](#)", "[Statistics: Connection Limit](#)" and "[Report: Connection Limit](#)".

### Log Interval

**Log Interval** : The log interval determines how often the system records when the number of the connections exceeds the limit defined in the rules table.



## Rules – Count Limit

- Source** : Match connections from a specified source (See ["Using the web UI"](#)).
- Count** : Set the limit for maximum number of the connections.
- L** : Check to enable logging. If the box is checked, logging will be enabled. Whenever the rule is matched, the system will record the event to the log file.

FortiWAN maintains a counter for every IP address that matches the specified source respectively, and monitors whether the connection count of each the IP address reaches the threshold (Count) defined to a Count Limit rule.

## Rules – Rate Limit

- E** : Enable: This rule can be matched. Disable: This rule does not need to be matched.
- When** : All of these three options are applicable 24 hours a day (See ["Busyhour Settings"](#)).
- Source** : Match connections from a specified source (See ["Using the web UI"](#)).
- Destination** : Match connections to specified Destination: This field is the same as the "Source" field, except that connections are matched with specified destination (See ["Using the web UI"](#)).
- Service** : The TCP/UDP service type to be matched. Select the matching criteria from publicly known service types (e.g. FTP), or enter the port number in TCP/UDP packets and specify the range. Type the starting port number plus hyphen "-" and then the ending port number. e.g. "TCP@123-234" (See ["Using the web UI"](#)).
- Conn/Sec** : Specify the number of connection allowed per second, under the conditions of [When], [Source], [Destination], and [Service] defined.
- L** : Check to enable logging. If the box is checked, logging will be enabled. Whenever the rule is matched, the system will record the event to the log file.

FortiWAN maintains one counter for every Rate Limit rule, which means that FortiWAN monitors whether the total number of the connections that match the rule and are established in recent second reaches the value of Conn/Sec specified to the rule.

## Cache Redirect

FortiWAN is capable of working with external cache servers. When a user requests a page from a web server on the internet, FortiWAN will redirect the request to the cache server. If the requested web page is already on the cache server, it will return the page to the user, thus saving time on data retrieval. Cache servers are configured here. However, cache servers have to support caching in transparent mode. Note: Cache Server can be in DMZ.

FortiWAN provides log mechanisms on events refer to the Connection Limit service, see ["Log"](#).

## Cache Group

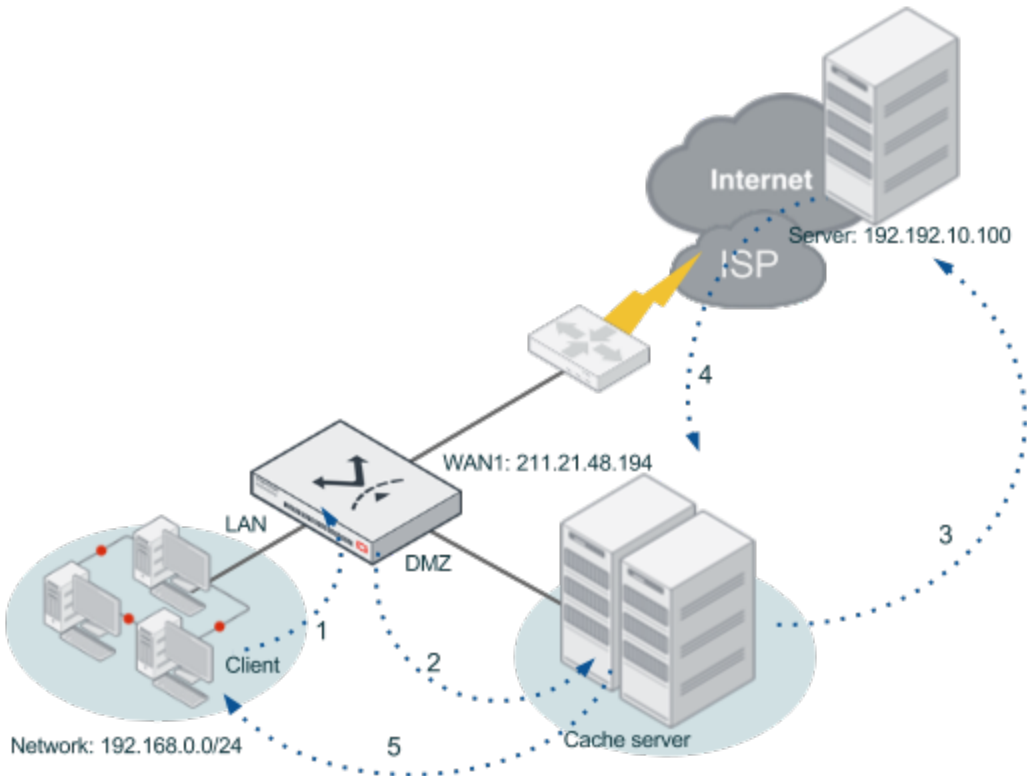
The first table configures cache server groups. Multiple groups can have different sets of rules which are then created on the second table. In addition, the number of cache servers is not limited to one. Therefore it is possible to have multiple cache servers with different weights in the cache server group.

|                       |                                                                                                                                                                                                                                                                                                                           |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Group Name</b>     | Assign a name for this cache server group.                                                                                                                                                                                                                                                                                |
| <b>IP</b>             | The IPv4 address of the cache server.                                                                                                                                                                                                                                                                                     |
| <b>Port</b>           | The port number of the cache server.                                                                                                                                                                                                                                                                                      |
| <b>Weight</b>         | The weight for redirecting the requests to this cache server. A higher value means a greater the chance.                                                                                                                                                                                                                  |
| <b>Associated WAN</b> | Select WAN link associated with the cache server. Cache redirect works only when both the selected WAN link and the cache server are available. Selecting "NO" means cache redirect is not associated with WAN links. No matter a WAN link is available or not, cache redirect can work if the cache server is available. |

## Redirect Rule

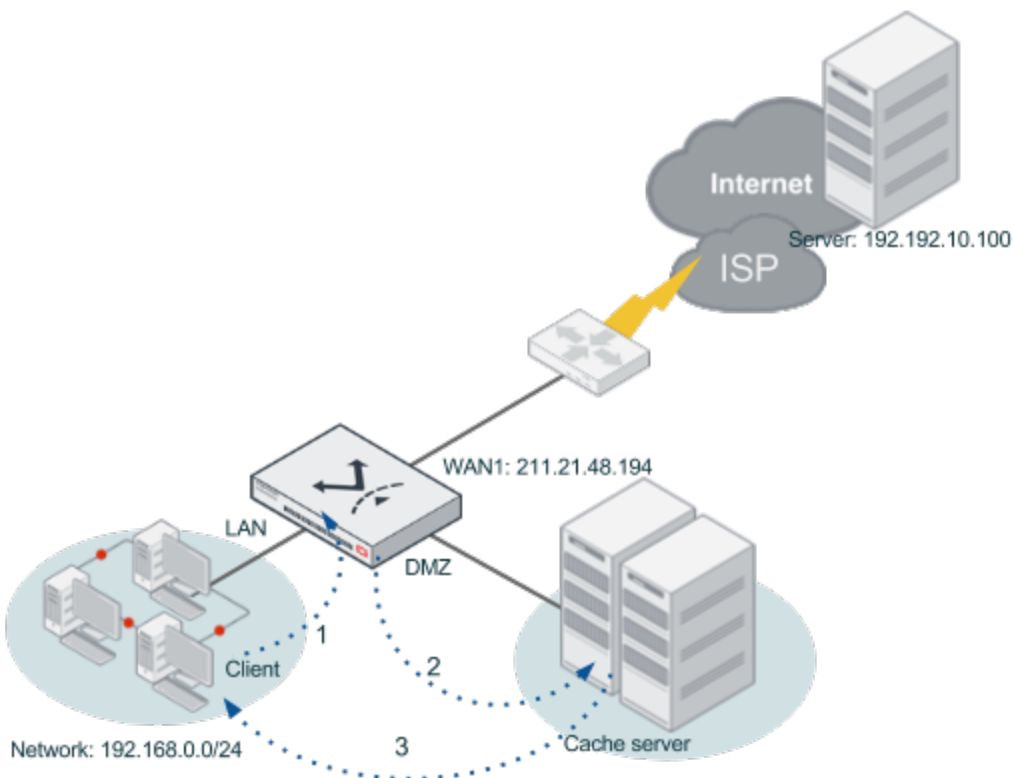
|                    |                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Source</b>      | The source where the request originates and it will be redirected to the cache server. Specify the IP(s) when selecting "IPv4 Address", "IPv4 Range" and/or IPv4 subnet (See <a href="#">"Using the web UI"</a> ).      |
| <b>Destination</b> | The destination where the request will be sent and it will be redirect to the cache server. Specify the IP(s) when selecting "IPv4 Address", "IPv4 Range" and/or IPv4 subnet (See <a href="#">"Using the web UI"</a> ). |
| <b>Port</b>        | The service port number and it will be redirected to the cache server.                                                                                                                                                  |
| <b>Group</b>       | Select "NO REDIRECT" for requests not to be directed. Or assign pre-existing group to redirect the requests.                                                                                                            |
| <b>L</b>           | Enable logging or not: If the box is checked, the logging will be enabled. Whenever the rule is matched, the system will write the event to the log file.                                                               |

Redirect rules can be established to match requests that will be redirected to the specific cache server group.

**Example 1 The Requested Web Page is NOT on the Cache Server**

When FortiWAN receives a request from a client, the request will be redirected to the cache server. The cache server will determine if the data requested already exists or not. If not, then the request will be performed on behalf of the client with the data returned from the web server to the client.

## Example 2 The Requested Web Page is on the Cache Server



When FortiWAN receives a request from a client, the request will be redirected to the cache server. In this case, the data requested already exists on the cache server. Therefore it will return the data requested to the client without passing the actual request to the internet.

## Internal DNS

Internal DNS is the DNS server built in FortiWAN used to manage your domain for internal users. Internal DNS resolve domain name for DNS requests coming from LAN or DMZ subnets. FortiWAN's Internal DNS is recursive DNS, which allows users to resolve other people's domains. The DNS servers set in **System > Network Setting > DNS Server** will be asked by Internal DNS while it recursively resolve an unknown domain (See "[Set DNS server to FortiWAN](#)"). In case that all the set DNS servers are not available or the DNS server is not configured, Internal DNS will ask the root domain name server for resolving the domain. Allocate the Internal DNS to users in LAN and DMZ subnets by manually set the DNS server on their computers to the gateways, which are LAN ports or DMZ ports. It is unable to automatically allocate FortiWAN's internal DNS to users by FortiWAN's DHCP. An user in LAN or DMZ subnet need to manually configure the DNS server on its computer to the gateway it connects to for using FortiWAN's Internal DNS. Activate DNS function by configuring fields below:

### Global Settings: IPv4 / IPv6 PTR Record

|                            |                                  |
|----------------------------|----------------------------------|
| <b>Enable Internal DNS</b> | Turn on/off internal DNS server. |
|----------------------------|----------------------------------|

|                        |                                                                                                                                                                                                                                                                                                  |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IPv4 PTR Record</b> | <ul style="list-style-type: none"> <li>• TTL: Specifies the amount of time other DNS servers and applications are allowed to cache the record.</li> <li>• IPv4 Address: Enter the reverse lookup IPv4 address.</li> <li>• Host Name: Enter the corresponding FQDN for the reverse IP.</li> </ul> |
| <b>IPv6 PTR Record</b> | <ul style="list-style-type: none"> <li>• TTL: Specifies the amount of time other DNS servers and applications are allowed to cache the record.</li> <li>• IPv6 Address: Enter the reverse lookup IPv6 address.</li> <li>• Host Name: Enter the corresponding FQDN for the reverse IP.</li> </ul> |

## Domain Settings

|                            |                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------|
| <b>Domain Name</b>         | Enter domain names for the internal DNS. Press “+” to add more domains.                      |
| <b>TTL</b>                 | Assign DNS query response time.                                                              |
| <b>Responsible Mail</b>    | Enter domain administrator's email.                                                          |
| <b>Primary Name Server</b> | Enter primary server's name.                                                                 |
| <b>IPv4 Address</b>        | Query IPv4 address. It can be: IPv4 single address, range, subnet, or predefined IPv4 group. |
| <b>IPv6 Address</b>        | Query IPv6 address. It can be: IPv6 single address, range, subnet, or predefined IPv6 group. |

## NS Record

|                     |                                                                                            |
|---------------------|--------------------------------------------------------------------------------------------|
| <b>Name Server</b>  | Enter server name's prefix. For example: if a server's FQDN is "nsl.abc.com", enter "nsl". |
| <b>IPv4 Address</b> | Enter the IPv4 address corresponding to the name server.                                   |
| <b>IPv6 Address</b> | Enter the IPv6 address corresponding to the name server.                                   |

## A/AAAA Record

|                   |                                                                                                           |
|-------------------|-----------------------------------------------------------------------------------------------------------|
| <b>Host Name</b>  | Enter the prefix name of the primary workstation. For example: if the name is "www.abc.com", enter "www". |
| <b>IP Address</b> | Enter the IPv4/IPv6 address of the primary workstation.                                                   |

## CName Record

|               |                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Alias</b>  | Enter the alias of the domain name. For example, if "www1.abc.com" is the alias of "www.abc.com", (domain name), enter "www1" in this field. |
| <b>Target</b> | Enter the real domain name. For example, if "www1.abc.com" is the alias of "www.abc.com", enter "www".                                       |

## SRV Record

|                 |                                                                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Service</b>  | Specify the symbolic name prepended with an underscore. (e.g. _http, _ftp or _imap)                                                                                                                   |
| <b>Protocol</b> | Specify the protocol name prepended with an underscore. (e.g. _tcp or _udp)                                                                                                                           |
| <b>Priority</b> | Specify the relative priority of this service (0 - 65535). Lowest is highest priority.                                                                                                                |
| <b>Weight</b>   | Specify the weight of this service. Weight is used when more than one service has the same priority. The highest is most frequently delivered. Leave is blank or zero if no weight should be applied. |
| <b>Port</b>     | Specify the port number of the service.                                                                                                                                                               |
| <b>Target</b>   | The hostname of the machine providing this service.                                                                                                                                                   |
| <b>TTL</b>      | TTL (Time To Live) specifies the amount of time that SRV Record is allowed to be cached.                                                                                                              |

## MX Record

|                    |                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Host Name</b>   | Enter the prefix of the mail server's domain name. For example, if domain name is "mail.abc.com", enter "mail". |
| <b>Priority</b>    | Enter the priority of the mail servers. The higher the priority is, the lower the number is.                    |
| <b>Mail Server</b> | Enter the IP address of the mail server.                                                                        |

## External Subdomain Record

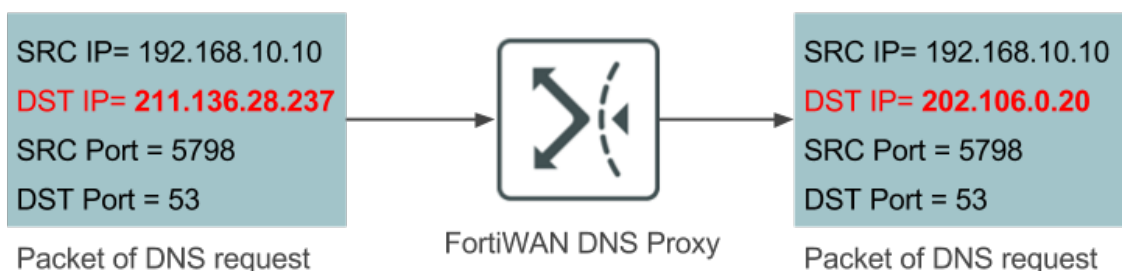
|                       |                                                                                   |
|-----------------------|-----------------------------------------------------------------------------------|
| <b>Subdomain Name</b> | Enter the name of an external subdomain. To add an additional subdomain, press +. |
|-----------------------|-----------------------------------------------------------------------------------|

**NS Record**

- Name server - Enter the prefix of domain name (e.g. if the FQDN of the host is "ns1.abc.com", enter "ns1")
- IPv4 address - Enter the corresponding IPv4 address of the domain name.
- IPv6 address - Enter the corresponding IPv6 address of the domain name.

## DNS Proxy

Conceptually, FortiWAN's DNS Proxy is a function to dynamically redirect outgoing DNS requests (UDP 53) to an appropriate DNS server according to FortiWAN's WAN link loading. It is implemented by dynamically replacing the original destination IP address of outgoing DNS requests with another DNS server IP address. No matter what the DNS server that an internal host is configured with, for any outgoing DNS request passing through FortiWAN, DNS Proxy replaces the original destination IP address of the DNS requests with the DNS server IP address determined by a load balancing algorithm. Basically, FortiWAN's DNS Proxy selects a WAN link with lighter traffic loading and replace original destination of the DNS query packet with another DNS server that is associated with the WAN link.

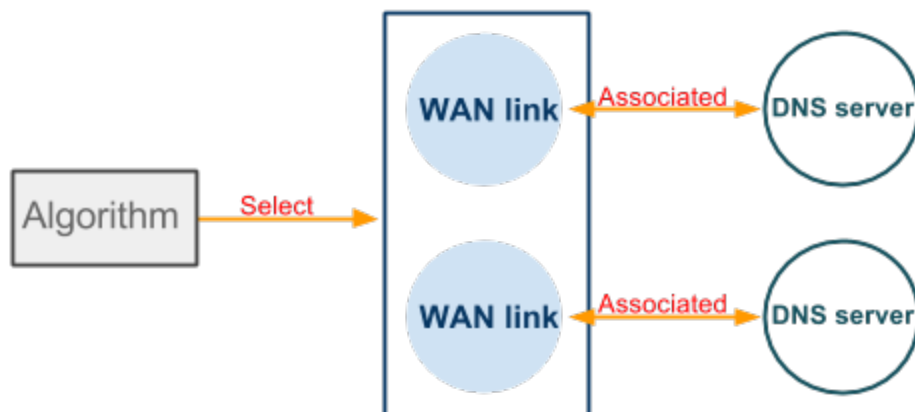


### How the DNS Proxy works and its configurations

Once DNS Proxy is enabled, any DNS request (UDP 53) received on FortiWAN's **LAN** and **DMZ** ports will be evaluated. DNS Proxy contains two phases; selecting a WAN link with lighter traffic loading (depends on the specified algorithm) and replacing the destination of DNS queries. Configuration of DNS Proxy contains three basic elements:

- An algorithm used to select a WAN link
- Participating WAN links
- The DNS servers used to replace the original destination of packets

DNS Proxy determines the DNS server for replacement by selecting one of the participating WAN links.



## DNS Proxy Setting Fields

**Enable DNS Proxy** Enable/disable DNS Proxy.

**Algorithm** Select an algorithm (See [Load Balancing Algorithms](#)) for selecting one of the participating WAN links:

- **By Weight:** select a WAN link from the participants in weighted round-robin.
- **By Down Stream:** always select the WAN link that has the lightest downstream traffic.
- **By Up Stream:** always select the WAN link that has the lightest upstream traffic.
- **By Total Traffic:** always select the WAN link that has the lightest total traffic.

The algorithm specified here determines a WAN link only for getting the associated DNS server to replace destination of the DNS packets. The selected WAN link is not for routing the packets. Auto Routing determines the WAN link to transfer the packets outward according to the policies.



**WAN**

Select the participating WAN links by specifying the DNS servers and weight. From the drop-down menu, select a WAN link and configure the following fields Weight and Server 1 - 3. Then the WAN link becomes one of the participating WAN links for DNS Proxy selects according to the specified algorithm.

After DNS Proxy selects a WAN link for a DNS request according to the specified algorithm, the destination of the DSN packet will be replaced with the DNS server associated to the WAN link. You can associate maximum of three DNS server IP addresses to a WAN link. DNS Proxy detects availability of the specified DNS servers and chooses the first available server for every replacement. A replacement will not take place if no specified server is available.

IP addresses of DNS servers specified here can be internal or external IP addresses. DNS packets processed by DNS Proxy will be transferred toward the internal or external IP address according routing rule set in Network Setting (see [Configuring your WAN](#) and [LAN Private Subnet](#)) and Auto Routing (see [Auto Routing](#)).

No matter which algorithm is specified, if only one WAN link is configured here, DNS packets will be always processed with the DNS server associated with the WAN link. In other words, DNS Proxy redirects DNS requests to a fixed DNS server regardless of traffic loading on WAN links.

**Weight**

Give a weight to the WAN link. This field is visible when By Weight is selected in Algorithm.

**Server 1**

Specify IP address of the first DNS server to the WAN link. This IP address will be used to replace the destination of a DNS packet if the associated WAN link is selected.

Getting this field configured is necessary to have a WAN link participated in DNS Proxy. A WAN link without configuring this field will not participate in DNS Proxy.

**Server 2**

Specify IP address of the second DNS server to the WAN link. This IP address will be used for the replacement if Server 1 is not available. This is optional.

**Server 3**

Specify IP address of the third DNS server on the WAN link. This IP address will be used for the replacement if Server 1 and Server 2 are not available. This is optional.

**Source**

DNS request packets coming from the specified source will be matched. Enter a single IPv4 address, IPv4 range (in format xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx) or a IPv4 subnet (in format xxx.xxx.xxx.xxx/netmask). Keep it blank for matching any source.

**Domain Name**

DNS requests for the specified domain name will be matched. A wildcard character is accepted for the left-most label of a domain name, e.g. *\*.fortinet.com* or *\*fortinet.com*.

Note that other formats such as *www.\*.com*, *www.fortinet.\** or *\*.fortinet.\** are not supported. Keep it blank for any domain name.

What DNS Proxy performs to DNS packets is only replace the destination of DNS packets; it does not involve routing for the packets. DNS Proxy select a WAN link only for the destination replacement, not for routing the packets. Auto Routing determines the route for the outgoing DNS packets (actually, Auto Routing is the only function routing for all outbound traffic, see [Auto Routing](#)). For example, although DNS Proxy selects WAN 1 for replacing destination of a DNS packet with IP of the DNS server associated with WAN 1, FortiWAN routing function might transfer it through other WAN links (WAN 2 or WAN 3) or a LAN port.

## Scenario

Here is an example using algorithm By Weight to select the DNS server for the destination replacement in the weight WAN1:WAN2 = 2:1.

### Algorithm

By Weight

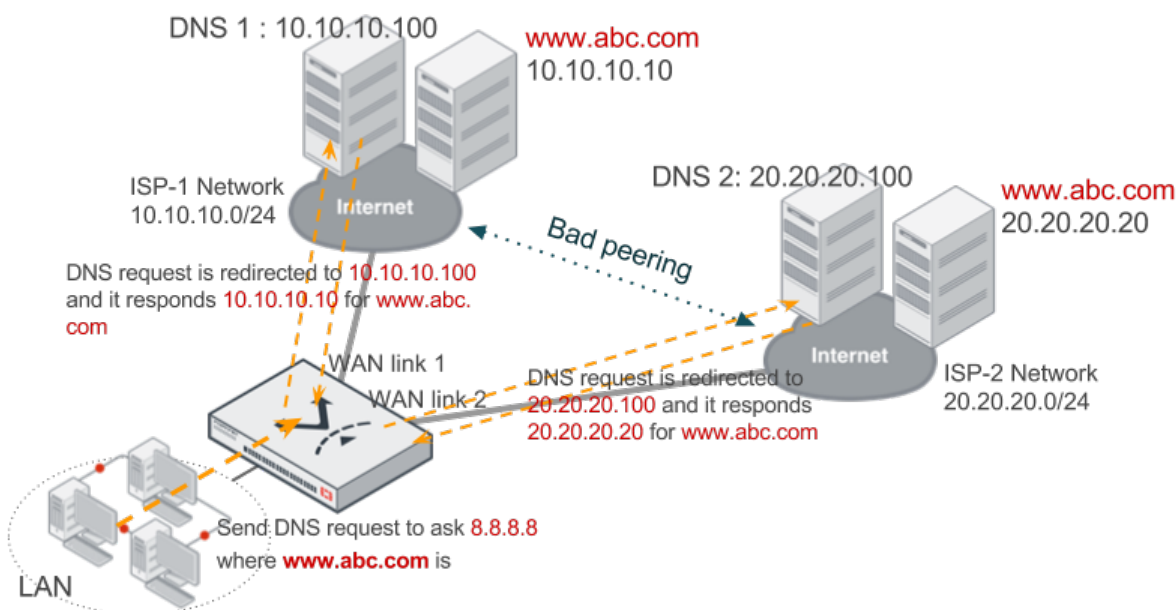
| DNS Server      |                |              |
|-----------------|----------------|--------------|
| <b>WAN</b>      | 1              | 2            |
| <b>Weight</b>   | 2              | 1            |
| <b>Server 1</b> | 211.136.28.237 | 202.106.0.20 |
| <b>Server 2</b> | -              | -            |
| <b>Server 3</b> | -              | -            |

According to the configuration, all the DNS requests received on FortiWAN's LAN ports and DNS ports will be reworked as followings:

| Packet   | Source        | Request A record for | Original destination | Hit WAN link | Replaced destination  |
|----------|---------------|----------------------|----------------------|--------------|-----------------------|
| Packet 1 | 192.168.0.10  | www.abc.com          | 8.8.8.8              | <b>WAN1</b>  | <b>211.136.28.237</b> |
| Packet 2 | 192.168.0.101 | www.def.com          | 202.96.209.5         | <b>WAN1</b>  | <b>211.136.28.237</b> |
| Packet 3 | 192.168..0.66 | www.ijk.com          | 202.96.209.133       | <b>WAN2</b>  | <b>202.106.0.20</b>   |
| Packet 4 | 192.168.0.23  | www.opq.com          | 211.136.150.66       | <b>WAN1</b>  | <b>211.136.28.237</b> |
| Packet 5 | 192.168.0.7   | www.rst.com          | 223.5.5.5            | <b>WAN1</b>  | <b>211.136.28.237</b> |
| Packet 6 | 192.168.0.211 | www.xyz.com          | 211.136.112.50       | <b>WAN2</b>  | <b>202.106.0.20</b>   |

## DNS Proxy for peering issue

Actually, DNS Proxy is mainly used to resolve potential traffic congestion on single WAN link due to the usage of Optimum Route for resolving ISP peering issue (certainly, it can also be used for just redirecting DNS requests to another DNS server, which is unrelated to peering issue). As mentioned in [Optimum Route Detection](#), Optimum Route does resolve the inefficient transmission resulted by bad peering between ISPs. No matter which detection mode is used for Optimum Route, traffic to a particular destination will be almost fixed by Optimum Route on particular WAN links (which the WAN links connect to the same ISP subnet that the particular destination is located in) if this ISP has bad peering with other ISPs (other WAN links). In real practice, most of service providers or internet content providers will not deploy their servers in only one ISP network if peering issue exists between ISPs. To provide service to users located in different ISP networks, they will logically deploy servers in several ISP networks, and maintain DNS servers (or appropriate settings on ISP's DNS) for a common domain in each of the ISP networks. Each of the DNS servers will answer the IP address of corresponding application server that is located in the same ISP network together with the DNS server to any DNS query for the server name. In other words, asking different DNS servers (located in different ISP networks) for the same server name will be responded with different IP addresses, which belong to different ISP networks. Users in an ISP network can access the server located in the same ISP network without passing across others ISPs if they ask an appropriate DNS.



Even if FortiWAN connects to multiple ISP networks, the problem is that users behind FortiWAN are usually configured with a fixed DNS server (that is probably located in one of the connected ISP networks), which means they always ask the same DNS server for a server name and are responded with the same IP address of the server. A user will not know other IP addresses of the same server name in other ISP networks unless they change DNS configuration to others.

For example a FortiWAN transfers outbound traffic by Auto Routing with Optimum Route (see [Auto Routing](#) and [Optimum Route](#)). In the above diagram, the DNS 1 (10.10.10.100) in ISP-1 network answers 10.10.10.10 to query for server name **www.abc.com**, while the DNS 2 (20.20.20.100) in ISP-2 network answers 20.20.20.20 to the query for the same server name. In other words, traffic to **www.abc.com** will be routed to WAN 1 by Optimum Route if a client asks DNS 1 for **www.abc.com**, or traffic will be routed to WAN 2 by Optimum Route if the client

asks DNS 2 for *www.abc.com*. However, the clients in LAN are configured with a static DNS address no matter manually or by DHCP. If all the clients in LAN are configured with `DNS Server = 10.10.10.100`, all the traffic to *www.abc.com* will fixedly be destined to 10.10.10.10 through WAN 1. This is what we mentioned traffic congestion on single WAN link resulted by usage of Optimum Route for resolving ISP peering issue.

For this reason, FortiWAN's DNS Proxy is a mechanism used to detect a WAN link with lighter traffic loading and redirect a DNS query to the DNS server located in the ISP network connected by the WAN link. For example, if DNS Proxy detects WAN 2 has lighter traffic loading than WAN 1, DNS queries for *www.abc.com* will be redirected to DNS 2 (20.20.20.100) and the response for *www.abc.com* will be 20.20.20.20. With appropriate configuration on Optimum Route, traffic to *www.abc.com* can be routed to WAN 2. No matter what the original DNS server (destination IP) of the query is, DNS Proxy replace it with another DNS according to current WAN link loading. Therefore, accessing to the same service can be distributed into multiple WAN links with Auto Routing by Optimum Route for this case.

To use DNS Proxy with Optimum Route to improve the bad transmission efficiency resulted by bad peering between ISPs, here is the basic premise for using DNS Proxy:

- FortiWAN connects to the bad-peering ISP networks through different WAN links.
- Optimum Route Detection is appropriately configured, and corresponding Auto Routing policy and filters are created for routing traffic by the algorithm: By Optimum Route. Without these configurations, the basic peering issue does not get resolved, and DNS Proxy becomes meaningless for this.
- Make sure that a service provider deploys different servers in the bad-peering ISP networks, and maintains DNS servers to answer corresponding IP address of the server that is located in the same ISP network with the DNS server. DNS Proxy will become helpless for this case if the service is only deployed in a ISP network.
- List these particular DNS servers located in each of the ISP networks. A DNS server must be associated with a WAN link connected to the ISP network that the DNS server is located in.

## Scenario

Base on the above example, make sure Optimum Route Detection and Auto Routing are configured before going on DNS Proxy. We assume that the Optimum Route Policy (see [Optimum Route Detection](#)) is configured as Static IP Table as followings:

|                   | ISP-1 Network                                                                       | ISP-2 Network                                                                       |
|-------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>Table Name</b> | ISP1                                                                                | ISP2                                                                                |
| <b>Setting</b>    | Upload the IP file of ISP 1. The IP subnet 10.10.10.0/24 is maintained in the file. | Upload the IP file of ISP 2. The IP subnet 20.20.20.0/24 is maintained in the file. |
| <b>Parameter</b>  | Check WAN1                                                                          | Check WAN2                                                                          |

You can also set the Optimum Route Policy as Dynamic Detect, Static & Dynamic or Dynamic & Static, see [Optimum Route Detection](#) for the details.

The Auto Routing policy and filter rule are correspondingly configured as followings (see [Auto Routing](#) for details):

| Label    | Algorithm        | Parameter           |
|----------|------------------|---------------------|
| OR_W1_W2 | By Optimum Route | Check WAN1 and WAN2 |

| When     | Input Port | Source      | Destination | Service | Routing Policy |
|----------|------------|-------------|-------------|---------|----------------|
| All-Time | Any Port   | Any Address | WAN         | Any     | OR_W1_W2       |

The above settings provides the basic solution of bad peering between ISP 1 and ISP 2. In this example, servers of *www.abc.com* are deployed in both ISP 1 and ISP 2 networks, and the DNS server in each ISP network answers corresponding IP to requests for *www.abc.com*. To introduce DNS Proxy to the case to dynamically distribute sessions to *www.abc.com* through the two WAN links, it requires the following settings of DNS Proxy configured:

We use algorithm By Total Traffic to select the DNS server associated with the lightest-loaded WAN link for the destination replacement (you can try other algorithms).

### Algorithm

By Total Traffic

| DNS Server |              |              |
|------------|--------------|--------------|
| WAN        | 1            | 2            |
| Server 1   | 10.10.10.100 | 20.20.20.100 |
| Server 2   | -            | -            |
| Server 3   | -            | -            |

### Proxy Domains

www.abc.com

The configurations guarantees that destinations of DNS packets querying for *www.abc.com* will be replaced with DNS servers 10.10.10.100 or 20.20.20.100 in circular order according to weight 2:1. DNS packets processed by DNS Proxy will be transferred outward according the Auto Routing policies. In this case (bad peering exists between the two ISPs), it is better to let DNS packets destined to 10.10.10.100 be routed to WAN 1 and DNS packets destined to 20.20.20.100 be routed to WAN 2. Packets might be stuck by the bad peering if packets destined to 10.10.10.100 be routed to WAN 2. Here, with Optimum Route being used in the Auto Routing policy, DNS packets processed by DNS Proxy will be routed to appropriate WAN link to avoid the bad peering.

### Possible query loop

Since DNS Proxy forwards queries, you should be careful with the deployments to avoided possible query loop. Here are the two cases that DNS Proxy might cause query loops.

#### Case 1

If DNS Proxy is configured to forward DNS queries to a DNS server located in FortiWAN's LAN or DMZ subnets, and this DNS server resolves queries by interacting with other DNS servers in the Internet through FortiWAN, a

query loop will happen. DNS Proxy forwards the queries that the DNS server in LAN or DMZ sends to the DNS servers outside FortiWAN back to the DNS server in LAN or DMZ.

## Case 2

FortiWAN's Internal DNS (see [Internal DNS](#)) provides service on IP address 223.255.255.2 that FortiWAN uses it for internal operations. However, if the DNS server in Network Setting (*System > Network Setting > DNS Server*, see [Set DNS server to FortiWAN](#)) is configured, Internal DNS will forward queries to the configured DNS servers rather than resolving them itself. Now, if you configure *System > Network Setting > DNS Server* with DNS servers located in FortiWAN's LAN or DMZ subnets, enable the Internal DNS, and configure Proxy DNS to forward queries to 223.255.255.2, a query loop will happen.

All the DNS queries are forwarded by DNS Proxy to 223.255.255.2 which is the Internal DNS, then these queries are forwarded again by Internal DNS to the DNS servers in LAN or DMZ which are configured in *System > Network Setting > DNS Server*. The DNS servers might resolve queries by interacting with other DNS servers in the Internet through FortiWAN. DNS Proxy forwards the queries that the DNS server in LAN or DMZ sends to the DNS servers outside FortiWAN back to Internal DNS on 223.255.255.2, and the queries are eventually forwarded back to the DNS servers in LAN or DMZ.

## SNMP

SNMP (Simple Network Management Protocol) is often used in managing TCP/IP networks by providing system information and sending event notifications to a SNMP manager. A SNMP manager is typically a host running the SNMP manager application. The SNMP manager communicates with the SNMP agent running on a FortiWAN unit; sends out SNMP requests and receives incoming event notification (SNMP trap) from the SNMP agent. The agent responds FortiWAN's system information for SNMP requests and sends SNMP traps to the SNMP manager.

To monitor your FortiWAN system via SNMP, you must:

- Compile the FortiWAN MIB file to your SNMP manager.
- Make sure at least one network interface is well-configured to send out SNMP traps and receive SNMP requests. The SNMP manager can communicate with a FortiWAN unit via the IP addresses configured on the localhost of a WAN port, DMZ port or LAN port (See "[Network Settings](#)").
- Make sure SNMP is acceptable to FortiWAN's firewall (See "[Firewall](#)").
- Configure SNMP settings and Event Notification to FortiWAN unit.

### SNMP agent configuration

To configure SNMP settings, go to **Service > SNMP**. Check the box **Enable SNMP** to enable SNMP agent on FortiWAN and select the SNMP version. FortiWAN supports SNMP v1, v2 and v3 protocols.

#### SNMP v1/2

|                    |                                                |
|--------------------|------------------------------------------------|
| <b>Community</b>   | Enter the community which the SNMP belongs to. |
| <b>System Name</b> | Enter a string to represent this system.       |

|                       |                                                                |
|-----------------------|----------------------------------------------------------------|
| <b>System Contact</b> | Enter a string to represent a person in charge of this system. |
|-----------------------|----------------------------------------------------------------|

|                        |                                                          |
|------------------------|----------------------------------------------------------|
| <b>System Location</b> | Enter a string to represent the location of this system. |
|------------------------|----------------------------------------------------------|

### SNMP v3

|                  |                                                |
|------------------|------------------------------------------------|
| <b>Community</b> | Enter the community which the SNMP belongs to. |
|------------------|------------------------------------------------|

|                    |                                          |
|--------------------|------------------------------------------|
| <b>System Name</b> | Enter a string to represent this system. |
|--------------------|------------------------------------------|

|                       |                                                                |
|-----------------------|----------------------------------------------------------------|
| <b>System Contact</b> | Enter a string to represent a person in charge of this system. |
|-----------------------|----------------------------------------------------------------|

|                        |                                                          |
|------------------------|----------------------------------------------------------|
| <b>System Location</b> | Enter a string to represent the location of this system. |
|------------------------|----------------------------------------------------------|

|                 |                                          |
|-----------------|------------------------------------------|
| <b>Username</b> | Enter user name used for authentication. |
|-----------------|------------------------------------------|

|                 |                                             |
|-----------------|---------------------------------------------|
| <b>Password</b> | Enter the password used for authentication. |
|-----------------|---------------------------------------------|

|                    |                                                            |
|--------------------|------------------------------------------------------------|
| <b>Privacy Key</b> | Enter the privacy key code. Eg: 12345678 , ABCDEFGHUI.etc. |
|--------------------|------------------------------------------------------------|

|                     |                                                                                                         |
|---------------------|---------------------------------------------------------------------------------------------------------|
| <b>AuthProtocol</b> | Select the authentication protocol used for transferring the authenticated password, either MD5 or SHA. |
|---------------------|---------------------------------------------------------------------------------------------------------|

|                     |                                                                                         |
|---------------------|-----------------------------------------------------------------------------------------|
| <b>PrivProtocol</b> | Select the authentication protocol used for transferring the authenticated privacy key. |
|---------------------|-----------------------------------------------------------------------------------------|

|                       |                                                                                                           |
|-----------------------|-----------------------------------------------------------------------------------------------------------|
| <b>Authentication</b> | Select the authentication method for user and privacy key, either authentication with or without privacy. |
|-----------------------|-----------------------------------------------------------------------------------------------------------|

### SNMP trap for even notification

FortiWAN (SNMP agent) sends traps to a SNMP manager for notification when significant events occur. Enable the function by configuring the settings of Log Notification to FortiWAN (See "Notification").

### FortiWAN MIB

The FortiWAN MIB defines the structure of the management data maintained on FortiWAN. It contains the fields, information and traps that are specific to a FortiWAN units. The FortiWAN MIB file is available on the Fortinet Customer Service & Support website, <https://support.fortinet.com/>.

## IP MAC Mapping

Users can specify the IP-MAC table by classifying periods like peak hours and idle hours. Once the IP-MAC table is set up, a packet from a certain IP address can pass through FortiWAN only when its MAC address matches the table list and time period.

FortiWAN provides log mechanism to the IP MAC Mapping service, see "[Log](#)".

**E** : Enable/Disable

**When** : Select the time period: busy hour, idle hour and all time. All time is defined in 24-hour system. For details, refer to [System] -> [Busyhour Settings] (See "[Busyhour Settings](#)").

**IP Address** : Enter the IP address of the network interface card.

**MAC Address** : Enter the MAC address of the network interface card.

**L** : Check it to activate the rule and record results in log file. Otherwise, the rule is inactive and data will not be stored.



## Statistics

This topic deals with FortiWAN network surveillance system. Comprehensive statistics are collected to monitor networking status, bandwidth usage of traffic class, and dynamic IP WAN link. These data offer deep insight into the network, and help detect unexpected network failures, boosting network reliability and efficiency.

## Traffic

It sorts and displays real-time traffic of traffic class over WAN link. Select traffic direction (inbound/outbound) in Traffic Type to view statistics.

The table below shows 3 sorts of statistics:

- Maximum/Minimum bandwidth allocation and priority
- Traffic for the last 3 seconds
- Traffic for the last minute

The statistics are analyzed based on individual WAN connection and traffic direction. To view statistics, select from Traffic Type (Inbound/Outbound), traffic direction and WAN Link number.

|                              |                                                                                                                                                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Traffic Type</b>          | : Traffic flow direction: inbound and outbound.                                                                                                          |
| <b>WAN Link</b>              | : The number of WAN links for inspection.                                                                                                                |
| <b>Automatic Refresh</b>     | : Time interval to refresh statistical table.                                                                                                            |
| <b>Traffic Class</b>         | : The name of the traffic class defined on Inbound/Outbound Bandwidth Management page. Among these, unclassified classes are labeled as "Default Class". |
| <b>Min. ~ Max.(Priority)</b> | : The maximum/minimum traffic volume allowed for a specific traffic class of different priority levels.                                                  |
| <b>3-Second Statistics</b>   | : Displays packet numbers or traffic flow volume in Kilobyte/sec for the last 3 seconds.                                                                 |
| <b>1-Minute Statistics</b>   | : Displays packet numbers or traffic flow volume in Kilobyte/sec for the past 60 seconds.                                                                |
| <b>Top 10</b>                | : Displays the data flow for the last five seconds with corresponding IP address. Statistics can be ranked by By Source and By Destination.              |

## Bandwidth management statistics

Unlike traffic statistics in previous section that focuses on real-time monitor of network status, statistics in BM (Bandwidth Management) is intended for long-term analysis. For particular traffic class in a given traffic direction,

administrators can view bandwidth usage in bar graph during the past 60 minutes, 30 hours, 50 days, and 20 months.

Go to **Statistics > BM**, the followings are the options for you to query a statistics chart:

| Fields               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Traffic Type</b>  | Specify traffic flow direction for displaying the BM statistics: Inbound and Outbound.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Traffic Class</b> | Specify the name of the traffic class defined on the Service > Bandwidth Management page for displaying the BM statistics. The listed options are: <ul style="list-style-type: none"> <li>Sum of All Classes: Traffic distributions of all the BM classes are displayed in the statistics chart. It displays the sum of traffic of all the classes at every time point.</li> <li>User-defined Classes: Traffic distributions of the user-defined classes.</li> <li>Default Class: Traffic distributions of the default class.</li> </ul> |
| <b>WAN Link</b>      | Specify the WAN link for displaying the BM statistics. The listed options are: <ul style="list-style-type: none"> <li>Sum of All Links: Traffic distributions of all the WAN links are displayed in the statistics chart. It displays the sum of traffic of all the WAN links at every time point.</li> <li>WAN Link #: Traffic distributions of a single WAN link.</li> </ul>                                                                                                                                                           |
| <b>Refresh</b>       | Click to refresh statistical charts (auto-refresh is not supported).                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

The three conditions for querying the BM statistics are combined with AND operator. For example, if you have the conditions as following:

Traffic Type=Outbound, Traffic Class=Default Class, WAN Link=WAN link #1

It displays the statistics of the outbound default class on WAN link 1.

Traffic Type

Traffic Class

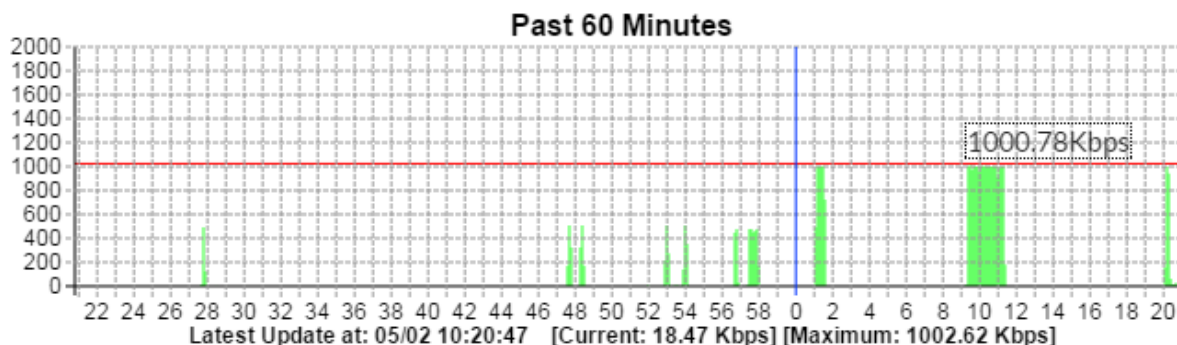
WAN Link

Refresh

Outbound

Default Class

WAN Link #1



A BM statistics chart consists of the following items:

| Fields                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Bandwidth (X axis)</b> | Bandwidth scale in Kbps.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Time (Y axis)</b>      | Time scale in minutes (past 60 minutes), hours (past 30 hours), days (past 50 days) and months (past 20 months).                                                                                                                                                                                                                                                                                                                                                          |
| <b>Latest Update</b>      | The last refresh time.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Current</b>            | Current bandwidth usage. The bandwidth usage at the last-right time point in the chart.                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Maximum</b>            | The maximum bandwidth usage in the time period.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Limit Line</b>         | <p>A limit line is displayed to indicate the maximum allowed bandwidth that the default BM class defines to the WAN link when the real traffic is very close to the limitation.</p> <p>The limit line function is available only when <b>Traffic Class</b> is selected as <b>Sum of All Classes</b> or <b>Default Class</b>. When WAN link is selected as Sum of All Links, only one limit line will be displayed for the WAN link with the highest limitation value.</p> |
| <b>Information</b>        | Moving the mouse over the BM statistics chart displays the corresponding exact bandwidth usage.                                                                                                                                                                                                                                                                                                                                                                           |

## Persistent Routing

It shows details with respect to persistent routing status. With persistent routing, administrators can view connections and manually reset these connections as well.

Clear All: Clear all the connections via persistent routing.

Automatic Refresh: Time interval to refresh persistent routing data.

### IPv4/IPv6 IP Pair

**IP Pair Entry** : Shows connection entries that match IP Pair Rules.

**Source IP** : Source IP of the current persistent routing connection.

**Destination IP** : Destination IP of the current persistent routing connection.

**Count** : Number of connections that the current persistent routing rule applies to.

**Timeout** : Length of time to lapse before the current connection times out.

**WAN** : The WAN link through which the current persistent routing connection travels.

## IPv4/IPv6 Web Service

- Web Service Entry** : Shows connection entries that match Web Service Rules.
- Source IP** : Source IP of the current persistent routing connection.
- Count** : Number of connections that the current persistent routing rule applies to.
- Timeout** : Length of time to lapse before the current connection times out.
- WAN** : The WAN link through which the current persistent routing connection travels.

Note that IP Pair and Web Service show at most 50 entries respectively.

## WAN Link Health Detection

It shows WAN link health detection results regarding the reliability of a specific WAN connection. The data are derived based on ping results from destination IP list configurations in **System > WAN Link Health Detection** (See "[WAN Link Health Detection](#)"). It enables to observe the number of sent requests, number of received responses, and the success ratio for a given destination. These statistics assist administrators in further analyzing network status and user behavior.

- WAN Link** : The WAN link to be monitored.
- Automatic Refresh** : Time interval for refreshing tables.
- Destination IP** : The destination IP address to which ping requests will be sent.
- Number of Requests** : The number of requests sent to the Destination IP so far. A request indicates a ping packet if Detection Protocol is ICMP, or a TCP connection request if Detection Protocol is TCP.
- Number of Replies** : The number of responses received so far from the Destination IP. A reply indicates a ICMP echo reply or a time\_exceed if Detection Protocol is ICMP, or a system acknowledge indicating TCP connection is established if Detection Protocol is TCP. Both indicate the success of a single WAN link detection.
- Success Ratio (%)** : The percentage of responses divided by requests. The higher the percentage, the greater the reliability.

## Dynamic IP WAN Link

It shows dynamic IP WAN link details like its IP address obtained via PPPoE or DHCP. It also enables to create new IP addresses by re-establishing connections to the WAN.

- Re-Connect All** : Reconnect all WAN links via PPPoE or DHCP.
- Automatic Refresh** : Time interval to refresh table results.
- WAN** : WAN connected by either PPPoE or DHCP.
- IP Address** : IP allocated to current WAN link.
- Gateway** : Gateway's IP address for current WAN link.
- Netmask** : Sub network mask.
- DNS** : Dynamic DNS Server IP.
- Connected Time** : Duration of WAN connectivity.
- Reconnect** : Reconnect a WAN link via PPPoE or DHCP.

## DHCP Lease Information

It shows data DHCP lease assigns, i.e. lease IP and MAC address, client-hostname, and expiration time. Once option of DHCP server is selected, a list regarding all existing DHCP servers in the network will display. Option Automatic Refresh sets the time interval to regularly update DHCP servers.

- DHCP Server** : Displays the DHCP server and IP range to be assigned.
- Automatic Refresh** : The time interval after which the table of DHCP leases information is updated.
- Lease IP** : WAN connected by either PPPoE or DHCP.
- IP Address** : Shows the IPv4 address assigned to the client's machine.
- MAC Address** : Shows the MAC address of the client's machine.
- Client-Hostname** : Shows the name of the client machine.
- Expiration Time** : Shows the time period when the IP address is valid.
- DHCPv6 Server** : Displays DHCPv6 server and range of IPv6 addresses which can be assigned.
- Lease IP** : Shows the IPv6 address assigned to client's machine.
- Client ID** : Shows the ID assigned to the lease IPv6 address.
- Expire Time** : Shows the time period during which the IPv6 address is valid.

## RIP & OSPF Status

It shows RIP status based on RIP and OSPF settings in [System] -> [Network Settings] -> [LAN Private Subnet]. Data on this page are used to inspect private subnet's Network IP, Netmask, and gateway list.

- Type** : Select from the list to view RIP or OSPF routing.
- Automatic Refresh** : Select auto-refresh interval, or disable the function.
- Network IP** : Shows the Network IP of the private subnet.
- Netmask** : Shows the Netmask of the private subnet.
- Gateway** : Shows the Gateway of the private subnet.

## Connection Limit

It enables administrators to inspect the number of established connections in real-time and to justify the maximum number of connections allowed on [Service] -> [Connection Limit] page, to avoid network congestion.

- Automatic Refresh** : Select auto-refresh interval, or disable the function.
- No.** : Numbering of IP addresses based on the number of connections established.
- IP** : Shows the source IP of the connection.
- Connections** : Shows the number of connections that are established by the source IP address and still active in system. An connection in system might be a connection with traffic flow existing or a idle connection. This number varies from connections closing to newly opened connections.
- Clear** : System maintains necessary tables and information for connections. Clicking the button to abort the connections established by the source IP address, and release the occupied memory then. When system is under attacks with high volumes of malicious connections, FortiWAN's Connection Limit (See "[Connection Limit](#)") stops subsequent connections established by the malicious IP addresses, but it takes time to recover system from the bandwidth and memory occupied by those malicious connections that are already in system. The Clear button terminates them immediately.

## Virtual Server Status

It displays status and statistics regarding virtual server defined in Service > Virtual Server (see [Virtual Server & Server Load Balancing](#)).

|                              |                                                                                                                                |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Automatic Refresh</b>     | Enable it and choose time interval for refreshing.                                                                             |
| <b>Virtual Server Status</b> | Green = OK; Red= Failed.                                                                                                       |
| <b>WAN IP</b>                | Displays WAN IPs defined in the rules on Service/Virtual Server page.                                                          |
| <b>Service</b>               | Displays services defined in the rules on Service/Virtual Server page. These services are those available for virtual servers. |
| <b>Server Pool</b>           | Display the backend server in the server pool that associated with the virtual server.                                         |
| <b>Server IP</b>             | Displays server IPs defined in the rules on Service/Virtual Server page. The server IPs denote those in real network usage.    |
| <b>Detect</b>                | Displays detection method, TCP or ICMP.                                                                                        |
| <b>Status</b>                | Displays detection result.                                                                                                     |

**Note** that only the enabled virtual servers and backend servers will be listed here.

## FQDN

The IPv4 and IPv6 addresses of the FQDNs that connected via FortiWAN are shown in this page.

### IPv4 FQDN

- FQDN** : The FQDN connected via FortiWAN.
- IPv4 Address** : IPv4 addresses of the FQDN connected via FortiWAN. It maintains 20 addresses at most.

### IPv6 FQDN

- FQDN** : The FQDN connected via FortiWAN.
- IPv6 Address** : IPv6 addresses of the FQDN connected via FortiWAN. It maintains 20 addresses at most.

## Tunnel Status

Tunnel Status displays the connectivity of every single GRE tunnel of each tunnel group defined in Service > Tunnel Routing (see [Tunnel Routing](#)) and statistics of the corresponding data transmission

|                          |                                                                                                                                                                                                                                                 |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tunnel Group</b>      | The drop-down menu lists all the tunnel groups defined in Service > Tunnel Routing. Select the tunnel group for monitoring it. The statistics of the specified tunnel group will be displayed in the Tunnel Health Status table below.          |
| <b>Automatic Refresh</b> | Enable automatic refresh by selecting the time interval (Every 3, 6, 9, 15, ... Seconds) for refreshing the statistics, or disable it by selecting Disabled. The statistics here will be automatically refreshed periodically if it is enabled. |

## Tunnel Health Status

This table displays the connectivity and statistics of specified tunnel group in the following four fields.

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tunnel</b>              | The GRE tunnel defined in the specified tunnel group, represented by the pair of its local and remote IP addresses.                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>3-Second Statistics</b> | Statistics of data transmission through this tunnel in the past 3 seconds, represented by RX Packets, RX Kbps, TX Packets and TX Kbps.                                                                                                                                                                                                                                                                                                                                                                    |
| <b>1-Minute Statistics</b> | Statistics of data transmission through this tunnel in the past 1 minute, represented by RX Packets, RX Kbps, TX Packets and TX Kbps.                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Status</b>              | <p>Indicating the connectivity of the tunnel with color schemes:</p> <p>Green indicates the tunnel is available (OK).</p> <p>Red indicates the tunnel is unavailable (failed).</p> <p>Moreover, the round trip time (RTT) and Jitter between the two endpoints of the tunnel is provided here for reference. The two fields will become blank if the tunnel is failed. You can also get the RTT of the tunnel by running Tunnel Routing's benchmark (see <a href="#">Tunnel Routing - Benchmark</a>).</p> |

## Default Rule Subnets

This table lists the subnets (in the local and remote sites) that the default rules of the specified tunnel group consist of. See [How to set up routing rules for Tunnel Routing](#) for the details of default rule of a tunnel group.

|                         |                                                                                                                                                                     |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Local Subnets</b>    | The local subnets (subnets in the local site) of the default routing rules of the specified tunnel group. It will be blank if there is no default rule enabled.     |
| <b>Opposite Subnets</b> | The opposite subnets (subnets in the remote site) of the default routing rules of the specified tunnel group. It will be blank if there is no default rule enabled. |

The default rule subnets listed here and corresponding page on remote Web UI are supposed to be equal for a tunnel group, just the position is switched. Local subnets here are the opposite subnets for the remote site, and the opposite subnets here are the local subnets for the remote site.



## Tunnel Traffic

It collects inbound/outbound traffic statistics regarding tunnel routing in the past 60 minutes, 24 hours, and 30 days. Statistics are displayed on chart.

**Traffic Type** : Traffic flow direction.

**Time** : Collect statistics in the past 60 minutes, 24 hours, and 30 days.

**Tunnel Routing Group** : Select a group from the list. Depending on N tunnels the group gets, N statistical charts will show.

## IPSec

IPSec Statistics reports the usages and states of your configured IPSec Security Associations (See "[IPSec](#)"). Go to **Statistics > IPSec**, a select bar and two statistics tables are displayed.

### Selector

Select the combination of Mode and Phase 1 here, and then the statistics of related IPSec SAs are reported.

|                     |                                                                                                                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Mode</b>         | Select the mode, Tunnel mode or Transport mode, of the security associations that you ask for.                                                                                                     |
| <b>Phase 1 Name</b> | All the configured Phase 1 names of the mode you selected above are list in the drop-down menu. Select a Phase 1 name (ISAKMP SA) to display the statistics of the associated IPSec SAs (Phase 2). |
| <b>Refresh</b>      | Click to refresh the statistics page.                                                                                                                                                              |

Statistics of the IPSec SAs associated to the ISAKMP SA you selected is displayed in two tables, Security Association Database and Security Policy Database.

### Security Association Database

List information of each IPSec SA including local and remote IP addresses, negotiated encryption and authentication algorithms, timing and the states.

|                   |                                                     |
|-------------------|-----------------------------------------------------|
| <b>Local IP</b>   | The local IP address of the IPSec SA.               |
| <b>Remote IP</b>  | The remote IP address of the IPSec SA.              |
| <b>Encryption</b> | The encryption algorithm that the IPSec SA employs. |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authentication</b>  | The authentication algorithm that the IPSec SA employs.                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Used time (s)</b>   | The past time since the IPSec SA is established.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Life time (s)</b>   | The time interval (in seconds) that the secret key of the IPSec SA is valid during. For the expiration of a key, IKE Phase 2 is performed automatically to establish a new IPSec SA (a new key is negotiated). The value here is equal to value of Keylife of the correspondent Phase 2 configuration.                                                                                                                                                            |
| <b>Change time (s)</b> | The time point that system starts to establish a new IPSec SA for replacing the current IPSec SA which is going to expire. New IPSec SA will be prepared in advance so that it takes over the expired IPSec SA in time. This value is related to Life time and determined by system.                                                                                                                                                                              |
| <b>Status</b>          | <p>States of the IPSec SA:</p> <ul style="list-style-type: none"> <li>• larval: an IKE Phase 2 is in progress to establish an IPSec SA</li> <li>• mature: the IPSec SA is established and still within validity</li> <li>• dying: the IPSec SA is about to expire, and another IKE Phase 2 is in progress for taking over</li> <li>• dead: the connectivity between two endpoints communicating through the IPSec SA is down; the peer is unavailable.</li> </ul> |

## Security Policy Database

List information of Quick Mode selector of each IPSec SA and the related time stamps.

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>              | The unique name of the IPSec SA (the name configured to the Phase 2)                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Source[port]</b>      | <p>For IPSec in Tunnel mode, this is the Source and Source Port of the Quick Mode selector of the IPSec SA (the Source and Port configured to the Phase 2).</p> <p>For IPSec in Transport mode, this is the source IP address of the Tunnel Routing packets (GRE encapsulated), which is equal to the Local IP of the IPSec SA (the Local IP configured to the Phase 1). Port information will not be list for this case.</p>                       |
| <b>Destination[port]</b> | <p>For IPSec in Tunnel mode, this is the Destination and Destination Port of the Quick Mode selector of the IPSec SA (the Destination and Port configured to the Phase 2).</p> <p>For IPSec in Transport mode, this is the destination IP address of the Tunnel Routing packets (GRE encapsulated), which is equal to the Remote IP of the IPSec SA (the Remote IP configured to the Phase 1). Port information will not be list for this case.</p> |

|                       |                                                                                                                                                                                               |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Protocol</b>       | For IPSec in Tunnel mode, this is the Protocol of the Quick Mode selector of the IPSec SA (the Protocol configured to the Phase 2).<br><br>For IPSec in Transport mode, this is always "gre". |
| <b>Created time</b>   | The time that the IPSec SA is established.                                                                                                                                                    |
| <b>Last used time</b> | The time that the IPSec SA is applied last to a data packet.                                                                                                                                  |

For the details of parameters of IPSec, see ["IPSec VPN in the Web UI"](#).

## Traffic Statistics for Tunnel Routing and IPSec

Compare with general IP transmission, traffic transferred through FortiWAN's Tunnel Routing or IPSec is charged extra on GRE/ESP encapsulation and decapsulation (See ["Tunnel Routing"](#) and ["IPSec VPN"](#)). In order to individually allocate bandwidth to applications encapsulated in GRE and ESP packets, Tunnel Routing and IPSEC are designed to be transparent to Bandwidth Management (See ["Bandwidth Management"](#)). Bandwidth Management shapes the traffic before packet encapsulation or after packet decapsulation. FortiWAN's traffic statistics is associated with the operation of Bandwidth Management, which implies traffic of Tunnel Routing and IPSec is partially transparent to the statistics function. FortiWAN gives the traffic statistics in three ways: BM log, statistics on Web UI and FortiWAN Reports. Traffic statistics for Tunnel Routing and IPSec in the three ways are discussed as follows.

### BM logs

A BM log is actually a traffic statistics (inbound-pkts, inbound-bytes, outbound-pkts, outbound-bytes, total-pkts and total-bytes) in a time period for a traffic (source IP, destination IP, source port and destination port) that matches the Bandwidth Management filter (See Log format in ["Log View"](#)). Bandwidth Management treats the traffic equally no matter whether it is later transferred through Tunnel Routing and IPSec. The BM log tells nothing directly (through the source port and destination port fields) that a transmission is actually done by Tunnel Routing, IPSec or normal IP routing. You might be aware of a Tunnel Routing and IPSec transmission through the source IP and destination IP in the logs, if you those IP addresses are already predefined just for the Tunnel Routing and IPSec transmission. The only situation that you see the GRE or ESP indicated by source port and destination fields in a BM log is when the traffic comes from other VPN devices.

### Statistics on Web UI

Pages **Statistics > Traffic** and **Statistics > BM** (See ["Statistics > Traffic"](#) and ["Statistics > BM"](#)) the traffic statistics by WAN links and defined Bandwidth Management classes, which tells nothing directly about Tunnel Routing and IPSec traffic. The way to identify the traffic that is transferred through Tunnel Routing or IPSec is to create a BM class and BM filter to classify the traffic by the source IP and destination IP that are defined in Tunnel Routing's routing rules or IPSec's Quick Mode selectors.

Page **Statistics > Tunnel Traffic** (See ["Statistics > Tunnel Traffic"](#)) is the only page reports the traffic statistics about Tunnel Routing. Although traffic statistics is reported by the defined Tunnel Routing groups, statistics of the individual application in the tunnel traffic is unavailable here.

Page **Statistics > IPSec** (See "[Statistics > IPSec](#)") tells nothing about traffic statistics of IPSec, only IPSec connectivity states are reported here.

## FortiWAN Reports

Similar to BM logs, application traffic processed by Tunnel Routing or IPSec is marked as its original application name in Reports (See "[Reports > Bandwidth Usage > Services](#)"). Individual service type of the original packets encapsulated by Tunnel Routing or IPSec is visible in Reports. Only the GRE or ESP traffic generated by other devices and passed through FortiWAN will be counted as GRE or ESP in the Reports > Services page. Although you can not easily identify whether the traffic is processed by FortiWAN's Tunnel Routing or IPSec from the Service report, but the In Class and Out Class reports can tell you the information and statistics if an exclusive BM class is used for this kind of traffic.

Here are a summary of discussion above.

### Traffic transferred through IPSec Tunnel mode

|                   | Original traffic | ESP encapsulated traffic |
|-------------------|------------------|--------------------------|
| <b>BM Control</b> | O                | X                        |
| <b>BM log</b>     | O                | X                        |
| <b>Reports</b>    | O                | X                        |

### Traffic transferred through Tunnel Routing or IPSec Transport mode

|                   | Original traffic | GRE encapsulated traffic | ESP encapsulated traffic |
|-------------------|------------------|--------------------------|--------------------------|
| <b>BM Control</b> | O                | X                        | X                        |
| <b>BM log</b>     | O                | X                        | X                        |
| <b>Reports</b>    | O                | X                        | X                        |

We have a simple example to explain the difference between the statistics ways. Consider that user A generates 60MB FTP traffic and 80MB HTTP traffic and transfer them through Auto Routing, user B generates 40MB FTP traffic and 20MB HTTP traffic and transfer them through Tunnel Routing (through one tunnel group). We create two BM classes, class-AR and class-TR, to control traffic of user A and user B respectively (identifying by their input port, source or destination IP addresses).

Go to **Log > View**, the BM logs tell the statistics as following:

- user A (source IP) generates FTP traffic (source or destination port) in 60MB
- user B (source IP) generates FTP traffic (source or destination port) in 40MB
- user A (source IP) generates HTTP traffic (source or destination port) in 80MB
- user B (source IP) generates HTTP traffic (source or destination port) in 20MB

From the BM logs, we have no idea which one is transferred through Tunnel Routing. The thing we know from the logs is 100MB FTP traffic and 100MB HTTP traffic passed through FortiWAN, and they are 200MB in total.

Go to **Statistics > Tunnel Traffic**, we see 60MB tunnel traffic (parts of the 200MB) belongs to the tunnel group. However, it tells nothing about the statistics for the individual services (FTP and HTTP) in the tunnel traffic.

Go to **Reports > Service**, statistics by service is displayed as follows:

- FTP = 100MB
- HTTP = 100MB
- Total = 200MB

Similarly, you can not identify how much the bandwidth is used by Tunnel Routing by a glance. You still can have the information as long as you give each of the services a drill-down query by Internal IP, but this is not a complete report for the entire Tunnel Routing usage.

Go to **Reports > Out Class**, statistics by outbound BM class is displayed as follows:

- class-AR = 140MB
- class-TR = 60MB
- Total = 200MB

You can have the complete report from the class-TR and all the drill-down queries.

# Logs

This topic deals with how to configure logging and how to forward logs. Log records keep FortiWAN data and are capable of storing a wide variety of data concerning System, Firewall, Routing, and bandwidth management, etc (see [Log View](#)). Log files are stored in FortiWAN's hard disk and can be forwarded to other servers for archiving or for notifying events via emails (see [Log Control](#) and [Log Notification](#)).

Additionally, FortiWAN offers a powerful reporting and analysis tool: Reports. The web-based analysis software that is embedded in FortiWAN or running on an independent machine enables administrators to gain insights into network traffic without manually filtering through large volumes of log data (See [Enable Reports](#)).

## Log View

In **Log > View** there is a sub-menu of 13 log types (see the table below). Choose the desired log type, and its corresponding events will show in display window. Click the Refresh button to get the latest log records. Please be aware that this page is only for online viewing of current events. For log data pushing and archiving, see [Log Control](#).

| Fields              | Descriptions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Type</b>     | Choose log type to view its events in display window. The log types are: <ul style="list-style-type: none"><li>• System Log</li><li>• Firewall Log</li><li>• NAT Log</li><li>• Auto &amp; Persistent Routing Log</li><li>• Virtual Server Log</li><li>• BM Log</li><li>• Connection Limit Log</li><li>• Cache Redirect Log</li><li>• Multihoming Log</li><li>• Backup Line Log</li><li>• Dynamic IP Log</li><li>• IP-MAC Mapping Log</li><li>• Tunnel Routing Log</li><li>• IPSec Log</li></ul> |
| <b>Recent Event</b> | Log events of the selected log type are listed here.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Refresh</b>      | Refresh to get the latest log events.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Clear</b>        | Remove the log records from hard disk.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Log format

A log listed here consists of three parts:

```
{TIMESTAMP} {LOG_TYPE} {LOG_CONTENT}
```

The `{TIMESTAMP}` is in the format 'yyyy-mm-dd HH:MM:SS' and is always an UTC time. The details of `{LOG_TYPE}` and `{LOG_CONTENT}` are described as follows.

### Notation Conventions

`{ADDRPORT}` follows TCPDUMP format, for example:

- **IPv4:** 8.8.8.8.80
- **IPv6:** 2001::8:8:8:8.80

`{IP-5-TUPLE}`

- **ICMP:**PROTO=1 SRC=<ip> DST=<ip> ID=<icmpid> TYPE=<icmptype> CODE=<icmpcode> (BM log doesn't have TYPE and CODE fields, because they are bypacket)
- **TCP:**PROTO=6 SRC=<{ADDRPORT}> DST=<{ADDRPORT}>
- **UDP:**PROTO=17 SRC=<{ADDRPORT}> DST=<{ADDRPORT}>
- **ICMPv6:**PROTO=58 SRC=<ip> DST=<ip> TYPE=<icmpv6type> CODE=<icmpv6code>
- **Others:**PROTO=<protocol num> SRC=<ip> DST=<ip>

## Firewall

```
FW {IP-5-TUPLE} ACTION=[ACCEPT|DENY] TOTLEN=<pktlen>
```

The first packet of session `{IP-5-TUPLE}` matching a Firewall rule triggers the log. System generates only one log for this session. This log indicates all the packets of the session `{IP-5-TUPLE}` are accepted or denied by Firewall, and the first packet size is `<pktlen>`. In reality, the event ACCEPT will not be logged by system.

See "[Firewall](#)" for further information.

## NAT

```
NAT {IP-5-TUPLE} NEW_SRC={ADDR}
```

The first packet of session `{IP-5-TUPLE}` matching a NAT rule triggers the log. System generates only one log for this session. This log indicates source addresses of the packets of `{IP-5-TUPLE}` are translated to the new address `{ADDR}` by NAT.

See "[NAT](#)" for further information.

## Auto & Persistent Routing

```
AR {IP-5-TUPLE} AR=[<widex>|NONE] TOTLEN=<pktlen>
```

The first packet of session {IP-5-TUPLE} matching a Auto Routing rule triggers the log. System generates only one log for this session. This log indicates packets of the session {IP-5-TUPLE} are transferred outward through WAN link <widx>, or all the WAN links defined in the routing and fail-over policies fail to transfer the packets (AR=NONE). The first packet size of the session is <pktlen>. See ["Auto Routing"](#) for further information.

```
PR {IP-5-TUPLE} PR=[<widx>|WAIT_AR|NONE] TOTLEN=<pktlen>
```

The first packet of session {IP-5-TUPLE} matching a Persistent Routing rule triggers the log. System generates only one log for this session. This log indicates packets of the session {IP-5-TUPLE} are transferred outward through WAN link <widx> (the persistence entry of the session is not expired), or Auto Routing determines the WAN link for the session (PR=WAIT\_AR, the persistence entry of the session is expired or absent), or the action to this session is No PR (PR=NONE). The first packet size of the session is <pktlen>. See ["Persistent Routing"](#) for further information.

If a PR log that PR=WAIT\_AR, the PR log and a correspondent AR log are generated in pairs.

## Virtual Server

```
VS {IP-5-TUPLE} NEW_DST={ADDR} TOTLEN=<pktlen>
```

The first packet of session {IP-5-TUPLE} matching a Virtual Server rule triggers the log. System generates only one log for this session. This log indicates destination addresses of the packets of {IP-5-TUPLE} are translated to the new address {ADDR} by Virtual Server. The first packet size of the session is <pktlen>.

See ["Virtual Server"](#) for further information.

## BM

```
BM {IP-5-TUPLE} INPKTS=<%lu> INBYTES=<%lu> OUTPKTS=<%lu> OUTBYTES=<%lu>  
TOTALPKTS=<%lu> TOTALBYTES=<%lu> DURATION=<%lu>SECS
```

Session {IP-5-TUPLE} matching a Bandwidth Management filter triggers the log when it is closed. System generates only one log for this session. This log indicates the traffic statistics (INPKTS, INBYTES, OUTPKTS, OUTBYTES, TOTALPKTS, TOTALBYTES and DURATION) of the session {IP-5-TUPLE}.

See ["Bandwidth Management"](#) for further information.

## Connection Limit

### Count Limit

```
CL SRC=<ip> DROP=<pkt_number>
```

This log is triggered every time-period if the number of connections generated by a source SRC=<ip> exceeds the limitation defined in Connection Limit > Count Limit. This log indicates connections generated by SRC=<ip> and passing through FortiWAN are more that the limitation, and there are <pkt\_number> packets are dropped for the reason.



## Rate Limit

```
RL RULE=<ridx> DROP=<pkt_number>
```

This log is triggered every time-period if a rule <ridx> of Connection Limit > Rate Limit is matched. This log indicates connections defined in the Rate Limit rule <ridx> are generated in a rate higher than the limitation, and there are <pkt\_number> packets are dropped for the reason.

See "[Connection Limit](#)" for further information.

## Cache Redirect

```
CR {IP-5-TUPLE} NEW_DST={ADDR-PORT}
```

The first packet of session {IP-5-TUPLE} matching a Cache Redirect rule triggers the log. System generates only one log for this session. This log indicates destination addresses and ports of the packets of {IP-5-TUPLE} are translated to {ADDR} by Virtual Server. The first packet size of the session is <pktlen>.

See "[Cache Redirect](#)" for further information.

## Multihoming

```
MH FROM=<ip> TYPE=<A|AAAA> WLINK=<widx> REPLY=<ip>
```

An DNS response (queried for A or AAAA records) by Multihoming triggers the log. System generates the log only for DNS queries for A and AAAA records. This log indicates a DNS query whose type is TYPE=<A|AAAA> and comes from FROM=<ip> is responded by Multihoming with REPLY=<ip>, which is the IP address of WAN link <widx>. System generates two logs for A and AAAA records if the DNS query type is ANY.

See "[Multihoming](#)" for further information.

## Dynamic IP

### DHCP

```
DHCP WLINK=<widx> ACTION=<init|renew|rebind|expired|failed|release|stop|bind>  
[IP=<ip>]
```

System triggers the log when a DHCP WAN link <widx> is acted for ACTION. ACTION=bind and IP=<ip> must be generated in pairs for a log.

### PPPoE

```
PPPOE WLINK=<widx> ACTION=<start|terminated|bind> [IP=<ip>]
```

System triggers the log when a PPPoE WAN link <widx> is acted for ACTION. ACTION=bind and IP=<ip> must be generated in pairs for a log. Three more logs are introduced when a PPPoE WAN link goes to failure:

- PPPOE config-requests timeout
- PPPOE connection no response
- PPPOE authentication failed

## IP-MAC Mapping

```
MAC {IP-5-TUPLE} BAD_SRC_MAC=<MAC>
```

The first packet of session {IP-5-TUPLE} blocked by IP-MAC Mapping triggers the log. System generates only one log for this session. This log indicates source MAC addresses <MAC> of the packets of {IP-5-TUPLE} and the MAC address defined in IP-MAC table are mismatched, and so that the packets are blocked.

```
MAC {IP-5-TUPLE} BAD_DST_MAC=<MAC>
```

The first packet of session {IP-5-TUPLE} blocked by IP-MAC Mapping triggers the log. System generates only one log for this session. This log indicates destination MAC addresses <MAC> of the packets of {IP-5-TUPLE} and the MAC address defined in IP-MAC table are mismatched, and so that the packets are blocked.

See "[IP-MAC Mapping](#)" for further information.

## Tunnel Routing

```
TR {IP-5-TUPLE} GROUP=<group name> TOTLEN=<pktlen>
```

The first packet of session {IP-5-TUPLE} being transferred by Tunnel Routing triggers the log. System generates only one log for this session. This log indicates packets of {IP-5-TUPLE} are transferred through the Tunnel Group <group name>, and the first packet size of the session is <pktlen>.

```
TUN FROM=<ip> TO=<ip> ACTION=<start|stop|fail|recover>
```

This log is triggered when a single GRE tunnel FROM=<ip> TO=<ip> is acted for actions ACTION.

See "[Tunnel Routing](#)" for further information.

## IPSec

```
ISAKMP-SA <established|expired|deleted> <LOCAL_IP_PORT>-<REMOTE_IP_PORT>
```

An ISAKMP SA between <LOCAL\_IP\_PORT> and <REMOTE\_IP\_PORT> is established, expired or deleted.

```
IPsec-SA <established|expired>: ESP/<Transport|Tunnel> <LOCAL_IP_PORT>-><REMOTE_IP_PORT>
```

A Transport mode or Tunnel mode IPSec SA between <LOCAL\_IP\_PORT> and <REMOTE\_IP\_PORT> is established or expired.

```
<initiate|respond> new phase <1|2> negotiation: <LOCAL_IP_PORT><=><REMOTE_IP_PORT>
```

After an ISAKMP SA or IPSec SA is expired, new IKE phase 1 or 2 negotiation between <LOCAL\_IP\_PORT> and <REMOTE\_IP\_PORT> is initiated or responded.

NOTIFY: the packet is retransmitted by <IP\_PORT>

Packets of IKE negotiation are retransmitted due to the failure in authentication (pre-shared keys of the two entities might not be correspondent with each other).

```
<IP> INFO: request for establishing IPsec-SA was queued due to no phase1 found.
```

Request for establishing IPSec SA from <IP> was queued due to the failure in phase 1 negotiation (Phase 1 proposals of the two entities might not be correspondent with each other).

```
<IP> INFO: received INITIAL-CONTACT
```

```
<IP> received the request for negotiation from the peer.
```

```
ERROR: phase1 negotiation failed due to time up.
```

A queued or retransmitted phase 1 negotiation is declared to failure because the time is up.

```
<IP> ERROR: notification NO-PROPOSAL-CHOSEN received in informational exchange.
```

<IP> does not receive any proposal in the phase 2 negotiation messages (Phase 2 proposals of the two entities might not be correspondent with each other).

See "[IPSec VPN](#)" for further information.

## System

### Admin session

- <account> logged in from <ip>
- <account> logged out from <ip>

### Account change

- Administrator account <account> removed
- Monitor account <account> removed
- Administrator account <account> password successfully changed
- Administrator account <account> successfully added
- Monitor account <account> password successfully changed
- Monitor account <account> successfully added

## Access deny

- Incorrect <account> password from <ip>
- Maximum # of Administrator/<account> login reached
- Maximum # of Monitor/<account> login reached

## UI command

- There is no slave
- Configuration synchronization finished successfully
- Configuration synchronization failed
- Peer information is not available
- ARP caches are updated
- Neighbor Discovery caches are updated
- System time synchronized
- No NTP servers in system settings
- License key <key> is applied successfully, system rebooting...
- License key <key> is applied successfully
- Test email is sent to <receiver>
- Failed to send test email to <receiver>

## UI setting

- Settings are applied for page System -> <page name>
- Settings are applied for page Service -> <page name>
- Settings are applied for page Log -> <page name>
- Unable to add account. The maximum number of Administrator accounts have been reached.
- Unable to add account. The maximum number of Monitor accounts have been reached.
- Settings are applied for RADIUS Authentication
- Error starting notification daemon
- Error in starting daemon for page Service -> Internal DNS
- Error in starting daemon for page Service -> Multihoming

## Info access error

- Cannot save log/event settings

## Update

- System firmware updated

## Config

- System configuration restored
- Multihoming daemon file write error

## Shutdown

- System reset to factory default settings
- System reboot

## Instant push

- Pushing <logtype> is initiated
- Failed to push <logtype>

## Service error

- Restarting Internal DNS Error

## Connection overflow

- Current Connection Number(<connections>) reach <limit>

## Rate overflow

- Current Rate Number(<connection rate>) reach <limit>

## Undefined code

- Undefined event code <event code>

## VRRP

- VRRP become master
- VRRP become backup
- VRRP double-check failed

## HA

- Peer version changed from "<Model>" to "<Model>"
- Peer serial number changed from "<Serial Number>" to "<Serial Number>"
- Peer state changed from "<State>" to "<State>"
- Responded to Slave's Time Synchronization Request
- Responded to Slave's Configuration Synchronization Request
- Stopped configuration synchronization due to errors
- Finished configuration synchronization with the Slave
- Won precedence over the booting peer. Enter the Master state.
- Preceded by the booting peer. Enter the Slave state.
- Master heartbeat detected. Enter the Slave state.
- Slave heartbeat detected. Enter the Master state.
- Panic heartbeat detected. Enter the Master state.
- No heartbeat detected. Enter the Master state.

- Won precedence over the incompatible peer. Enter the Master state.
- Preceded by the incompatible peer. Enter the Panic state.
- Peer heartbeat stopped. Enter the Master state to take over services.
- Preceded by another Master. Reboot to enter the Slave state.
- Too Much port down. Reboot to enter the Slave state.
- Preceded by the incompatible peer. Enter the Panic state.
- Peer heartbeat stopped. Enter the Master state to take over services.
- Two Slaves linked at the same time. Restart HA after random delay.
- Master is gone. Enter the Master state to take over services.
- Peer heartbeat stopped
- Time synchronization failed.
- Configuration synchronization failed.

## Log Control

Control sets to forward data from FortiWAN to servers via FTP, E-mail and Syslog (protocol) for archiving and analysis. Configure log push method one log type by another, or use “Copy Settings to All Other Log Types”. It copies and applies settings of one log type to others avoiding unnecessary duplicating of settings.

**Log Type :** Select log type to be forwarded to servers.

- System Log
- Firewall Log
- NAT Log
- Auto & Persistent Routing Log
- Virtual Server Log
- BM Log (Bandwidth Management)
- Connection Limit Log
- Cache Redirect Log
- Multihoming Log
- Backup Line Log
- Dynamic IP Log
- IP-MAC Mapping Log
- Tunnel Routing Log
- IPSec

**Copy Settings to All Other Log Types :** Copy and apply settings of a log type to other ones.

**Method :** E-Mail, FTP and Syslog

**Push Now :** Click this button and logs are pushed immediately.

**Push Log When Out of Space :** Check Enable to avoid losing data in case of space shortage.

**Enable Scheduled Push** : Check to enable pushing schedule.

**Initial Time** : Start time for scheduled push.

**Period** : Duration for scheduled push.

## Methods

FortiWAN transfer logs with FTP, Email and Syslog. It either forwards logs to external FTP server, administrator's mail account via SMTP or a remote syslog servers.

### FTP

**Server** : FTP Server's IP or domain name

**Account** : FTP user account

**Password** : FTP user password

**Path** : FTP server path

### E-Mail

**SMTP Server** : SMTP server for logging

**Account** : Authenticated account for mail server

**Password** : Authenticated password for mail server

**Mail From** : Sender

**Mail To** : Receiver(s). Separate receivers with ",", or ".".

### Syslog

**Server** : IP address of remote syslog server.

**Facility** : Assign a facility to the logging message to specify the program type.

Note: If the Server is applied with a FQDN, then the DNS Server must be set in the Web UI [System]->[Network Settings]->[DNS Server] (See "[Set DNS server for FortiWAN](#)").

## Notification

Two methods are provided to send out the notifications for important system events: E-mail and SNMP trap. Please configure the settings for the methods and select the event type to notify.

## E-Mail Settings

The table below summarizes the event notification mail setup:

|                             |                                                                                                                                                                                                          |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SMTP Server</b>          | SMTP Server                                                                                                                                                                                              |
| <b>SMTP Port</b>            | When SSL is enabled, specify the port (465 by default) that the SSL encrypted SMTP is using.<br><br>When SSL is disabled, specify the port (25 by default) for STARTTLS encrypted or non-encrypted SMTP. |
| <b>SSL</b>                  | Check to enable SMTP transfers over SSL via the specified port, or STARTTLS will be performed if the SMTP server supports it.                                                                            |
| <b>Account</b>              | Authenticated account for the mail server                                                                                                                                                                |
| <b>Password</b>             | Authenticated password for the mail server                                                                                                                                                               |
| <b>Mail From</b>            | Sender                                                                                                                                                                                                   |
| <b>Mail To</b>              | Receiver(s). Separate receivers with “,” or “.”.                                                                                                                                                         |
| <b>Send Test E-mail Now</b> | Click the button to run test for the email settings above.                                                                                                                                               |

Note: If the SMTP Server is applied with a FQDN, then the DNS Server must be set in the Web UI **System > Network Settings > DNS Server** (See "[Set DNS server for FortiWAN](#)").

## SNMP Trap Settings

Event notification can also be sent via SNMP traps. These can only be sent if there is an existing SNMP manager for receiving FortiWAN's SNMP traps.

|                       |                             |
|-----------------------|-----------------------------|
| <b>Destination IP</b> | The SNMP managing device IP |
| <b>Community Name</b> | Community name              |



## Types of Events to Notify

| Event Types to Notify |                                        | Check to select the events. Enter the threshold to number of connections, rate of connections and total WAN traffic to trigger the notification.                                                  |
|-----------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | WAN link failure and recovery          | Send notification when a WAN link fails or recovers from failure. A integer used to indicate the failed or recovered WAN link.                                                                    |
|                       | Account change                         | Send notification when an account is added, removed or password-changed.                                                                                                                          |
|                       | HA slave failure and recovery          | Send notification when the slave unit in HA deployment fails or recovers from failure. Integer 1 indicates the slave unit recovered and integer 2 indicates it failed.                            |
|                       | HA takeover                            | Send notification when the local unit in HA deployment was took over by its slave unit. Integer 1 indicates the truth of HA takeover and integer 2 indicates the falseness of HA takeover.        |
|                       | VRRP takeover                          | Send notification when the local unit in VRRP deployment was took over by its backup unit. Integer 1 indicates the truth of VRRP takeover and integer 2 indicates the falseness of VRRP takeover. |
|                       | Number of connections reaches ____     | Set the threshold and the number of connections being processed in system will be sent as an event notification when it exceeds the threshold.                                                    |
|                       | Rate of connections reaches ____ / sec | Set the threshold and the number of connections established in system every second will be sent as an event notification when it exceeds the threshold.                                           |
|                       | Total WAN traffic reaches ____ Kbps    | Set the threshold and the number of current total WAN traffic (sum of inbound and outbound traffic of every WAN link) will be sent as an event notification when it exceeds the threshold.        |
| <b>Select All</b>     | Click to check all the event types     |                                                                                                                                                                                                   |
| <b>Clear All</b>      | Click to uncheck all the event types   |                                                                                                                                                                                                   |

## Enable Reports

FortiWAN's Reports provides long-term and advanced data analysis by processing system logs to database. The original logs FortiWAN generates contains raw data which is yet to be processed, and Reports can organize and analyze these data into readable statistics.

Every FortiWAN unit embeds the Reports system (See "[Reports](#)"), or the Reports could be also a stand-alone system running on a computer. Here is the settings to specify the ways of log push for Reports servers.

### Embedded Reports

**Enable Reports DB** : Enable the embedded Reports (See "[Reports](#)"). Logs will be processed directly to the database stored in the built-in hard disk. Analysis and statistics are displayed via Web UI.

The Reports displays no data without enabling this.

### Stand-alone Reports

**Enable Reports UDP** : Enable it to push logs to specified stand-alone Reports server.

**Recipient IP Address** : Specify location of the stand-alone Reports server that logs are pushed to. This field is available only if Enable Reports UDP is checked.

The stand-alone Reports displays no data without enabling this.

A stand-alone Reports and the embedded Reports can run at the same time, but both servers use the same logs.

### Events

Select the log type for FortiWAN to send to Reports.

- Firewall
- Virtual Server
- Bandwidth Usage
- Connection Limit
- Multihoming
- Tunnel Routing

Selected logs here will be pushed to embedded Reports and stand-alone Reports, if any or both of them are enabled.

# Reports

Reports is the built-in monitoring and traffic pattern analysis tool for instant status of WAN connections and traffic statistics analysis. MIS personnel can perform offline and more detailed analysis of the data to gain insight into user traffic patterns for better network design and management policy definition. However, FortiWAN generates large volumes of raw activity logs during the process of monitoring its functions. For long-term or trend analysis, Reports is an online companion tool that greatly simplifies the analysis of the data.

## Reports Features

- Provides historical detail and reporting over longer periods of time (See "[Create a Report](#)").
- Provides more fine-grained subcategories of analysis and reports (See "[Advanced Functions of Reports: Drill in](#)").
- Provides customized filters on reports (See "[Advanced Functions of Reports: Custom Filter](#)").
- Provides instant email of reports in PDF formats (See "[Advanced Functions of Reports: Report Email](#)").
- Reports can be saved in PDF format (See "[Advanced Functions of Reports: Export](#)").
- Supports user-select report date range (See "[Create a Report](#)").
- Supports user-specified backup of original log and database data (See "[Reports Database Tool](#)").

Reports provides analysis and reporting capabilities on device status, top bandwidth utilization and function status. MIS personnel can gain complete understanding of the detailed network statistics via the various reports. Such statistics include, for example, the exact time of failure of every WAN link, the peak rate and amount of bandwidth of every WAN link, the minimum and maximum traffic volume for a given specified day range, the traffic volume and service conditions of a certain server during a specified day range. Bandwidth Usage presents the analysis of how the bandwidth of every WAN link is used: what connections are constructed between which internal IP and external IP hosts, what services operate on the connections, and what and how much traffic is transferred through which WAN link? For example, you can obtain, from Reports analysis, the external traffic destinations from any or all devices inside the LAN or look at what internet servers attracted the most traffic from your enterprise.

It is important to have a solid grasp of the functionality and operational theory of Reports in order to effectively analyze network traffic patterns and various statistics of FortiWAN for optimal management policy definition.

Reports reporting function is calendar-based (in the upper right portion of the UI screen). Reporting can be done for a specific day, by highlighting that date in the calendar. Reporting can be done over a range of dates by specifying the start date and the end date on the Calendar.

Reports reporting function is divided into three categories and eighteen subcategories:

- Device Status: Dashboard, Bandwidth, CPU, Session, WAN Traffic, WAN Reliability, WAN Status, TR Reliability and TR Status (See "[Device Status](#)").
- Bandwidth Usage: In Class, Out Class, WAN, Service, Internal IP and Traffic Rate (See "[Bandwidth Usage](#)").
- Function Status: Connection Limit, Firewall, Virtual Server and Multihoming (See "[Function Status](#)").

**To make those data and analysis available, please enable Reports via Log > Reports (See "[Enable Reports](#)") or Reports > Settings > Reports (See "[Settings > Reports](#)").**

## Create a Report

Report's reporting function is calendar-based (in the upper right portion of the UI screen). Reporting can be done for a specific day, by highlighting that date in the calendar. Reporting can be done over a range of dates by specifying the start date and the end date on the Calendar.

### Enable Reports

Please complete the necessary setting to **enable FortiWAN Reports** via Log > Reports (See "[Enable Reports](#)") or Reports > Settings > Reports (See "[Settings > Reports](#)"), or data is unavailable for Reports.

### Select a Report Type

On the left of the main page is the Category Area where you can select a report type.

### Specify a Date or Date Range

At the upper right corner of the Display Area exists a date selector where you can specify a single date or date range. Click on the magnifier icon next to the date selector to start with date selection.

- Time between 00:00 to 23:59 (of a selected date)
- Days from start to end if Date Range specified (max 90 days)

### Single Date

Start date:

- Click on the field under "Start date" to call up a calendar for further selection.
- Select a date from the calendar, and reports will be generated on the selected date from 00:00 to 23:59. The selected date is highlighted in white, while the other dates are displayed in gray, and today's date is circled in yellow.
- Click the right or left arrow to go to the next or previous month.
- Click Apply to complete date selection, and reports will then be generated accordingly.
- Choose a different report type from the Category Area to generate reports on the same date selected if needed.

### Date Range

To select a date range:

The screenshot displays a date range selection dialog. On the left, the 'Start date' field contains '2016-10-03' and the 'Start time' field contains '00:00'. On the right, the 'End date' field contains '2016-10-07' and the 'End time' field contains '24:00'. A 'To' checkbox is checked between the two date pickers. At the bottom right, there are 'Cancel' and 'Apply' buttons.

- Click the checkbox between Start date and the End date, and then Start time, End date and End time will become available for selection (as shown below):
- Put a Start date and End date by clicking the input field and selecting from the calendar.
- Input the Start time and End time in the format of HH:MM. Note that the duration cannot exceed 90 days.
- Click Apply to complete date range selection and start generating reports.
- Choose a different report type from the Category Area to generate reports on the same date range selected if needed.

## Export and Email

All reports generated by FortiWAN can be exported in PDF format to your local computer; just simply click the Export button on the upper side of any report page, and select PDF.

All reports generated by FortiWAN can be sent to users via email. Reports saved in PDF format can be sent out as email attachments. Click the Email button on the right upper corner of any report page to edit settings of the report email. In the settings dialog, you may send current report through email immediately or arrange a scheduled email for it. No matter which report page you're at, you can always click the Email button on that page to send the current report through email, or the Schedule button to get the report email scheduled (see [Report Email](#)).

## Device Status

The Device Status report shows the top-level view of the analysis of the traffic flowing through FortiWAN. Device Status includes 9 categories showing the average data rate through FortiWAN, the number of sessions (connections) in use, the status of WAN links and TR connections and FortiWAN hardware statistics.

## Bandwidth

The Bandwidth report shows the traffic distribution by the date range defined. Your FortiWAN model is rated by its data throughput (and number of simultaneous connections). This report will help you determine if you are using the correct FortiWAN model and bandwidth capability for the data volumes at our location.

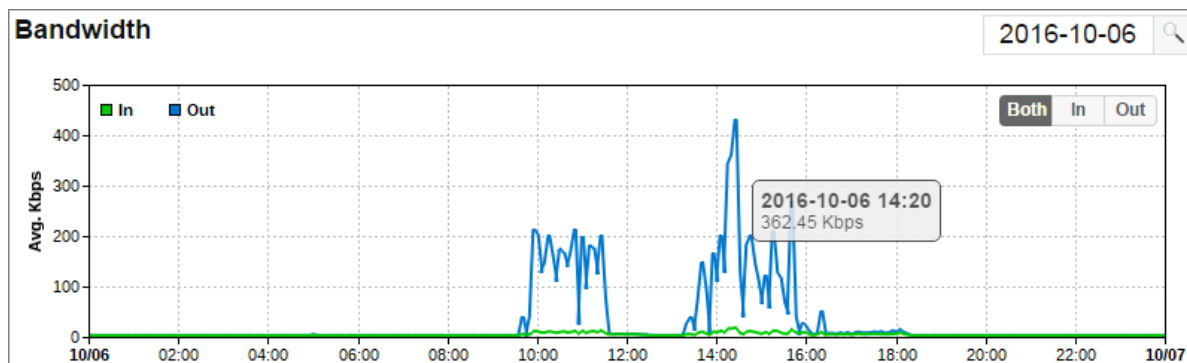
Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").

### Bandwidth Distribution:

- X axis: Time between 00:00 to 23:59 (of a selected date). Days from start to end if Date Range specified (max 90 days).
- Y axis: Bandwidth in Kbps or Mbps.
- Green indicates inbound data rate.
- Blue indicates outbound data rate.
- Clicking on Both, In or Out buttons at the right upper corner of the graph allows you to see bandwidth distribution in different directions:
- Both: Displays both inbound and outbound bandwidth distribution.

- In: Displays only inbound bandwidth distribution.
- Out: Displays only outbound bandwidth distribution.
- Moving the mouse over the graph will display time, date and corresponding traffic distribution (as shown below):



### Statistics Table:

- Lists the average inbound and outbound traffic rate distributed by the date range defined. This is the numerical presentation of the same information in the Bandwidth Distribution Charts.
- Time: Time periods or dates if a date range is defined.
- Inbound bps: Traffic originating from outside of FortiWAN, going into the internal port.
- Outbound bps: Traffic originating from inside of FortiWAN, going to the external port.

## CPU

The CPU report shows the distribution of CPU usage of FortiWAN by the date range defined. CPU usage is a measure of how much traffic is being managed or how much services the FortiWAN is required to do on that traffic. Sustained usage near 80% is a good indicator that a larger FortiWAN model is required to handle the required traffic and services load. Use this chart to compare your target maximum usage with the actual usage over time.

Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").

### CPU Usage Distribution

- X axis: Time between 00:00 to 23:59 (of a selected date). Days from start to end if Date Range specified (max 90 days).
- Y axis: CPU usage in %.
- Moving the mouse over the graph will display time, date and corresponding CPU usage in percentage.

### Statistics Table

- Lists the CPU usage distributed in percentage (%) by the date range defined. This is the numerical presentation of the same information in the CPU Usage Distribution Charts.
- Time: Time periods or dates if a date range is defined.
- % Usage: CPU usage in %.

## Session

The Session report shows the distribution of sessions (connections) by the date range defined. Your FortiWAN model is rated by the number of simultaneous connections it can process (among other things as noted above). This report will help you determine if you are using the correct FortiWAN model for the number of connections in use by your users.

Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").

### Session Amount Distribution:

- X axis: Time between 00:00 to 23:59 (for a selected date). Days from start to end if Date Range specified (max 90 days).
- Y axis: Number of Sessions in 1,000's.
- Moving the mouse over the graph will display time, date and corresponding number of sessions.

### Statistics Table:

- Lists the number of sessions distributed by the date range defined. This is the numerical presentation of the same information in the Session Distribution Charts.
- Time: Time periods or dates if a date range is defined.
- Count: Number of Sessions.

## WAN Traffic

The WAN Traffic report shows the traffic distribution of every FortiWAN's WAN link by the date range defined. This report will help you to determine if WAN links are capable for the data volumes.

Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").

### WAN Traffic Distribution

- Traffic distributions of every WAN links are presented individually.
- X axis: Time between 00:00 to 23:59 (of a selected date). Days from start to end if Date Range specified (max 90 days).
- Y axis: Bandwidth in Kbps or Mbps.
- Green indicates inbound data rate.
- Blue indicates outbound data rate.
- Clicking on Both, In or Out buttons at the right upper corner of the graph allows you to see bandwidth distribution in different directions:
- Both: Displays both inbound and outbound bandwidth distribution.
- In: Displays only inbound bandwidth distribution.
- Out: Displays only outbound bandwidth distribution.
- Moving the mouse over the graph will display time, date and corresponding traffic distribution.

## WAN Reliability

The WAN Reliability report shows the statistics on the failures happened on FortiWAN WAN links.

Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").

### Statistics Table

- Lists the times of failure happened on WAN links by the date range defined.
- WAN: WAN links that are enabled on FortiWAN. (Disabled WAN links will not be shown in the table).
- Fails: Times of failure happened on this WAN link.
- Drill in: Click to check the status (OK and Fail) over time on this WAN link (See "[Drill In](#)").

## WAN Status

FortiWAN supports various numbers of WAN links, for example, FortiWAN 700 supports 25 WAN links, FortiWAN 5000 and FortiWAN 6000 support 50 WAN links. The WAN Status report shows the statuses on every FortiWAN's WAN link. The various statuses are defined as below.

- OK: WAN link is enabled, configured and connected physically.
- Fail: WAN link is enabled and configured, but disconnected.
- Disable: WAN link is not enabled from FortiWAN Web UI.

Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").

### Statistics Table

- Lists the statuses of every WAN link by the date range defined.
- Time: Time periods or dates if a date range is defined.
- WAN: The WAN link.
- Status: The status happened on the WAN link at the time.

## TR Reliability

Tunnel Routing (TR) is FortiWAN's important function used to construct intranets between multiple LANs anywhere in the world. Tunnel Routing also boosts performance by supporting link aggregation and fault tolerance over multiple links for services such as VPN and live video streaming. A Tunnel Group represents the configuration of Tunnel Routing on FortiWAN between two specific sites; it includes related internal IP addresses of both sites and routing policies between sites (See "[Tunnel Routing](#)").

The TR Reliability report shows the statistics on the failures happened on FortiWAN's TR links. Please reference FortiWAN User Manual for more information about Tunnel Routing.

Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").



## Statistics Table

- Group: Tunnel Group configured on FortiWAN; the failed TR link belongs to. Select "Group" as primary sorting via clicking on the column title "Group".
- Local IP: Local IP address of the failed TR link in the Tunnel Group. Select "Local IP" as primary sorting via clicking on the column title "Local IP".
- Remote IP: Remote IP address of the failed TR link in the Tunnel Group. Select "Remote IP" as primary sorting via clicking on the column title "Remote IP".
- Fails: the count of failures occurring on the IP pair in this Tunnel Group for the reporting period.
- Drill in: Click to check the status (OK and Fail) of the TR link (See "[Drill In](#)").
- Note: A "▲" or "▼" is shown aside the column header while the column is selected as primary sorting, e.g. Group ▲. The sorting order will be switched by clicking on the same column header.

## TR Status

The TR Status report shows the statuses of every FortiWAN's TR link (See "[Tunnel Routing](#)") by date the range defined.

Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").

The various statuses are defined as below.

- OK: TR link is enabled, configured and connected physically.
- Fail: TR link is enabled and configured, but disconnected.
- Disable: TR link is not enabled from FortiWAN Web UI.

### Statistics Table

- Lists the statuses of every TR link by the date range defined.
- Time: Time periods or dates if a date range is defined.
- Local IP: Local IP address of the TR link.
- Remote IP: Remote IP address of the TR link.
- Status: the OK/Fail Status of this Source IP -> Destination IP pair at that time.

## Bandwidth Usage

This report category is the core function of the Reports and also serves as the basis for traffic analysis to gain insights for better policy management. This category can further be divided into In Class, Out Class, WAN, Service, Internal IP and Traffic Rate.

The Bandwidth Usage Report includes: Charts (upper) and Statistics Table (lower).

- Pie Charts display respective percentage of all the traffic patterns that sorted (default) by the total data volume (IN + OUT) shown on the page. The Pie Charts display will change depending upon which column in the Statistics Table is selected for primary sorting. This Pie Chart shows the percentage of the traffic pattern of the top 10 items only, which might not match the percentage value listed in the Statistics Table. Use it only as a visual reference to see who the major users are.

- Bar Charts illustrate the total volume of each traffic pattern shown on the page, and the percentage of each traffic pattern out of total traffic. The Bar Chart display will change depending upon which column in the Statistics Table is selected for primary sorting.
- The Statistics Table is the numerical presentation of the same information illustrated in the Pie chart and Bar Charts. The traffic statistics includes information of total traffic, inbound traffic, outbound traffic and percentage of total traffic.
  - Inbound Bytes: The volume of traffic originating from outside of FortiWAN, going into the internal network.
  - Outbound Bytes: The volume of traffic originating from inside of FortiWAN, going to the external network.
  - Total Bytes: (Default primary sorting) The volume of total traffic = Inbound Bytes + Outbound Bytes.

The statistics table lists 10, 20, 50 or 100 entries sorted by default in declining order by total data volume. By default the first screen shows the top 10 entries, but navigation buttons and a direct-entry page box at the lower right corner of the screen allow you to examine all items found. The default number of rows to be listed on the report page can be defined in account settings.

The Statistics Table may be re-sorted by Inbound Bytes, Outbound Bytes or Total Bytes, by selecting the appropriate column header. The Pie and Bar charts will reformat to reflect the selected traffic measurement.

Note that the percentage of total traffic shown in the Statistics Table may not be the same as that shown on the Pie Chart. The Statistics Table shows the percentage of total traffic in all traffic patterns, while the Pie Chart only shows the total of the top 10 traffic users.

See also:

- [Report: Inclass](#)
- [Report: Outclass](#)
- [Report: Service](#)
- [Report: WAN](#)
- [Report: Internal IP](#)
- [Report: Traffic Rate](#)

## Inclass

This report shows the statistics of each inbound class as defined in FortiWAN's Bandwidth Management function (See "[Bandwidth Management](#)"). Each class is a classification (by service, by IP address and etc.) of incoming traffic passed through FortiWAN. This statistic will help you realize if the Bandwidth Management policies of FortiWAN are running well, or if any adjustment is necessary for the specified bandwidth class.

Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").

- Pie Chart: Pie chart of traffic statistics is generated based on Inbound Classes of FortiWAN's Bandwidth Management.
- Bar Chart: Bar chart statistics show the actual data volume used by the top 10 Inbound Classes.
- Statistics Table:
  - List the Inbound Class the most traffic being classified into.
  - In Class: The Inbound Classes defined in FortiWAN.
  - Inbound Bytes: The volume of inbound traffic of the Inbound classes.
  - Outbound Bytes: The volume of outbound traffic of the Inbound Classes.

- Total Bytes: The volume of total traffic of the Inbound Classes (Inbound Bytes + Outbound Bytes).
- Note: Select "Inbound Bytes", "Outbound Bytes" or "Total Bytes" as primary sorting by clicking on the column title. A "▲" is shown aside the column header while the column is selected as primary sorting, e.g. Inbound Bytes ▲.
- % Total Bytes: The volume of total traffic of the Inbound Classes in %.
- % Inbound Bytes: The volume of inbound traffic of the Inbound Classes in %.
- % Outbound Bytes: The volume of outbound traffic of the Inbound Classes in %.
- Only one of the three statistics data (% Inbound Bytes, % Outbound Bytes, or % Total Bytes) will be displayed in the statistics table depending on the primary sort column.
- This page and this table describe total traffic volume, not traffic rate. Data transferred are measured in KBytes, MBytes or GBytes over the period of time selected.
- Drill in (See "[Drill In](#)"):
  - Clicking the magnifier icon located under the "Drill in" column in the statistics table allows you to perform an additional 'drill-down' analysis on traffic for the selected In Class, shown by Out Class, WAN, Service, Internal IP, External IP, Internal Group, External Group and Traffic Rate (Trend) via the selected policy In Class:
  - Out Class – Out Classes that are associated with this In Class.
  - WAN – WAN links that are associated with this In Class.
  - Service – Services (L3-L7) that are associated with this In Class.
  - Internal IP – Any monitored internal IP addresses that are associated with this In Class.
  - External IP – Any monitored external IP addresses that are associated with this In Class.
  - Internal Group – Any monitored internal IP group (set up under the Settings menu) that the internal IP addresses are associated with this In Class.
  - External Group – Any monitored external IP group (set up under the Settings menu) that the external IP addresses are associated with this In Class.
  - Traffic Rate: bandwidth distribution generated by this In Class by the date range defined.

## Outclass

This report shows the statistics of each outbound class as defined in FortiWAN's Bandwidth Management function (See "[Bandwidth Management](#)"). Each class is a classification (by service, by IP address and etc.) of outgoing traffic passed through FortiWAN.

Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").

- Pie Chart: Pie chart of traffic statistics is generated based on Outbound Classes of FortiWAN's Bandwidth Management.
- Bar Chart: Bar chart statistics show the actual data volume used by the top 10 Outbound Classes.
- Statistics Table:
  - List the Outbound Class the most traffic being classified into.
  - Out Class: The Outbound Classes defined in FortiWAN.
  - Inbound Bytes: The volume of inbound traffic of the Outbound Classes.
  - Outbound Bytes: The volume of outbound traffic of the Outbound Classes.
  - Total Bytes: The volume of total traffic of the Outbound Classes (Inbound Bytes + Outbound Bytes).

- Note: Select “Inbound Bytes”, “Outbound Bytes” or “Total Bytes” as primary sorting by clicking on the column title. A “▲” is shown aside the column header while the column is selected as primary sorting, e.g. Inbound Bytes ▲.
- % Total Bytes: The volume of total traffic of the Outbound Classes in %.
- % Inbound Bytes: The volume of inbound traffic of the Outbound Classes in %.
- % Outbound Bytes: The volume of outbound traffic of the Outbound Classes in %.
- Only one of the three statistics data (% Inbound Bytes, % Outbound Bytes, or % Total Bytes) will be displayed in the statistics table depending on the primary sort column.
- This page and this table describe total traffic volume, not traffic rate. Data transferred are measured in KBytes, MBytes or GBytes over the period of time selected.
- Drill in (See ["Drill In"](#)):
  - Clicking the magnifier icon located under the “Drill in” column in the statistics table allows you to perform an additional ‘drill-down’ analysis on traffic for the selected policy Out Class, shown by In Class, WAN, Service, Internal IP, External IP, Internal Group, External Group and Traffic Rate (Trend) via the selected policy Out Class:
  - In Class – In Classes that are associated with this Out Class.
  - WAN – WAN links that are associated with this Out Class.
  - Service – Services (L3-L7) that are associated with this Out Class.
  - Internal IP – Any monitored internal IP addresses that are associated with this Out Class.
  - External IP – Any monitored external IP addresses that are associated with this Out Class.
  - Internal Group – Any monitored internal IP group (set up under the Settings menu) that the internal IP addresses are associated with this Out Class.
  - External Group – Any monitored external IP group (set up under the Settings menu) that the external IP addresses are associated with this Out Class.
  - Traffic Rate: bandwidth distribution generated by this Out Class by the date range defined.

## WAN

This report shows the statistics of traffic passed through FortiWAN via the WAN Links.

Create a report for a specific day or over a range of dates (See ["Create a Report"](#)).

Export reports and send reports through email (See ["Export and Email"](#)).

- Pie Chart: Pie chart of traffic statistics is generated based on WAN links defined on FortiWAN.
- Bar Chart: Bar chart statistics show the actual data volume used by the top 10 WAN links.
- Statistics Table :
  - List the WAN links on the FortiWAN that traffic passed through.
  - WAN: The WAN links defined on the FortiWAN.
  - Inbound Bytes: The volume of inbound traffic of the WAN links.
  - Outbound Bytes: The volume of outbound traffic of the WAN links.
  - Total Bytes: The volume of total traffic of the WAN links (Inbound Bytes + Outbound Bytes).
  - Note: Select “Inbound Bytes”, “Outbound Bytes” or “Total Bytes” as primary sorting by clicking on the column title. A “▲” is shown aside the column header while the column is selected as primary sorting, e.g. Inbound Bytes ▲.
  - % Total Bytes: The volume of total traffic of the WAN links in %.
  - % Inbound Bytes: The volume of inbound traffic of the WAN links in %.

- % Outbound Bytes: The volume of outbound traffic of the WAN links in %.
- Only one of the three statistics data (% Inbound Bytes, % Outbound Bytes, or % Total Bytes) will be displayed in the statistics table depending on the primary sort column.
- This page and this table describe total traffic volume, not traffic rate. Data transferred are measured in KBytes, MBytes or GBytes over the period of time selected.
- Drill in (See "[Drill In](#)"):
  - Clicking the magnifier icon located under the "Drill in" column in the statistics table allows you to perform an additional 'drill-down' analysis on traffic for the selected WAN link, shown by In Class, Out Class, Service, Internal IP, External IP, Internal Group, External Group and Traffic Rate (Trend) via the selected WAN link:
  - In Class – In Classes that traffic is passed through this WAN link.
  - Out Class – Out Classes that traffic is passed through this WAN link.
  - Service – Services (L3-L7) that traffic is passed through this WAN link.
  - Internal IP – Any monitored internal IP addresses that traffic is passed through this WAN link.
  - External IP – Any monitored external IP addresses that traffic is passed through this WAN link.
  - Internal Group – Any monitored internal IP group (set up under the Settings menu) that traffic is passed through this WAN link.
  - External Group – Any monitored external IP group (set up under the Settings menu) that traffic is passed through this WAN link.
  - Traffic Rate: bandwidth distribution generated by this WAN link by the date range defined.

## Services

This report shows the statistics of traffic passed through FortiWAN by various services.

Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").

- Pie Chart: Pie chart of traffic statistics is generated based on the traffic incurred by Services.
- Bar Chart: Bar chart statistics show the actual data volume used by the top 10 Services.
- Statistics Table:
  - List the Services generating (as a source or termination) the most traffic.
  - Service: The Service that traffic passed through FortiWAN.
  - Inbound Bytes: The volume of inbound traffic of the Service.
  - Outbound Bytes: The volume of outbound traffic of the Service.
  - Total Bytes: The volume of total traffic of the Service (Inbound Bytes + Outbound Bytes).
  - Note: Select "Inbound Bytes", "Outbound Bytes" or "Total Bytes" as primary sorting by clicking on the column title. A "▲" is shown aside the column header while the column is selected as primary sorting, e.g. Inbound Bytes ▲.
  - % Total Bytes: The volume of total traffic of the Service in %.
  - % Inbound Bytes: The volume of inbound traffic of the Service in %.
  - % Outbound Bytes: The volume of outbound traffic of the Service in %.
  - Only one of the three statistics data (% Inbound Bytes, % Outbound Bytes, or % Total Bytes) will be displayed in the statistics table depending on the primary sort column.
  - This page and this table describe total traffic volume, not traffic rate. Data transferred are measured in KBytes, MBytes or GBytes over the period of time selected.

- Drill in (See ["Drill In"](#)):
  - Clicking the magnifier icon located under the "Drill in" column in the statistics table allows you to perform an additional 'drill-down' analysis on traffic for the selected service, shown by In Class, Out Class, WAN, Internal IP, External IP, Internal Group, External Group and Traffic Rate (Trend) via the selected service:
  - In Class – In Classes where this Service traffic is classified into.
  - Out Class – Out Classes where this Service traffic is classified into.
  - WAN – WAN links that this Service traffic passed through.
  - Internal IP – Any monitored internal IP addresses that are associated with this Service.
  - External IP – Any monitored external IP addresses that are associated with this Service.
  - Internal Group – Any monitored internal IP group (set up under the Settings menu) that the internal IP addresses are associated with this Service.
  - External Group – Any monitored external IP group (set up under the Settings menu) that the external IP addresses are associated with this Service.
  - Traffic Rate: bandwidth distribution generated by this Service by the date range defined.

## Internal IP

This report shows the statistics of traffic passed through FortiWAN by Internal IP addresses.

Create a report for a specific day or over a range of dates (See ["Create a Report"](#)).

Export reports and send reports through email (See ["Export and Email"](#)).

- Pie Chart: Pie chart of traffic statistics is generated based on traffic incurred (as a source or termination) by Internal IP addresses.
- Bar Chart: Bar chart statistics show the actual data volume used by the top 10 Internal IP addresses.
- Statistics Table:
  - List the Internal IP addresses generating (as a source or termination) the most traffic.
  - IP: The Internal IP addresses.
  - Inbound Bytes: The volume of inbound traffic of the Internal IP addresses.
  - Outbound Bytes: The volume of outbound traffic of the Internal IP addresses.
  - Total Bytes: The volume of total traffic of the Internal IP addresses (Inbound Bytes + Outbound Bytes).
  - Note: Select "Inbound Bytes", "Outbound Bytes" or "Total Bytes" as primary sorting by clicking on the column title. A "▲" is shown aside the column header while the column is selected as primary sorting, e.g. Inbound Bytes ▲.
  - % Total Bytes: The volume of total traffic of the Internal IP addresses in %.
  - % Inbound Bytes: The volume of inbound traffic of the Internal IP addresses in %.
  - % Outbound Bytes: The volume of outbound traffic of the Internal IP addresses in %.
  - Only one of the three statistics data (% Inbound Bytes, % Outbound Bytes, or % Total Bytes) will be displayed in the statistics table depending on the primary sort column.
  - This page and this table describe total traffic volume, not traffic rate. Data transferred are measured in KBytes, MBytes or GBytes over the period of time selected.
- Drill in (See ["Drill In"](#)):
  - Clicking the magnifier icon located under the "Drill in" column in the statistics table allows you to perform an additional 'drill-down' analysis on traffic for the selected Internal IP address, shown by In Class, Out Class, WAN, Service, External IP, Internal Group, External Group and Traffic Rate (Trend) via the selected Internal IP address:
  - In Class – In Classes that are associated with this Internal IP address.

- Out Class – Out Classes that are associated with this Internal IP address.
- WAN – WAN links that are associated with this Internal IP address.
- Service – Services (L3-L7) that are associated with this Internal IP address.
- External IP – Any monitored external IP addresses that are associated with this Internal IP address.
- Internal Group – Any monitored internal IP group (set up under the Settings menu) where this Internal IP address belongs to.
- External Group – Any monitored external IP group (set up under the Settings menu) that the external IP addresses are associated with this Internal IP address.
- Traffic Rate: bandwidth distribution generated by this Internal IP address by the date range defined.

## Traffic Rate

This report shows the statistics of traffic passed through FortiWAN by Traffic Rate.

Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").

### Bandwidth Distribution:

- X axis: Time between 00:00 to 23:59 (of a selected date). Days from start to end if Date Range specified (max 90 days).
- Y axis: Bandwidth in Kbps or Mbps.
- Green indicates inbound data rate.
- Blue indicates outbound data rate.
- Clicking on Both, In or Out buttons at the right upper corner of the graph allows you to see bandwidth distribution in different directions:
- Both: Displays both inbound and outbound bandwidth distribution.
- In: Displays only inbound bandwidth distribution.
- Out: Displays only outbound bandwidth distribution.
- Moving the mouse over the graph will display time, date and corresponding traffic distribution.

### Statistics Table:

- List the average inbound and outbound traffic rate distributed by the date range defined. This is the numerical presentation of the same information in the Bandwidth Distribution Charts.
- Time: The time periods or date ranges defined.
- Inbound bps: The inbound traffic rate in the time periods or date ranges.
- Outbound bps: The outbound traffic rate in the time periods or date ranges.

### Drill in:

- Clicking the magnifier icon located under the "Drill in" column in the statistics table allows you to perform an additional 'drill-down' analysis on traffic for the selected Time period, shown by In Class, Out Class, WAN, Service, Internal IP, External IP, Internal Group and External Group via the selected Time period:
- In Class – In Classes that are associated within this time period.
- Out Class – Out Classes that are associated within this time period.
- WAN – WAN links that traffic passed through within this time period.

- Service – Services (L3-L7) that are associated within this time period.
- Internal IP – Any monitored internal IP addresses that are associated within this time period.
- External IP – Any monitored external IP addresses that are associated within this time period.
- Internal Group – Any monitored internal IP group (set up under the Settings menu) that the internal IP addresses are associated within this time period.
- External Group – Any monitored external IP group (set up under the Settings menu) that the external IP addresses are associated within this time period.

## Function Status

This report category is the function to monitor the status of FortiWAN's major functions for a long period. Long term statistics of function status is helpful to administrators. This category can further be divided into Connection Limit, Firewall, Virtual Server and Multihoming.

### Connection Limit

To prevent network congestion, FortiWAN's Connection Limit function limits the number of connections from each source IP. A Connection Limit event means the number of connections from a given source IP has exceeded the limit (See "[Connection Limit](#)"). Reports produces a summary report for Connection Limit events.

Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").

#### Statistics Table

- List the Source IP generating the most accesses while connections exceeding the limit, sorted by the volume of Drops in declining order.
- Source IP: The IP address generating connections exceeding the limit.
- Drops: The counts of denied access (try to construct new connection) while the connections exceeding the limit.

### Firewall

Firewall is the most popular tool to control network access and deny illegal access. FortiWAN's Firewall function limits network access by service, source IP and/or destination IP. A Firewall event means that network access has been denied according to the Firewall rules (See "[Firewall](#)"). Reports produces a summary report for Firewall events.

Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").

#### Statistics Table

- Lists the Service, Source IP and Destination IP of denied network access, sorted by the volume of Drops in declining order.
- Service: The Service of denied access.
- Source IP: The Source IP address of denied access.



- Destination IP: The Destination IP address of denied access.
- Drops: The counts of denied access.

## Virtual Server

FortiWAN's Virtual Server function the linking of multiple servers in an internal (or private) network to external network (public) IP addresses. It is usually used to share multiple servers with single public IP addresses – a simple server load balancing application (See "[Virtual Server & Server Load Balancing](#)"). Reports produces a summary and detailed report for Virtual Server.

Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").

### Statistics Table

- Lists the Virtual Server IP (Service) and count of access, sorted by the Server IP (default).
- WAN IP: the public IP address for external users to access the virtual server.
- WAN Service: the service for external users to access the virtual server.
- Server IP: the IP address of the Virtual Server.
- Server Service: the service ran on the virtual server.
- Requests: the count of accessing this Server Service ran on the Virtual Server IP from the WAN IP address.
- Note: Select "WAN IP", "WAN Service", "Server IP" and "Server Service" as primary sorting via clicking on the column title. A "▲" or "▼" is shown aside the column header while the column is selected as primary sorting, e.g. Server IP ▲. The sorting order will be switched by clicking on the same column header.

## Multihoming

FortiWAN's Multihoming function performs load balancing and fault tolerance between WAN links for inbound traffic. Users from the public network are told dynamically by FortiWAN the best available WAN link to access in order to reach specific resources on the internal network (See "[Inbound Load Balancing and Failover \(Multihoming\)](#)"). Reports produces a summary and detailed report for Multihoming.

Create a report for a specific day or over a range of dates (See "[Create a Report](#)").

Export reports and send reports through email (See "[Export and Email](#)").

### Statistics Table

- Lists the Domain Name and the count of the number of times this domain was accessed, sorted by the FQDN (default).
- FQDN: the domain name configured on FortiWAN. Select "FQDN" as primary sorting via clicking on the column title "FQDN".
- WAN: which WAN links this FQDN was accessed through. Select "WAN" as primary sorting via clicking on the column title "WAN".
- WAN IP: the WAN IP address in this FQDN accessed through the WAN link. Select "WAN IP" as primary sorting via clicking on the column title "WAN IP".
- Access: the counts of accessing this domain by external users via the WAN IP address.

- Note: Select “FQDN”, “WAN” and “WAN IP” as primary sorting via clicking on the column title. A “▲” or “▼” is shown aside the column header while the column is selected as primary sorting, e.g. FQDN ▲. The sorting order will be switched by clicking on the same column header.

## Advanced Functions of Reports

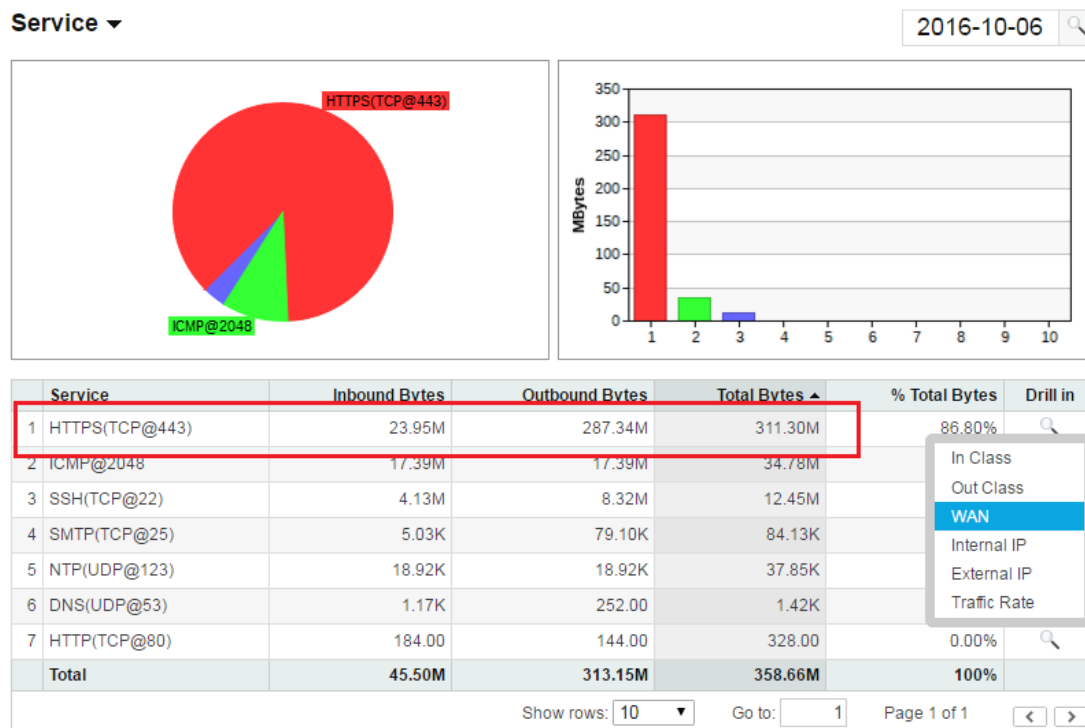
Reports provides advanced functions beyond the basic reports to give an accurate analysis. Drill In and Custom Filter are the functions about querying the reports with complex conditions. It delivers only the data that a user needs from large data sets. Export and Report Email are the functions about documentations and delivering of the on-line reports. The details of the advanced functions are described as follows.

### Drill In

There are 7 different query conditions for Bandwidth Usage, including In Class, Out Class, WAN, Service, Internal IP, External IP and Traffic Rate. In every Bandwidth Usage report, analysis can be further drilled-in to include more traffic data statistics; in other words, Reports allows traffic to be queried based on combination of multiple conditions. For example, select Service as the query subject from the menu in the category area, and the Service report will be displayed accordingly, as shown below:

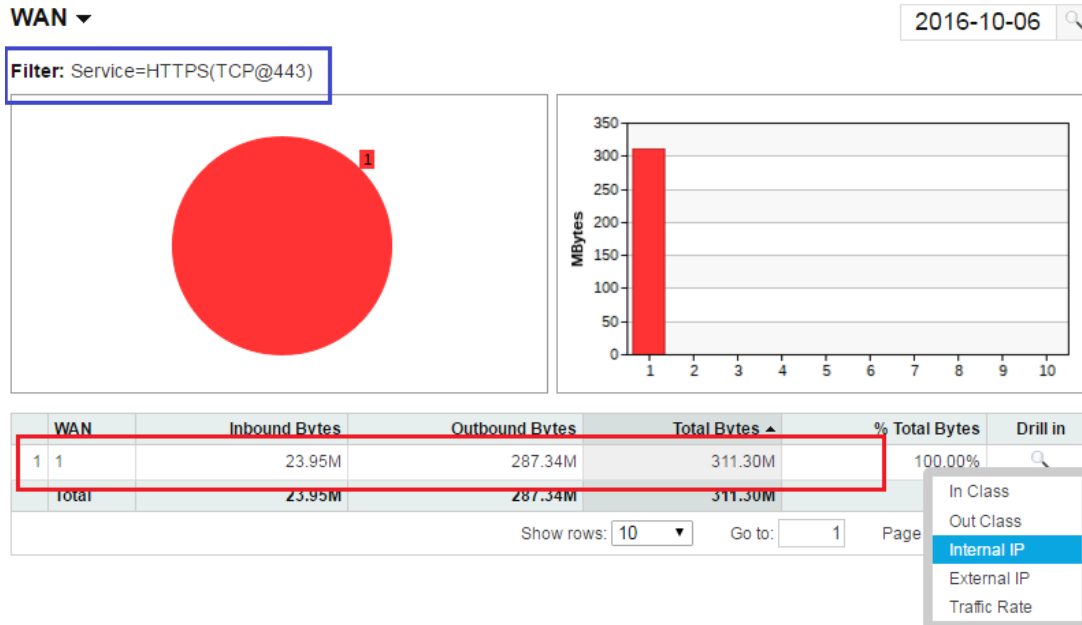
#### Service=All

Go to **Reports > Service**, you can have an overall service report which gives the traffic statistics of all the service usages (query result is as shown below).



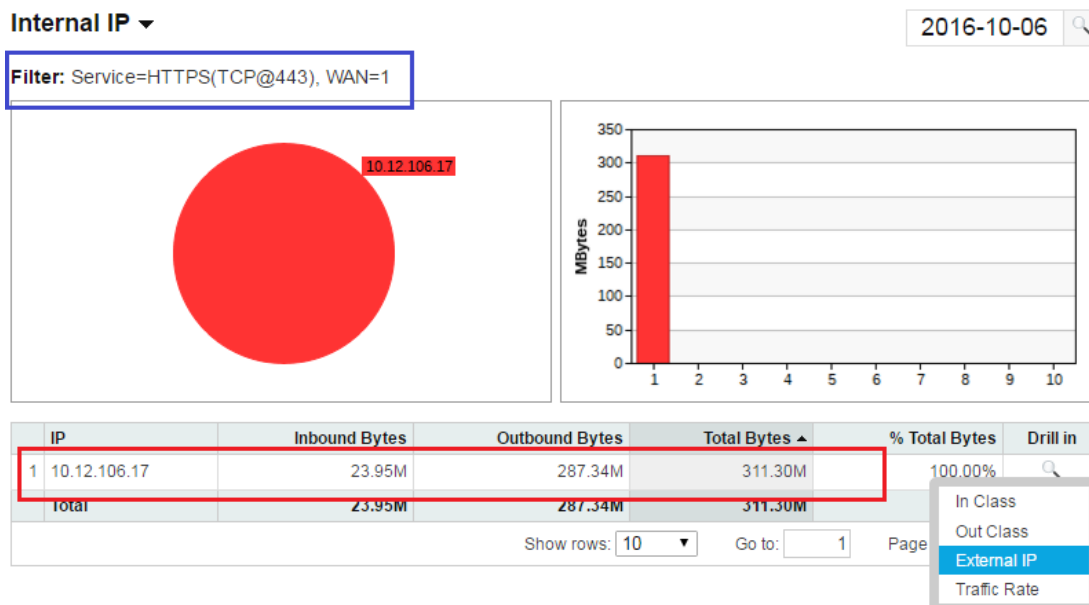
The HTTPS(TCP@443) service can be further drilled in to query which WAN link of FortiWAN are utilizing this service by clicking the Drill In magnifier icon in the row of HTTPS(TCP@443) listed in the table and select WAN (query result is as shown below):

### Service=HTTPS(TCP@443) & WAN=All



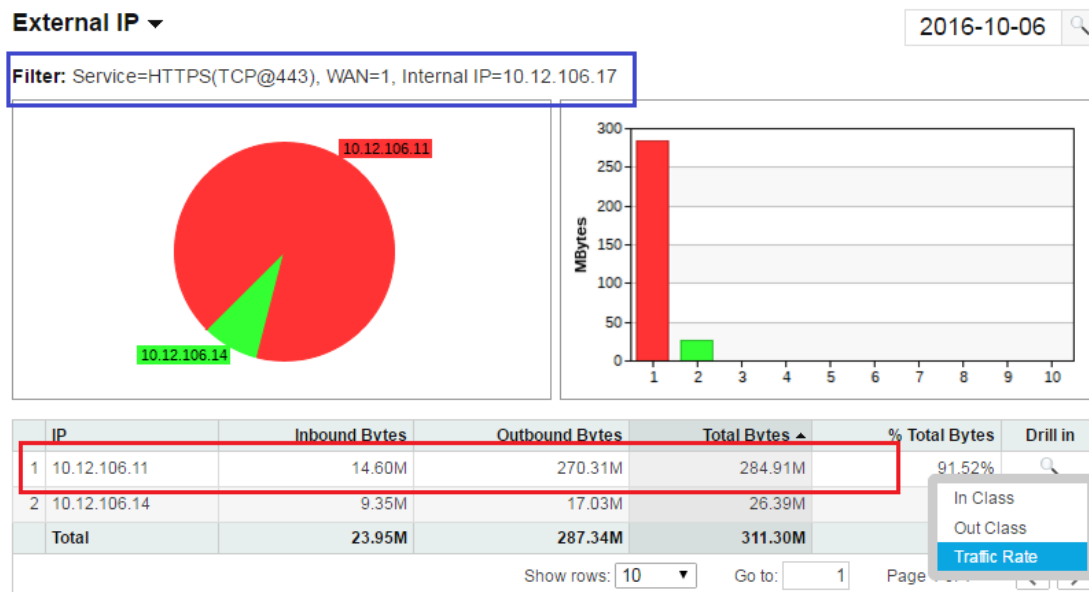
As indicated in the blue box (shown in the figure above), this page presents the data of HTTPS(TCP@443) traffic in the WAN report. In the statistics table, the WAN link 1 can be further drilled in to query what internal IP addresses are included by clicking the Drill In magnifier icon in the row of WAN 1 listed in the table and select Internal IP (query result is as shown below):

### Service=HTTPS(TCP@443) & WAN=1 & Internal IP=All



As indicated in the blue box (shown in the figure above), this page presents the data of Internal IP report that includes the traffic of WAN 1 (WAN) using HTTPS(TCP@443) (Service), The IP address: 10.12.106.17 can be further drilled in to query what External IP addresses it is connected to by clicking the Drill In magnifier icon in the row of 10.12.106.17 IP listed in the table and select External IP (query result is as shown below):

### Service=HTTPS(TCP@443) & WAN=1 & Internal IP=10.12.106.17 & External IP=All

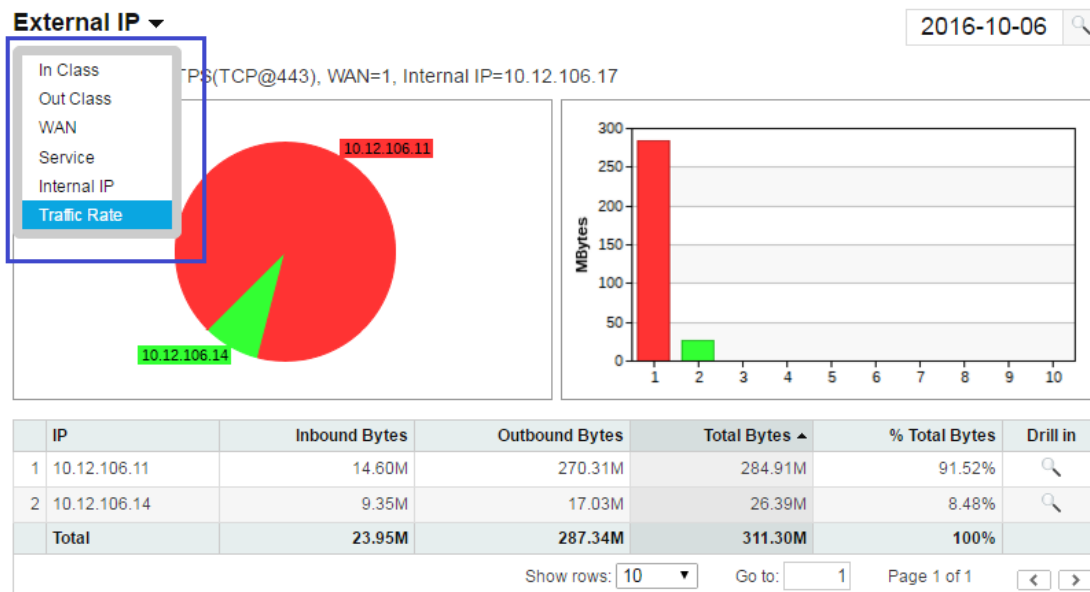


As indicated in the blue box (shown in the figure above), this page presents the data of External IP report that includes the traffic of WAN 1 (WAN) at internal IP=10.12.106.17 (Internal IP) using HTTPS(TCP@443) (Service).

From the example illustrated above, administrators can easily query the traffic flow based on combination of various conditions needed, while analysis can be drilled in to more details for better review. In the upper section of the report page, you'll see a summary of the query conditions used in the existing report (highlighted in blue as shown in the image above), making it clear for administrators to keep track of the query details.

### Service=HTTPS(TCP@443) & WAN=1 & Internal IP=10.12.106.17 & Traffic Rate=All

Continuing the example described above, the query submitted returns a result that the IP address: 10.12.106.17 via WAN 1 is connecting to External IP addresses, via the HTTPS(TCP@443) service. You can change the last Drill In condition (External IP) to a different one (such as traffic rate of bandwidth usage) using the same filter: WAN=1, Internal IP=10.12.106.17 and Service=HTTPS(TCP@443), by selecting Traffic Rate from the drop-down menu of External IP (as shown below):

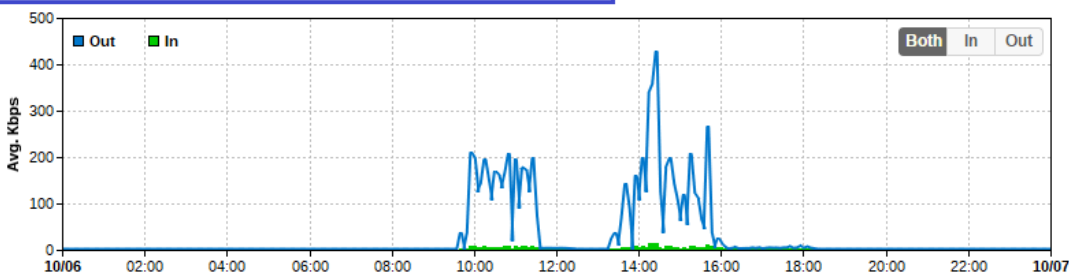


The report presented by Traffic Rate using the same filter: Service=HTTP(TCP@443), WAN=1 and Internal IP=10.12.106.17 is illustrated as follows.

## Traffic Rate ▾

2016-10-06 🔍

Filter: Service=HTTPS(TCP@443), WAN=1, Internal IP=10.12.106.17



| Time                     | Inbound bps | Outbound bps | Drill in |
|--------------------------|-------------|--------------|----------|
| 2016-10-06 00:00 - 00:05 | 830.72      | 1.51K        | 🔍        |
| 2016-10-06 00:05 - 00:10 | 933.89      | 1.70K        | 🔍        |
| 2016-10-06 00:10 - 00:15 | 830.72      | 1.51K        | 🔍        |
| 2016-10-06 00:15 - 00:20 | 831.79      | 1.51K        | 🔍        |
| 2016-10-06 00:20 - 00:25 | 937.09      | 1.70K        | 🔍        |
| 2016-10-06 00:25 - 00:30 | 829.65      | 1.51K        | 🔍        |
| 2016-10-06 00:30 - 00:35 | 828.59      | 1.51K        | 🔍        |
| 2016-10-06 00:35 - 00:40 | 931.76      | 1.70K        | 🔍        |
| 2016-10-06 00:40 - 00:45 | 830.72      | 1.51K        | 🔍        |
| 2016-10-06 00:45 - 00:50 | 830.72      | 1.51K        | 🔍        |
| 2016-10-06 00:50 - 00:55 | 933.89      | 1.70K        | 🔍        |
| 2016-10-06 00:55 - 01:00 | 832.85      | 1.51K        | 🔍        |
| 2016-10-06 01:00 - 01:05 | 831.79      | 1.51K        | 🔍        |
| 2016-10-06 01:05 - 01:10 | 934.96      | 1.70K        | 🔍        |
| 2016-10-06 01:10 - 01:15 | 831.79      | 1.51K        | 🔍        |
| 2016-10-06 01:15 - 01:20 | 833.92      | 1.52K        | 🔍        |
| 2016-10-06 01:20 - 01:25 | 936.03      | 1.70K        | 🔍        |

As illustrated in the example above, Reports offers two kinds of advanced query: you can either keep drilling in with different conditions to get a report with more specific details, or change query condition at any Drill In level; in other words, network flow data can be queried either vertically or horizontally.

## Custom Filter

Reports offers 6 fixed reports of bandwidth usage by default; In Class, Out Class, WAN, Service, Internal IP, and External IP. Usually, administrators will need to check drilled-in information for particular target regularly. As discussed previously, Drill-in function can be used to obtain more report specifics, while Filter helps to directly obtain more traffic data of a specific target. In order to quickly perform a query based on a specific filter without going through those tedious steps over again, Custom Filter allows users to apply their own filters based on particular requirements for query on bandwidth usage reports.

Click Filter above every Bandwidth Usage report to see an extended block for further settings.

### Add new condition:

- A Filter can be composed of multiple conditions. Click Add new condition and select an option from the drop-down menu to start setting your filter: In Class, Out Class, WAN, Service, Internal IP, External IP, Internal Group and External Group.

### Conditions:

- There are two actions for options while setting the condition:
  - Including: Extract only those records that fulfill the specified criterion.
  - Excluding: Extract those records that not fulfill the specified criterion.
- Configurations for report categories:
  - In Class: Enter the Inbound Class name you want to query (include or exclude) in the input field.
  - Out Class: Enter the Outbound Class name you want to query (include or exclude) in the input field.
  - WAN: Enter the WAN number you want to query (include or exclude) in the input field.
  - Service: Enter the Service you want to query (include or exclude) in the input field. Click on the arrow next to the input field to see more Service options. Predefined L4 and L3 protocols are available. Entering a single or a range of port number is also allowed.
  - Internal IP: Enter the Internal IP address you want to query (include or exclude) in the input field.
  - External IP: Enter the External IP address you want to query (include or exclude) in the input field.
- Delete: Delete the extended block of condition settings in the filter.

### Cancel:

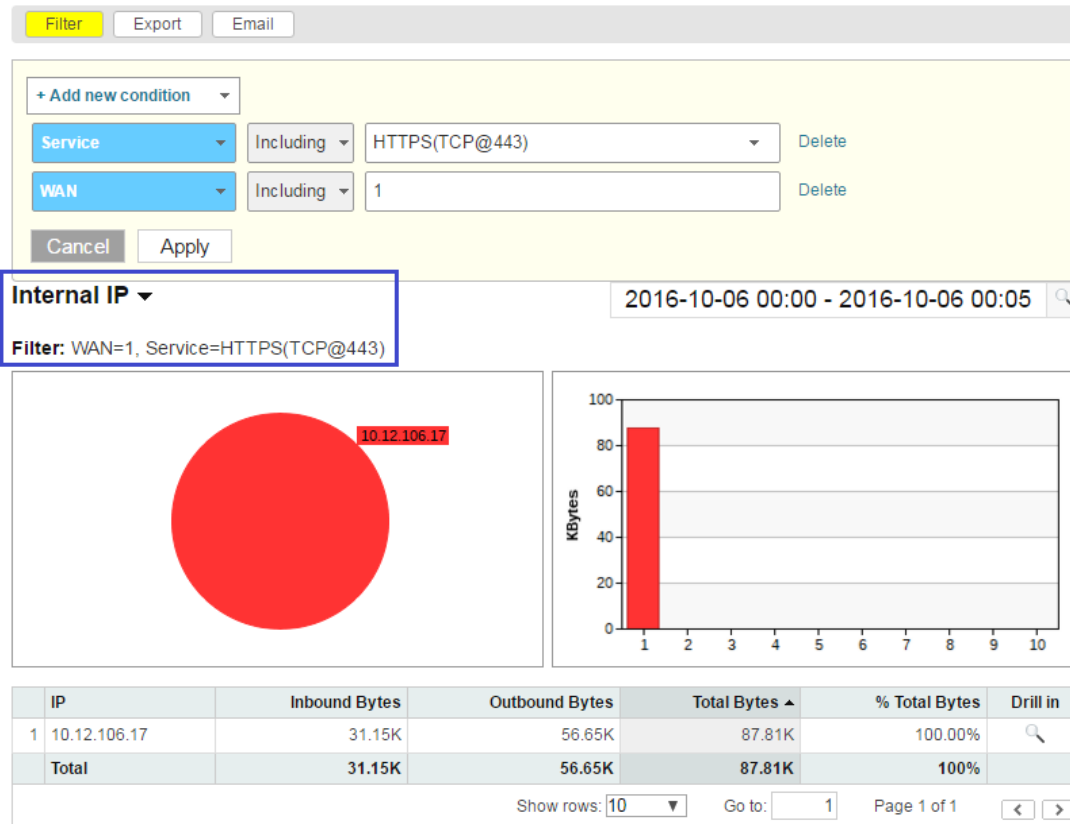
Click Cancel to close the extended block of filter settings.

### Apply:

Click Apply to start the query based on the filter conditions defined. The result is presented in the report area. Note both the result and filter conditions will not be saved in user profile. When the page moves to other report categories, the filter conditions will be invalid.

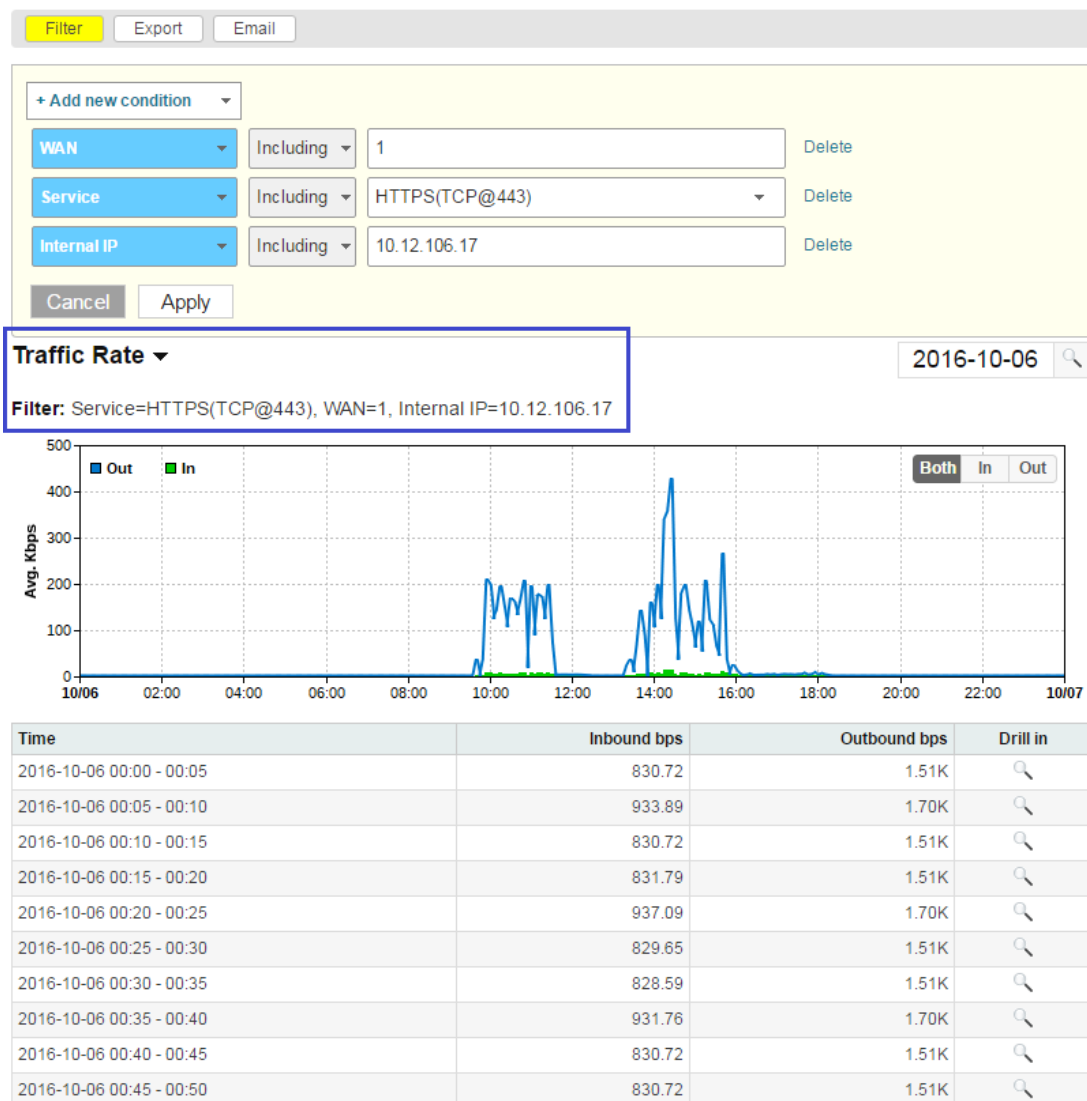
### Example

Check out the Internal IP report first, and create and apply a customer filter, for example, with the conditions WAN = 1 and Service = HTTPS(TCP@443). The query result of traffic statistics that are associated with the Service HTTPS(TCP@443) and passed through FortiWAN via WAN1 will then be displayed by Services accordingly. As illustrated below, the block marked in blue indicates the query subject of current report:



Continuing the example described above, apply the custom filter: Service=HTTPS(TCP@443), WAN=1 and Internal IP=10.12.106.17 in the Traffic Rate report, and the query result will show the corresponding traffic statistics by traffic rate as follows (the block marked in blue indicates the query subject of current report):





Note: Saved custom filters are kept in user account profile. Users can edit and delete custom filters from their account profile. Please refer to section of Customer Filters in Account Settings for more information.

## Export

All reports generated by Reports can be exported as PDF or CSV format. By clicking Export button on the upper side of any report page, PDF and CSV are displayed for options.

Filter Export Email

PDF | CSV |

## Report Email

All reports generated by Reports can be sent to users via email. Reports saved in PDF or CSV format can be sent out as email attachments.

**Note:** Prior to creating emails, you must first configure an email server used to transfer report emails to Reports. You can set the email server through [Reports > Settings > Email Server](#), or the [email function](#) on every report page.

Click the Email button on the right upper corner of any report page to configure email settings to current report page. For example, in the settings dialog below, you are currently in Traffic Rate report (see the header "Email : Traffic Rate" on the setting dialog), then you can:

- Send Traffic Rate through email immediately
- Configure the email server used to transfer report emails
- Set Traffic Rate email scheduled
- Add Traffic Rate to an existing scheduled report email

The Email function is also available for custom-filter reports and drill-in reports. No matter which report page you're at, you can always click the Email button on that page to determine when you want to send the current report through email.

### Send now

Click the **Send now** tab on the setting dialog. This feature requires a email server configured first.

|                   |                                                                    |
|-------------------|--------------------------------------------------------------------|
| <b>Recipients</b> | Enter the email address of report email recipients.                |
| <b>Format</b>     | Select the format of reports included in this email: PDF or CSV.   |
| <b>Cancel</b>     | Click to cancel current configuration and close the dialog window. |
| <b>Send</b>       | Click to send the report email immediately.                        |

## Email Server

Click the **Email Server** tab on the setting dialog. You can also set the email server through [Reports > Settings > Email Server](#). Both ways directs to one Reports to one email server.

|                    |                                                            |
|--------------------|------------------------------------------------------------|
| <b>SMTP Server</b> | Enter the SMTP server used to transfer emails.             |
| <b>Port</b>        | Enter the port number of the SMTP server.                  |
| <b>SSL</b>         | Click to allow SMTP server to transfer emails through SSL. |
| <b>Account</b>     | Enter the user name for SMTP server authentication.        |
| <b>Password</b>    | Enter the password for SMTP server authentication.         |
| <b>Mail From</b>   | Fill in the sender's name of emails.                       |

## Schedule

Click the **Schedule** tab on the setting dialog to set the report email scheduled. This feature requires a email server configured first.

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Recipients</b> | Enter the email address of report email recipients.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Format</b>     | Select the format of reports included in this email: PDF or CSV.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Schedule</b>   | <p>Select the period for automatic report email sending.</p> <ul style="list-style-type: none"> <li>• <b>Daily:</b> the report bounded in previous day 00:00 ~ 24:00 will be automatically sent at 05:00 everyday.</li> <li>• <b>Weekly:</b> the report bounded in the last week (Monday 00:00 ~ Sunday 24:00) will be automatically sent at 05:00 every Monday.</li> <li>• <b>Monthly:</b> the report bounded in the last month (the first day 00:00 ~ the last day 24:00) will be automatically sent on the first day of every month at 05:00.</li> </ul> |

## Add to existing

Click the **Add to existing** tab on the setting dialog to list the schedule. By clicking the button "Add to this" on the right upper corner of every schedule item, you can add current report category to one of the scheduled report emails. You can edit the schedule through [Reports > Settings > Scheduled Emails](#).

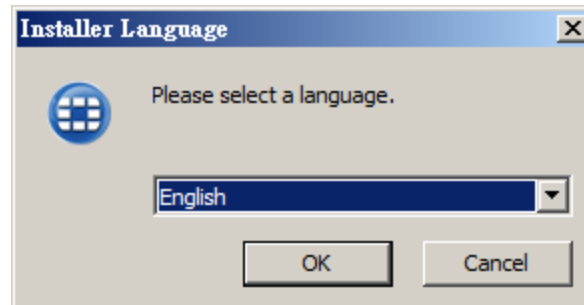
## Reports Database Tool

FortiWAN's Reports stores database in the built-in hard disk (HDD) for long-term analysis and reports. As the data increases, storage consumption increases. The Reports database tool (DB tool) is an application running on your local computer to manage remote FortiWAN Reports database. Note that the DB tool must be ran on a host that can access FortiWAN Web UI. Please contact Fortinet CSS to get the tool and install it following the instructions below.

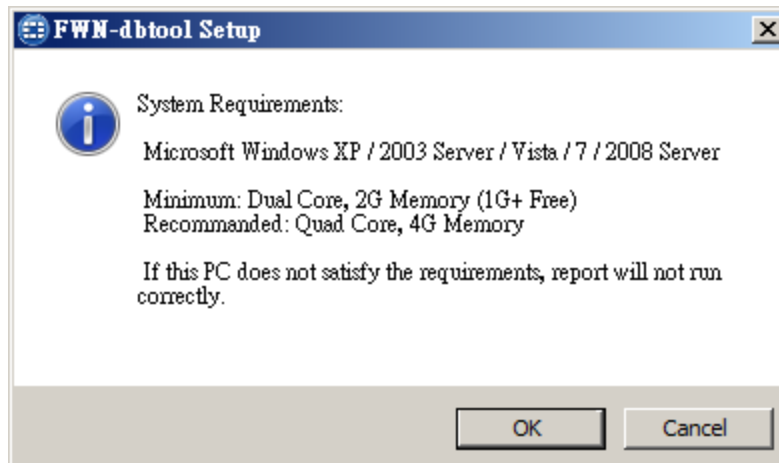
A Web-based Reports database management tool providing limited functions similar to the Reports database tool is available, see [Database Data Utility](#).

## Installation Procedures

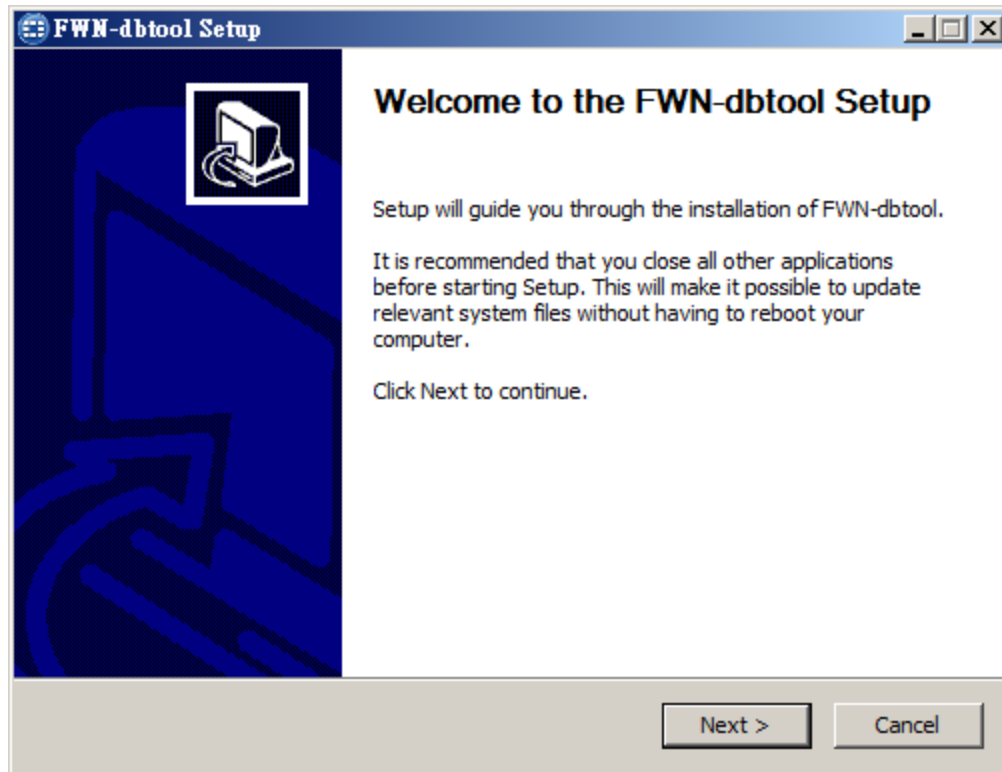
Step 1: Click the installation file (such as FWN-dbtool-4.0.0-B20150303.exe) to run the installer. Select the language of your choice.



Step 2: Read the System Requirements.



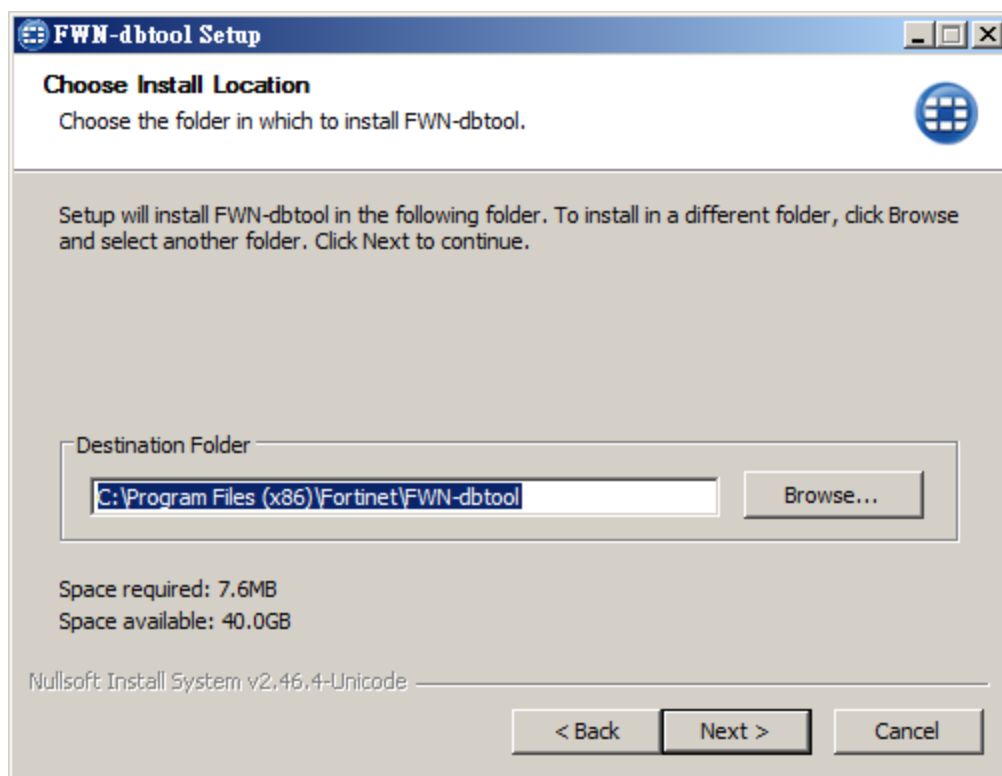
Step 3: Click 'Next' to begin the setup.



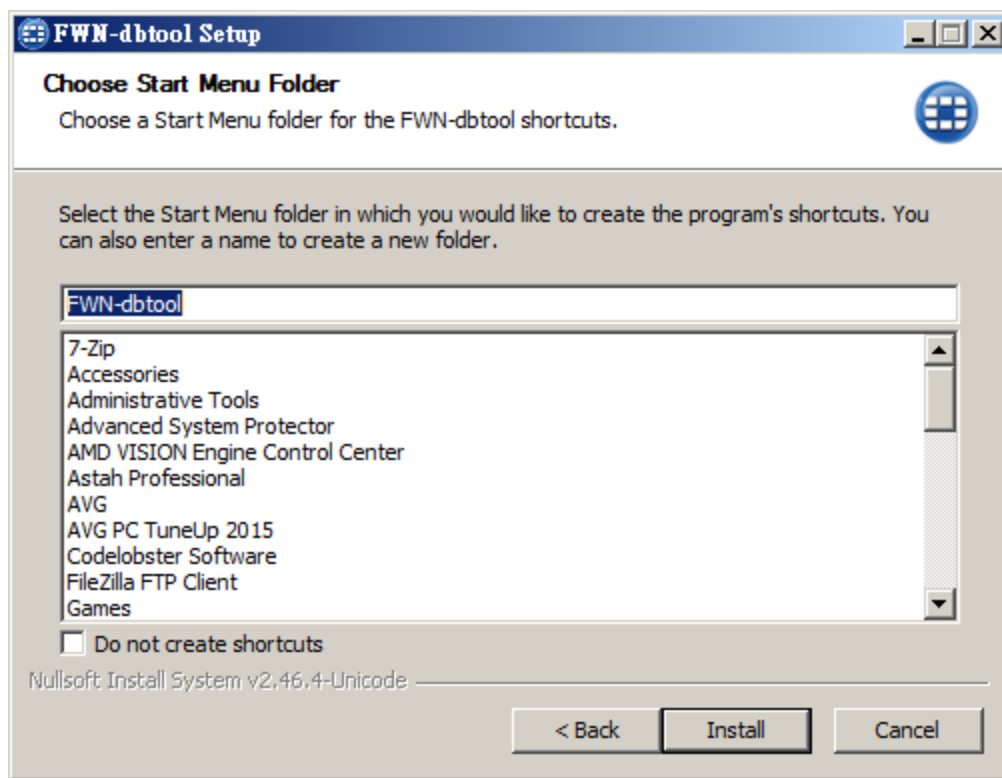
Step 4: Read the License Agreement carefully. Click the 'I Agree' button to accept the agreement and begin the installation process. Otherwise, please click 'Cancel'.



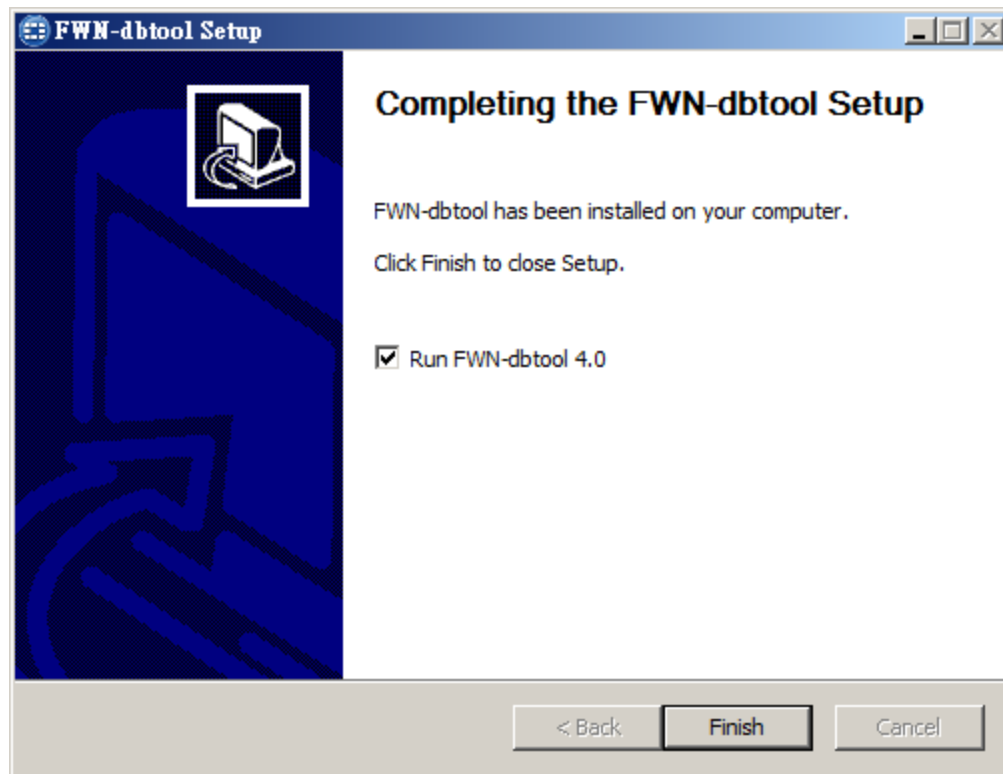
Step 5: Choose a destination folder for setup and click 'Next'.



Step 6: Choose a Start Menu folder (or check 'Do not create shortcuts' to ignore it). Click 'Install' and then the installation process will begin.



Step 7: Click 'Finish' to complete Reports DB Tool setup.



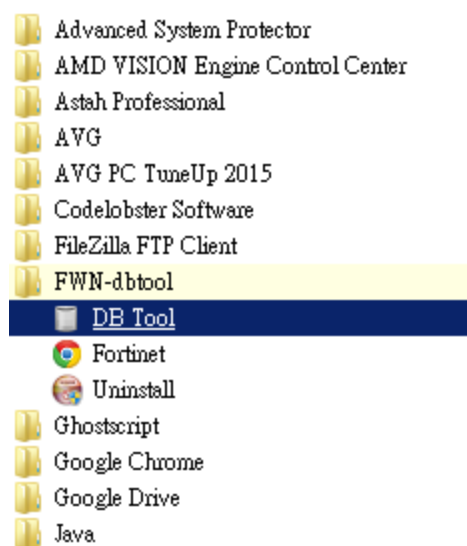
## Start DB Tool

To perform the database tool, please go to: **Start > Programs > FWN-dbtool**, and DB Tool utility is available for selection.

DB Tool: Tool to manage report data from the Reports database.

Fortinet: Link to Fortinet web site.

Uninstall: Uninstalls DB Tool.



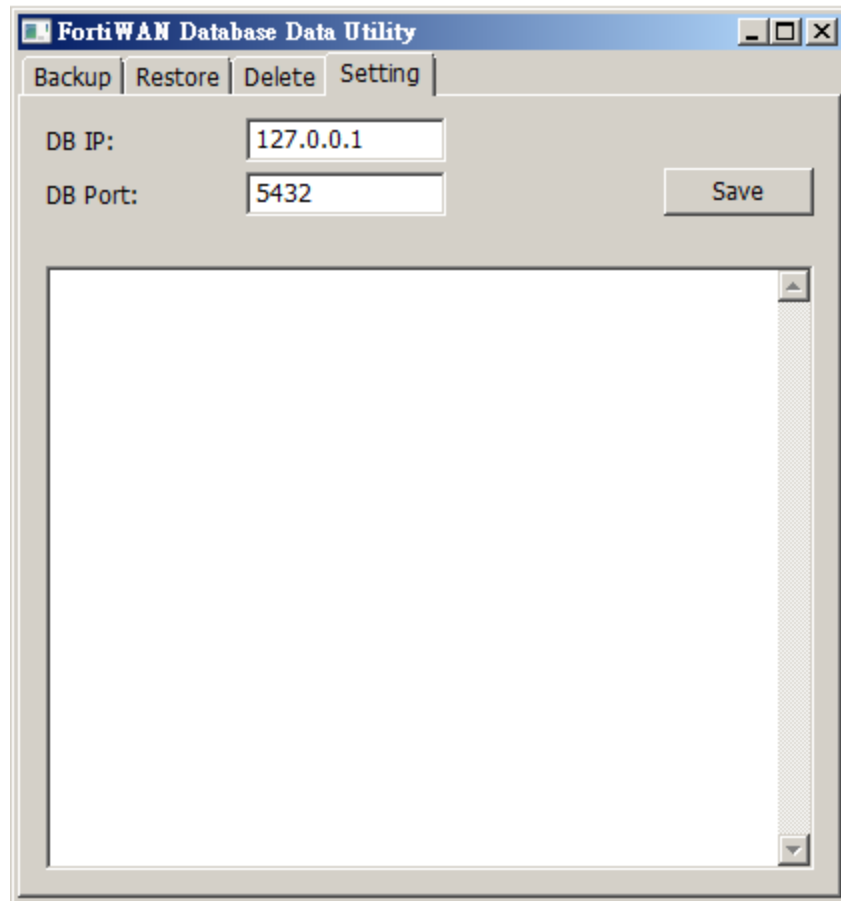
## Setting

The first time when you use the DB tool, please go to Setting to specify the database to be managed.

**DB IP** Specify the location of the Reports database. it would be the IP address of FortiWAN Web UI.

**DB Port** Specify the port number that Reports database is listening. Please use the default port 5432.

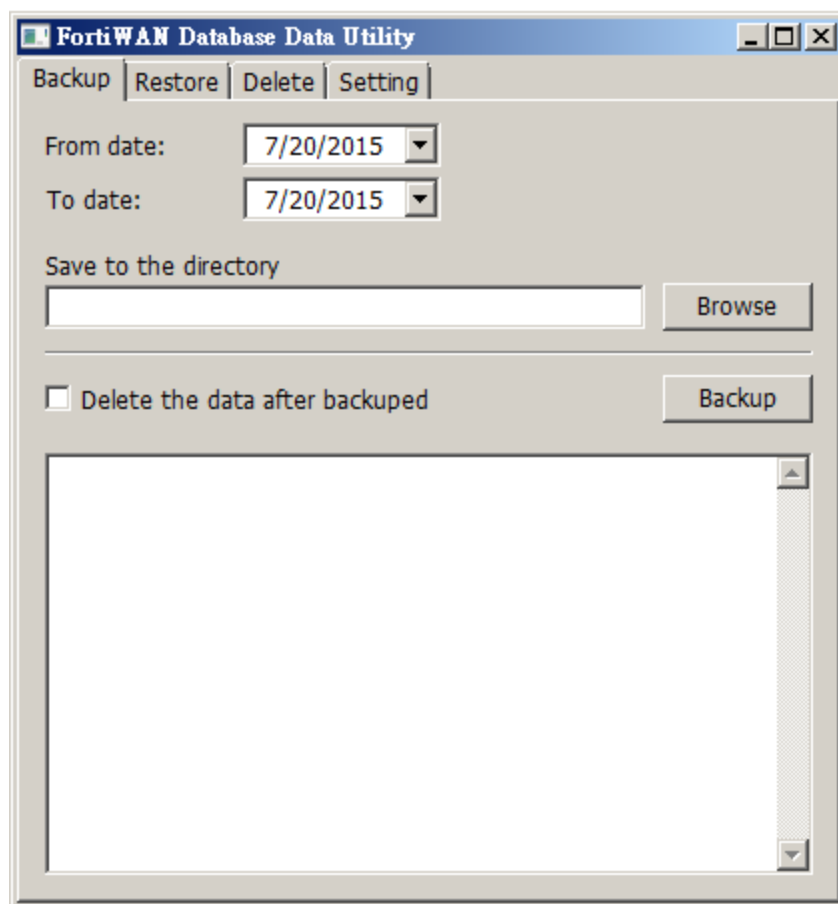
**Save** Click to save the setting.



The DB tool can be used to backup, restore and delete data from FortiWAN's Reports database.



## Backup



|                  |                                                                                             |
|------------------|---------------------------------------------------------------------------------------------|
| <b>From date</b> | Specify the start date to back up the data by selecting a date from the drop-down calendar. |
|------------------|---------------------------------------------------------------------------------------------|

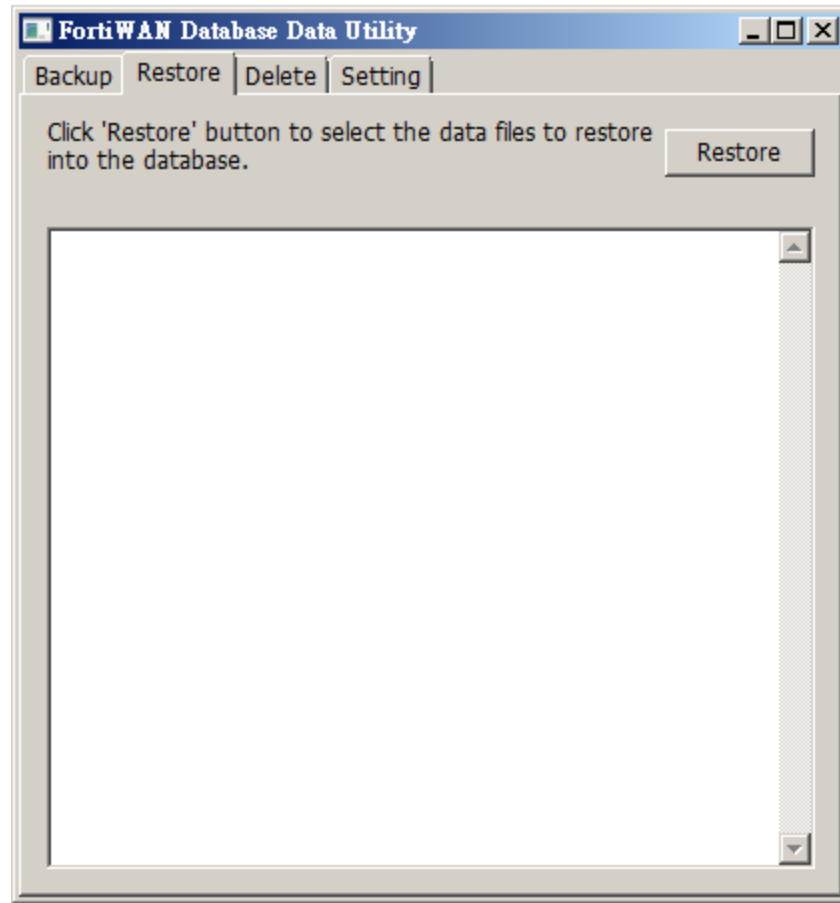
|                |                                                                                           |
|----------------|-------------------------------------------------------------------------------------------|
| <b>To date</b> | Specify the end date to back up the data by selecting a date from the drop-down calendar. |
|----------------|-------------------------------------------------------------------------------------------|

|                              |                                                                          |
|------------------------------|--------------------------------------------------------------------------|
| <b>Save to the directory</b> | Click Browse to select a location where the backup data should be saved. |
|------------------------------|--------------------------------------------------------------------------|

|                                       |                                                                        |
|---------------------------------------|------------------------------------------------------------------------|
| <b>Delete the data after exported</b> | Check it to delete the data in Reports database after it is backed up. |
|---------------------------------------|------------------------------------------------------------------------|

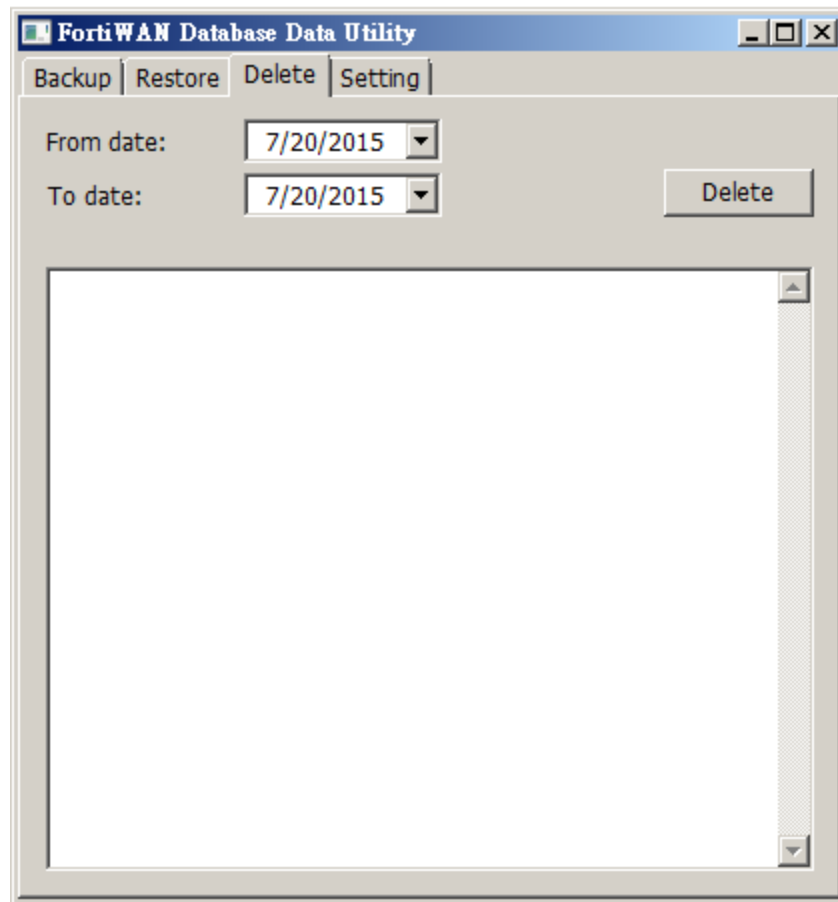
|               |                                                       |
|---------------|-------------------------------------------------------|
| <b>Backup</b> | Click to start backing up the data of selected dates. |
|---------------|-------------------------------------------------------|

## Restore



**Restore** Click to select backup files to restore to database.

## Delete



**From date** Select a date from the drop-down calendar to specify the start date to delete the data.

**To date** Select a date from the drop-down calendar to specify the end date to delete the data.

**Delete** Click to start deleting data of selected dates.

**Note** that although operations that Backup and Restore data of the current date (today) are allowed, it might cause damages the report data since FortiWAN Reports is receiving and processing the data for today. Backup and Restore are strongly recommend to be used for data before today.

## Reports Settings

The Settings here is used to simply manage the Reports on database, disk space and the SMTP server used to email reports. Click the listed settings and you can further configure them:

**Reports** : Enable/disable Reports (See "[Reports](#)").

- IP Annotation** : Create, modify and delete the notes of IP addresses (See "[IP Annotation](#)").
- Dashboard Page Refresh Time** : Auto refresh dashboard page according the time interval you specify (See "[Dashboard Page Refresh Time](#)").
- Email Server** : Manage email server settings for sending emails (See "[Email Sever](#)").
- Scheduled Emails** : Manage the existing email scheduling (See "[Scheduled Emails](#)")
- Disk Space Control** : Monitor disk free space, and send alerts or purge data when it is low (See "[Disk Space Control](#)").
- DB Data Utility** : Manage the Reports database via backup, restore and delete operations (See "[Database Data Utility](#)")
- Bandwidth Report Log Filter** : Filter off the negligible traffic (See [Filter the negligible traffic off](#))

Please note that this function is only available for the users log-in as administrator permission.

## Reports

FortiWAN Reports works by parsing and analyzing the various system logs. Before using the FortiWAN Reports, you have to enable it by specifying the way and the events to push system logs to Reports. You will be redirected to Log > Reports to complete the necessary settings to enable the FortiWAN Reports (See "[Log > Reports](#)").

## IP Annotation

IP annotation helps users to recognize IP addresses shown in Reports by predefined notes. An annotation icon will appear next to the IP address listed in a report page. Users can read the content of the annotation through clicking the icon. Click Settings > IP Annotation to enter the IP Annotation settings page.

### Search IP Annotations

The search function for IP annotations is on the right upper corner of the page.

- Search** : Type in the IP address or annotation content that you want to search in the search field and click the magnifier icon to start searching. The searching result based on existing IP annotation information will be listed in the table under the field.
- Prev** : Click to return to previous page of IP annotation list.
- Next** : Click to go to next page of IP annotation list.
- Show rows** : Allow you to select the number of IP annotation to be displayed in the search result per page: 10, 20 or 50 rows.

### List the IP Annotations

All IP annotations are displayed in the table on the center of the page.

- IP address** : List the IP address of an annotation.
- Note** : Lists the annotation content of the IP address.
- Action** : Click **Edit** to edit the content of an IP annotation. The edit interface is the same as what for adding a new annotation (See below). Click **Delete** to delete an IP annotation.

### Add a New IP Annotation

Click the **New Note** button on the left upper corner to enter the page for adding a new IP annotation.

- IP address** : Enter the IP address for the IP annotation.
- Note Content** : Enter the annotation content.
- Save** : Click to save the configuration and complete adding an IP annotation.

## Email Server

Individual reports (See "[Report Email](#)") and system alerts (See "[Disk Space Control](#)") can be sent to users via email. It is necessary to configure the email server first to deliver the report and alert emails to users. Note that configuration here is the same as the configuration made in the tab "Email" of every report page (See "[Report Email](#)"). You can maintain the unique configuration of mail server for Reports via Settings > Email Server or the "Email" function of every report page. The mail servers used for Reports, log push (See "[Log Control](#)") and notifications (See "[Notification](#)") could be different. Click Settings > Email Server to enter the Email Server settings page.

- SMTP Server** : Enter the SMTP server used to transfer emails.
- Port** : When SSL is enabled, specify the port (465 by default) that the SSL encrypted SMTP is using.  
  
When SSL is disabled, specify the port (25 by default) for STARTTLS encrypted or non-encrypted SMTP.
- SSL** : Check to enable SMTP server to transfer emails through SSL, or STARTTLS will be performed if the SMTP server supports it..
- Mail From** : Fill in the sender's name of emails.
- Account** : Enter the user name for SMTP server authentication.
- Password** : Enter the password for SMTP server authentication.
- Save** : Click to save the configuration.

## Scheduled Emails

You may have get some report emails scheduled (see [Report Email](#)). Go to **Reports > Settings > Scheduled Emails**, then you can edit or delete the schedules.

**Email** The scheduled report email. You can see the information of the email:

- Period: Daily, weekly or monthly.
- Reports: The report categories included in the email.
- Recipients: Email addresses of report email recipients
- Format: Format that the reports are attached in, PDF or CSV.

**Action** Edit or Delete the report email.

### Edit a scheduled report email

**Recipients** Edit the email address of report email recipients.

**Format** Select the format that the reports are attached in: PDF or CSV.

**Schedule** Select the period for automatic email sending: Daily, Weekly or Monthly.

**Reports** Delete report categories from the report email. The only way to add report categories to a scheduled report email is the "Add to existing" function on every report page (see [Report Email](#)).

**Save** Click to save the changes.

## Disk Space Control

Disk space of the FortiWAN Reports is being consumed by increasing report database. Once the disk space is used up, Reports will fail to continue log processing. Disk Space Control monitors the disk space status of Reports and triggers actions (purge and alert) according to user-defined conditions. Click Settings > Disk Space Control to enter the Disk Space Control settings page.

### Purge old data from database

The Purge function is triggered by two conditions, day duration and percentage of free disk space. It will purge the old data from database when any of the two conditions is satisfied. This function purges data from database without data backup. Please refer section of Reports Database Utility in Advanced Functions for more information about database backup (See "[Reports Database Tool](#)").

**Days** : Enter the number of days for the duration. When database data exceeds the day duration, Reports keeps the latest data of the day duration in database and purges the earlier data. Leave the field empty if you want disable the condition.

- Percentage (%)** : Enter the percentage. When disk free space is less than the percentage of total disk space, Reports purges the earlier data from database to keep disk free space more than the amount. Leave the field empty if you want disable the condition.
- Send notification after purge data** : Click to enable notification via email after data purging. Settings > Email Server must be configured to ensure the notification (See "[Reports Email Server](#)").

## Send Alerts

The alert function is triggered by two conditions, day duration and percentage of free disk space. It will alert administrator via email when any of the two conditions is satisfied. Settings > Email Server must be configured to ensure the notification (See "[Reports Email Server](#)").

- Days** : Enter the number of days for the duration. Reports sends an alert to users when database data exceeds the day duration. Leave the field empty if you want disable the condition.
- Percentage (%)** : Enter the percentage. Reports sends an alert to users when disk free space is less than the percentage of total disk space. Leave the field empty if you want disable the condition.

Note that system schedules condition check for database purge and sending alerts at 04:00 A.M. everyday. You are suggested to set a looser condition for sending alerts than database purge so that you get the alert earlier before the data being purged, if you need to backup the data (via Reports database tool) in advance.

## Mail To

- e-mail address** : Enter the email address for system delivers alerts and notifications to. Settings > Email Server must be configured to ensure the notification (See "[Reports Email Server](#)").

## Disk Space Status

Current usage of disk space is displayed here for reference. A pie chart of disk space usage is generated based on free space, database used and other used. Moving the mouse over the three parts of the chart displays the correspondent amount of space.

- Free Space** : Display the amount of free disk space in MB and percentage.
- Database Used** : Display the disk amount used by Reports database in MB and percentage.
- Other Used** : Display the amount of disk overhead or pre-allocated space in MB and percentage.
- Total Space** : Display the total disk space in MB.
- Save** : Click to save the configuration.

## Database Data Utility

FortiWAN's Reports keeps report data in the built-in hard disk (HDD) for long-term analysis and reports. As the data increases, disk storage consumption increases. The DB data utility provides functions to manage FortiWAN

Reports database:

- Backup: Backup report data for migration.
- Delete: Delete report data to release disk space.
- Restore: Restore backup data to Reports' database.

The DB data utility is a Web-based management tool providing limited features very similar to the [Reports database tool](#).

Go to **Reports > Settings > DB Data Utility**, an operation panel with tabs Backup, Restore and Delete is shown.

## Backup

This feature allows you a database backup for a single day. For having backups of a couple of days, you will need to either perform the backups individually (day by day) or install a [Reports Database tool](#) on your local computer to perform a single database backup for a couple of days.

To backup report data of a single date, click the Backup tab on the panel and simply follow the steps:

1. Click the **Date** field to open the calendar and specify a date for backup.
2. Click the **Backup** button to start data backup procedure. The backup file will be named in form *Default\_yyyymmdd.data* by default, such as Default\_20161007.data. This backup file will be required when you are restoring it back to FortiWAN.

## Restore

To restore a data backup to Reports, click the Restore tab on the panel and simply follow the steps:

1. Click the filed **Select the data file to restore** to select a backup file (.data file) for restoring.
2. Click the **Restore** button to start data restore procedure.

**Note** that it is not allowed to backup or restore report data of the current date (today) since FortiWAN Reports is receiving and processing the data for today. The operations are available for data before today.

**Note** that both the Web-based database data utility and the Reports database tool use the common backup file format (.data), which implies that a backup file (.data), whether is generated by the Web-based database data utility or the Reports database tool, can be restored back to Reports database in both the ways.

## Delete

To delete report data from the database, click the Delete tab on the panel and simply follow the steps:

1. Click the **From date** field to open the calendar and specify the start date for deleting.
2. Click the **To date** field to open the calendar and specify the end date for deleting.
3. Click the **Delete** button to delete the report data of the specified period.

## Filter the negligible traffic off

For statistics of bandwidth usage (see [Bandwidth Usage](#)), FortiWAN counts the inbound and outbound bytes of data transmission of every session passing through FortiWAN every minute (or when a session is closed) and then pushes a bandwidth management log to Reports to update its database. This bandwidth log indicates the



transferred inbound and outbound bytes in a minute or a period. You can filter the bandwidth management log off by setting a lower bound to evaluate the inbound and outbound bytes in the log, so that the traffic fragment will be ignored in all of the bandwidth usage reports (see [Bandwidth](#), [WAN Traffic](#), [Inclass](#), [Outclass](#), [WAN](#), [Services](#), [Internal IP](#) and [Traffic Rate](#)) if both the transferred inbound and outbound traffic are less than the bound. In case that FortiWAN is suffering attacks such as network scanning which is characterized by tiny traffic but large number of IP pairs, Reports might remain high CPU usage because of highly frequented database update. Filtering the negligible traffic off can protect Reports from this.

Go to **Reports > Reports Settings > Bandwidth Report Log Filter** and configure the following settings:

| Fields             | Descriptions                                                                                     |
|--------------------|--------------------------------------------------------------------------------------------------|
| <b>Enable</b>      | Click the checkbox to enable/disable the bandwidth logs filter                                   |
| <b>Lower bound</b> | Set the lower bound in Kbytes to evaluate the inbound and outbound bytes of every bandwidth log. |



The lower bound is used to filter off certain bandwidth logs of a session, not the total traffic of the entire session.

For example, a session spent 3 minutes to complete 2048/1024 Kbytes data transmission; 48/24 Kbytes in the first minute, 500/250 Kbytes in the second minute and 1500/750 Kbytes in the last minute. If the lower bound is set to 50 Kbytes, Reports will filter the first log off and ignore the 48/24 Kbytes in database for this session. Related bandwidth usage reports will show that this session used 2000/1000 Kbytes. However, if the lower bound is 500 Kbytes, Reports will filter off the first and second logs, which means 548/274 Kbytes are ignored in database for this session. Related reports will show that this session used 1500/750 Kbytes.

Please make sure that the lower bound filters the negligible traffic off only.

## Appendix A: Default Values

In console, enter the command 'resetconfig', or on the Web UI select "Factory Default" to do a hard reset and restore all settings to factory default.

When restored to factory default, accounts and passwords for access of CLI, Web UI and SSH login will also be reset to:

| FortiWAN Log-ins          |                          |                               |
|---------------------------|--------------------------|-------------------------------|
|                           | < V4.0.x                 | V4.1.0                        |
| Web-based Manager Default | Administrator/1234       | Administrator/1234            |
|                           | Monitor/5678 (read-only) | Monitor/5678 (read-only)      |
|                           |                          | admin/null (Fortinet default) |
| CLI Default               | Administrator/fortiwan   | Administrator/1234            |
|                           |                          | admin/null (Fortinet default) |

The Web UI login port will be restored to the default port 443.

FortiWAN also supports SSH logins. The interface for SSH login is the same as the console with identical username and password.

### WAN Link Health Detection Default Values

- System default values contain 13 fixed servers IPs for health detection.
- Values for all Port Speed and Duplex Settings will also be reset.
- All ports are restored back to AUTO state.

### Network default Values (FortiWAN 200B)

#### Port 1: WAN

- WAN Link: 1
- WAN Type: DHCP Client
- Bandwidth: 100000/100000 Kbps
- WAN Port: Port 1
- IP Address: 0.0.0.0
- Netmask : 0.0.0.0
- Default Gateway 0.0.0.0

**Port 2: WAN**

- WAN Link: 2
- WAN Type: Routing Mode
- Bandwidth: 10000/10000 Kbps
- WAN Port: Port 2
- Default Gateway 192.168.2.254
- Basic Subnet: Public Subnet in WAN/DMZ
- IP(s) on Localhost: 192.168.2.1
- IP(s) in DMZ 192.168.2.2~192.168.2.253
- Netmask: 255.255.255.0
- DMZ at Port 5

**Port 3: WAN**

- WAN Link: 3
- WAN Type: Routing Mode
- Bandwidth: 10000/10000 Kbps
- WAN Port: Port 3
- Default Gateway 192.168.3.254
- Basic Subnet: Public Subnet in WAN/DMZ
- IP(s) on Localhost: 192.168.3.1
- IP(s) in DMZ 192.168.3.2~192.168.3.253
- Netmask: 255.255.255.0
- DMZ at Port 5

**Port 4: LAN**

- IP: 192.168.0.1
- Netmask: 255.255.255.0
- DHCP Server Disabled

**Port 5: DMZ**

Fields such as Domain Name Server, VLAN and Port Mapping, WAN/DMZ Subnet Settings are all cleared

**Service Category Default Values**

- Automated Local Configuration: Enabled
- Firewall: default security rules apply
- Persistent Routing: Enabled
- Auto Routing: By Downstream Traffic as default
- Virtual Server: Disabled
- Bandwidth Managemet: Disabled
- Cache Redirection: Disabled

- Multihoming: Disabled
- All fields in the Log/Control Category are cleared

## Appendix B: Suggested Maximum Configuration Values

FortiWAN's Web UI does not set maximum limitations to numbers of most services rules and policies, but as the configured rules and policies increase interminably, performance of both FortiWAN and its Web UI decrease, especially for FortiWAN's critical services, such as Bandwidth Management, Multihoming and Tunnel Routing. Not only FortiWAN appliances use more and more hardware resources to run and handle traffic with a large number of configurations, but also your local computer spends more time to run the Web UI pages. The following table shows the suggested maximum configuration values to FortiWAN's services. Remember that FortiWAN Web UI allows you to create configurations more than the value, but the performance may not be guaranteed.

|                                     | FWN-200B | FWN-1000B | FWN-3000B |
|-------------------------------------|----------|-----------|-----------|
| <b>WAN link health detection</b>    |          |           |           |
| Ping lists                          | 1024     | 1024      | 1024      |
| <b>Optimum route detection</b>      |          |           |           |
| Static IP-ISP tables                | 1024     | 1024      | 1024      |
| Total rules of static IP-ISP tables | 1024     | 1024      | 1024      |
| <b>Backup line setting</b>          |          |           |           |
| Backup line rules                   | 1024     | 1024      | 1024      |
| <b>IP grouping</b>                  |          |           |           |
| IP groups                           | 300      | 300       | 300       |
| IPv4 rules of an IP group           | 1024     | 1024      | 1024      |
| IPv6 rules of an IP group           | 1024     | 1024      | 1024      |
| <b>Service grouping</b>             |          |           |           |
| Service group                       | 300      | 300       | 300       |
| IPv4 rules of a service group       | 1024     | 1024      | 1024      |
| IPv6 rules of a service group       | 1024     | 1024      | 1024      |
| <b>Busyhour setting</b>             |          |           |           |
| Busyhour rules                      | 1024     | 1024      | 1024      |
| <b>Date/Time</b>                    |          |           |           |

|                                                  | FWN-200B | FWN-1000B | FWN-3000B |
|--------------------------------------------------|----------|-----------|-----------|
| Time servers                                     | 4        | 4         | 4         |
| <b>Administration</b>                            |          |           |           |
| Administrator accounts                           | 1000     | 1000      | 1000      |
| Monitor accounts                                 | 1000     | 1000      | 1000      |
| <b>Firewall</b>                                  |          |           |           |
| IPv4 rules                                       | 1024     | 1024      | 1024      |
| IPv6 rules                                       | 1024     | 1024      | 1024      |
| <b>NAT</b>                                       |          |           |           |
| 1-to-1 NAT rules                                 | 1024     | 1024      | 1024      |
| NAT rules                                        | 1024     | 1024      | 1024      |
| IPv6 NAT rules                                   | 1024     | 1024      | 1024      |
| <b>Persistent routing</b>                        |          |           |           |
| IPv4 web service rules                           | 1024     | 1024      | 1024      |
| IPv4 IP pair rules                               | 1024     | 1024      | 1024      |
| IPv6 web service rules                           | 1024     | 1024      | 1024      |
| IPv6 IP pair rules                               | 1024     | 1024      | 1024      |
| <b>Auto routing</b>                              |          |           |           |
| Policies                                         | 1024     | 1024      | 1024      |
| IPv4 filters                                     | 1024     | 1024      | 1024      |
| IPv6 filters                                     | 1024     | 1024      | 1024      |
| <b>Virtual Server</b>                            |          |           |           |
| IPv4 virtual servers                             | 1024     | 1024      | 1024      |
| Server IPs of an IPv4 virtual server             | 50       | 50        | 50        |
| Total server IPs of enabled IPv4 virtual servers | 512      | 512       | 512       |

|                                      | FWN-200B | FWN-1000B | FWN-3000B |
|--------------------------------------|----------|-----------|-----------|
| IPv6 virtual servers                 | 1024     | 1024      | 1024      |
| <b>Bandwidth management</b>          |          |           |           |
| Inbound classes                      | 99       | 99        | 99        |
| Inbound IPv4 filters                 | 299      | 299       | 299       |
| Inbound IPv6 filters                 | 1024     | 1024      | 1024      |
| Outbound classes                     | 99       | 99        | 99        |
| Outbound IPv4 filters                | 299      | 299       | 299       |
| Outbound IPv6 filters                | 1024     | 1024      | 1024      |
| <b>Connection limit</b>              |          |           |           |
| Count limit rules                    | 1024     | 1024      | 1024      |
| Rate limit rules                     | 512      | 512       | 512       |
| <b>Cache redirect</b>                |          |           |           |
| Cache groups                         | 1024     | 1024      | 1024      |
| Group servers of a cache group       | 1024     | 1024      | 1024      |
| Redirect rules                       | 1024     | 1024      | 1024      |
| <b>Multihoming</b>                   |          |           |           |
| <b>Global setting</b>                |          |           |           |
| IPv4 PTR records                     | 1024     | 1024      | 1024      |
| PTR entries of an IPv4 PTR record    | 1024     | 1024      | 1024      |
| IPv6 PTR records                     | 1024     | 1024      | 1024      |
| PTR entries of an IPv6 PTR record    | 1024     | 1024      | 1024      |
| <b>A record policy</b>               |          |           |           |
| A record policies                    | 1024     | 1024      | 1024      |
| Total WAN links of A record policies | 1024     | 1024      | 1024      |

|                                                 | FWN-200B | FWN-1000B | FWN-3000B |
|-------------------------------------------------|----------|-----------|-----------|
| <b>AAAA record policy</b>                       |          |           |           |
| AAAA record policies                            | 1024     | 1024      | 1024      |
| Total WAN links of AAAA record policies         | 1024     | 1024      | 1024      |
| <b>Domain setting</b>                           |          |           |           |
| Domains                                         | 1024     | 1024      | 1024      |
| DNSSEC private keys of a domain                 | 100      | 100       | 100       |
| NS records of a domain                          | 1024     | 1024      | 1024      |
| A records of a domain                           | 1024     | 1024      | 1024      |
| AAAA records of a domain                        | 1024     | 1024      | 1024      |
| CName records of a domain                       | 1024     | 1024      | 1024      |
| DName records of a domain                       | 1024     | 1024      | 1024      |
| SRV records of a domain                         | 1024     | 1024      | 1024      |
| MX records of a domain                          | 1024     | 1024      | 1024      |
| TXT records of a domain                         | 1024     | 1024      | 1024      |
| External subdomains of a domain                 | 1024     | 1024      | 1024      |
| NS records of an external subdomain of a domain | 1024     | 1024      | 1024      |
| <b>Multihoming – Backup</b>                     |          |           |           |
| Remote master servers                           | 100      | 100       | 100       |
| <b>Internal DNS</b>                             |          |           |           |
| <b>Global setting</b>                           |          |           |           |
| IPv4 PTR records                                | 1024     | 1024      | 1024      |
| IPv6 PTR records                                | 1024     | 1024      | 1024      |
| <b>Domain setting</b>                           |          |           |           |
| <b>Domains</b>                                  | 1024     | 1024      | 1024      |



|                                                 | FWN-200B | FWN-1000B | FWN-3000B |
|-------------------------------------------------|----------|-----------|-----------|
| NS records of a domain                          | 1024     | 1024      | 1024      |
| A records of a domain                           | 1024     | 1024      | 1024      |
| AAAA records of a domain                        | 1024     | 1024      | 1024      |
| CName records of a domain                       | 1024     | 1024      | 1024      |
| SRV records of a domain                         | 1024     | 1024      | 1024      |
| MX records of a domain                          | 1024     | 1024      | 1024      |
| External subdomains of a domain                 | 1024     | 1024      | 1024      |
| NS records of an external subdomain of a domain | 1024     | 1024      | 1024      |
| <b>DNS proxy</b>                                |          |           |           |
| Intranet source rules                           | 1024     | 1024      | 1024      |
| Proxy domain rules                              | 1024     | 1024      | 1024      |
| <b>IP-MAC mapping</b>                           |          |           |           |
| Mapping rules                                   | 1024     | 1024      | 1024      |
| <b>Tunnel Routing</b>                           |          |           |           |
| Tunnel groups                                   | 100      | 400       | 1000      |
| Tunnels of a tunnel group                       | 16       | 16        | 16        |
| Total enabled tunnels                           | 2500     | 2500      | 2500      |
| Default rules of a tunnel group                 | 1024     | 1024      | 1024      |
| Routing rules                                   | 1024     | 1024      | 1024      |
| Persistent rules                                | 1024     | 1024      | 1024      |
| <b>Reports</b>                                  |          |           |           |
| IP annotations                                  | 1024     | 1024      | 1024      |
| Scheduled emails                                | 20       | 20        | 20        |

## Appendix C: What if your password is lost?

In case that the local password for FortiWAN Web UI and CLI is lost, which means you can not login to Web UI or CLI and are unable to reset password, reset or reactivate system to factory default, here are two ways that you can take to recover it.

### Firmware downgrade to V4.0.x

In V4.0.x, FortiWAN uses separated account/password for Web UI and CLI. V4.0.x uses a unchanged account/password that is Administrator/fortiwan. Even if you lost the password to Web UI, you can get into the CLI to execute the `resetpasswd` command to reset password of Administrator to default 1234 for Web UI.



Configurations for any features introduced after 4.0.0 will be lost, using this method. If you do not have a backup config file, consider using the Password-Reset file (see the next subject).

Here is the steps:

1. Prepare the V4.0.x firmware file on a TFTP server and downgrade you FortiWAN through the TFTP. See [Firmware Upgrade/Downgrade via CLI](#) for details.
2. Login to CLI with Administrator/fortiwan.
3. Execute `resetpasswd` (see [resetpasswd](#)).
4. Login to Web UI with Administrator/1234.
5. Upgrade firmware to the original version.

### Password-Reset firmware file

This is a file that can reset account/password to default without firmware downgrade/upgrade. Please contact your nearest TAC for the reset-password file. TAC will require the Serial Number of the FortiWAN that requires password reset and that Serial Number must be registered to you or your customer's account.



This file will only work on the FortiWAN with the matching Serial Number. It cannot be used for other devices.

After you have the particular file, please follow the steps to run the process:

#### Before you begin:

- You must be able to use TFTP to transfer the firmware file to the FortiWAN. Download and install a TFTP server, like `tftpd` (Windows, Mac OS X, or Linux), on a server on the same subnet as the FortiWAN.
- Download the firmware file from the Fortinet Customer Service & Support website: <https://support.fortinet.com/>
- Copy the firmware image file to the root directory of the TFTP server.
- Connect to CLI (see [To connect to the CLI](#))



TFTP is not secure, and it does not support authentication. You should run it only on trusted administrator-only networks, and never on computers directly connected to the Internet. Turn off tftpd off immediately after completing this procedure.

### To run the reset-password process:

1. Connect your management computer to the FortiWAN console port using an RJ-45-to-DB-9 serial cable.
2. Use an Ethernet cable to connect FortiWAN's HA port to the TFTP server directly, or connect it to the same subnet as the TFTP server.
3. Turning the power off and on.
4. Press any key when you see the following information on the screen:

```
FortiBootLoader
FortiWAN-200B (18:52-01.08.2015)
Ver:00010001
Serial number:FWN2HB3616000032
Total RAM: 2048MB
Boot up, boot device capacity: 971MB.
Press any key to display configuration menu...
...
```

5. You will see the menu as the following:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
```

```
Enter Selection [G]:
Enter G,F,B,Q,or H:
```

6. Enter **G** for download the reset-password file from TFTP server.
7. Configure the following settings:

```
Enter TFTP server address [192.168.1.168]: The IP address of the TFTP server, such
as 192.168.0.12.
```

```
Enter local address [192.168.1.188]: The IP address assigned to the HA port for TFTP
transmission, such as 192.168.0.2.
```

```
Enter firmware image file name [image.out]: The file name of the reset-password file,
such as FWN2HB-V400-build0312-FORTINET-FWN2HB3616000040.out.
```

8. It starts get the file from the TFTP server
9. Enter **B** to locate the firmware in backup partition when you see the following information:

```
MAC:000D48309D17
#####
#####
Total 94177227 bytes data downloaded.
Verifying the integrity of the firmware image..

Total 103376kB unzipped.
Save as Default firmware/Backup firmware:[D/B]?
```

10. Let the FortiWAN continues the booting:

```
Programming the boot device now.
```

```
.....
```

```
Reading boot image 4265472 bytes.
```

```
Initializing FortiWAN...
```

```
fortiwan login:
```

11. Turning the power off and on again.

12. The same, press any key when you see the following information on the screen:

```
FortiBootLoader
```

```
FortiWAN-200B (18:52-01.08.2015)
```

```
Ver:00010001
```

```
Serial number:FWN2HB3616000032
```

```
Total RAM: 2048MB
```

```
Boot up, boot device capacity: 971MB.
```

```
Press any key to display configuration menu...
```

```
...
```

13. Enter **B** to boot with the backup partition when you see the following information on the screen:

```
[G]: Get firmware image from TFTP server.
```

```
[F]: Format boot device.
```

```
[B]: Boot with backup firmware and set as default.
```

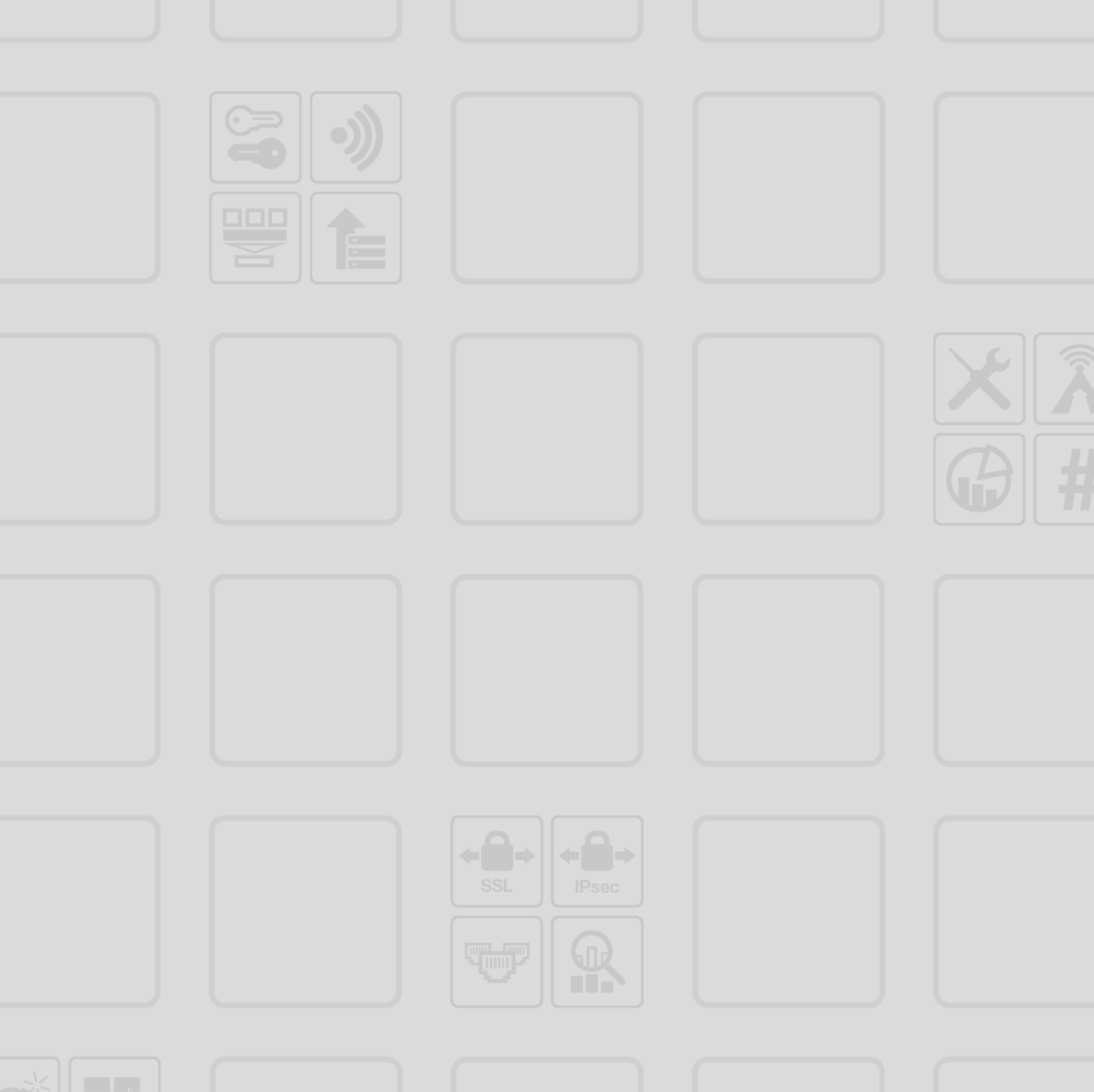
```
[Q]: Quit menu and continue to boot with default firmware.
```

```
[H]: Display this list of options.
```

```
Enter Selection [G]:
```

```
Enter G,F,B,Q,or H:
```

14. When you see `Initializing FortiWAN...`, the image is resetting password to default. Then FortiWAN will automatically reboot again, with the original firmware this time. Let it just complete booting without pressing any key this time, and you can login with default password that is Administrator/1234 or admin/null-password.



**FORTINET®**

*High Performance Network Security*



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.