FORTINET
High Performance Network Security

FortiWAN - Release Notes

VERSION 4.2.3

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

July 28, 2016

FortiWAN 4.2.3 Release Notes Revision 3

38-423-374477-20160728

TABLE OF CONTENTS

Introduction

This document provides a list of new/changed features, upgrade instructions and caveats, resolved issues, and known issues for FortiWAN 4.2.3, build 0144, for model 200B, 1000B, 3000B, VM-02 and VM-04.

FortiWAN is a Link Load Balancing, Multi-Homing and Tunnel Routing system that distributes outbound or inbound internet traffic across multiple WAN links of differing technologies as well as building multi-link VPNs between sites.

For additional documentation, please visit:

http://help.fortinet.com/fwan/4-2-3/index.htm

What's new

The following list summarizes new and enhanced features. For details, see the FortiWAN Handbook.

- Tunnel Routing - Performance of transmission in a tunnel group can be greatly enhanced (increased) by disabling Generic Receive Offload (GRO) mechanism on each of network interfaces receiving outgoing packets (the LAN ports and DMZ ports) on both of the participating FortiWAN units. A new parameter "generic-receive-offload" is added to CLI command sysctl to enable/disable the GRO module.
- 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.
- 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.
- 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.

  Note that if you are upgrading from a previous version, please ensure that there are no duplicate label names among your aggregated LAN or DMZ ports. If there are duplicates, system will fail to boots up after upgrading to this release. If you are downgrading to a previous release, you must delete all aggregated port settings before downgrade, or system will fail to boots up after downgrading.
- 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.
- Multihoming - 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.
- 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.
- Statistics - Measurement of Round Trip Time (RTT) is added to Statistics > Tunnel Status for each GRE tunnel of configured tunnel groups.

Hardware Support

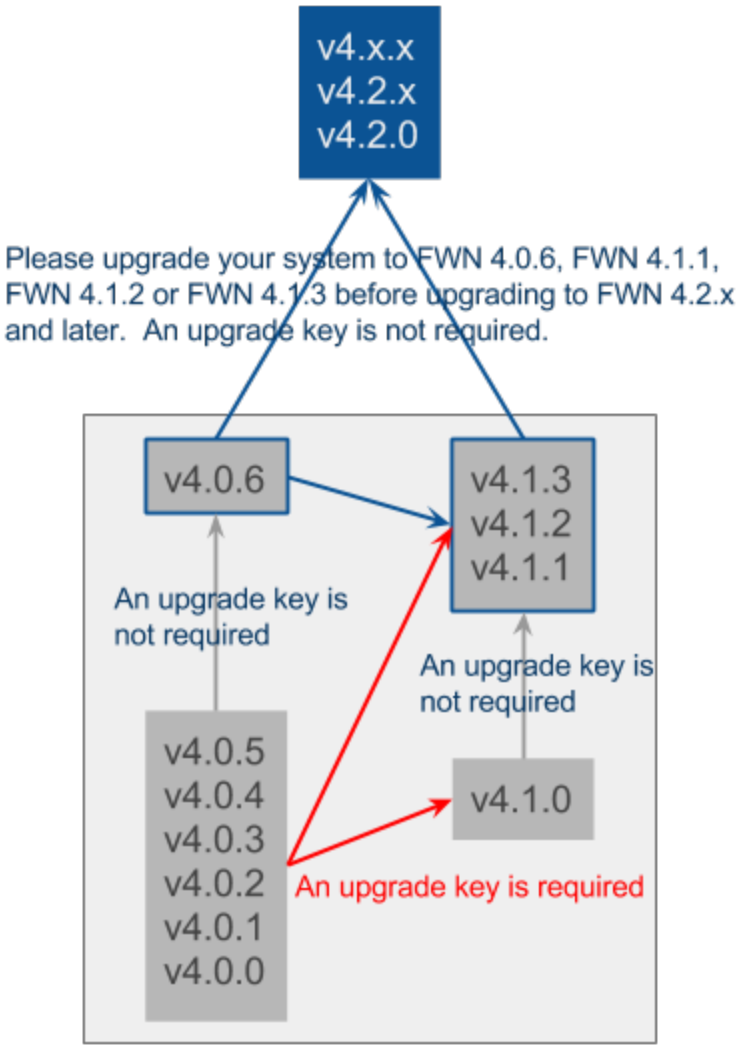
FortiWAN 4.2.3 for FortiWAN supports FortiWAN 200B, FortiWAN 1000B, FortiWAN 3000B, FortiWAN-VM-02 and FortiWAN-VM-04.

AscenLink series models are not supported.

Upgrading

FortiWAN 200B, FortiWAN 1000B and FortiWAN 3000B may have FWN 4.0.x installed respectively. In that case upgrade to FWN 4.2.3 as follows:

In early versions of FortiWAN firmware, it was necessary to obtain a Firmware Upgrade License Key to upgrade major releases of firmware (4.0.x - 4.1.x - 4.2.x). In late 2015, Fortinet decided to align the FortiWAN firmware upgrade policy with other Fortinet products, Firmware Upgrade Keys would no longer be required. In order to implement that, changes needed to be made in some maintenance releases of FortiWAN firmware. Please use the diagram below to select the current firmware you have and the desired latest firmware. You might need to first upgrade to a higher maintenance release (e.g. 4.0.1 - 4.0.6) of your current firmware (this never requires a key) before you can upgrade to the latest major release.



In the past FortiWAN (and AscenLink) required sequential major firmware upgrades (e.g. 4.0.x-4.1.x-4.2.x). With the above changes to “keyless” upgrades you will be able to upgrade directly to any release after the current one, “jumping” unneeded releases (e.g. 4.0.6-4.2.x).

After that, start the upgrade procedure as follow:

- Always back up your system configurations and store in a safe place before upgrading.
- Note that if you are upgrading from a previous version, please ensure that:
  - There are no duplicate label names among your aggregated LAN or DMZ ports (go to *System > Network Setting > VLAN and Port Mapping* on Web UI). If there are duplicates, system will fail to boots up after upgrading to this release.
  - There are no Auto Routing filter rules associated with an aggregated port by the Input Port field (go to *Service > Auto Routing* on Web UI). System will fail to boots up after upgrading to this release if there is a rule associated with an aggregated port. The suggested steps to handle such the AR rules are:
    - Before upgrading, change Input Port field of the rules from the aggregate port to Any Port, and click the Apply button.
    - Complete the upgrading process.
    - After upgrading to this release, log onto Web UI, go to *System > Network Setting*, and click the Apply button.
    - Go to *Service > Auto Routing*, re-associate those rules with the original aggregated ports from the Input Port field, apply it and reboot the system.
- Log on to FortiWAN as Administrator and go to [System > Administrator] page.
- Click Update to start the upgrade procedure
  - Click Browse to select the path where the new firmware image is saved.
  - Select Upload.
- Be patient while firmware is being upgraded. During the upgrade, do not turn off the system, unplug the power or repeatedly click the Submit button.
- The message “Update succeeded” will appear after the upgrade is completed. Please reboot the system afterward for the firmware to take effect.

Note that upgrade from AscenLink is not supported.

Downgrading

In that case downgrade to previous releases of firmware (4.0.x, 4.1.x or 4.2.0 - 4.2.2), you can downgrade directly to any release before the current one without any key being required. The downgrade procedure is similar to the upgrade one as follow:

- Always back up your system configurations and store in a safe place before downgrading.
- Note that if you are downgrading to a previous release from FWN 4.2.3, you must delete all aggregated port settings (go to *System > Network Setting > VLAN and Port Mapping* on Web UI) before downgrading, or system will fail to boots up after downgrading.
- Log on to FortiWAN as Administrator and go to [System > Administrator] page.
- Click Downgrade to start the downgrade procedure
    - Click Browse to select the old firmware image that you want to downgrade to.
    - Select Upload.
- Be patient while firmware is being downgraded. During the downgrade, do not turn off the system, unplug the power or repeatedly click the Submit button.
- The message “Downgrade succeeded” will appear after the downgrade is completed. Please reboot the system afterward for the firmware to take effect.

Note that downgrade from AscenLink is not supported.

Resolved issues

This section lists the resolved issues of this release, but is not a complete list. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
367585	A FortiWAN's LACP aggregated port was not acceptable to particular switches if member-ports of the aggregated port were VLAN ports. These switches would accept a VLAN port that was defined on a LACP aggregated port (which its member-ports must be non-VLAN ports) to connect with, however, FortiWAN did not support the setting from Web UI. Web UI for port mapping was redesigned in this release to allow VLANs being defined on aggregated ports.
368455	FortiWAN's Reports would take longer time to parse Bandwidth Management logs to database if the traffic passed through FortiWAN was generated by a large number of source-destination IP pairs. This issue might cause data inconsistent between FortiWAN's Reports and FortiWAN's BM Statistics, or delay the report data (no data was displayed on Reports pages) for minutes to hours.
368938	The PHP package employed in FortiWAN was upgraded to version 5.5.34 to fix related security vulnerabilities.
370054	Compared with FortiWAN V4.0.x, data transmission performance of Tunnel Routing running on FortiWAN V4.1.x and V4.2.0 - V4.2.2 was lower. This was because of a mistake occurred in Tunnel Routing's packet receiving procedure in these versions. By fixing the bug in this release, the expected Tunnel Routing performance comes back.
370571	FortiWAN would fail to perform auto-negotiation with a device connected through Gigabite Ethernet if hot swapping the SFP-GE-T (FG-TRAN-GC) transceiver module of the connected network interface on the FortiWAN. This resulted in a downed interface unless the Network Settings page was reapplied. This issue happened when hot swapping the SFP-GE-T transceiver module after booting up (or rebooting) the FortiWAN device that has connected to a device in advance through a SFP-GE-T transceiver module.
371134	The OpenSSL employed in FortiWAN was upgraded to version 1.0.1t to fix related security vulnerabilities.
372122	With HA monitor enabled on specified physical network ports (the HA field in *System* > *Port Speed/Duplex Setting*), HA takeover between master and slave units might be triggered incorrectly when applying Web UI pages *System* > *Network Setting* and *System* > *Port Speed/Duplex Setting*.
372282	A Null-pointer might occur in the Persistent Routing function, which resulted in system crash and rebooting.
372296	With DNS Proxy and its domain name filter enabled, FortiWAN might be crashed by malformed UDP 53 packets (contents of the packets could not be dissected by DNS Proxy).

Bug ID	Description
373196	DNS Proxy became not functioning every time after FortiWAN booted up or rebooted. It had to reapply the DNS Proxy settings through Web UI (click the Apply button on *Service* > *DNS Proxy*) to recover the service.
373199	A dot character was not acceptable to Alias and Target fields of Multihoming's CName records on Web UI. Besides, Multihoming would fail to respond to DNS queries if any resource record contained an underscore in Host Name, Name Server, Alias or Target fields. Both the issues resulted in inability and failure to create DNS records for DKIM signing.
373704	The NTP package employed in FortiWAN was upgraded to version 4.2.8p7 to fix related security vulnerabilities.
374512	FortiWAN kernel was patched to fix security vulnerabilities CVE-2016-0723 and CVE-2016-2847.

Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 2: Known issues

Bug ID	Description
272709	The Status LEDs on the front panel of FortiWAN units do not function currently. They are reserved for future use.

FORTINET

High Performance Network Security