FortiDDoS REST API Reference

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

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

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

Monday, May 14, 2018

FortiDDoS REST API Reference

Version 4.6.0

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-05-14	Revision 1 of FortiDDoS REST API document

What's new

4.6.0

- REST APIs are added for blacklisted domains and IPv4 addresses.

4.5.0

- REST API is added for FortiView. See Chapter 5.

Chapter 1: FortiDDoS REST API Overview

This reference has the following sections:

About this guide

The guide is a reference for the FortiDDoS REST API. It covers the HTTP methods, URLs, and URL parameters that enable you to monitor and manage a FortiDDoS appliance.

The examples in this document make requests using cURL. cURL is more flexible than using a browser alone, works across platforms, and most scripts can call it. It is not as flexible as native scripting languages, but it is useful for illustrating how the API functions.

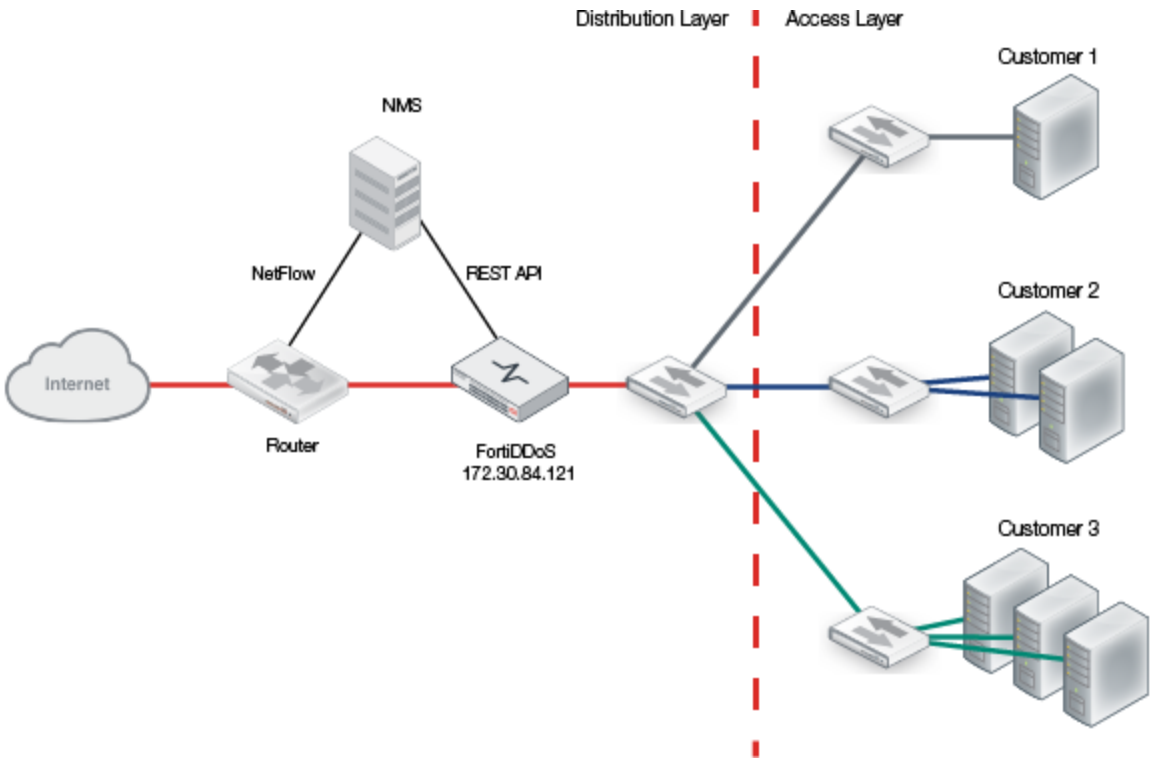
REST API to integrate with other appliances

You can use the REST API to integrate FortiDDoS with other appliances in your network. For example, the API allows you to automate the following tasks:

- Change the configuration of FortiDDoS based on statistics generated by router and switch technologies such as NetFlow, jFlow, and sFlow.
- Change the configuration of FortiDDoS based on an analysis of the FortiDDoS syslog by an internal Network Management System (NMS).
- Add ACLs to the FortiDDoS that block traffic to an application server based on information from a Web Application Firewall or an IPS (intrusion prevention system) that monitors the server.

In the following figure, the NMS monitors a router in the service provider's network. The NMS, in turn, communicates with FortiDDoS using the REST API.

Figure 1: NMS using the REST API



Supported API methods

The FortiDDoS REST API supports the following methods.

Method	URL	Operation description	Success response code

`GET`(list)	`/[resource]/`
	`/drop_stats...`
	`/monitor_stats...`
		Retrieves all records, the specified attack mitigation statistics, or the specified traffic graph information	200 OK

`POST` (detail)	`/[resource]/`	Creates a new record	201 Created
`PUT` (detail)	`/[resource]/`	Updates an existing record	204 NO CONTENT
`DELETE` (detail)	`/[resource]/` `[id]`	Deletes a single record	204 NO CONTENT

Supported data formats

The FortiDDoS REST API provides responses are in JSON format for FortiDDoS settings and other resources, and for traffic statistics (`drop_stats`). For traffic graph information (`monitor_stats`), responses are in XML format.

Accessing the REST API

You can access the FortiDDoS API from most browsers using the GET method. However, your browser may require add-ons for extended operations such as PUT. You can make more complicated, scripted queries using utilities such as cURL. Most scripting languages such as Perl or Python have built-in library calls that can interact with a REST API.

Chapter 2: REST API to manage configuration

Only local admin users can access REST API calls. Remote or Local non-admin users cannot perform any actions using REST API calls.

The URLs that you use to access configuration settings or other system resources have the following format:

`http://<server>/api/<version>/<group>/<resource>/[id]/`

where:

- `<server>` is the name or IP address of the management interface.
- `<version>` is the API version (for example, `v1`).
- `<group>` is one of the following values:
  - `system`
  - `ddos/global`
  - `spp/<name>`, where `<name>` is the name of the SPP.
  - `log`
- `<resource>` is the name of the configuration setting or other resource.
- `[id]` is a unique identifier for a configuration setting or other resource (required for DELETE only).

Table 1: Resources names

Group	Resource name	Method	Web UI location
system			
	interface	GET PUT	System > Network > Interface
	dns	GET PUT	System > Network > DNS
	route	GET POST PUT DELETE	System > Network > Static Route
	HA	GET PUT	System > High Availability
	snmp_sysinfo	GET PUT	System > SNMP > SNMP System Information

Group	Resource name	Method	Web UI location
	snmp_threshold	GET PUT	System > SNMP > SNMP Threshold
	snmp_community	GET POST PUT DELETE	System > SNMP > Community
	auth_radius	GET PUT	System > Authentication > RADIUS
	auth_LDAP	GET PUT	System > Authentication > LDAP
	auth_tacacsplus	GET PUT	System > Authentication > TACACS+
	adminuser	GET POST PUT DELETE	System > Admin > Administrator
	accprofile	GET POST PUT DELETE	System > Admin > Access Profile
	sysglobal	GET PUT	System > Admin > Settings
	certificate_local	GET	System > Certificates > Local Certificate
ddos/global			
	ddos-global-spp-switching-policy	GET PUT	Global Settings > Service Protection Profiles > Switching Policy
	ddos-global-spp-policy	GET POST PUT DELETE	Global Settings > Service Protection Profiles > SPP Policy

Group	Resource name	Method	Web UI location
	ddos_global_spp_policy_group	GET POST PUT DELETE	Global Settings > Service Protection Profiles > SPP Policy Group
	ddos_global_setting	GET PUT	Global Settings > Settings > Settings
	ddos_global_http_service_ports	GET POST PUT DELETE	Global Settings > Settings > HTTP Service Ports
	ddos_global_udp_service_ports	GET POST PUT DELETE	Global Settings > Settings > UDP Service Ports
	ddos_global_sp_fdd	GET POST PUT DELETE	Global Settings > Settings > Signaling
	ddos_global_service_provider_address	GET POST PUT DELETE	Global Settings >Settings > Service Provider Address
	ddos_global_ip_reputation	GET PUT	Global Settings > IP Reputation
	ddos_global_domain_reputation	GET PUT	Global Settings > Domain Reputation
	ddos_global_proxy_ip	GET PUT	Global Settings > Proxy IP
	ddos_global_proxyip_policy	GET POST PUT DELETE	Global Settings > Proxy IP Policy

Group	Resource name	Method	Web UI location
	ddos_global_firewall_local_address	GET POST PUT DELETE	Global Settings > Address > Local Address Config
	ddos_global_firewall_local_address6	GET POST PUT DELETE	Global Settings > Address > Local Address Config IPv6
	ddos_global_firewall_address	GET POST PUT DELETE	Global Settings > Address > Address Config
	ddos_global_firewall_address6	GET POST PUT DELETE	Global Settings > Address > Address Config IPv6
	ddos_global_do_not_track_policy	GET POST PUT DELETE	Global Settings > Do Not Track Policy > Do Not Track Policy
	ddos_global_do_not_track_policy6	GET POST PUT DELETE	Global Settings > Do Not Track Policy > Do Not Track Policy IPv6
	ddos_global_firewall_policy	GET POST PUT DELETE	Global Settings > Access Control List > Access Control List
	ddos_global_firewall_policy6	GET POST PUT DELETE	Global Settings > Access Control List > Access Control List IPv6
	ddos_global_distress_acl	GET POST PUT DELETE	Global Settings > Access Control List > Advanced Settings > Distress ACL

Group	Resource name	Method	Web UI location
	ddos_global_bypass_macs	GET POST PUT DELETE	Global Settings > Bypass MAC > Bypass MAC
spp/<name>			
	ddos_spp_setting	GET PUT	Protection Profiles > SPP Settings
	ddos_spp_firewall_service	GET POST PUT DELETE	Protection Profiles > Service Config
	ddos_spp_firewall_policy	GET POST PUT DELETE	Protection Profiles > Access Control List
	ddos_spp_firewall_address	GET POST PUT DELETE	Protection Profiles > Address Config
	ddos_spp_firewall_address6	GET POST PUT DELETE	Protection Profiles > Address Config IPv6
	ddos_spp_tcp_session_ extended_timeout_policy	GET POST PUT DELETE	Protection Profiles > Extended Timeout Policy
	ddos_spp_reset	GET PUT	Protection Profiles > Factory Reset
	ddos_spp_threshold_scalar	GET POST PUT DELETE	Protection Profiles > Thresholds > Thresholds > Scalars

Group	Resource name	Method	Web UI location
	ddos_spp_threshold_http_methods	GET POST PUT DELETE	Protection Profiles > Thresholds > Thresholds > HTTP Methods
	ddos_spp_threshold_protocol	GET POST PUT DELETE	Protection Profiles > Thresholds > Thresholds > Protocols
	ddos_spp_threshold_tcp_ports	GET POST PUT DELETE	Protection Profiles > Thresholds > Thresholds > TCP Ports
	ddos_spp_threshold_udp_ports	GET POST PUT DELETE	Protection Profiles > Thresholds > Thresholds > UDP Ports
	ddos_spp_threshold_icmp_type_codes	GET POST PUT DELETE	Protection Profiles > Thresholds > Thresholds > ICMP Types/Codes
	ddos_spp_threshold_http_urls	GET POST PUT DELETE	Protection Profiles > Thresholds > Thresholds > URLs
	ddos_spp_threshold_http_hosts	GET POST PUT DELETE	Protection Profiles > Thresholds > Thresholds > Hosts
	ddos_spp_threshold_http_referers	GET POST PUT DELETE	Protection Profiles > Thresholds > Thresholds > Referers
	ddos_spp_threshold_http_cookies	GET POST PUT DELETE	Protection Profiles > Thresholds > Thresholds > Cookies

Group	Resource name	Method	Web UI location
	ddos_spp_threshold_http_user_agents	GET POST PUT DELETE	Protection Profiles > Thresholds > Thresholds > User Agents
log			
	log_local	GET PUT	Log & Report > Log Configuration > Local Log Settings
	log_remote	GET POST PUT DELETE	Log & Report > Log Configuration > Event Log Remote
	log_setting_ddos_attack_remote	GET POST PUT DELETE	Log & Report > Log Configuration > DDoS Attack Log Remote
	ddos_global_attack_event_purge	GET PUT	Log & Report > Log Configuration > Log Purge Settings
	log_setting_snmp_trap_receivers	GET POST PUT DELETE	Log & Report > Log Configuration > SNMP Trap Receivers
	log_report	GET POST PUT DELETE	Log & Report > Report Configuration
	ddos_global_attack_report_purge	GET PUT	Log & Report > Report Purge Settings
	log_setting_remote_log_settings	GET PUT	Log & Report > Log Configuration > Remote Log Settings
	alertemail_recipient	GET POST PUT DELETE	Log & Report > Log Configuration > Alert Email Settings > Recipient

Group	Resource name	Method	Web UI location
	alertemail_server	GET PUT	Log & Report > Log Configuration > Alert Email Settings > Mail Server
	alertemail_setting	GET PUT	Log & Report > Log Configuration > Alert Email Settings > Setting

Examples

Retrieve all global addresses (GET)

```
curl -u rest_api_user:rest_api_password '
'http://172.30.84.121/api/v1/ddos/global/ddos_global_firewall_address/'
{"query":"full","success":true,"message":"data generated","data":[{"mkey":"a","type":"ip-
netmask","ip-netmask":"1.1.0.0\/23","ip-address":"0.0.0.0","geo-location":"A1"}]}
[root@xengv ~]
```

Create a new global address (POST)

```
curl -v -X POST -H "Content-Type: application/json" -d '{"data":{"mkey":"a1","type":"ip-
address","address":"","ip-netmask":"","ip-address":"1.1.1.1","geo-location":""}}' -u
admin: 'http://172.30.84.121/api/v1/ddos/global/ddos_global_firewall_address/'
```

Update an existing global address (PUT)

```
curl -v -X PUT -H "Content-Type: application/json" -d '{"data":{"mkey":"a1","type":"ip-
address","address":"","ip-netmask":"","ip-address":"2.2.2.2","geo-location":""}}' -u
admin: 'http://172.30.84.121/api/v1/ddos/global/ddos_global_firewall_address/'
```

Delete an existing global address (DELETE)

```
curl -v -X DELETE -u admin: 'http://172.30.84.121/api/v1/ddos/global/ddos_global_firewall_
address/a1/'
```

Download user-uploaded files for blacklisted domains

```
curl -u rest_api_user:rest_api_password
'http://172.30.153.121/api/v1/download_blacklisted_domains' -o domain.txt
```

Download user-uploaded files for blacklisted IPs

```
curl -u rest_api_user:rest_api_password
'http://172.30.153.121/api/v1/download_blacklisted_ipv4_addresses' -o ip.txt
```

Change the service protection profile (SPP) policy

Service protection profile (SPP) policies specify the SPP that monitors and regulates a subnet. By changing the SPP policy, you can change how FortiDDoS handles traffic on that subnet.

For example, you can move the subnet from a profile that simply detects and reports traffic anomalies (detection mode) to one that actively drops anomalous packets (prevention mode).

This example moves subnet 1.1.1.0/24 from SPP-0, which is in detection mode, to SPP-1, which is in prevention mode.

1. Get mkey name using a GET call.

```
curl -u rest_api_user:rest_api_password 'http://172.30.84.121/api/v1/ddos/global/ddos-global-spp-policy/'
```

FortiDDoS responds with the following information:

```
{"query":"full","success":true,"message":"data generated","data":[{"mkey":"1","subnet-id":"1","ip-addr":"1.1.1.0\/24","ipv6-addr":"::\/0","spp":"SPP-0","alt-spp-enable":"disable","alt-spp":"","threshold":"0","comment":""}]}
```

2. Execute a PUT call with the same mkey value and the name of the new SPP.
3. Replace mkey with the new SPP using a PUT call.

```
curl -X PUT -u rest_api_user:rest_api_password -H "Content-Type: application/json" -d '{"data":
{"mkey":"1","spp":"SPP-1"}}' 'http://172.30.84.121/api/v1/ddos/global/ddos-global-spp-policy/'
```

Use an ACL to deny access to a specific TCP port

This example configures the service protection profile SPP-0 to deny access to TCP port 3000.

1. Create a service record.

```
curl -X POST -u rest_api_user:rest_api_password -H "Content-Type: application/json" -d '{"data":
{"mkey":"s1","type":"tcp-port","destination-port-start":"3000","destination-port-end":"3000"}}' 'http://172.30.84.121/api/v1/spp/SPP-0/ddos_spp_firewall_service/'
```

2. Create an ACL record for the service record you created.

```
curl -X POST -u rest_api_user:rest_api_password -H "Content-Type: application/json" -d '{"data":
{"mkey":"acl1","service": "s1","type":"service","service-action":"deny"}}'
'http://172.30.84.121/api/v1/spp/SPP-0/ddos_spp_firewall_policy/'
```

Change a specific threshold

This example changes the value of the TCP protocol threshold to 100 packets per second inbound and 200 packets per second outbound.

```
curl -X POST -u rest_api_user:rest_api_password -H "Content-Type: application/json" -d '{"data":
{"mkey":"t1","protocol-start":"6","protocol-end":"6","inbound-threshold":"100","outbound-threshold":"200"}}' 'http://172.30.84.121/api/v1/spp/SPP-0/ddos_spp_threshold_protocol/'
```

Increase all SPP thresholds by a specified percentage

You can use a value expressed in percent to adjust all the threshold values for a service protection profile (SPP). This mechanism is useful in situations where you expect a sharp rise in server traffic that is not tied to regular patterns, such as after a news release or sales promotion.

This example increases all thresholds for SPP-0 by 10%.

```
curl -X POST -u rest_api_user:rest_api_password -H "Content-Type: application/json" -d '{"data":{"threshold-adjustment-type":"percent-adjust","threshold-percent-adjust":"10"}}'
'http://172.30.84.121/api/v1/spp/SPP-0/ddos_spp_threshold_adjust/'
```

Decrease all SPP thresholds by a specified percentage

This example decreases all thresholds for SPP-0 by 10%.

```
curl -X POST -u rest_api_user:rest_api_password -H "Content-Type: application/json" -d '
    {"data":{"threshold-
adjustment-type":"percent-adjust","threshold-percent-adjust":"-10"}}'
'http://172.30.84.121/api/v1/spp/SPP-0/ddos_spp_threshold_adjust/'
```

Get the full backup configuration file

```
curl -u rest_api_user:rest_api_password 'http://172.30.153.121/api/v1/backup_config/all/'
    -o <output_file_name>
```

Get the backup configuration of a specified SPP

```
curl -u rest_api_user:rest_api_password 'http://172.30.153.121/api/v1/backup_config/SPP-
    0/' -o <output_file_name>
```

Chapter 3: REST API to get monitor graph data

You can use the REST API to retrieve the information displayed in Monitor graphs, such as port statistics, packet counts by protocol, or aggregated counts of dropped packets.

The URLs that you use to retrieve DDoS attack activity statistics use the following format (values in square brackets are not always required):

```
http://<server>/api/<version>/monitor_stats?subtype=<type>&subtype_val=<value>
[&dir={Inbound|Outbound}][&spp_name=<name>&period=<period>
```

where:

- `<server>` is the FQDN or IP address of the management interface.
- `<version>` is the API version (for example, `v1`).
- `<name>` is the name of the SPP. You do not specify SPP for Port Statistics graphs.
- `&subtype=<type>` is the monitor graph to retrieve.
- `&subtype_val=<value>` is a value for specific graphs, such as the protocol number for protocol graphs.
- `&dir={Inbound|Outbound}]` is the traffic direction. You do not specify direction for aggregate graphs.
- `&period=<period>` is the time period. Specify one of the following periods: `1%20hour|8%20hour| 1%20day|1%20week|1%20month|1%20year`

Table 2: Monitor graph subtypes

Subtype	Subtype values	Web UI location
PortPackets	1,2,3,4…15,16 (For 2000B: 1,2,…17,18)	Port Statistics > Packets
PortBits	1,2,3,4…15,16 (For 2000B: 1,2,…17,18)	Port Statistics > Bits
spppkt	N/A	SPP Statistics > Packets
sppbyte	N/A	SPP Statistics > Bits
SubnetPackets	SPP Policy name	SPP Policy Statistics > Packets
SubnetBits	SPP Policy name	SPP Policy Statistics > Bits
SPPPolicyGroupPkts	SPP Policy Group name	SPP Policy Group Statistics > Packets
SPPPolicyGroupBits	SPP Policy Group name	SPP Policy Group Statistics > Bits

Subtype	Subtype values	Web UI location
PacketLength	packet length	Packet Length > Statistics
Agg	N/A	Aggregate Drops > Aggregate
AggFlood	N/A	Flood Drops > Aggregate
AggL3	N/A	Flood Drops > Layer 3
AggL4	N/A	Flood Drops > Layer 4
AggL7Flood	N/A	Flood Drops > Layer 7 > Aggregate
AggL7HTTP	N/A	Flood Drops > Layer 7 > HTTP
AggL7DNS	N/A	Flood Drops > Layer 7 > DNS
AggACL	N/A	ACL Drops > Aggregate
L3ACLAgg	N/A	ACL Drops > Layer 3
L4ACLAgg	N/A	ACL Drops > Layer 4
AggL7ACL	N/A	ACL Drops > Layer 7 > Aggregate
L7HTTPACLAgg	N/A	ACL Drops > Layer 7 > HTTP
L7DNSACLAgg	N/A	ACL Drops > Layer 7 > DNS
AggAnom	N/A	Anomaly Drops > Aggregate
Layer3AnomalyDrops	N/A	Anomaly Drops > Layer 3 Anomaly Drops
AggL4Anom	N/A	Anomaly Drops > Layer 4 > Aggregate
L4Misc	N/A	Anomaly Drops > Layer 4 > Header
TCPAnomDrops	N/A	Anomaly Drops > Layer 4 > State
AggL7Anom	N/A	Anomaly Drops > Layer 7 > Aggregate
HTTPHeaderAnom	N/A	Anomaly Drops > Layer 7 > HTTP Header Anomalies

Subtype	Subtype values	Web UI location
AggDNSAnom	N/A	Anomaly Drops > DNS > Aggregate
DNSHeaderAnomaly	N/A	Anomaly Drops > DNS > Header
DNSRequestAnomaly	N/A	Anomaly Drops > DNS > Query
DNSResponseAnomaly	N/A	Anomaly Drops > DNS > Response
DNSBufferOverflowAnomaly	N/A	Anomaly Drops > DNS > Buffer Overflow
DNSExploitAnomaly	N/A	Anomaly Drops > DNS > Exploit
DNSInfoAnomaly	N/A	Anomaly Drops > DNS > Info
DNSDataAnomaly	N/A	Anomaly Drops > DNS > Data
AggHLL	N/A	Hash Attack Drops > Aggregate
AggL3HLL	N/A	Hash Attack Drops > Layer 3 > Aggregate
SrcHashAttack	N/A	Hash Attack Drops > Layer 3 > Source Table
DestHashAttack	N/A	Hash Attack Drops > Layer 3 > Destination Table
TCPHashAttack	N/A	Hash Attack Drops > Layer 4 > TCP Connection Table
DNSHashAttack	N/A	Hash Attack Drops > Layer 7 > DNS Query Response Table
AggFLP	N/A	Out of Memory Drops > Aggregate
AggL3FLP	N/A	Out of Memory Drops > Layer 3 > Aggregate
SrcOutOfMemory	N/A	Out of Memory Drops > Layer 3 > Source Table
DestOutOfMemory	N/A	Out of Memory Drops > Layer 3 > Destination Table

Subtype	Subtype values	Web UI location
TCPOutOfMemory	N/A	Out of Memory Drops > Layer 4 > TCP Connection Table
DNSOutOfMemory	N/A	Out of Memory Drops > Layer 7 > DNS Query Response Table
MostActiveSource	N/A	Layer 3 > Most Active Source
MostActiveDestination	N/A	Layer 3 > Most Active Destination
UniqueSources	N/A	Layer 3 > Count of Unique Sources
Fragment	N/A	Layer 3 > Fragmented Packets
AddressDenied	N/A	Layer 3 > Address Denied
Protocol	0 to 255	Layer 3 > Protocols
GREDelivery	N/A	Layer 3 > Delivery GRE
SYN	N/A	Layer 4 > SYN Packets
SYNPerSource	N/A	Layer 4 > SYN Per Source
SYNPerDst	N/A	Layer 4 > SYN Per Destination
ConnPerSrc	N/A	Layer 4 > Connection Per Source
LIP	N/A	Layer 4 > New Connections
NonSpoofedIPs	N/A	Layer 4 > Non-Spoofed IPs
TCPStateTable	N/A	Layer 4 > Established Connections
slowconn	N/A	Layer 4 > Slow Connections
TCP	0 to 65535	Layer 4 > TCP Ports
UDP	0 to 65535	Layer 4 > UDP Ports
ICMP	0 to 255	Layer 4 > ICMP Types/Codes

Subtype	Subtype values	Web UI location
HTTPMethod	GET HEAD OPTIONS TRACE POST PUT DELETE CONNECT	Layer 7 > HTTP > Methods
URL	Any text or hash index	Layer 7 > HTTP > URLs
Host	Any text or hash index	Layer 7 > HTTP > Hosts
Referer	Any text or hash index	Layer 7 > HTTP > Referrers
Cookie	Any text or hash index	Layer 7 > HTTP > Cookies
UserAgents	Any text or hash index	Layer 7 > HTTP > User Agents
DNSQuery	N/A	Layer 7 > DNS > Query
QueryPerSrc	N/A	Layer 7 > DNS > Query Per Source
PacketTrackPerSrc	N/A	Layer 7 > DNS > Suspicious Sources
DNSQues	N/A	Layer 7 > DNS > Question Count
DNSMailb	N/A	Layer 7 > DNS > QType MX
DNSAll	N/A	Layer 7 > DNS > QType All
DNSZoneXfer	N/A	Layer 7 > DNS > QType Zone Transfer
RRType	N/A	Layer 7 > DNS > DNS Resource Record Type
DNSFrag	N/A	Layer 7 > DNS > Fragment
DQRMDrop	N/A	Layer 7 > DNS > Unsolicited Response
DNSDupQuery	N/A	Layer 7 > DNS > Unexpected Query
LQDrop	N/A	Layer 7 > DNS > LQ Drop

Subtype	Subtype values	Web UI location
TTLDrop	N/A	Layer 7 > DNS > TTL Drop
CacheDrop	N/A	Layer 7 > DNS > Cache Drop
SpoofedIPDrop	N/A	Layer 7 > DNS > Spoofed IP Drop
DNSRcode	0-15	Layer 7 > DNS > DNS Rcodes

Examples

Retrieve Port Statistics > Packets graph information

```
curl -u rest_api_user:rest_api_password 'http://172.30.153.121/api/v1/monitor_
    stats?subtype=PortPackets
    &subtype_val=1,2&dir=Inbound&period=1 hour'
```

Response:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xport>
   <meta>
      <start>1394639670</start>
      <step>30</step>
      <end>1394639670</end>
      <rows>121</rows>
      <columns>2</columns>
      <legend>
         <entry>Port 1 Egress Packets/sec</entry>
         <entry>Port 2 Ingress Packets/sec</entry>
      </legend>
   </meta>
   <data>
      <row><t>1394639670</t><v0>0.0000000000e+00</v0><v1>0.0000000000e+00</v1></row>
      <row><t>1394639700</t><v0>0.0000000000e+00</v0><v1>0.0000000000e+00</v1></row>
      ............
      <row><t>1394643270</t><v0>0.0000000000e+00</v0><v1>0.0000000000e+00</v1></row>
   </data>
</xport>
```

Table 3: Monitor graph XML structure

XML tag	Description
<start>	Start time in Unix epoch format. For example, if `period=1 hour`, it is 60 minutes before the current time. If `period=8 hours`, it is 8 hours before the current time.
<step>	Time interval in seconds. For example, if `period=1 hour`, the interval is 30 seconds.
<end>	Current time in Unix epoch format.
<rows>	Number of samples received.
<columns>	Number of legends.
<legend>	Label that describes the values provided in the `<data>`section. The first `<entry>` element describes the `<v0>` element, second `<entry>`element describes the `<v1>` element.
<data>	A time in Unix epoch format. The value of `<t>`in the first `<row>` element is the value of `<start>`. The value of `<t>` in subsequent row elements is the previous value increased by the value of the `<step>` element value.

Retrieve Layer 3 > Protocols graph information

```
curl -u rest_api_user:rest_api_password 'http://172.30.153.121/api/v1/monitor_
    stats?subtype=Protocol&
    subtype_val=6&dir=Inbound&spp_name=SPP-0&period=1 hour'
```

Retrieve Aggregate Flood Drops > Aggregate graph information

```
curl -u rest_api_user:rest_api_password 'http://172.30.153.121/api/v1/monitor_
    stats?subtype=AggMain
    &spp_name=SPP-0&period=1 hour'
```

Chapter 4: REST API to get attack graphs and executive summary reports

You can use the REST API to retrieve the drop count reports that are displayed on the Attack Graphs and Executive Summary dashboards.Use the following formats for:

Attack Graphs

```
http://<server>/api/<version>/drop_stats?spp_
name=<name>&subtype=<type>&period=<period>&dir={Inbound|Outbound}&graphquery=true
```

Executive Summary - summary reports

```
http://<server>/api/<api_version>/drop_stats?spp_
name=<name>&subtype=<type>&period=<period>&dir={Inbound|Outbound}
```

Executive Summary - detailed reports

```
http://<server>/api/<api_version>/drop_stats?spp_name=<name>&subtype=<type>
[&allevents=true]&period=<period>&dir={Inbound|Outbound}&field=<field>
```

where:

- `<server>` is the FQDN or IP address of the management interface.
- `<version>` is the API version, for example, `v1`.
- `<name>` is the name of the SPP.
- `&subtype=<type>` is the type of DDoS attack activity statistics to retrieve.
- `&dir={Inbound|Outbound}]` is the traffic direction.
- `&period=<period>` is the time period. Specify one of the following periods: `1%20hour|8%20hour| 1%20day|1%20week|1%20month|1%20year`
- `&graphquery=true` specifies an Attack Graph query.
- `<field>` indicates the field for which details need to be retrieved (Use subnet ID for subnet reports).
- `&acl={true|false}` specifies whether it is an ACL graph/report or not.
- `&allevents=true` indicates to retrieve the Executive Summary detailed report.

Table 4: Attack Graph / Executive Summary subtypes

Subtype	Value
Top Attacks	top_attacks
Top Attackers	top_attackers
Top ACL Drops	top_acl_attacks

Subtype	Value
Top Attacked SPPs	top_attacked_spps
Top SPPs with Denied Packets	top_attacked_acl_spps
Top Attacked Subnets	top_attacked_subnets
Top Attacked Subnets with Denied Packets	top_acl_subnets
Top Attacked Destinations	top_attacked_destinations
Top Attacked Protocols	top_attacked_protocols
Top Attacked TCP Ports	top_attacked_tcp_ports
Top Attacked UDP Ports	top_attacked_udp_ports
Top Attacked ICMP Type Codes	top_attacked_icmp_type_codes
Top Attacked HTTP Methods	top_attacked_http_methods
Top Attacked HTTP Cookies	top_attacked_http_cookies
Top Attacked HTTP Referrers	top_attacked_http_referers
Top Attacked HTTP User Agents	top_attacked_http_user_agents
Top Attacked HTTP Hosts	top_attacked_http_hosts
Top Attacked HTTP URLs	top_attacked_http_urls
Top Attacked DNS Servers	top_attacked_dns_servers
Top Attacked DNS Anomalies	top_attacked_dns_anomalies

Examples

Executive summary (Top Attacked Destinations)

```
curl -u rest_api_user:rest_api_password 'http://172.30.84.121/api/v1/drop_
stats?spp_name=SPP-0&subtype=top_attacked_
destinations&period=1%20week&dir=Inbound'
```

Executive summary Details (Top Attacked Subnets)

```
curl -u rest_api_user:rest_api_password 'http://172.30.84.121/api/v1/drop_
stats?spp_name=SPP-0&allevents=true&subtype=top_attacked_
subnets&period=1%20week&field=0&dir=Inbound'
```

Graph query (Top Attacks)

```
curl -u rest_api_user:rest_api_password 'http://172.30.84.121/api/v1/drop_
stats?spp_name=SPP-0&subtype=top_
attacks&period=1%20day&dir=Inbound&graphquery=true'
```

Chapter 5: REST API for FortiView

You can use the REST API to view FortiView - Threat Map and Tree View. Use the following formats to:

Get Threat Map data for last 1 year (Bar chart):

```
http://<server>/api/<version>/threatmap/<type>/<spp_name>/
```

Get threat map data for last 1 day:

```
http://<server>/api/<version>/threatmap/<type>/<spp_name>/<date>/
```

Generate graphs in tree view:

```
http://<server>/api/<version>/treeview/<time_period>/<direction>/
```

Download the images in tree view:

```
http://<server>/api/<version>/downloadImage?imgPath=<full path to file>/
```

This creates graph images for all configured SPP policies (Graphs: SPP Statistics, Aggregate graphs and SPP Policy graphs)

where:

- `<server>` is the FQDN or IP address of the management interface.
- `<version>` is the API version (for example, `v1`).
- `<type>` is the type of DDoS attack activity statistics to retrieve.
- `<spp_name>` is the name of the SPP.
- `<date>` is the date for which the threatmap has to be displayed.
- `<direction>` is the traffic direction - `{Inbound|Outbound}`.
- `<time_period>` is the time period.

Examples

Get threat map data for last 1 year

```
curl -v -u rest_api_user:rest_api_password
'http://172.30.84.121/api/v1/threatmap/chart/SPP-0/'
```

Get threat map data for last 1 day

```
curl -v -u rest_api_user:rest_api_password
'http://172.30.84.121/api/v1/threatmap/map/SPP-0/2018-01-10/'
```

Generate graphs in tree view

```
curl -v -u rest_api_user:rest_api_password
'http://172.30.84.121/api/v1/treeview/1h/Inbound/'
```

Download the images in tree view:

```
curl -v -u rest_api_user:rest_api_password
'http://172.30.84.121/api/v1/downloadImage?imgPath=%2Fhtml%2Fui%2Fthemes%2Fadc%2Fimg%2F20
18_01_18_11_09_39%2Fsppstats_aggdrop_SPP-0_0_2018_01_18_11_09_39.png'
```

Chapter 6: Error codes

If a REST API request fails for any reason, the response contains the application error code and the HTTP response code is 400 (bad request).

For example, the response code ('-13') in the following example provides the reason for the failure.

Table 5: Error codes

Code	Meaning
-10	Invalid gateway address.
-11	Invalid length of value.
-12	Value out of range.
-13	Entry not found.
-14	Maximum number of entries has been reached.

Code	Meaning
-15	A duplicate entry already exists.
-16	Failed to allocate memory.
-17	Invalid name.
-18	Invalid IP address.
-19	Invalid IP netmask.
-20	Blank entry.
-23	Entry is used.
-24	Error opening file.
-25	Error reading from shared memory.
-26	File error.
-27	Insufficient memory.
-28	File is not an update file.
-30	Invalid username or password.
-36	Blank or incorrect email address.
-37	Permission denied.
-39	Configuration file error.
-45	Invalid IP range.
-46	Port number duplicated or in use.
-47	IP is duplicated.
-48	Failed to change address type.
-49	Password does not match policy.
-50	Invalid replacement message format.
-51	Password is too short.

Code	Meaning
-52	Password must contain at least one uppercase letter.
-53	Password must contain at least one lowercase letter.
-54	Password must contain at least one number.
-55	Password must contain at least one non-alphanumeric character.
-56	Empty value is not allowed.
-57	New password must have at least four characters different from the old password.
-60	Invalid address type.
-61	Input is not as expected.
-67	Physical interface cannot be deleted.
-68	Data interface can not be deleted.
-76	System API error.
-87	Image CRC error.
-89	Invalid number.
-130	Invalid date input.
-131	Invalid year input.
-132	Invalid month input.
-133	Invalid day input.
-134	Invalid time input.
-135	Invalid hour input.
-136	Invalid minute input.
-137	Invalid second input.
-145	The imported local certificate is invalid.
-146	The imported CA certificate is invalid.

Code	Meaning
-147	The certificate is being used.
-173	Initialization context failed.
-174	Set context failed.
-203	IP has been blocked.
-204	Invalid username or password.
-211	Invalid mode.
-215	Invalid entry.
-280	Command timeout.
-281	Failed to add entry.
-282	User canceled.
-283	CMDB API error.
-284	CLI parsing error.
-285	Config condition is not fulfilled.
-286	CLI internal error.
-287	CMDB SQL API error.
-288	Configuration file error
-514	Creating entry error.
-515	Maximum allocated quota is reached.
-516	Failed to delete table entry.
-602	Invalid arguments.
-801	The new image's signature is invalid or contains invalid data.
-802	The new image does not contain a signature.
-803	System upgrade to the new image failed.

Code	Meaning
-804	The new image's signature is invalid or contains invalid data.
-1001	Please wait while the system restarts.
-1002	System shutting down.
-1013	Invalid device ID.
-1014	Device blocked.
-1015	Connection ignored.
-1016	Device added as unregistered.
-1100	Low encryption: Maximum certificate key length.
-1101	Low encryption: Unsupported certificate.
-1103	No more cache can be enabled for LDAP profiles.
-1108	Error changing password.
-1110	Supported key size: 512, 1024, 1536, 2048.
-1900	Log category is not supported.
-2000	PHP internal error (for example, failed to allocate memory).
-2001	PHP invalid arguments.
-2002	Something is wrong while uploading.
-2003	Upload failed (not finished).
-2004	Upload category not supported.
-2005	Download category not supported.
-2006	Failed to convert string to data (PHP internal).
-2007	Failed to do configuration synchronization.
-2008	Failed to set system time.
-2009	Failed to log report run once.

Code	Meaning
-2010	Failed to do alert email connect.
-2011	Failed to set filter for event log.
-2012	Failed to set filter for traffic log.
-2013	Log is not ready.
-2014	User count reached the limit.
-2015	Failed to set filter for DDoS attack log.
-2016	Log subtype is not supported.