FortiDDoS REST API Reference

Version 5.7

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

Friday, June 2, 2023

FortiDDoS REST API Reference

Version 5.7

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-06-30	Initial release of FortiDDoS 5.5.0 REST API Reference

What's new

5.1.0

- REST APIs v2
- SSL Anomaly graph

4.6.0

- REST APIs are added for blocklisted 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 HTTPS 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.

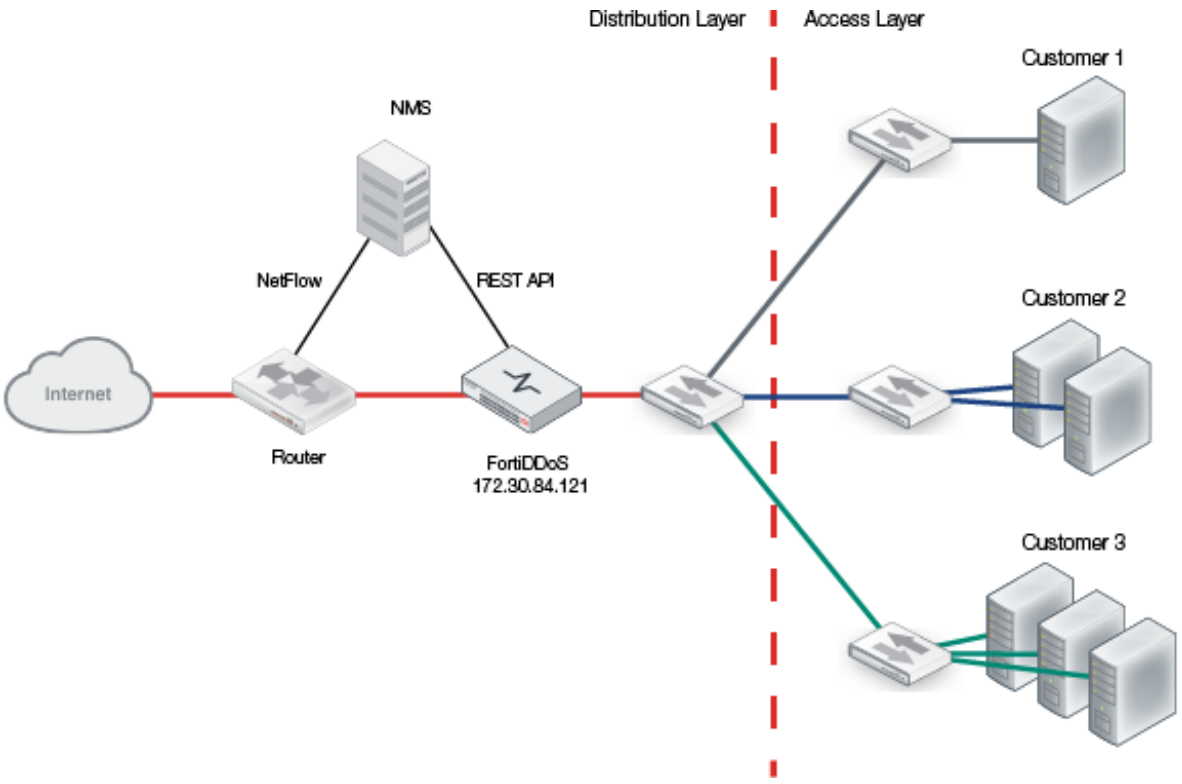
REST API to integrate with other appliances

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.

Configuring FortiDDoSto allow REST API:

FortiDDoS REST API user should have permissions to allow API access. This can be enabled from FortiDDoS UI.

Login to FortiDDoS WebUI

1. Go to System > Admin > Administrator.
2. (Optional) Create a new user.
3. Edit user configuration.
4. Enable allow API access.
5. Save.

Once the user has API access, use the following API to get the authentication token. This authentication tokens will be used for any consecutive REST API calls.

Example:
Step 1: Get the authentication token using the following REST API call.

```
[root@201 ~]# curl -H "ContentType:application/json" -X POST -d '
{"username":"rest_api_admin","password":"rest_api_password"}'
https://172.30.153.169/api/authenticate/ -k
```

Response:

```
{"success":true,"message":"successfully authenticated","access_
token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1ODUxODAwODksImFwaV9pZCI6I
jEifQ.WattuhEO72Zd-Q-JtUJ4-inDWolmPCu7LmWv4YBK7QE","expire":1585180089}
```

Step 2: Use the token from the previous REST API call.

```
curl -H "Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1ODUxODAwODksImFwaV9pZCI6IjEifQ.Wa
ttuhEO72Zd-Q-JtUJ4-inDWolmPCu7LmWv4YBK7QE"
'https://172.30.153.169/api/v2/ddos/global/ddos_global_firewall_address/' --
insecure
```

Response:

```
{"query":"full","success":true,"message":"data generated","data":
[{"mkey":"1","type":"ip-address","ip-netmask":"0.0.0.0\/0","ip-
address":"1.1.1.1","geo-location":"A1"},{"mkey":"10","type":"ip-netmask","ip-
netmask":"10.0.0.0\/8","ip-address":"0.0.0.0","geo-location":"A1"}]}
```

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:

`https://<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, `v2`).
- `<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 -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-LLla9T4Ehf_EFol1O9M2KGm-
rOIGHJ2xDbECPQQm0" 'https://172.30.84.121/api/v2/ddos/global/ddos_global_firewall_
address/' --insecure{"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"}]}
```

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":""}}' -H
"Authorization: Bearer eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-LLla9T4Ehf_EFol1O9M2KGm-
rOIGHJ2xDbECPQQm0" 'https://172.30.84.121/api/v2/ddos/global/ddos_global_firewall_
address/' --insecure
```

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":""}}' -H
"Authorization: Bearer eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-LLla9T4Ehf_EFol1O9M2KGm-
rOIGHJ2xDbECPQQm0" 'https://172.30.84.121/api/v2/ddos/global/ddos_global_firewall_
address/' --insecure
```

Delete an existing global address (DELETE)

```
curl -v -X DELETE -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-LLla9T4Ehf_EFol1O9M2KGm-
rOIGHJ2xDbECPQQm0" 'https://172.30.84.121/api/v1/ddos/global/ddos_global_firewall_
address/a1/' --insecure
```

Download user-uploaded files for blocklisted domains

```
curl -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-LLla9T4Ehf_EFol1O9M2KGm-
rOIGHJ2xDbECPQQm0" 'https://172.30.153.121/api/v2/download_blocklisted_domains' -o
```

```
domain.txt --insecure
```

Download user-uploaded files for blocklisted IPs

```
curl -H "Authorization: Bearer "eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-LLla9T4Ehf_EFol1O9M2KGm-
rOIGHJ2xDbECPQQm0" ' 'https://172.30.153.121/api/v2/download_blocklisted_ipv4_addresses' -
o ip.txt --insecure
```

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 -H "Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-
LLla9T4Ehf_EFol1O9M2KGmrOIGHJ2xDbECPQQm0" 'https://172.30.84.121/api/v2/ddos/global/ddos-
global-spp-policy/' - - insecure
```

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

```
curl -X PUT -H "Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-
LLla9T4Ehf_EFol1O9M2KGmrOIGHJ2xDbECPQQm0" -H "Content-Type: application/json" -d '{"data":
{"mkey":"1","spp":"SPP-1"}}' 'https://172.30.84.121/api/v2/ddos/global/ddos-global-spp-policy/' --insecure
```

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 -H "Authorization: Bearer "eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PCLLla9T4Ehf_EFol1O9M2KGm-
rOIGHJ2xDbECPQQm0" -H "Content-Type: application/json" -d '{"data":
{"mkey":"s1","type":"tcp-port","destination-port-start":"3000","destination-port-
end":"3000"}}' 'https://172.30.84.121/api/v2/spp/SPP-0/ddos_spp_firewall_service/' --
insecure
```

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

```
curl -X POST -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-LLla9T4Ehf_EFol1O9M2KGm-
rOIGHJ2xDbECPQQm0" -H "Content-Type: application/json" -d '{"data":
```

```
{"mkey":"acl1","service":"s1","type":"service","service-action":"deny"}}'
'https://172.30.84.121/api/v2/spp/SPP-0/ddos_spp_firewall_policy/' --insecure
```

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 -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-LLla9T4Ehf_EFol1O9M2KGm-
rOIGHJ2xDbECPQQm0" -H "Content-Type: application/json" -d '{"data":{"mkey":"t1","protocol-
start":"6","protocol-end":"6","inbound-threshold":"100","outbound-threshold":"200"}}'
'https://172.30.84.121/api/v2/spp/SPP-0/ddos_spp_threshold_protocol/' --insecure
```

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 -H "Authorization: Bearer "eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-LLla9T4Ehf_EFol1O9M2KGm-
rOIGHJ2xDbECPQQm0" -H "Content-Type: application/json" -d '{"data":{"threshold-adjustment-
type":"percent-adjust","threshold-percent-adjust":"10"}}' 'https://172.30.84.121/ap-
i/v2/spp/SPP-0/ddos_spp_threshold_adjust/' --insecure
```

Decrease all SPP thresholds by a specified percentage

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

```
curl -X POST -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-LLla9T4Ehf_EFol1O9M2KGm-
rOIGHJ2xDbECPQQm0" -H "Content-Type: application/json" -d '{"data":{"threshold-adjustment-
type":"percent-adjust","threshold-percent-adjust":"-10"}}' 'https://172.30.84.121/ap-
i/v2/spp/SPP-0/ddos_spp_threshold_adjust/' --insecure
```

Get the full backup configuration file

```
curl -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-LLla9T4Ehf_EFol1O9M2KGm-
rOIGHJ2xDbECPQQm0" 'https://172.30.153.121/api/v1/backup_config/all/' -o <output_file_
name> --insecure
```

Get the backup configuration of a specified SPP

```
curl -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-LLla9T4Ehf_EFol1O9M2KGm-
rOIGHJ2xDbECPQQm0" 'https://172.30.153.121/api/v2/backup_config/SPP-0/' -o <output_file_
name> --insecure
```

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):

```
https://<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
SSLStateAnom	N/A	Anomaly Drops > Layer 7 > SSL
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

Subtype	Subtype values	Web UI location
DestOutOfMemory	N/A	Out of Memory Drops > Layer 3 > Destination Table
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

Subtype	Subtype values	Web UI location
LQDrop	N/A	Layer 7 > DNS > LQ Drop
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 -H "Authorization: Bearer
    eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-
    LLla9T4Ehf_EFol1O9M2KGmrOIGHJ2xDbECPQQm0" 'https://172.30.153.121/api/v2/monitor_
    stats?subtype=PortPackets&subtype_val=1,2&dir=Inbound&period=1 hour' --insecure
```

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 -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-LLla9T4Ehf_EFol1O9M2KGm-
rOIGHJ2xDbECPQQm0" 'https://172.30.153.121/api/v2/monitor_stats?subtype=Protocol&subtype_
val=6&dir=Inbound&spp_name=SPP-0&period=1 hour' --insecure
```

Retrieve Aggregate Flood Drops > Aggregate graph information

```
curl -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-LLla9T4Ehf_EFol1O9M2KGm-
rOIGHJ2xDbECPQQm0" 'https://172.30.153.121/api/v2/monitor_stats?subtype=AggMain
&spp_name=SPP-0&period=1 hour' --insecure
```

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

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

Executive Summary - summary reports

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

Executive Summary - detailed reports

```
https://<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-H "Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.P
C-LLla9T4Ehf_EFol1O9M2KGmrOIGHJ2xDbECPQQm0"'https://172.30.84.121/api/v2/drop_
stats?spp_name=SPP-0&subtype=top_attacked_
destinations&period=1%20week&dir=Inbound' --insecure
```

Executive summary Details (Top Attacked Subnets)

```
curl -H "Authorization: Bearer
```

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.P
C-LLla9T4Ehf_EFol1O9M2KGmrOIGHJ2xDbECPQQm0" 'https://172.30.84.121/api/v2/drop_
stats?spp_name=SPP-0&allevents=true&subtype=top_attacked_
subnets&period=1%20week&field=0&dir=Inbound' --insecure
```

Graph query (Top Attacks)

```
curl -H "Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.P
C-LLla9T4Ehf_EFol1O9M2KGmrOIGHJ2xDbECPQQm0" 'https://172.30.84.121/api/v2/drop_
stats?spp_name=SPP-0&subtype=top_
attacks&period=1%20day&dir=Inbound&graphquery=true' --insecure
```

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):

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

Get threat map data for last 1 day:

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

Generate graphs in tree view:

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

Download the images in tree view:

```
https://<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, `v2`).
- `<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 -H "Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-
LLla9T4Ehf_EFol1O9M2KGmrOIGHJ2xDbECPQQm0"
'https://172.30.84.121/api/v2/threatmap/chart/SPP-0/' --insecure
```

Get threat map data for last 1 day

```
curl -v -H "Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-
LLla9T4Ehf_EFol1O9M2KGmrOIGHJ2xDbECPQQm0"
'https://172.30.84.121/api/v2/threatmap/map/SPP-0/2018-01-10/' --insecure
```

Generate graphs in tree view

```
curl -v -H "Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-
LLla9T4Ehf_EFol1O9M2KGmrOIGHJ2xDbECPQQm0"
'https://172.30.84.121/api/v2/treeview/1h/Inbound/' --insecure
```

Download the images in tree view:

```
curl -v -H "Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1ODQxNDgzNDYsImFwaV9pZCI6IjEifQ.PC-
LLla9T4Ehf_EFol1O9M2KGmrOIGHJ2xDbECPQQm0"
'https://172.30.84.121/api/v2/downloadImage?imgPath=%2Fhtml%2Fui%2Fthemes%2Fadc%2Fimg%2
F2018_01_18_11_09_39%2Fsppstats_aggdrop_SPP-0_0_2018_01_18_11_09_39.png' --insecure
```

Chapter 6: REST API for Flowspec

You can use the REST API to initiate Flowspec and retrieve the BGP Flowspec from FortiDDoS.

You can do this to integrate this with an upstream service provider to send them BGP Flowspec messages so that they can block very specific attacks right in their network before forwarding rest of the traffic to your network.

To do this:

1. Authenticate to receive token
2. Get Global Destinations Under Attack
3. Generate Flowspec
4. Confirm Status that file is available to download
5. Download BGP Flowspec File

Examples:

Authenticate to receive token

Sample Request:

```
curl -H "ContentType:application/json" -XPOST -d
{"username":"admin","password":"fdd"}'
https://172.30.153.161/api/authenticate/ -k
```

- Ensure that the user has API Access
- The token received will then be used for all subsequent calls

Sample Response:

```
{"success":true,"message":"successfully authenticated","access_
token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2MjQ2NDMzNDUsImFwaV9pZ
CI6IjEifQ.5MkcOINWnQNYQ3IFjNKMGIjvPEf7NYg8h7v0P-YG5h4","expire":1624643345}
```

Get Global Destinations Under Attack

Sample Request:

```
curl -k -H "Authorization:Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2MjQzODgxMzgsImFwaV9pZCI6IjEif
Q.fXrmSsT8b6Bb7Bbh7neAZZZhrfpo646nY6r3uOWvSxs"
'https://172.30.153.161/api/v2/flowspec_destinations’
```

Sample Response:

```
Array
(:: [
1] => Array
   (
      [mkey] => 1
      [ip-address] => 21.10.9.236
      [dropcount] => 361187365
```

```
        [events] => 0
        [suggested-threshold] => 0
    )
:
:
:
}
```

Request to Generate Flowspec for One of the Top Attacked Destinations

Sample Request:

```
curl -k -v -X PUT -H "Content-Type: Application/json" -d '{"mkey":"-1",
"data": {"generate":"enable","destination":"1.1.1.1", "threshold":"10000",
"vendor":"Cisco"}}' -H "Authorization:Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2MjQzODgxMzgsImFwaV9pZCI6IjEif
Q.fXrmSsT8b6Bb7Bbh7neAZZZhrfpo646nY6r3uOWvSxs"
'https://172.30.153.161/api/v2/flowspec_generate'
```

Confirm Status that file is available to download

Sample Request:

```
curl -k -H "Authorization:Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2MjQzODgxMzgsImFwaV9pZCI6IjEif
Q.fXrmSsT8b6Bb7Bbh7neAZZZhrfpo646nY6r3uOWvSxs"
'https://172.30.153.161/api/v2/flowspec_status' -o flowspec_status.json
```

Sample Response

```
{"generate":"disable","destination":"0","dropcountthreshold":"
    1000","vendor":"Cisco","report-status":"Available, generated on 2020-06-24
    15:13:00"}
```

Download BGP Flowspec File

Sample Request:

```
curl -k -H "Authorization:Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2MjQzODgxMzgsImFwaV9pZCI6IjEif
Q.fXrmSsT8b6Bb7Bbh7neAZZZhrfpo646nY6r3uOWvSxs"
'https://172.30.153.161/api/v2/flowspec_config' -o flowspec_json
```

Sample Response: Flowspec_json

```
configure
   class-map type traffic match all block-21.10.9.236-1
      match destination-address 21.10.9.236/32
      match protocol 6
      match tcp-flag 2 any
end-class-map
```

Chapter 7: REST API for Dropped Packet Capture

Before you begin:

- DPC ports must be configured from the GUI or CLI. Please see system documentation for Network Interfaces and Appendix H: Dropped Packet Capture.
- To use the REST API, you must have API system access and obtain an Authentication. See pages 9 and 10 of this document.

Note: Thresholds and Anomaly parameters must be set in order for drops to be seen via Drop Packet Capture.

Overview

Drop Packet Capture allows you to capture a wide range of dropped packets while under flood. FortiDDoS does not store dropped packets, it outputs them through a traffic port where a PC of server running Wireshark, tcpdump or similar applications captures the packets for further analysis.

The packet capture REST call is structured with:

- A DPC “module” which defines the general parameter of the capture such as:
  - AggL7DNS where all DNS flood drops are defined
  - AggL3 where all Layer 3 flood drops are defined
- A DPC “legend” or label where the specific drop parameter is defined, such as:
  - AggL7DNS | LQ Drop
  - AggL7DNS | Aggregate
  - AggL3 | Fragmented Packets
  - AggL4 | Aggregate
- In some cases a DPC “specific value” where a more specific parameter is defined, such as:
  - Protocol |Packets Dropped | 17
  - UDP | Packets Dropped | 53

Please see the table below for a list of all Modules and associated Legends for DPC.

Duration of the capture can be:

- *Timed* – Timer is determined by **Global Settings > Settings > Settings: Dropped Packet Capture Timeout**. Timer range is 0-3600 seconds.
- *Perpetual* – capture until stopped
- *Stop* – Stop either a “perpetual” or a “timed” capture (before the timer expires)

Examples

Request a *Perpetual* capture for Aggregate L7 NTP, NTP Response Flood drops, inbound

```
curl -L -w "%{http_code} %{url_effective}\\n" -X PUT \
-H"Authorization:Bearer\eyJ0eXAiOiJKV1QiLCJhbGciOi JIUzI1NiJ9.eyJleHAiOjE2NTA0Nz
UxNTMsImFwaV9pZCI6IjEifQ.B1PyfGyrVej qeKfUS3xakvuPoSLIWzXuXcRxefejHzs" \-H "Content-
    Type:application/json" \-d '{"data":{"spp":"SPP-0",
"direction":"inbound",
"module":"AggL7NTP", "legend":"Response Flood Drops", "mode":"perpetual"}}' \
```

```
'https://172.30.153.127/api/v2/dropped_packets_capture/' -insecure
```

Sample Response:

```
200 https://172.30.153.127/api/v2/dropped_packets_capture/
```

Note: This is the expected response for any good Query. See "Chapter 9: Error codes" on page 47 for error codes.

Request a timed capture for Protocol 17 (UDP) dropped packets, inbound

```
curl -L -w "%{http_code} %{url_effective}\\n" -X PUT \
-H "Authorization:Bearer \ eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
eyJleHAiOjE2NTA0NzUxNTMsImFwaV9pZCI6IjEifQ.B1PyfGyrVejqeKfUS3xakvuPoSLIWzXuXcRxefejHzs"
    \
-H "Content-Type:application/json" \
-d '{"data":{"spp":"SPP-0","direction":"inbound",
"module":"Protocol","legend":"Packets Dropped", "mode":"timed", "specific_
    value":"17"}}' \
'https:172.30.153.127/api/v2/dropped_packets_capture/' --insecure
```

Request a timed capture for UDP Source/Destination Port 53 dropped packets, inbound

```
curl -L -w "%{http_code} %{url_effective}\\n" -X PUT \
-H "Authorization:Bearer \ eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
eyJleHAiOjE2NTA0NzUxNTMsImFwaV9pZCI6IjEifQ.B1PyfGyrVejqeKfUS3xakvuPoSLIWzXuXcRxefejHzs"
    \
-H "Content-Type:application/json" \
-d '{"data":{"spp":"SPP-0","direction":"inbound",
"module":"UDP","legend":"Packets Dropped", "mode":"timed", "specific_value":"53"}}' \
'https:172.30.153.127/api/v2/dropped_packets_capture/' --insecure
```

Request a timed capture for Aggregate L7 DNS, Legitimate Query Table (LQ) drops, inbound

```
curl -L -w "%{http_code} %{url_effective}\\n" -X PUT \
-H "Authorization:Bearer\eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9
.eyJleHAiOjE2NTA0NzUxNTMsImFwaV9pZCI6IjEifQ.B1PyfGyrVe
jqeKfUS3xakvuPoSLIWzXuXcRxefejHzs"
\-H "Content-Type:application/json" \-d '{"data":{"spp":"SPP-0",
"direction":"inbound",
"module":"AggL7DNS", "legend":"LQ Drop", "mode":”timed"}}' \
'https://172.30.153.127/api/v2/dropped_packets_capture/' -insecure
```

Request a timed capture for all Aggregate L7 DNS drops, inbound

```
curl -L -w "%{http_code} %{url_effective}\\n" -X PUT \
-H "Authorization:Bearer\eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9
.eyJleHAiOjE2NTA0NzUxNTMsImFwaV9pZCI6IjEifQ.B1PyfGyrVe
jqeKfUS3xakvuPoSLIWzXuXcRxefejHzs"
\-H "Content-Type:application/json" \-d '{"data":{"spp":"SPP-0",
"direction":"inbound",
"module":"AggL7DNS", "legend":"Aggregate", "mode":”timed"}}' \
'https://172.30.153.127/api/v2/dropped_packets_capture/' -insecure
```

Stop the previous perpetual capture

```
curl -L -w "%{http_code} %{url_effective}\\n" -X PUT \
-H"Authorization:Bearer\eyJ0eXAiOiJKV1QiLCJhbGciOi JIUzI1NiJ9.eyJleHAiOjE2NTA0Nz
UxNTMsImFwaV9pZCI6IjEifQ.B1PyfGyrVej qeKfUS3xakvuPoSLIWzXuXcRxefejHzs" \-H "Content-
    Type:application/json" \-d '{"data":{"spp":"SPP-0",
"direction":"inbound",
"module":"AggL7NTP", "legend":"Response Flood Drops", "mode":"stop"}}'
\'https://172.30.153.127/api/v2/dropped_packets_capture/' -insecure
```

Sample Response:

```
200 https://172.30.153.127/api/v2/dropped_packets_capture/
```

Module	Legend	Specific value
AggL3	Aggregate	
	Protocols	
	Fragmented Packets	
	Source Flood	
	Destination Flood	
AggL4	Aggregate	
	SYN	
	TCP Ports	
	UDP Ports	
	ICMP Types/Codes	
	Zombie Flood	
	SYN Per Source	
	Connections Per Source	
	SYN Per Destination	
	Slow Connection	

Module	Legend	Specific value
AggL7DNS	Aggregate	
	Unsolicited DNS Response Drop	
	LQ Drop	
	TTL Drop	
	Cache Drop	
	Spoofed IP Drop	
	Unexpected Query Drop	
	Query Per Source Drop	
	Suspicious Sources Drop	
	Fragment Drop	
	TCP Query Drop	
	TCP Question Drop	
	TCP MX Drop	
	TCP All Drop	
	TCP Zone Transfer Drop	
	DNS Response Code Flood Drop	
AggL7HTTP	Aggregate	
	Method Flood	
	Method Per Source	
	URL Flood	
	Host Flood	
	User Agent Flood	
	Cookie Flood	
	Referer Flood	

Module	Legend	Specific value
AggL7NTP	Aggregate	
	Request Flood Drops	
	Response Flood Drops	
	Broadcast Flood Drops	
	Response per Destination Flood Drops	
DNSBufferOverflowAnomaly	Message too long	
	Name too long	
	Label length too large	
DNSDataAnomaly	Pointer loop	
	Zone Transfer	
	Class not in	
	Buffer Underflow	
	Empty message	
	Message ends prematurely	
DNSHeaderAnomaly	Invalid Opcode	
	Illegal Flag	
	Source/Destination both port 53	
DNSInfoAnomaly	Type all used	
DNSRequestAnomaly	Query Bit Set	
	RA Bit Set	
	Null Query	
	QD Count not One	

Module	Legend	Specific value
DNSResponseAnomaly	QClass in Response Qtype in Response Query bit not set QD count not 1	
HTTPHeaderAnom	Known Method Unknown Method Invalid HTTP Version Range Present Incomplete HTTP Request	
ICMP Note: to capture all ICMP Type/Code drops use Protocol 1	Packets Dropped Packets Blocked	Type/Code index. Note: converting Types/Codes to an index requires decimal to binary conversion and multiplication. One way to convert is to create an SPP Service ACL for ICMP Type Code. Enter a single Type and Code in both Start and End fields (8:0, for example) and Save. The index will show (2048).
L3ACLAgg	Aggregate Protocol Denied Drops Fragmented Packet Denied Drops Geo Location Denied Drops Address Denied Drops IP Reputation Denied Drops Local Address Anti	

Module	Legend	Specific value
L4ACLAgg	Aggregate	
	TCP Port Denied Drops	
	UDP Port Denied Drops	
	ICMP Type/Code Denied Drops	
L4Misc	Aggregate	
	TCP Checksum Error	
	UDP Checksum Error	
	ICMP Checksum Error	
	TCP Invalid Flag Combination	
	Anomaly Detected	
	Invalid ICMP Type/Code	
	GRE Checksum Error	
	GTP	
L7DNSACLAgg	Aggregate	
	Frag Drops	
	MX Drops	
	Qtype All Drops	
	Zone Transfer Drops	
	Query Restricted To Specific Subnet Drops	
	Query Blocked (Blocklisted Domains)	
	DNS Resource Record Type Drops	
L7NTPACLAgg	NTP Reflection ACL Drops	

Module	Legend	Specific value
L7HTTPACLAgg	Aggregate URL Denied Drops Host Denied Drops Cookie Denied Drops Referer Denied Drops UserAgent Denied Drops	
Layer3AnomalyDrops	Aggregate IP Header Checksum Error Layer 3 Source and Destination Address Match Source/Destination as LocalHost	
NTPHeaderAnomaly	Version Stratum Data Length Control Header	
NTPStateAnomaly	Duplicate Requests Before Response Unsolicited Response Sequence Mismatch Mode Mismatch	
Protocol	Aggregate Packets Dropped Packets Blocked	Enter no “specific value” for “legend” = Aggregate Otherwise “specific value” = Layer 3 Protocol Number

Module	Legend	Specific value
SSLStateAnom	Aggregate SSL Renegotiation (Both legends capture the same info)	
TCP	Aggregate Packets Dropped Packets Blocked	Enter no “specific value” for “legend” = Aggregate Otherwise “specific value” = Port Number
TCPAnomDrops	Aggregate Forward Transmission Not Within Window Reverse Transmission Not Within Window TCP State Transition Foreign Packets (Out of State) Foreign Packets (Aggressive Aging and Slow Connections)	
UDP	Packets Dropped Packets Blocked	Enter no “specific value” for “legend” = Aggregate Otherwise “specific value” = Port Number

Chapter 8: REST API for Legitimate Query list

Before you use REST for LQ upload:

- Enable *Allow Only Valid Queries Under Flood (LQ)* on the SPP used for mitigation.
- Read the Handbook or Online Help section on Configuring Legitimate Query (LQ) lists
- Prepare an upload file in CSV (comma delimited) format. File content must be FQDN (e.g. 12.3.45.fortinet.com), Type (Resource Record), Class (always Internet = 1) with one entry per line. Examples:

- ortinet.com,1,1 (for an A-record)
- email.fortinet.com,15,1 (for an MX-record)
- fortinet.com,28,1 (for an AAAA-record)

Notes:

- Uploading a new file, replaces any existing file, including any manually-added single FQDNs (see below)
- When uploaded via REST, the file is immediately applied to the hardware after removing any previous list
- LQ table will be automatically re-applied (and previous upload and any LQs from passing traffic cleared) based on the **Global Settings > Settings: LQ Apply Schedule**
- LQ table will not be re-applied if DNS attack drops are over the Threshold configured in **Global Settings > Settings: LQ Drop Threshold**
- The LQ Table is global and will be used by any SPP where Allow Only Valid Queries Under Flood (LQ) is enabled

The following commands assume you have obtained the authentication token described earlier.

To Upload the LQ List

```
curl -L -w "%{http_code} %{url_effective}\\n" -X POST \
-H "Authorization:Bearer \
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NTA0NzUxNTMsImFwaV9pZCI6IjEifQ.B1PyfGy
    rVejqeKfUS3xakvuPoSLIWzXuXcRxefejHzs" \
-H "Content-Type:text/csv" \
--data-binary \
@lq.txt \
'https://172.30.153.127/api/v2/legitimate_queries/' --insecure
```

Note: To Clear an LQ list, upload a blank file or a file with one dummy LQ entry.

To Download the LQ List

```
curl -H "Authorization: Bearer \
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NTA0NzUxNTMsImFwaV9pZCI6IjEifQ.B1PyfGy
    rVejqeKfUS3xakvuPoSLIWzXuXcRxefejHzs" \
'https://172.30.153.127/api/v2/download_legitimate_queries' -o lq.txt --insecure
```

To Add a single LQ entry:

```
curl -L -w "%{http_code} %{url_effective}\\n" -X POST \
-H "Authorization:Bearer \
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NTA0NzUxNTMsImFwaV9pZCI6IjEifQ.B1PyfGy
    rVejqeKfUS3xakvuPoSLIWzXuXcRxefejHzs" \
-H "Content-Type:application/json" \
-d '{"data":{"query":"sample.com","type":"1","class":"1"}}' \
'https://172.30.153.127/api/v2/legitimate_queries/' --insecure
```

To Delete a single LQ entry:

```
curl -L -w "%{http_code} %{url_effective}\\n" -X DELETE \
-H "Authorization:Bearer \
```

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NTA0NzUxNTMsImFwaV9pZCI6IjEifQ.B1PyfGy
    rVejqeKfUS3xakvuPoSLIWzXuXcRxefejHzs" \
-H "Content-Type:application/json" \
'https://172.30.153.127/api/v2/legitimate_queries/?query.com,1,1' -insecure
```

Chapter 9: 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.

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.