DDoS Attack Mitigation

FortiDDoS™ 4.1.6

REST API Reference

FortiDDoS 4.1.6 REST API Reference

May 15, 2015

1st Edition

Technical Documentation	http://docs.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forum
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

What's new

The following features are new or changed since FortiDDoS 4.0:

FortiDDoS 4.1.6

- Updated "Traffic graph subtypes and subtype parameters" on page 16 to reflect the 4.1.6 set of graphs.

FortiDDoS 4.1

- **Access blocked and dropped traffic statistics** — You can now use the REST API to retrieve statistics counts of packets that FortiDDoS has dropped or blocked. This is the information that the web UI displays on the Attack Graphs and Executive Summary dashboards. See "Accessing dropped and blocked traffic statistics" on page 13.
- **Access traffic graph information** — You can now use the REST API to retrieve the information the web UI displays as traffic graphs, such as port statistics, packet counts by protocol, or aggregated counts of dropped packets. See "Accessing traffic graph information" on page 15.

FortiDDoS API

REST API overview

FortiDDoS provides a Representational State Transfer (REST) API that you can use to interact with its components. Programs communicate with the REST API over HTTP, the same protocol that your web browser uses to interact with web pages.

The REST API is based on interactions with a web page. Data is treated like a static web page.

- Add data by POSTing a web page
- Fetch data by GETing a web page
- Update data by PUTing a web page
- Delete data by DELETEing a web page

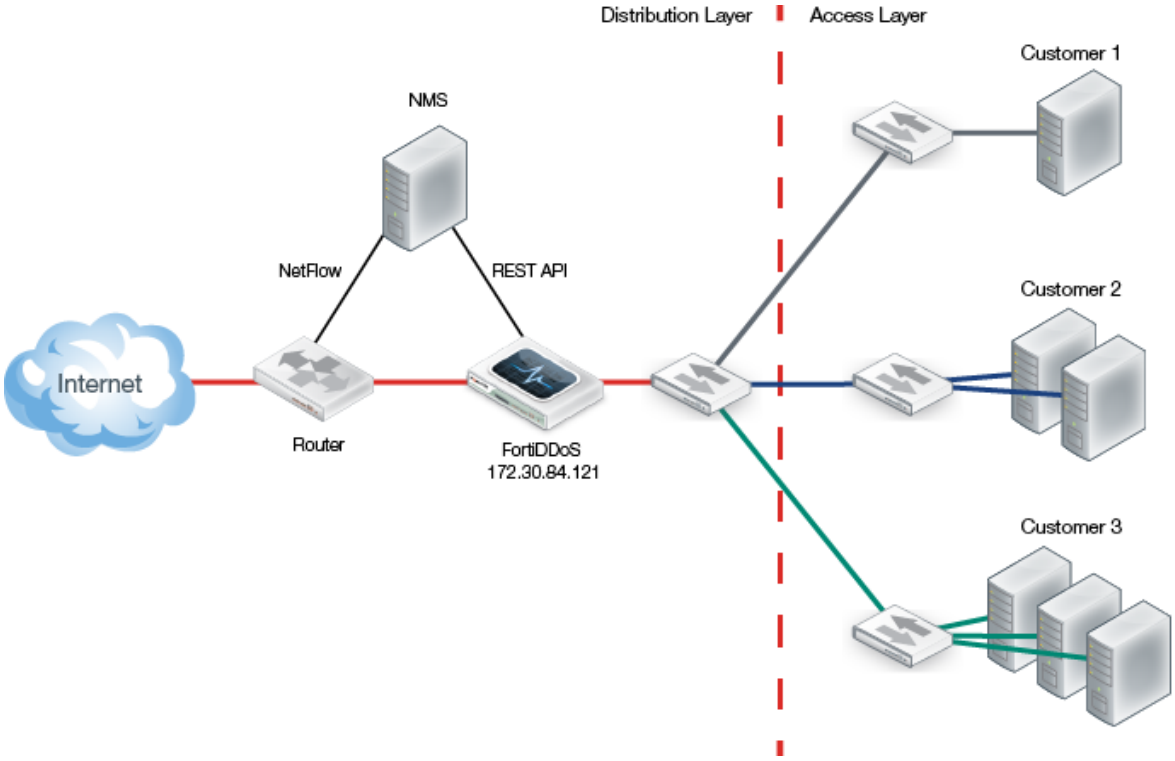
After it receives the request, the FortiDDoS API returns an HTTP response code. These codes are discussed later in this reference.

Using the 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 example in the illustration, the NMS monitors a router in the service provider's network. The NMS, in turn, communicates with FortiDDoS using the REST API.



For examples of the API calls that this integration can use, see "Examples" on page 14.

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.

Examples

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.

Supported API methods

The FortiDDoS REST API supports the following methods.

For access to attack mitigation statistics and traffic graph information, only the `GET` method is available.

Method	URI	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

Accessing FortiDDoS settings and other resources

Format

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

```
http://<server_name>/api/<api_version>/<group_name>/
  <resource_name>/[id]/
```

where:

- `<server_name>` is the name or IP address of the FortiDDoS appliance
- `<api_version>` is the API version (for example, `v1`)
- `<group_name>` is one of the following values:
  - `system`
  - `ddos/global`
  - `spp/<profile_name>`, where `<profile_name>` is the name of the service protection profile (SPP)
  - `log`
- `<resource_name>` is the name of the FortiDDoS setting or other resource
- `[id]` is a unique identifier for a FortiDDoS setting or other resource (required for DELETE only)

For more information on the `<group_name>` and `<resource_name>` values, see “Specifying resources” on page 8.

Specifying resources

Currently, you can use the API to access the following resources:

Group name	Resource name	Supported methods	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 > Config > High Availability
	snmp_sysinfo	GET, PUT	System > Config > SNMP > SNMP System Information
	snmp_threshold	GET, PUT	System > Config > SNMP > SNMP Threshold
	snmp_community	GET, POST, PUT, DELETE	System > Config > SNMP > Community
	adminuser	GET, POST, PUT, DELETE	System > Admin > Administrators
	accprofile	GET, POST, PUT, DELETE	System > Admin > Access Profile
	sysglobal	GET, PUT	System > Admin > Settings
	certificate_local	GET, POST, DELETE	System > Certificates > Local

Group name	Resource name	Supported methods	Web UI location
ddos/global	ddos-global-spp-switching-policy	GET, PUT	Global Settings > Service Protection Profiles > Switching Policy
	ddos_global_setting	GET, PUT	Global Settings > Settings > Settings
	ddos_global_ipreputation	GET, PUT	Global Settings > IP Reputation > IP Reputation
	ddos_global_proxy_ip	GET, PUT	Global Settings > Proxy IP > Proxy IP
	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_policy	GET, POST, PUT, DELETE	Global Settings > Do Not Track Policy > Do Not Track PolicyIPv6
	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_bypass_macs	GET, POST, PUT, DELETE	Global Settings > Bypass MAC > Bypass MAC

Group name	Resource name	Supported methods	Web UI location
spp/ <profile_name>	ddos_spp_setting	GET, PUT	Protection Profiles > SPP Settings > SPP Settings
	threshold	GET, POST, PUT, DELETE	Protection Profiles > Thresholds > Thresholds
	ddos_spp_threshold_adjust	POST	Protection Profiles > Thresholds > Factory Defaults
	ddos_spp_threshold_adjust	POST	Protection Profiles > Thresholds > Percent Adjust
	ddos_spp_threshold_adjust	POST	Protection Profiles > Thresholds > Emergency Setup
	ddos_spp_threshold_adjust	POST	Protection Profiles > Thresholds > System Recommendation
	ddos_spp_firewall_address	GET, POST, PUT, DELETE	Protection Profiles > Address > Address Config
	ddos_spp_firewall_address6	GET, POST, PUT, DELETE	Protection Profiles > Address > Address Config IPv6
	ddos_spp_firewall_service	GET, POST, PUT, DELETE	Protection Profiles > Service > Service Config
	ddos_spp_firewall_policy	GET, POST, PUT, DELETE	Protection Profiles > Access Control List > Access Control List
	ddos_spp_reset	GET, POST, PUT, DELETE	Protection Profiles > Factory Reset > Factory Reset
log	log_local	GET, PUT	Log & Report > Log Configuration > Log Settings
	log_remote	GET, POST, PUT, DELETE	Log & Report > Log Configuration > Log Remote
	log_report	GET, POST, PUT, DELETE	Log & Report > Report Configuration > Report Configuration

Examples

Retrieve all global addresses (GET)

```
curl -u admin:
'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/'
```

Change the service protection profile (SPP) that regulates a subnet

Service protection profile (SPP) policies specify the SPP that monitors and regulates a subnet. By changing the SPP, 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 admin
   '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\/2
   4","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 admin -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 admin -H "Content-Type: application/json" -d
'{"data":{"mkey":"s1","type":"tcp-port","destination-port-start":"30
00","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 admin -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 admin -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 admin -H "Content-Type: application/json" -d
'{"data":{"threshold-adjustment-type":"percent-adjust","threshold-perc
ent-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 admin -H "Content-Type: application/json" -d
'{"data":{"threshold-adjustment-type":"percent-adjust","threshold-perc
ent-adjust":"-10"}}'
'http://172.30.84.121/api/v1/spp/SPP-0/ddos_spp_threshold_adjust/'
```

Accessing dropped and blocked traffic statistics

You can use the REST API to retrieve counts of packets that FortiDDoS has dropped or blocked. The API can retrieve the same information that FortiDDoS displays on the Attack Graphs and Executive Summary dashboards.

Format

The URLs that you use to retrieve DDoS attack activity statistics use the following format:

```
http://<server_name>/api/<api_version>/drop_stats?spp_name=<profile_name>
&subtype=<subtype_name>[&dir={Inbound|Outbound}]&period{1 hour|8 hour|1 day|1 week|1 month|1 year}
```

where:

- `<server_name>` is the name or IP address of the FortiDDoS appliance
- `<api_version>` is the API version (for example, `v1`)
- `<profile_name>` is the name of the service protection profile (SPP)
- `<subtype_name>` is the type of DDoS attack activity statistics to retrieve. For a list of valid types, see "Attack activity statistics subtypes" on page 13.
- `[&dir={Inbound|Outbound}]` is the direction of traffic; not used for subtypes that end with the suffix `_summary`
- `{1 hour|8 hour|1 day|1 week|1 month|1 year}` is the time period

Attack activity statistics subtypes

Currently, you can use the API to access the following types of detailed attack activity statistics, which are also displayed on the Attack Graphs dashboard in the web UI:

Subtype	Value
SPP Attacks	`spp_graph_query`
Top Attacked Subnets	`top_attacked_subnets`
Top Attacked Protocols	`top_attacked_protocols`
Top Attacks	`top_attacks`
Top Attackers	`top_attackers`
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`

Subtype	Value
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
SPP ACL Drops	spp_graph_query_acl
Top ACL Subnet Drops	top_attacked_subnets_acl
Top ACL Drops	top_attacks_acl

Use the API to access the following types of summary attack activity statistics, which are also displayed on the Executive Summary dashboard in the web UI:

Subtype	Value
Top Attacks	top_attacks_summary
Top Attacked Subnets	top_attacked_subnets_summary
Top Attacked Protocols	top_attacked_protocols_summary
Top Attackers	top_attackers_summary
Top Attacked TCP Ports	top_attacked_tcp_ports_summary
Top Attacked UDP Ports	top_attacked_udp_ports_summary
Top Attacked ICMP Type Codes	top_attacked_icmp_type_codes_summary
Top Attacked URLs	top_attacked_http_urls_summary
Top Attacked HTTP Methods	top_attacked_http_methods_summary
Top Attacked HTTP Cookies	top_attacked_http_cookies_summary
Top Attacked HTTP Referrers	top_attacked_http_referers_summary
Top Attacked HTTP User Agents	top_attacked_http_user_agents_summary
Top Attacked HTTP hosts	top_attacked_http_hosts_summary
Top ACL Subnet Drops	top_attacked_subnets_acl_summary
Top ACL Drops	top_attacks_acl_summary

Examples

Retrieve the total number of dropped or blocked packets

```
curl -u admin
'http://172.30.153.121/api/v1/drop_stats?spp_name=SPP-0&subtype=spp_gr
aph_query&dir=Inbound&period=1 hour'
```

Response:

```
{"data":[{"sppid":"0","dir":"Inbound","timestamp":"2014\/03\/07
10:58:00","dropcount":"4984"},
  {"sppid":"0","dir":"Inbound","timestamp":"2014\/03\/07
  10:59:00","dropcount":"4989"},
  ....
  ],"total":10,"success":true,"message":""}
```

Retrieve the total number of dropped or blocked packets by subnet

```
curl -u admin
'http://172.30.153.121/api/v1/drop_stats?spp_name=SPP-0&subtype=
top_attacked_subnets &dir=Inbound&period=1 hour'
```

Response:

```
{"data":[{"subnetid":"0","dir":"Inbound","timestamp":"2014\/03\/07
11:10:00","dropcount":"24882"},
  {"subnetid":"0","dir":"Inbound","timestamp":"2014\/03\/07
  11:15:00","dropcount":"24879"},
  ....
  ],"total":10,"success":true,"message":""}
```

Retrieve the total number of packets blocked by the ACL configuration

```
curl -u admin
'http://172.30.153.121/api/v1/drop_stats?spp_name=SPP-0&subtype=spp_gr
aph_query&dir=Inbound&period=1 hour&acl=true'
```

Retrieve a summary of top attacks

```
curl -u admin
'http://172.30.153.121/api/v1/drop_stats?spp_name=SPP-0&subtype=top_at
tacks_summary&period=1 week'
```

Accessing traffic graph information

You can use the REST API to retrieve the information displayed in FortiDDoS traffic graphs, such as port statistics, packet counts by protocol, or aggregated counts of dropped packets. The API can retrieve the same information that FortiDDoS displays in the graphs you use the *Monitor* menu to access.

Format

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_name>/api/<api_version>/monitor_stats?subtype=<subtype_
name>[&subtype_val=<subtype_value>[&dir={Inbound|Outbound}]
[&spp_name=<profile_name>&period{1 hour|8 hour|1 day|1 week|1 month|1
year}
```

where:

- `<server_name>` is the name or IP address of the FortiDDoS appliance
- `<api_version>` is the API version (for example, `v1`)
- `<subtype_name>` is the type of traffic graph to retrieve
- `<subtype_value>` specifies the traffic graph values to retrieve
- `{Inbound|Outbound}` is the direction of traffic
- `<profile_name>` is the name of the service protection profile (SPP)
- `{1 hour|8 hour|1 day|1 week|1 month|1 year}` is the time period

For the subtypes, valid subtype values, and information on required parameters, see

Traffic graph subtypes and subtype parameters

Currently, you can use the API to access the following types information, which are also displayed in the traffic graphs in the web UI:

Subtype	Subtype values	spp_name	dir	Web UI location
`PortPackets`	`1,2,3,4…15,16` (For 2000B: `1,2,3,4…17,18`)	N/A	Required	Port Statistics >Packets
`PortBits`	`1,2,3,4…15,16` (For 2000B: `1,2,3,4…17,18`)	N/A	Required	Port Statistics > Bits
`Protocol`	0 to 255	Required	Required	Specific Graphs > Protocols
`TCP`	0 to 65535	Required	Required	Specific Graphs > TCP Ports
`UDP`	0 to 65535	Required	Required	Specific Graphs > UDP Ports
`ICMP`	0 to 255	Required	Required	Specific Graphs > ICMP Types/Codes
`URL`	Any text or hash index	Required	Required	Specific Graphs > URLs
`Host`	Any text or hash index	Required	Required	Specific Graphs > Hosts
`Referer`	Any text or hash index	Required	Required	Specific Graphs > Referrers
`Cookie`	Any text or hash index	Required	Required	Specific Graphs > Cookies
`UserAgents`	Any text or hash index	Required	Required	Specific Graphs > User Agents

Subtype	Subtype values	spp_name	dir	Web UI location
Agg	N/A	Required	N/A	Aggregate Drops > Aggregate
AggFlood	N/A	Required	N/A	Flood Drops > Aggregate
AggL3	N/A	Required	N/A	Flood Drops > Layer 3
AggL4	N/A	Required	N/A	Flood Drops > Layer 4
AggL7	N/A	Required	N/A	Flood Drops > Layer 7
AggACL	N/A	Required	N/A	ACL Drops > Aggregate
L3ACLAgg	N/A	Required	N/A	ACL Drops > Layer 3
L4ACLAgg	N/A	Required	N/A	ACL Drops > Layer 4
L7ACLAgg	N/A	Required	N/A	ACL Drops > Layer 7
AggAnom	N/A	Required	N/A	Anomaly Drops > Aggregate
Layer3AnomalyDrops	N/A	Required	Required	Anomaly Drops > Layer 3 Anomaly Drops
L4Misc	N/A	Required	Required	Anomaly Drops > Layer 4 Header Anomalies
TCPAnomDrops	N/A	Required	Required	Anomaly Drops > TCP State Anomalies
HTTPHeaderAnom	N/A	Required	Required	Anomaly Drops > HTTP Header Anomalies
SrcHashAttack	N/A	Required	Required	Hash Attack Drops > Source Table
DestHashAttack	N/A	Required	Required	Hash Attack Drops > Destination Table
TCPHashAttack	N/A	Required	Required	Hash Attack Drops > Connection Table
SrcOutOfMemory	N/A	Required	Required	Out of Memory Drops > Source Table
DestOutOfMemory	N/A	Required	Required	Out of Memory Drops > Destination Table
TCPOutOfMemory	N/A	Required	Required	Out of Memory Drops > Connection Table
MostActiveSource	N/A	Required	Required	Layer 3 > Most Active Source
MostActiveDestination	N/A	Required	Required	Layer 3 > Most Active Destination
UniqueSources	N/A	Required	N/A	Layer 3 > Count of Unique Sources
Fragment	N/A	Required	Required	Layer 3 > Fragmented Packets
DeniedCountries	N/A	Required	Required	Layer 3 > Address Denied
SYN	N/A	Required	Required	Layer 4 > SYN Packets
SYNPerSource	N/A	Required	Required	Layer 4 > SYN Per Source
SYNPerDst	N/A	Required	Required	Layer 4 > SYN Per Destination
ConnPerSrc	N/A	Required	Required	Layer 4 > Connection Per Source

Subtype	Subtype values	spp_name	dir	Web UI location
ConnPerDst	N/A	Required	Required	Layer 4 > Connection Per Destination
ACKPerDst	N/A	Required	Required	Layer 4 > ACK Per Destination
RSTPerDst	N/A	Required	Required	Layer 4 > RST Per Destination
FINPerDst	N/A	Required	Required	Layer 4 > FIN Per Destination
ESTABPerDst	N/A	Required	Required	Layer 4 > ESTAB Per Destination
LIP	N/A	Required	Required	Layer 4 > New Connections
TCPStateTable	N/A	Required	Required	Layer 4 > Established Connections
HTTPMethod	GET, HEAD, OPTIONS, TRACE, POST, PUT, DELETE, CONNECT	Required	Required	Layer 7 > HTTP Methods

Examples

Retrieve Port Statistics > Packets graph information

```
curl -u admin
'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+0
    0</v1></row>
    <row><t>1394639700</t><v0>0.0000000000e+00</v0><v1>0.0000000000e+0
    0</v1></row>
    ............
    <row><t>1394643270</t><v0>0.0000000000e+00</v0><v1>0.0000000000e+0
    0</v1></row>
  </data>
</xport>
```

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.
`<entry>` (`<legend>` element)	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.
`<t>` (`<data>` element)	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 Specific Graphs > Protocols graph information

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

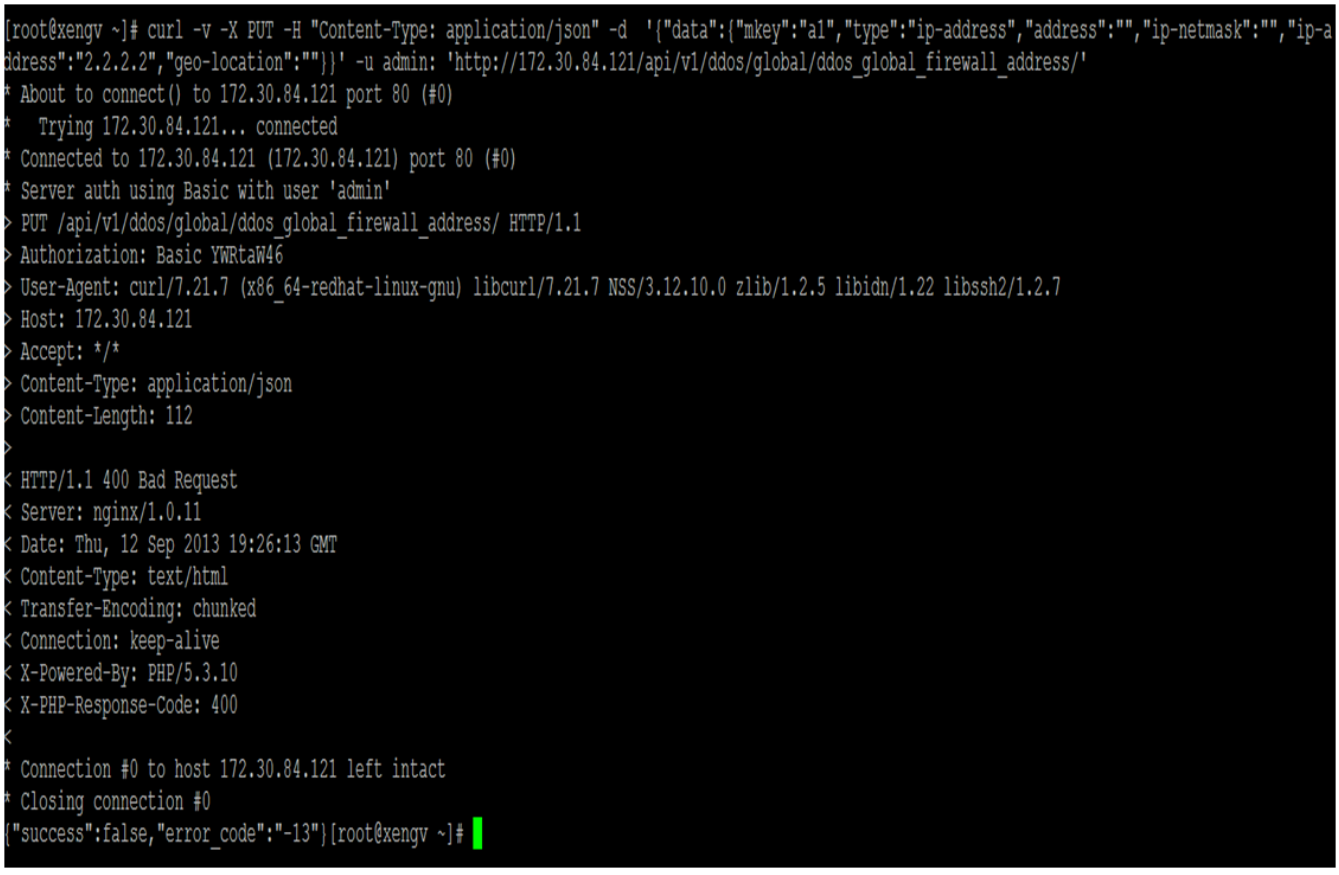
Retrieve Aggregate Flood Drops > Aggregate graph information

```
curl -u admin
'http://172.30.153.121/api/v1/monitor_stats?subtype=AggMain
&spp_name=SPP-0&period=1 hour'
```

Request failure

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. For a list of FortiDDoS API application error codes and descriptions, see "Error codes" on page 21.



Error codes

FortiDDoS displays the following error codes as negative values.

Code	
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.
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.

Code	
51	Password is too short.
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.
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.

Code	
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.
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.

Code	
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.
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.