FortiDDoS-F - Handbook

Version 6.1.1

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 7, 2021
FortiDDoS-F 6.1.1 Handbook
00-611-681153-20210507

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-07-22	Updated *What's New*
2021-06-04	Updated *Appendix D*
2021-05-19	Updated *Downgrading firmware*
2021-05-11	Updated *Appendix E*
2021-05-07	Initial release of FortiDDoS 6.1.1 Handbook

Introduction

FortiDDoS F-Series is a network behavior anomaly (NBA) distributed denial of service (DDoS) prevention system that detects and blocks attacks that intend to disrupt network service by overwhelming server and/or other network resources.

FortiDDoS uses a variety of methods, including anomaly detection, Source IP validation and statistical techniques, to provide nonstop protection, including as-yet unknown “zero-day” attacks. When FortiDDoS detects an attack, it immediately drops traffic from the offending source, thus protecting the systems it defends from floods.

Product features

The following features make FortiDDoS the best in its class:

Purpose-built for low latency and rapid response

The patented combination of high-performance platforms and heuristics allow you to deploy the FortiDDoS appliance inline between the external network and protected services, where it maintains high packet processing rates, even when under attack. FortiDDoS features very low latency, and identifies and begins responding to attacks within 2 seconds or less.

Massive-scale SYN, DNS, NTP, and Refelcted UDP flood mitigation

Among others, SYN, DNS, NTP and UDP Reflected flood mitigation techniques not only protect your network from DDoS attacks but, importantly, enable your business to continue to serve legitimate client purposes during attacks.

Flexible Network Environments

FortiDDoS operates inline with one or more Internet links at the very edge of your local network. It has no IP nor MAC addresses in the data path and is invisible to attackers. It fully supports asymmetric networks with:

- 2 or more links passing through the FortiDDoS
- The main inbound link passing through and the main outbound link bypassing FortiDDoS
- A FortiDDoS on each of the asymmetric links

FortiDDoS supports High Availability in a unique way. The Primary appliance or VM controls most configuration items and particularly Thresholds and service features but both devices pass traffic. This allows traffic to work in failover mode or active-active on 2 devices.

Initial learning periods

FortiDDoS learns based on inbound and outbound traffic rates for more than 230,000 parameters. First, deploy the system in Learning Mode (Detection Mode with no Thresholds), where the system learns traffic patters without dropping any packets.

At the end of the initial learning period, create system-recommended threshold from the learned traffic. Continue to use Detection Mode to review logs for false positives and false negatives. As needed, adjust thresholds and monitor the results.

When you are satisfied with the system settings, change to Prevention Mode. In Prevention Mode, the appliance validates and drops packets based on the set Thresholds, and other parameters such as anomalies and ACLs.

Continuous learning

FortiDDoS begins learning traffic patterns as soon as it begins monitoring traffic, and it never stops learning. It continuously analyzes traffic rates and dynamically adjusts the thresholds that differentiate between legitimate traffic volume and attacks. At any time, you can request new Traffic Statistics Reports for any period fro 1-hour to 1-year prior to the current time, compare those with previous reports and/or convert them to new System Recommended Thresholds.

Machine Learning Adaptive Thresholds

27 of the most important FortiDDoS Thresholds continuously adapt their thresholds based on machine learning algorithms continuously examining the last 6 weeks of traffic. The algorithms are fully autonomous but can be adjusted by the user for their circumstances. Adaptive Thresholds are intended to compensate for “seasonal” and special-event changes in traffic without forcing the user to make manual adjustments.

Zero Day attack prevention with granular attack detection and prevention

FortiDDoS’ massively parallel processing allows monitoring of parameters no one has thought of to create attacks – yet. Within the 230,000 parameters monitored, FortiDDoS protects all 256 Layer 3 Protocols, not just a few like competitors and ISP mitigation. FortiDDoS specifically protects more than 10,000 UDP Source Ports that can be used for Reflections even though only about 25 ports are know reflectors in 2020 and no competitor automatically monitors even those 25 ports.

Administrators do not need to intervene, and the appliance is “on guard” 24/7, automatically protecting your network systems and bandwidth.

Granular attack detection thresholds

100% packet inspection from Layer 3 t Layer 7 (no sampling) ensures even single anomalous packets are seen and dropped, reducing network scans and other “junk” traffic.

Deep packet inspection

FortiDDoS architecture enables deep packet inspection. FortiDDoS can identify header fields in HTTP, DNS and NTP packets and maintain specific thresholds for all 8 HTTP Methods as well as URLs, Hosts, Cookies, Referrers and User Agents. FortiDDoS inspects DNS and NTP Header and payload packets evaluating both packet rates and per-packet anomalies used by attackers. This granularity enables very accurate mitigation of attacks without disrupting legitimate traffic.

Source validation address matching and Response matching

Proprietary algorithms validate sources of SYN and DNS Query floods to eliminate spoofed sources while allowing legitimate users. DNS and NTP algorithms validate individual Responses to stop DNS and NTP Reflected Response attacks from the first packet while maintain service for your users and clients.

Service Protection Policies (SPPs)

FortiDDoS supports from 4 to 16 Service Protection Policiees (SPPs) which contain independent sets of protections for L3-L7 anomalies, validation and Thresholds for more than 230,000 parameters in each direction. Web servers use different thresholds and settings than email servers or firewalls. ISPs use different thresholds than enterprise.

Each SPP supports from 512 to 1023 Protection Subnets depending on the model and each subnet can range from a single IPv4/32 or IPv6/128 to larger than /16. SPPs support IPv4 and IPv6 simultaneously. Each Service Protection Policy learns traffic rates independently for all 230,000 parameters in each direction.

ACLs

While ACLs are not normally used for DDoS mitigation since most attacks use spoofed Source IPs, FortiDDoS architecture supports a wide range of high-performance ACLs that can be used to offload other network infrastructure. These include many thousands of ACLs for IPs, subnets, TCP and UDP Source and/or Destination Ports, Protocols, DNS Resource Records and others.

Cloud signaling

Cloud Signaling allows you to use Fortinet global DDoS cloud mitigation service Partners to assist with attacks that exceed the capacity of your Internet links.

FortiDDoS also supports Flowspec scripts that can be forwarded to ISPs to help them mitigate specific large attacks.

Intuitive analysis tools and reports

The 100% on-box reporting tools enable graphical analysis of network traffic history from five minutes to one year. You can analyze traffic profiles using a broad range of Layer 3, 4 or 7 parameters. With just a few clicks, you can create intuitive and useful reports such as top attackers, top attacks, top attack destinations, top connections, and so on.

Viewing traffic monitor graphs

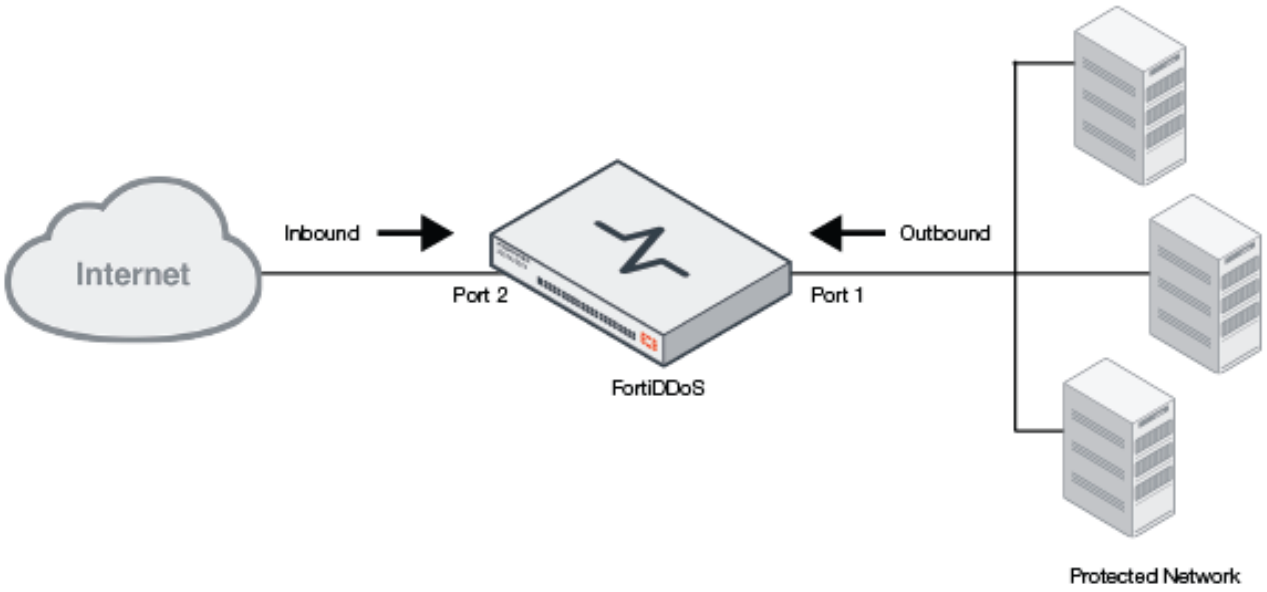
Traffic monitor graphs display trends in throughput rates and drop counts due to threat prevention actions. In Detection Mode, the drop count is hypothetical, but useful as you tune detection thresholds.

External Reporting

FortiDDoS supports a flexible suite of syslog and SNMP traps to allow external reporting and storage of attack information.

Deployment topology

The FortiDDoS appliance is deployed inline between the Internet and the local network to protect the local network servers from volume-based attacks like floods and attacks that send anomalous packets to exploit known vulnerabilities.



You can deploy FortiDDoS in more complex and specialized topologies.

Refer to the following sections:

- Deployment Topologies
- High Availability Deployments

Document Scope

FortiDDoS Manuals

- FortiDDoS Handbook describes how to get started with the system, how to modify and manage configurations, how to monitor traffic, and how to troubleshoot system issues.
- FortiDDoS QuickStart Guide for your appliance has details about the hardware components, ports, and LEDs.
- FortiDDoS Datasheet has detailed specifications. The product datasheet also lists throughput per model. Please use those resources to size your deployment, select the appropriate hardware models, and install the hardware into an appropriate location and machine environment.

What's New

This section provides a summary of the new features and enhancements in FortiDDoS.

What's New in FortiDDoS 6.x

6.1.0

New features

FortiDDoS-F6.1.1 is built on the feature base of FortiDDoS-F B/E-Series with these notable additions:

- VM support in VMware hypervisor environments
- NTP from E-Series on all models
- Additional SSL DDoS Mitigation settings
- 16x SPPs in1500F
- The System Recommendation changes from 5.4.0 (Separate L4 Scalars/ICMP / TCP Ports / UDP Port) are included
- DNS Rcode Scalars are included in Traffic Statistics and System Recommendation
- Split System Recommendation for Layer 4 Scalars/ICMP, TCP Ports and UDP Ports included from B/E 5.4.0
- Common UDP Source Reflection Ports are pre-populated in Global Service definitions for use with Global or SPP ACLs
- Service port definitions support Source Port or Destination Port. Source Port ACLs are very useful for permanently blocking kown UDP reflection ports.
- IP Address / Subnets definitions are created in the System menu and then assigned to Global or SPP ACLs, reducing multiple entries.
- Bogons IPs and/or Multicast IPs can be ACLed with option selection in any SPP.
- SPPs replace feature tabs with multiple Profiles for IP, ICMP, TCP, HTTP, SSL/TLS, NTP and DNS. One Profiles can be used by muliple SPPs or one SPP can use Multiple Profiles (TCP Detection and TCP Prevention, for example).
- Source MAC address for aggressive aging is configurable per SPP, if needed
- Strict Anomalies options are now included in several SPP Profile pages for Layer 2 to Layer 7 options.
- Cloud Signaling Thresholds are entered in both pps and Mbps (crossing either triggers Signaling. Thresholds are now per SPP Policy (subnet).
- Protection Subnets (subnets) are entered for each Service Protection Policy (SPP) instead of globally.
- Explicit TCP thresholds are added for DNS Query, Question Count, Fragment, MX and ALL. B/E-Series has TCP Thresholds but they are hidden and the same as the UDP Thresholds.
- IP Reputation and Domain Reputation are included in IP and DNS Profiles and thus are optional per SPP.
- SSL/TLS Profile includes additional Cipher Anomaly option
- tcpdump-style packet capture

- Several formerly-global features such as IP Reputation are now set per SPP for better control
- Additional Known Method Anomalies available

Removed/Changed/Deferred Features

B/E-Series Functionality not included in this release:

- Support for FortiDDoS-CM Central Manager
- Security Fabric Integration with FortiOS Dashboard
- GTP-U support
- Distress ACL nor Auto-Distress ACL
- Multi-tenant support (SPP or SPP Policy Group)
- Fewer files included in Offline analysis file
- SPP Backup/Restore
- Attack Reports are Global only and are on-demand or on-schedule only. Report periods are Last 7 Days, Last Month or Last year only. (Removed per-SPP, per-SPP Policy, per-SPP Policy Group reports, on-Threshold reports and some time periods)
- REST API changes and requires documentation
- Log & Report > DDoS Attack Graphs
- SPP Policy Groups
- Log & Report > Diagnostics
- SPP-to-SPP Switching Policies
- Restrict DNS Queries to specific subnets
- System Recommendation Option for Actual or System Max Outbound Threshold (5.4.0)
- Traffic Statistics Option for Peak or 95th Percentile Traffic (5.4.0)
- Syslog RFC 5424 or Fortinet proprietary secure "OFTP" protocol (5.4.0)
- CLI Commands for IP Reptution nor Domain Reputation updates (5.4.0)
- Search for IP addresses within various ACLs (5.3.0)

VM limits

- VMs do not support Fail-Open option. Fail-Open support will be determined by the underlying server
- TCP Port Thresholds are calculated to 65,535 but Thresholds/Ranges are created for ports 1-1023 with one range for ports above 1023.
- TCP Port Graphs display traffic and drops for Ports 1-1023. Port 1024 displays peak traffic rate for any port from 1024-65,535 and total drops associated with any of those ports. Attack logs show full port range 1-65,535.
- UDP Port Thresholds are calculated to 65,535 but Thresholds/Ranges are created for 1-10,239 only with one range above that.
- UDP Port Graphs display traffic and drops for Ports 1-10,239. Port 10,240 displays peak traffic rate for any port from 10,240-65,535 and total drops associates with any of those ports. Attack logs show full port range 1-65,535 as well as reflected attack drops from ports 1-9,999.
- ICMP Type/Code Thresholds are calculated from 0-65,535 but Threshold/Ranges are created for 0-10,239 only. Indexes from 10,240 to 65,535 are included in one range.
- ICMP Type/Code graphs show indexes from 0/0 to 39/255 with all others showing in 40/0. Attack logs will show drops for Types/Codes for all Types/Codes from 0/0 to 255/255.

Key Concepts

This section describes FortiDDoS-F concepts, terms, and features. If you are new to FortiDDoS-F, or distributed denial of service (DDoS), this section helps you to understand the problem and mitigation techniques.

DDoS attack overview

Computer network security is a challenge as old as the Internet itself. The sophistication and infamy of network-based system attacks has kept pace with the security technology and hackers only feel more challenged by the latest heuristics designed to foil their efforts.

Some attackers exploit system weaknesses for political purposes, disgruntled about the state of software or hardware in the market today. Others target specific systems out of spite or a grudge against a specific company.

Yet others are simply in search of the infamy of bringing a high-traffic site to its knees with a denial of service (DoS) attack. In such an attack, the hacker attempts to consume all the resources of a networked system so that no other users can be served. The implications for victims range from a nuisance to millions of dollars in lost revenue.

In distributed denial of service (DDoS) attacks, attackers write a program that will covertly send itself to dozens, hundreds, or even thousands of other computers. These computers are known as 'bots', 'agents' or 'zombies', because they act on behalf of the hackers to launch an attack against target systems. A network of these computers is called a botnet. An administrator of such a botnet is called a botmaster.

At a predetermined time, the botmaster will cause all of these bots to attempt repeated connections to a target site. If the attack is successful, it will deplete all system or network resources, thereby denying service to legitimate users or customers.

Control of such bots is automated now-a-days with bot-control-panels which are accessible via payment to the bot-master. Thus other users can choose to pay and attack a site of their own choice.

E-commerce sites, domain name servers, web servers, and email servers are all vulnerable to these types of attacks. IT managers must take steps to protect their systems—and their businesses—from irreparable damage.

Any computer can be infected, and the consequences can range from a nuisance popup ad to thousands of dollars in costs for replacement or repair. For this reason, antivirus software for all PCs should be a mandatory element of any network security strategy. But whether you measure cost in terms of lost revenue, lost productivity, or actual repair/restore expenses, the cost of losing a server to an attack is far more severe than losing a laptop or desktop.

Servers that host hundreds or thousands of internal users, partners, and revenue-bearing services are usually the targets of hackers, because this is where the pain is felt most. Protecting these valuable assets appropriately is paramount.

A massive DDoS attack against Dyn.com was launched in October 2016. This was done using Internet of Things (IoT) attack using an attack called Mirai.

Mirai spreads by compromising vulnerable IoT devices such as DVRs. Many IoT manufacturers failed to secure these devices properly, and they don't include the memory and processing necessary to be updated. They are also usually not in control of the destination of their outbound traffic, so if that information is changed or compromised there is nothing they can do.

As a result, the attack cannot be stopped at the egress point on the devices themselves. Instead, network segmentation is absolutely critical for protection against outbound attacks. The responsibility for protection from IoT-based DDoS attacks, however, lies at the ingress point of the attack.

To circumvent detection, attackers are either increasingly mimicking the behavior of a large number of clients or actually using a large number of IoT clients like in case of Mirai attack. The resulting attacks are hard to defend against with standard techniques, as the malicious requests differ from the legitimate ones in intent but not in content. Because each attacking system looks innocent, advanced techniques are required to separate the 'bad' traffic from the 'good' traffic.

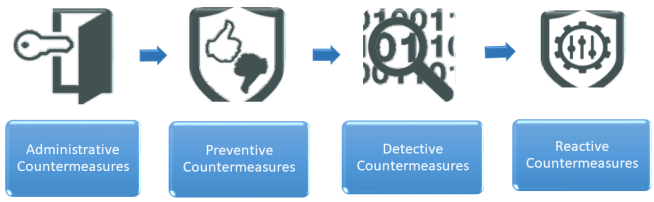
DDoS attack mitigation mechanisms

If you are new to FortiDDoS, you must first understand the tools available in your tool chest for Distributed Denial of Service (DDoS) attack mitigation. Since DDoS attacks can be of various types, FortiDDoS has a wide spectrum of capabilities for different attack types.

FortiDDoS supports the following type of countermeasures:

a. Administrative
b. Preventive
c. Detective
d. Reactive

These can be used for deployment in the order below:



Administrative Countermeasures

Security policies, general procedures, accepted safety guidelines and so on are considered as Administrative Countermeasures. These depend on the organizations that use FortiDDoS. Examples of Administrative countermeasures are restricting IP addresses for managing FortiDDoS and restricting access authorization to different users based on their roles. This should be the first set of decisions made while designing a FortiDDoS deployment.

Preventive Countermeasures

Proactive measures fall under prevention category. These include stringent security policies that can protect the system from unwanted activities. Examples of these include IP Reputation Service, Domain Reputation Service, Geo-location

ACLs, BCP-38 anti-spoofing, maintaining network hygiene by blocking unwanted protocols, ports and IP ranges and so on. These should be designed and used as the second step in the deployment.

Preventive Countermeasures	Description
Service Protection Policy (SPP)	This is a fundamental architectural component of FortiDDoS which ensures isolation. Every SPP, which is configured using a set of subnets/prefixes, has its own set of policies. This ensures that an attack on one SPP doesn't impact the others. For more information about configuring SPPs, see here.
Directional Protection	Attack mitigation in FortiDDoS is directional. Thus, an attack in one direction doesn't impact the other.
IP Reputation Service	The FortiGuard IP Reputation Service aggregates malicious source IP data from the Fortinet distributed network of threat sensors, CERTs, MITRE, cooperative competitors, and other global sources that collaborate to provide up-to-date threat intelligence about hostile sources. Near real-time intelligence from distributed network gateways combined with world-class research from FortiGuard Labs helps organizations stay safer and proactively block attacks. For more information about configuring IP Reputation Service, see here.
Domain Reputation Service	The FortiGuard Domain Reputation Service provides a regularly updated list of known malicious fully qualified domain names (FQDNs). This service is used to prevent DNS servers from reaching known malicious sites and helps prevent attacks that obfuscate source IPs using hijacked domain names. For more information about configuring Domain Reputation Service, see here.
Blocklisted IP addresses	This feature helps you to deny a large set of blocklisted IPv4 Addresses. For more information about configuring blocklisted IP addresses, see here.
Blocklisted DNS domains	This feature helps you to deny a large set of blocklisted Domains. For more information about configuring blocklisted DNS domains, see here.
Geo-location access control list	The geolocation policy feature enables you to block traffic from the countries you specify, as well as anonymous proxies and satellite providers, whose geolocation is unknown. For more information about configuring Geo-location access control list, see here.
Access control list for addresses	This feature allows you to block addresses, subnets, prefixes reaching a protected address. For more information about configuring Access control list for addresses, see here.
Access control list for services	This feature allows you to block services (such as protocols, ports, network parameters such as fragmentation, URLs, user-agents, etc.). For more information about configuring Access control list for services, see here.
Proxy IP settings	Enabling proxy IP settings avoids false detection of attacks for certain IPs. For more information about configuring Proxy IP settings, see here.

Detective countermeasures

A DDoS attack must be detected within the shortest time possible as accurate as it can be. A DDoS attack mitigation system must be able to separate legitimate packets from attack packets. This ensures that legitimate clients are served during attack. Examples of detective countermeasures include anomalies such as header, state, rate and so on. Other reactive countermeasures include similarity detection such as packet-length statistics.

Detective Countermeasures	Description
Rate anomaly detection using continuously adaptive threshold violation	This is the most well-known feature of FortiDDoS. This ensures that a single packet type (say SYN, or packet for a certain protocol or port) cannot exceed previously observed thresholds.
Slow attack detection	Apart from detecting fast attacks, FortiDDoS can also monitor attacks that are too slow but dangerous for servers via connection table overload.
Protocol header anomaly detection	This is done for 3, 4 and 7 protocols. Mitigation includes IPv4/v6, TCP, UDP, ICMP, DNS and HTTP header anomalies.
State anomaly detection	FortiDDoS maintains multiple state tables to ensure that protocol state transitions are not violated. These include: • TCP state table - This can identify attacks such as foreign packets, ACK flood, RST flood, FIN flood etc. • DNS query response matching table • DNS TTL table

Reactive countermeasures

After detecting an attack, the system need to take necessary actions to mitigate the attack. Examples of reactive mechanisms in FortiDDoS include rate limiting, selective packet dropping, aggressive aging, anti-spoofing, source tracking and so on. These are mostly event-driven countermeasures.

Reactive Countermeasures	Description
Rate Based	There are two types of attack mitigation: • High Rate Attack Mitigation: Some attacks are identified if they exceed the rate thresholds set by the administrator. Such thresholds can be selectively set on a wide variety of parameters. They get adaptively adjusted over time based on average, trend and seasonality. This is the most well-known feature of FortiDDoS which ensures that a single packet type (say SYN, or packet for a certain protocol or port) cannot exceed previously observed thresholds. • Slow Rate Attack Mitigation: Some attacks are identified if they are too slow to be real traffic. The administrator can set thresholds for such determination.
Aggressive Aging	FortiDDoS can detect slow connection attacks and combat them by “aggressively aging” idle connections. In addition to the slow connection detection, you can use the SPP aggressive aging TCP connection feature control options to reset the connection (instead of just dropping the packets)

Reactive Countermeasures	Description
	when the following rate anomalies are detected: • high-concurrent-connection-per-source • layer7-flood FortiDDoS maintains its own massive TCP connection table and to reserve space in this table for active traffic, FortiDDoS periodically uses aggressive aging to reset inactive connections. For more information about the above features, see here.
Anti-spoofing	This is done via the following Source Address Validation schemes: • SYN cookie • ACK cookie • SYN Retransmission • DNS Retransmission (DNS TC=1) • **Source tracking** - This isolates an offending source IP specifically via a differential punishment scheme. • **Caching** - In case of DNS, under-flood, this technique is used to respond to the client using data from the cache.

Mitigation Strategies

FortiDDoS supports the following mitigation strategies:

- **Standalone mitigation**
  - The appliance acts standalone and mitigates DDoS attacks up to the bandwidth of the pipe.
- **Hybrid mitigation**
  - With another FortiDDoS in the cloud - If your service provider allows another high-end FortiDDoS ahead of the pipe, FortiDDoS in the data center can communicate with the FortiDDoS in the service provider network and mitigate higher bandwidth attacks.
  - With a cloud scrubbing service in the cloud - FortiDDoS in the data center can signal third-party scrubbing services and mitigate bandwidth attacks collaboratively. While the cloud scrubbing center can mitigate layer 3 and layer 4 attacks, FortiDDoS in the data center can mitigate residual attacks such as application layer, slow attacks which cannot be mitigated in the cloud.

DDoS mitigation techniques overview

The best security strategies encompass people, operations, and technology. The first two typically fall within an autonomous domain, e.g. within a company or IT department that can enforce procedures among employees, contractors, or partners. But since the Internet is a public resource, such policies cannot be applied to all potential users of a public website or email server. Thankfully, technology offers a range of security products to address the various vulnerabilities.

Firewalls

Firewalls can go a long way to solving some problems by restricting access to authorized users and blocking unwanted protocols. As such, they are a valuable part of a security strategy. But public websites and eCommerce servers cannot know in advance who will access them and cannot 'prescreen' users via an access list. Certain protocols can be blocked by firewalls, but most DoS attacks utilize authorized ports (e.g. TCP port 80 for a web server) that cannot be blocked by a firewall without effectively blocking all legitimate HTTP traffic to the site, thereby accomplishing the hacker's objective.

Firewalls offer some security against a single user DoS attack by denying access to the offending connection (once it is known), but most DoS attacks today are distributed among hundreds or thousands of zombies, each of which could be sending legal packets that would pass firewall scrutiny. Firewalls perform a valuable service in an integrated security strategy, but firewalls alone are not enough.

Router access control lists

Likewise, access lists in the router can be used to block certain addresses, if such addresses can be known a priori. But websites open to the public are, by nature, open to connections from individual computers, which are exactly the agents hackers use to initiate attacks. In a DDoS attack, thousands of innocent looking connections are used in parallel. Although router access lists can be used to eliminate offending packets once they are identified, routers lack the processing power and profiling heuristics to make such identifications on their own.

In addition, complex access lists can cause processing bottlenecks in routers, whose main function is to route IP packets. Performing packet inspections at Layers 3, 4, and 7 taxes the resources of the router and can limit network throughput.

Antivirus software

End systems cannot be considered secure without antivirus software. Such software scans all inputs to the system for known viruses and worms, which can cause damage to the end system and any others they may infect. Even after a virus is known and characterized, instances of it are still circulating on the Internet, through email, on CDs and floppy disks. A good antivirus subscription that is frequently updated for the latest protection is invaluable to any corporate or individual computer user.

But even antivirus software is not enough to catch certain attacks that have been cleverly disguised. Once a system is infected with a new strain, the damage can be done before the virus or worm is detected and the system is disinfected.

Application protection

Such packages include software that watches for email anomalies, database access queries, or other behavior that may exploit vulnerability in the application. Because it must be very specific—and very close—to the application it is protecting, application protection is typically implemented as software on the host. Dedicated servers would benefit from well-designed application security software that will maintain the integrity of the code and detect anomalous behavior that could indicate an attack. Certain malicious code can attempt to overwrite registers on the end-system and thereby hijack the hardware for destructive purposes.

Intrusion detection systems

Intrusion Detection Systems (IDS) are designed to 'listen' to traffic and behavior and set an alarm if certain conditions are met. Some IDS implementations are implemented in the host, while others are deployed in the network. The IDS sensor monitors traffic, looking for protocol violations, traffic rate changes or matches to known attack 'signatures'. When a threat is detected, an alarm is sent to notify a (human) network administrator to intervene.

Host-based intrusion detection systems are designed as software running on general purpose computing platforms. Not to be confused with application security software (mentioned above), which runs on the end system and focuses primarily on Layers 5-7, software based intrusion systems must also focus on Layers 3 and 4 of the protocol stack. These packages rely on the CPU power of the host system to analyze traffic as it comes into the server. General purpose computers often lack the performance required to monitor real-time network traffic and perform their primary functions. Creating a bottleneck in the network or on the server actually helps the hacker accomplish his goal by restricting access to valuable resources.

End-systems provide the best environment for signature recognition because packets are fully reassembled and any necessary decryption has been performed. However, signature-based intrusion detection has its limitations, as described below.

The next step in the evolution of intrusion security was content-based Intrusion Prevention Systems (IPS). Unlike IDS, which require manual intervention from an administrator to stop an attack, a content-based IPS automatically takes action to prevent an attack once it is recognized. This can cut down response time to near zero, which is the ultimate goal of intrusion security.

IPS must be intelligent, however, or the remedy might actually accomplish the hacker's goal: denying resources to legitimate users.

Prevention mechanisms can also be harmful if detection is subject to false positives, or incorrect identification of intrusion. If the prevention action is to disable a port, protocol, or address, a false positive could result in denial of service to one or more legitimate users.

Network behavior analysis

An alternative to signature recognition is network behavior analysis (NBA). Rate-based systems must provide detailed analysis and/or control of traffic flow. A baseline of traffic patterns is established, usually during a learning mode in which the device only 'listens' without acting on any alarm conditions. A good system will have default parameters set to reasonable levels, but the 'listening' period is required to learn the traffic behavior on various systems. The listening period should be 'typical,' in the sense that no attacks or unusual traffic patterns should be present. For example, Saturday and Sunday are probably not good days to build a baseline for a corporate server that is much busier during the workweek. Periods of unusually high or low traffic also make bad listening intervals, such as Christmas vacation week, unusually high traffic due to external events (press releases, sales promotions, Super Bowl halftime shows, and so on).

Once a baseline is established, rate-based systems watch for deviations from the known traffic patterns to detect anomalies. Good systems will allow an administrator to override the baseline parameters if events causing traffic surges are foreseen, for example, a server backup scheduled overnight.

While signature-based systems are scrutinized for false-negatives, or failing to identify an attack, rate-based systems should be scrutinized for false positives, or misidentifying legitimate changes in traffic patterns as attacks. Whether setting alarms or taking preventative action, rate-based systems must be well-designed to avoid unnecessary overhead.

Equally important for rate-based systems are their analysis tools. Administrators should be able to view their traffic patterns on a variety of levels, and use this information to tune their network resources.

FortiDDoS compared with firewalls

FortiDDoS' state-aware NBA architecture for TCP, DNS and NTP (E-series) detection and line-rate mitigation is significantly different and better than firewalls.

Firewalls maintain state to ensure NAT operates correctly, among other things. They also often create timer-based "virtual" state machines for UDP packets to assist with UTM detections. For these reasons and others, they are vulnerable to:

- Small-packet random-source UDP floods which fill connection tables
- Fragmented UDP floods which fill IPS buffers
- TCP Flag floods which either fill connection tables with ½ open sessions (SYN Floods of various kinds) or exhaust resources by forcing the firewall to check SYN-ACK floods against the existing outbound ½ open session table.
- Most firewalls' performance degrades in the face of small-packet UDP and TCP Flag floods since processing many packets rapidly taxes the CPUs
- Simple blocking thresholds for these attacks often result in all new TCP connections blocked or all UDP traffic blocked
- Many UDP and non-standard Protocol floods result in outbound ICMP messages, further taxing the firewall CPUs.

FortiDDoS does not need state information to detect 99.99% of attacks:

- UDP Protocol and Port floods are rate-based and FortiDDoS detects floods to all 65,535 valid UDP ports as well as FROM UDP ports 1-9999 (a much wider range than currently known UDP reflected floods like DNS, NTP, CLDAP, and wider than any other DDoS vendor).
- Stateless mitigation of 3 different types of SYN Floods to the Internet link line rate. A SYN flood through a GE Internet link can reach 1.5 million pps.
- FortiDDoS unique hardware architecture with 100% small-packet line-rate inspection and mitigation allows the system to see and mitigate TCP illegal flag floods from the first packet, with no impact on system throughput.
- FortiDDoS is state-aware for the 9 TCP flag combinations that may happen during a real TCP session. For example, instead of setting a threshold for SYN-ACKs that would result in blocking all new connections when the inbound threshold is crossed, as firewalls and other DDoS vendors do, FortiDDoS monitors the state of up to 24 million TCP connections. If a SYN packet is seen outbound, it allows the matching inbound SYN-ACK to pass. If a SYN-ACK arrives without a corresponding SYN-ACK match, the packet is instantly dropped (again, at the line-rate of the link). This STOPS any SYN-ACK attack while continuing to allow "good" SYN-ACKs in response to outbound SYNs – something no other vendor can claim. Similarly, a single RST is allowed to take down an existing TCP session but no RSTs are allowed outside a connected session. By being aware of the session state, out-of-state RSTs are dropped instantly without thresholds. This also works for ACK, FIN-ACK, ACK-PSH, etc., all without interfering with legitimate traffic.
- FortiDDoS uses its superior state-aware NBA performance to support other stimulus-response applications such as DNS and NTP (E-series). Up to 12 million DNS Queries per second are monitored and matched with incoming DNS responses. Unmatched DNS responses are instantly dropped while DNS Responses from outbound Queries are allowed, stopping attacks instantly with no thresholds, while allowing continued internet access for legitimate users – performance and mitigation that firewalls and other DDoS vendors cannot approach.

FortiDDoS compared with conventional intrusion prevention systems

FortiDDoS-F is a rate-based IPS device that detects and blocks network attacks which are characterized by excessive use of network resources. It uses a variety of schemes, including anomaly detection and statistical techniques, to detect and block malicious network traffic. When it detects an intrusion, the FortiDDoS-F blocks traffic immediately, thus protecting the systems it is defending from being overwhelmed.

Unlike conventional content-based IPS, an NBA system does not rely on a predefined attack “signature” to recognize malicious traffic. An IPS is vulnerable to “zero-day” attacks, or attacks that cannot be recognized because no signature has been identified to match the attack traffic. In addition, attack traffic that is compressed, encrypted, or effectively fragmented can escape many pattern-matching algorithms in content-based IPS. And many rate-based attacks are based on genuine and compliant traffic being sent at high rates, effectively evading the IPS.

An NBA provides a network with unique protection capabilities. It delivers security services not available from traditional firewalls, IPS, or antivirus/spam detectors. The detection, prevention, and reporting of network attacks is based on traffic patterns rather than individual transaction or packet-based detection, which enables the FortiDDoS-F to serve a vital role in an effective security infrastructure. Rather than replacing these elements, an NBA complements their presence to form a defense-in-depth network security architecture.

Understanding FortiDDoS rate limiting thresholds

This section includes the following information:

Granular monitoring and rate limiting

Increasingly, instead of simple bandwidth attacks, attackers try to avoid detection by creating attacks that mimic the behavior of a large number of clients. Evading an NBA system is easy if attackers do coarse-grained rate-based control. Because the content of the malicious requests does not differ from that of legitimate ones, the resulting attacks are hard to defend against using standard techniques.

In contrast, FortiDDoS-F uses a combination of Layer 3, 4, and 7 counters and continuously adapts expected inbound and outbound rates for each of these traffic parameters.

Granular analytics also enable targeted mitigation responses. For example, if a few TCP connections are exceeding bandwidth, the system blocks those connections rather than all connections. If a single destination is under attack, FortiDDoS-F drops packets to that destination while others continue. During fragmented flood attacks, all non-fragmented packets continue as usual. During a port flood to a non-service port, the packets to other ports continue.

Granularity helps to increase the goodput (the throughput of useful data) of the system.

The table below lists the counters that FortiDDoS uses to detect subtle changes in the behavior of network traffic.

FortiDDoS-F counters

Type	200F	1500F	VM-04	VM-08	VM-16
Service Protection Policies (SPPs)	**8**	**16**	**4**	**8**	**16**
Protection Subnets per SPP	**512**	**1024**	**512**	**512**	**512**
ACLs (system unless noted)					
Global ACLs IPv4	1024				
Global ACLs IPv6	1024				
ACLs per SPP (IPv4 or IPv6)	1024				
Blocklist IPv4 upload list	1 million				
Blocklist Domains	1024				
Domain Blocklist upload list	1 million				
Layer 3					
Protocol flood (Protocol pps rate, per SPP, per direction)	1 counter/Threshold for each of 256 protocols				
Fragment flood (Fragment pps rate. Per SPP per direction)	3 counters/Thresholds for TCP/UDP/Other Fragments				
IP source flood & source tracking (Source IPs per system)	1 million	4 million	1 million	1 million	2 million
IP destination flood (Destination Ips per system)	1 million	4 million	1 million	1 million	2 million
Layer 4					
TCP port flood (Port data pps Thresholds per SPP per direction)	65,535 (Port 0 is anomaly)	65,535 (Port 0 is anomaly)	65,535 (Port 0 is anomaly). Ports above 1023 are all graphed into port 1024		
UDP port flood (Port data pps rate Thresholds per SPP per direction)	65,535 (Port 0 is anomaly)	65,535 (Port 0 is anomaly)	65,535 (Port 0 is anomaly). Ports above 10239 are all graphed into port 10240		
ICMP type/code flood (Type/Code pps rate Thresholds per SPP per direction)	65,536	65,536	65,536 Type/Code indexes. Indexes above 10239 are all graphed into index 10240		
TCP session table (sessions per system)	4 million	16 million	4 million	4 million	8 million
Legitimate IP table (IP addresses per system) (used to store legitimate Sources during SYN or DNS Query Floods)	1 million	4 million	1 million	1 million	2 million
SYN flood (SYN Rate pps per SPP per direction)	6.5 million	14.7 million	2 million	2 million	2 million

Type	200F	1500F	VM-04	VM-08	VM-16
SYN/source (Sources tracked per system)	1 million	4 million	1 million	1 million	2 million
SYN/destination (Destinations tracked per system)	1 million	4 million	1 million	1 million	2 million
Concurrent connections/source (Sources tracked per system)	1 million	4 million	1 million	1 million	2 million
Layer 7					
HTTP method (per Method pps rate per SPP per direction)	8 Method counters/Thresholds(GET, POST, HEAD, PUT, DELETE, CONNECT, OPTIONS, TRACE)				
HTTP Method/Source (1 Threshold per SPP per direction) Total Sources tracked per system	1 million	4 million	1 million	1 million	2 million
URLs (1 Threshold per SPP per direction) URLs tracked per SPP per direction	Top 64,000	Top 64,000	Top 64,000	Top 64,000	Top 64,000
Hosts (1 Threshold per SPP per direction) Hosts tracked per SPP per direction	Top 512	Top 512	Top 512	Top 512	Top 512
Referer (1 Threshold per SPP per direction) Referers tracked per SPP per direction	Top 512	Top 512	Top 512	Top 512	Top 512
Cookie (1 Threshold per SPP per direction) Cookies tracked per SPP per direction	Top 512	Top 512	Top 512	Top 512	Top 512
User-Agent (1 Threshold per SPP per direction) User-Agents tracked per SPP per direction	Top 512	Top 512	Top 512	Top 512	Top 512
DQRM (DNS Query/Responses tracked per system)	2 million	8 million	2 million	2 million	4 million
DNS LQ (cached Rcode-0 FQDNs per system)	131,000	524,000	131,000	131,000	262,000
DNS TTL (Cached TTLs for Rcode-0 FQDNs per system)	2 million	8 million	2 million	2 million	4 million
DNS Cache (Cached Rcode-0 Responses per system)	65,500	262,000	65,536	65,536	131,000
DNS query (QPS rate per SPP per direction)	2 million	8 million	2 million	2 million	4 million
DNS query rate/Source (Sources tracked per system)	1 million	4 million	1 million	1 million	2 million
DNS suspicious activity/source (Sources tracked per system)	1 million	4 million	1 million	1 million	2 million
DNS question count (Qcount sum per second per SPP per direction)	2 counters (UDP, TCP)				

Type	200F	1500F	VM-04	VM-08	VM-16
DNS MX count (Qps rate per SPP per direction)	2 counters (UDP, TCP)				
DNS All count (Qps rate per SPP per direction)	2 counters (UDP, TCP)				
DNS zone transfer count (Qps rate per SPP per direction)	1 counter				
DNS fragment count (DNS Fragments per second rate per SPP per direction)	2 counters (UDP, TCP)				
DNS Response Code count (Responses per second rate per SPP per direction)	16 counters, one for each Rcode				
NRM (NTP Requests/Responses tracked per system)	4 million	16 million	4 million	4 million	8 million
NTP Requests (Requests per second, per SPP per direction)	1 counter				
NTP Response (Responses per second, per SPP per direction)	1 counter				
NTP Broadcast (Broadcast pps , per SPP per direction)	1 counter				
NTP Response pre Destination (Responses per second) (Destinations Tracked)	1 million	4 million	1 million	1 million	2 million

Source tracking table

FortiDDoS maintains massive connection tables of 4-16 million entries and still performs with very low latency. FortiDDoS does not use its connection tables for non-TCP traffic and thus is immune to ICMP, Fragment and UDP table-filling attacks. SYN packets are validated under flood without populating the connection table (non-proxy).

The source tracking table enables FortiDDoS to correlate sources with attack events and apply a more stringent blocking period to the sources that exceeded maximum rate limits. The source tracking table also enables the special “per-source” thresholds described in the table below.

All per-source thresholds are part of FortiDDoS "Scalar" thresholds and as such all have a machine-learned adaptive Thresholds used in conjunction with the system Recommended Thresholds created from the learned traffic. This "Estimated Threshold" compensates for traffic seasonality over short periods of time (from a few minutes to 6 weeks).

Per-source thresholds

Counter	Description
most-active-source	This counter establishes a maximum packet rate for any IP packet from a single source. A rate that exceeds the adjusted baseline is anomalous and treated as a Source Flood attack event. In conjunction with the Source Multiplier, the most-active-source threshold is useful in tracking and blocking

Counter	Description
	non-spoofed sources that are participating in an attack. See the figure: System attack response timeline. How is the threshold determined? When it establishes baseline traffic statistics, FortiDDoS records the highest packet rate from a single source during the observation period. In a one hour observation period, FortiDDoS collects a data point for twelve five minute windows. The data point is the highest rate observed in any one second during the five minute window. If the packet rate data points for most-active-source are 1000, 2000, 1000, 2000, 1000, 2000, 1000, 2000, 3000, 2000, 1000, and 2000, the generated statistic is the highest one: 3000.
syn-per-src	This counter establishes a maximum packet rate for SYN packets from a single source. A rate that exceeds the adjusted baseline is anomalous and treated as a SYN Flood From Source attack event.
concurrent-connections-per-source	This counter establishes a maximum packet rate for concurrent connections from a single source. A count that exceeds the adjusted baseline is anomalous and treated as an Excessive Concurrent Connections Per Source attack event.
dns-query-per-src	This counter establishes the maximum rate of DNS queries from a single source. A count that exceeds the adjusted baseline is anomalous and treated as DNS Query Flood From Source attack event.
dns-packet-track-per-src	This counter is based on heuristics to detect suspicious actions from sources. The source tracking counter is incremented when a query is not found in the DQRM, when there are fragmented packets in the query or response, and when the response has an RCODE other than 0.
methods-per-source	Drops due to method per source threshold.

Destination tracking table

FortiDDoS destination table supports 1-4 million entries depending on the model.

This table tracks the packet rate for every destination and is used for “per-destination” thresholds.

The destination tracking table enables FortiDDoS to prevent destination flood attacks and slow connectionattacks that are targeted at individual destinations. The “per-destination” thresholds enable it to do so without affecting the rates for other destinations in the SPP.

All per-destination thresholds are part of FortiDDoS "Scalar" thresholds and as such all have a machine-learned adaptive Thresholds used in conjunction with the system Recommended Thresholds created from the learned traffic. This "Estimated Threshold" compensates for traffic seasonality over short periods of time (from a few minutes to 6 weeks).

The table below describes the per-destination thresholds.

Per-destination thresholds

Counter	Description
most-active-destination	This counter establishes a maximum packet rate to any one destination. A rate that exceeds the adjusted baseline is anomalous and treated as a Destination Flood attack event. How is the threshold determined? When it establishes baseline traffic statistics, FortiDDoS records the highest packet rate to any single destination during the observation period. In a one hour observation period, FortiDDoS collects a data point for twelve five minute windows. The data point is the highest rate observed in any one second during the five minute window. If the packet rate data points for most-active-destination are 100000, 200000, 100000, 200000, 100000, 200000, 100000, 200000, 300000, 200000, 100000, and 2000, the generated statistic is the highest one: 300000.
syn-per-dst	This counter establishes a maximum packet rate for particular TCP packets to a single destination. A rate that exceeds the adjusted baseline is anomalous and treated as a Excessive TCP Packets Per Destination flood attack event. When the syn-per-dst limits are exceeded for a particular destination, the SYN flood mitigation mode tests are applied to all new connection requests to that particular destination. Traffic to other destinations is not subject to the tests.
NTP Response per Destination	This counter establishes a maximum packet rate threshold for NTP Responses to any single destination. A rate that exceeds the Threshold is treated as an NTP per Destination flood attack event. When the NTP per Destination limits are exceeded for a particular destination, NTP Response Packets are rate-limited to that destination without affecting NTP traffic to any other destination.

Continuous learning and adaptive thresholds

Most NBA systems use fixed value thresholds. Traffic, however, is never static. It shows trends and seasonality (a predictable or expected variation).

FortiDDoS uses adaptive thresholds. Adaptive thresholds take into account the traffic's average, trend, and seasonality (expected or predictable variations).

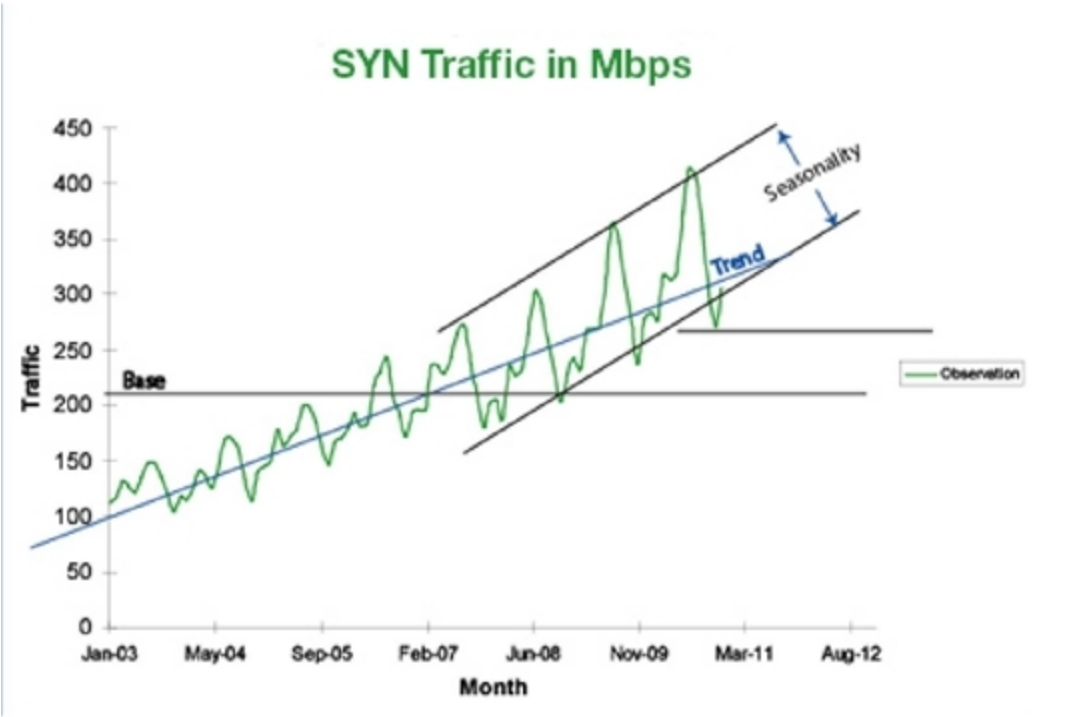
Traffic prediction

Unlike other network behavior analysis (NBA) systems, FortiDDoS-F never stops learning. It continuously models inbound and outbound traffic patterns for key Layer 3, Layer 4, and Layer 7 parameters.

FortiDDoS-F uses the following information to model normal and abnormal traffic:

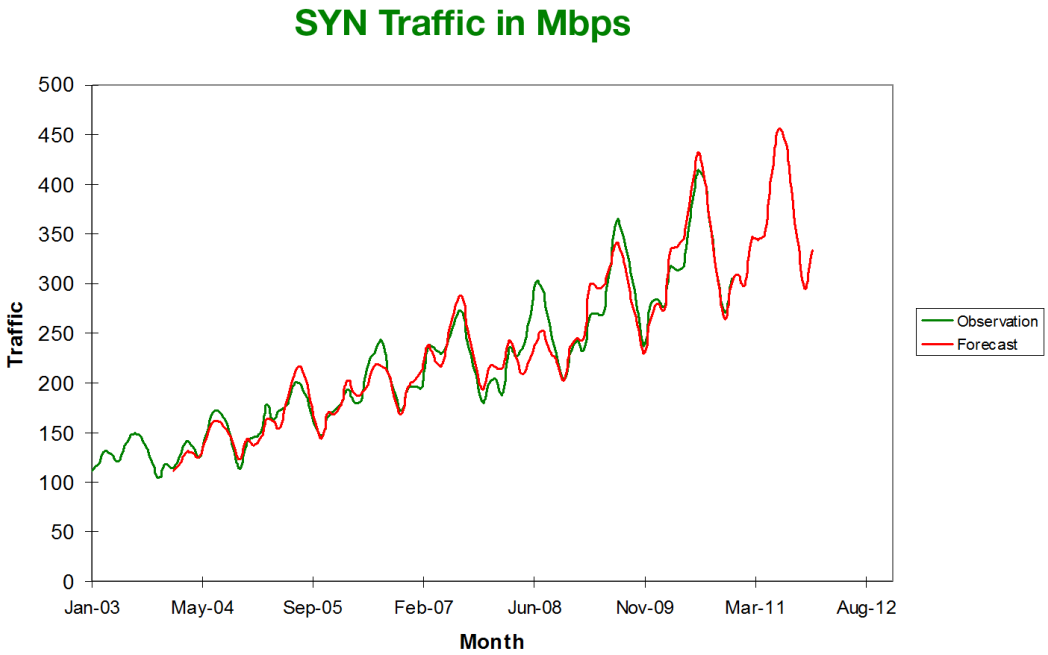
- The historical base, or weighted average, of recent traffic (more weight is given to recent traffic)
- The trend, or slope, of the traffic
- The seasonality of traffic over historical time periods

Trend, slope, and base of traffic



FortiDDoS-F uses these statistics to create a forecast for the next traffic period.

Forecast vs. actual traffic



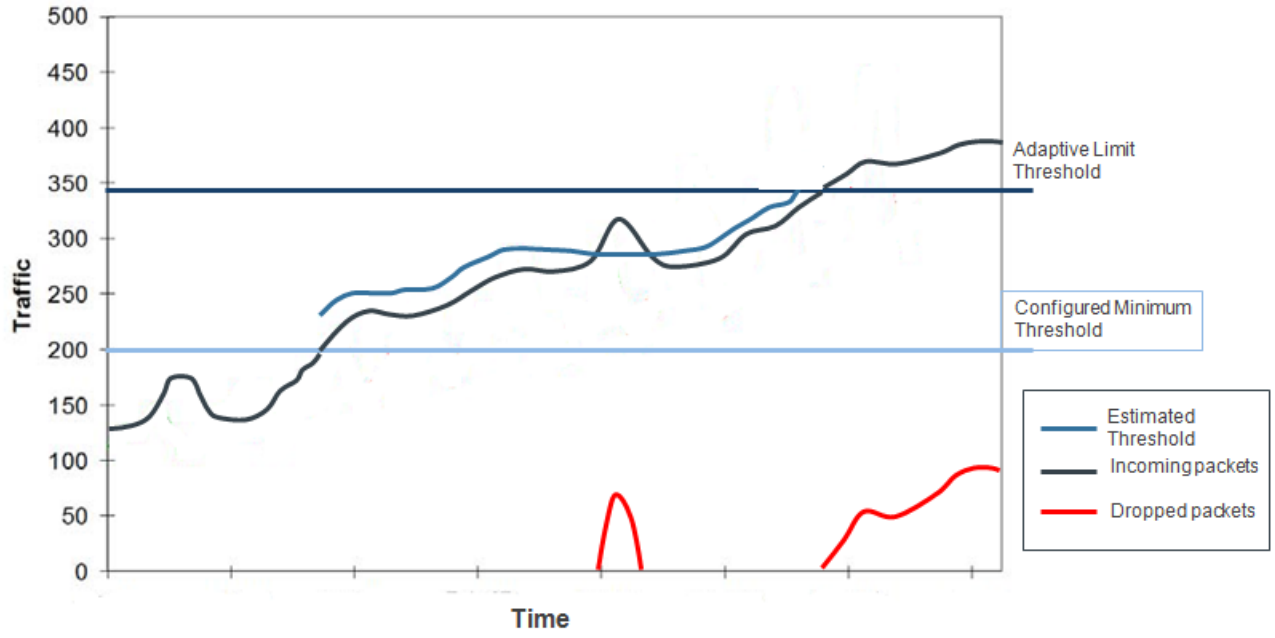
Traffic is non-deterministic; therefore, the forecast cannot be exact. The extent to which an observed traffic pattern is allowed to exceed its forecast is bounded by thresholds. Generally speaking, a threshold is a baseline rate that the system uses to compare observed traffic rates to determine whether a rate anomaly is occurring.

The FortiDDoS system maintains multiple thresholds for each key Layer 3, Layer 4, and Layer 7 parameter:

- Configured minimum threshold
- Estimated threshold
- Adaptive limit maximum threshold
- Adjustments for proxy IP addresses
- Packet count multipliers applied to traffic associated with an attack

The figure below illustrates how the system maintains multiple thresholds. The sections that follow explain the significance of each.

Adaptive, minimum and fixed



Configured minimum thresholds

The configured minimum threshold is a baseline of normal counts or rates. The baseline can be generated (based on statistics collected during the learning period) or stipulated (based on defaults or manually configured settings).

The configured minimum threshold is a factor in setting rate limits, but it is not itself the rate limit. Rate limits are set by the estimated threshold, a limit that is subject to heuristic adjustment based on average, trend, and seasonality.

Many of the graphs in the Monitor menu display the configured minimum threshold as a reference.

The table below summarizes the alternative methods for setting the configured minimum threshold.

Minimum threshold configuration settings

Settings	Usage
Thresholds	The thresholds configuration is open. You can set user-defined thresholds and fine-tune them. You can set reasonable values for port and protocol thresholds based on your knowledge of your network's services and server capacity. It is advised that you have a thorough understanding of FortiDDoS before manually setting values for scalar thresholds.
System Recommendation	The recommended method for setting the configured minimum thresholds. The configured minimum thresholds are a product of the observed rates adjusted by a percentage that you specify.
Emergency Setup	Use if you do not have time to use Detection Mode to establish a baseline.
Factory Defaults	Use to quickly restore the system to high values. The factory defaults are high to avoid possible traffic disruption when you first put the system inline. In general, these settings are used together with Detection Mode when you are setting an initial baseline or a new baseline.
Percent Adjust	Use when you expect a spike in legitimate traffic due to an event that impacts business, like a news announcement or holiday shopping season.

Estimated thresholds

The estimated threshold is a calculated rate limit, based on heuristic adjustments.

The system models an adjusted normal baseline based on average, trend, and seasonality. It uses the heuristics to distinguish attack traffic from increases in traffic volume that is the result of legitimate users accessing protected resources.

The minimum value of an estimated threshold is the configured minimum threshold. In other words, if it is not predicting normal traffic becoming heavier than the baseline, it allows a rate at least as high as the configured minimum threshold.

The maximum value of an estimated threshold is the product of the configured minimum threshold and the adaptive limit. In other words, the system does enforce an absolute maximum rate limit.

Adaptive limit

The adaptive limit is a percentage of the configured minimum threshold.

An adaptive limit of 100% means no dynamic threshold estimation adjustment takes place once the configured minimum threshold is reached (that is, the threshold is a fixed value).

The product of the configured minimum threshold and adaptive limit is the absolute maximum rate limit. If the adaptive limit is 150% (the default), the system can increase the estimated threshold up to 150% of the value of the configured minimum threshold.

There are scenarios where FortiDDoS-F drops legitimate traffic because it cannot adapt quickly enough to a sudden change in traffic patterns. For example, when a news flash or other important announcement increases traffic to a company's website. In these situations, you can use the Protection Profiles > Thresholds > Percent Adjust configuration page to increase all configured thresholds by a specific percentage.

Adjustments for proxy IP addresses

FortiDDoS can take account of the possibility that a source IP address might be a proxy IP address, and adjust the threshold triggers accordingly. If a source IP address is determined to be a proxy IP address, the system adjusts thresholds for a few key parameters by a factor you specify on the Global Settings > Proxy IP page.

Packet count multipliers applied to traffic associated with an attack

Packet count multipliers are adjustments to counters that are applied to traffic associated with an attack so that the thresholds that control drop and block responses are triggered sooner. You can configure multipliers for the following types of traffic:

- Source floods—Traffic from a source that the system has identified as the source of a flood.
- Layer 7 floods—Traffic for attacks detected based on a URL or Host, Referer, Cookie, or User-Agent header field.

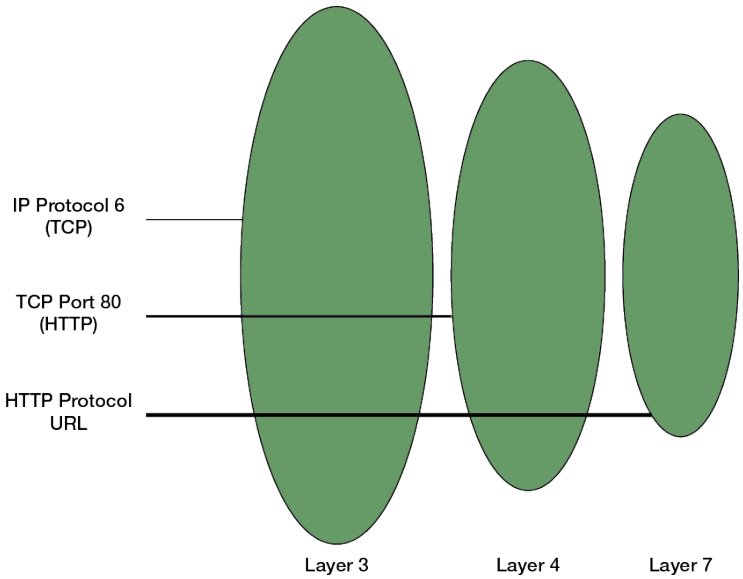
You can use the Protection Profiles > Settings page to specify packet count multipliers.

When both Source flood and Layer 7 flood conditions are met, the packet count multipliers are compounded. For example, when there is a User Agent flood attack, a source is sending a User-Agent that is overloaded. If the Source multiplier is 4 and the Layer 7 multiplier is 64, the total multiplier that is applied to such traffic is 4 x 64 = 264. In effect, each time the source sends a Layer 7 packet with that particular User-Agent header, FortiDDoS considers each packet the equivalent of 256 packets.

Hierarchical nature of protocols and implication on thresholds

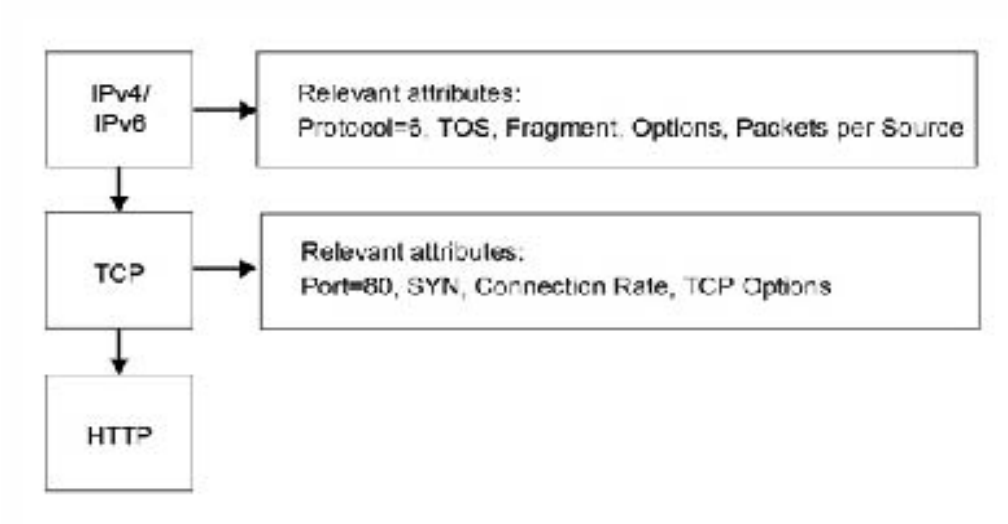
An HTTP packet has Layer 7, Layer 4 (TCP), and Layer 3 (IP) properties. A packet must be within the estimated thresholds of all these counters in order to pass through the FortiDDoS-F gateway. When it sets recommended thresholds, the system takes account of this complexity. If you set thresholds manually, you must also be sure that Layer 7 rates are consistent with Layer 4 and Layer 3 rates.

Protocol hierarchy for determining thresholds



The below illustrates system processing for an HTTP packet.

HTTP packet properties



The following IPv4/IPv6 packet properties are tracked:

- Protocol
- Fragment or not a fragment
- Source IP address (the system can monitor the packet rate from that specific source)

The following TCP packet properties are tracked:

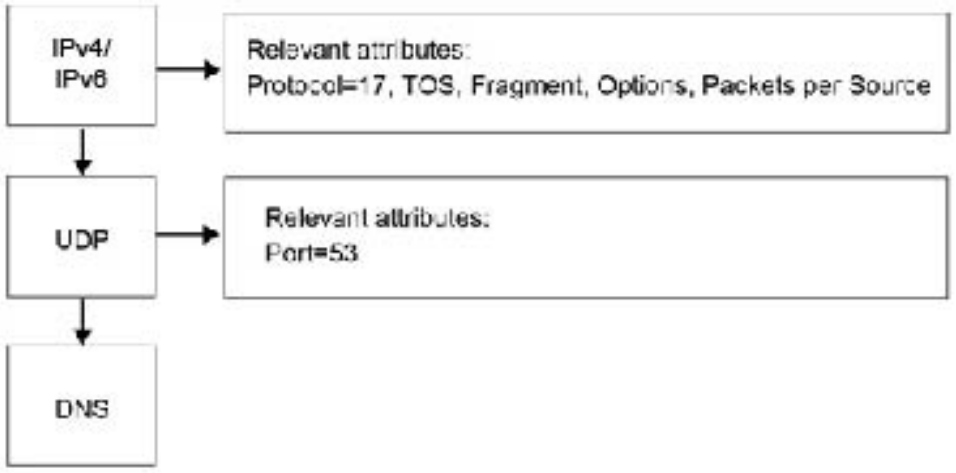
- Destination port
- SYN or not a SYN packet
- TCP connection tuple (the system can monitor the packet rate within that connection)

An HTTP packet has the following properties that can be tracked:

- Method (GET, HEAD, POST, PUT, TRACE DELETE, OPTIONS, CONNECT)
- Method per Source
- URL
- Headers

The figure below illustrates system processing for a UDP packet.

UDP packet properties



The following IPv4/IPv6 packet properties are tracked:

- Protocol
- Fragment or not a fragment
- IP option values
- Source IP address, and hence packet rate from that specific source

The following UDP packet properties are tracked:

- Destination port 1-65, 535 (Port 0 is invalid)
- Source port 1-9999, plus 32 user-entered ports

A DNS message has the following additional properties that can be tracked in queries and responses:

- 24 DNS header, Query, Response and exploit anomalies
- Rates for Queries, MX, ALL, ZT, Qcount, Query/Source, Suspicious Sources, DNS Fragments
- DNS Response Codes 0-15

To summarize, because determining thresholds is a hierarchical process, avoid setting low thresholds on common conditions that can cause FortiDDoS-F to block legitimate traffic as well as attack traffic. The more specific you are about the type of traffic you want to allow as ‘normal’, the more effective the FortiDDoS-F is in blocking other traffic.

Using FortiDDoS ACLs

This section includes the following information:

- Define SPP Access Control Lists on page 42
- Define Service Protection Profiles on page 43

ACL Overview

With some notable exceptions, ACLs are ineffective for DDoS mitigation since most DDoS attacks use spoofed Source IP addresses. Geolocation and Source IP ACLs will miss widely randomized Source IPs in DDoS attacks. However, ACLs can be useful for the following:

- Blocking known UDP reflection ports that have no legitimate use
- Offloading other infrastructure like firewalls from ACLing “normal” traffic from undesirable countries or prefixes
- Blocking known NTP Reflection packets (Mode 5/7) – please see the NTP Profile for this specific ACL

Note: ACLs are not connection-direction sensitive. If for example you ACL an external server IP address to prevent it from sending unsolicited traffic to you, any if your users attempting to connect to that server will be blocked because all inbound packets (a SYN-ACK, for example) will be blocked from that Source IP.

ACL Structure

ACLs are defined in several places for different reasons:

- Global ACLs always drop traffic no matter the Detection/Prevention Mode of SPPs.
  Global ACLs use System ACL Objects defined in *System* > *Address* and Service and apply those Objects to *Global Protection* > *Access Control Lists*
- Do Not Track Policy ACLs use the same System ACL Objects defined in *System* > *Address and Service* and apply those Objects to *Global Protection* > *Do Not Track Policy* > *Track and Allow* or *Do not Track ACLs*. Do Not Track Policies do not support Geolocation objects.
- SPP ACLs use the same System ACL Objects defined in *System* > *Address and Service* and apply those Objects to *Service Protection* > *Service Protection Policy* > *ACL*.
  SPP ACLs drop or report and allow packets along with other SPP features and threshold depending on the *Detection / Prevention Mode* status of the SPP.
- SPP Profile ACLs
  Some *Service Protection* > *Profiles* support ACLs that do not require System ACL Objects:
  - *Service Protection* > *ICMP Profile* allows the entry of ICMP Type/Code ACLs.
  - *Service Protection* > *HTTP Profile* > *HTTP Param ACL* allows the entry of Regex expressions for URLs, Hosts, Referers, Cookies or User Agents ACLs.
  - *Service Protection* > *NTP Profile* allows a checkbox ACL for *NTP Reflection Deny* (NTP packets using Mode 6 or Mode 7 parameters)
  - *Service Protection* > *DNS Profile* > *DNS Resource Record Type ACL* allows the entry of DNS Resource Record ranges.

  In all cases, these ACLs will apply to any SPP to which that Profile is applied and will follow SPP Detection/Prevention Mode rules.
- Blocklist ACLs are bulk Global ACLs populated by uploading:
  - Lists of IPv4 Addresses to *Blocklist* > *Blocklisted IPv4*
  - Lists of DNS FQDNs to *Blocklist* > *Blocklisted Domains*

  Please refer to the handbook section on these functions for additional information.
- IP Reputation and Domain Reputation are specialized, dynamic, subscription-based ACLs for malicious and botnet

IP Addresses and Domains. Other than subscription purchase there is no user management needed
Note: IP Reputation and Domain Reputation are not required for DDoS Mitigation.

Define system ACL objects

You can create System Objects for:

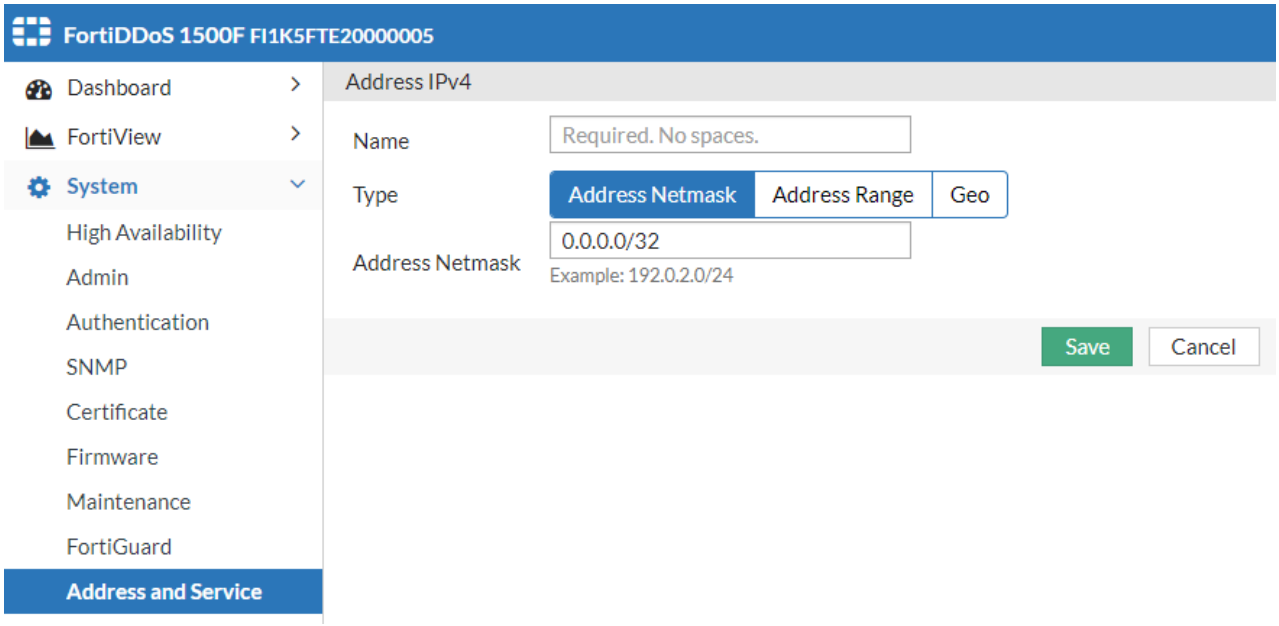
- IPv4 and/or IPv6 addresses, subnets and ranges, geolocation
- Services for Layer 3 Protocols, Layer 4 TCP and/or UDP Ports
- Address and Service Groups to include multiple objects from above

These objects/groups are then used to create:

- Global ACLs
- Global Do Not Track and Track and Allow ACLs
- Service Protection Policy (SPP) ACLs

Define System ACL objects via *System > Address and Service* for:

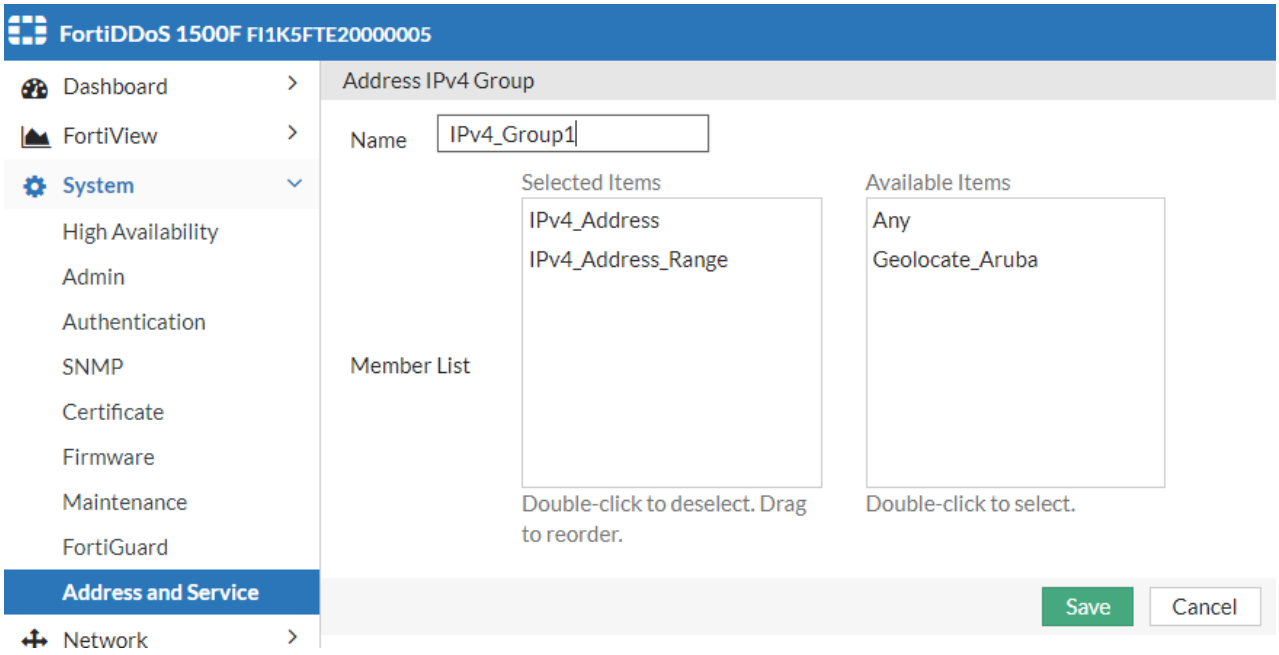
- Address IPv4
  - Address/netmask
  - Address Range
    Note: Address/netmask and Address Ranges can be ACLed as Sources or Destinations in the Access Control List. Destination ACLs should be used to block traffic to your inside protected public IPs. Source ACLs normally block traffic from outside public IP addresses.
  - Geolocation



To configure using the CLI:

```
config system address4
   edit addr1
      set type {ip-netmask|ip-range|geo}
      set ip-netmask <ip/mask>
      set ip-max <ip> set ip-min <ip>
      set country <string>
   next
end
```

- Address IPv4 Group
  - Groups IPv4 Addresses, Ranges and/or Geolocations from above into a single object.

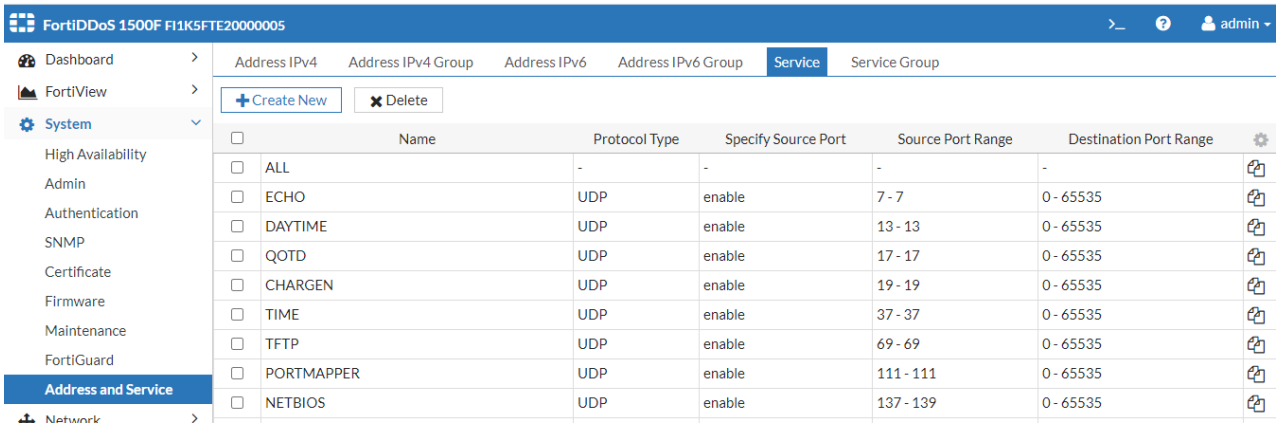


- Address IPv6
  - Address/netmask
  - Address Range
- Address IPv6 Group
  - Groups IPv6 Addresses or Ranges from above into a single Object.
- Service
  - IP Protocols (0-255)
  - ICMP (Protocol 1)
  - TCP, UDP or both TCP and UDP:
    - Destination Ports
    - Source Ports

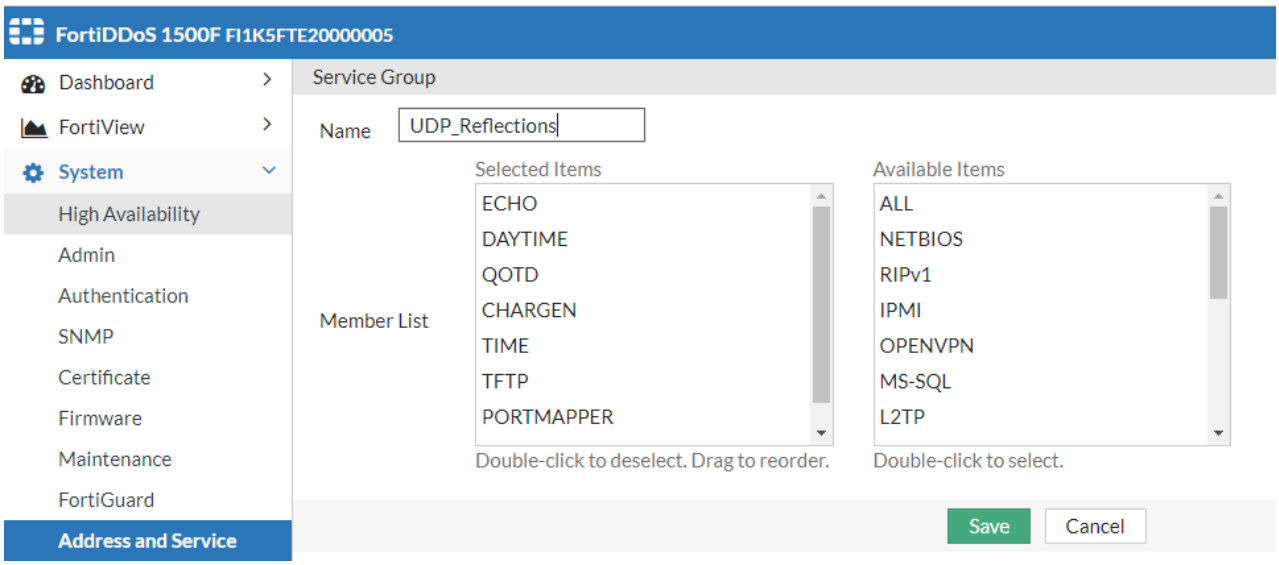
    Note: Common UDP Reflection Source Port Objects are pre-configured. These can be deleted, modified, added to Service Groups as desired.

To configure using the CLI:

```
config system service
   edit <name>
      set protocol-type {ip|icmp|tcp|udp|tcp-and-udp}
      set specify-source-port {enable|disable}
      set source-port-min <0-65535>
      set source-port-max <0-65535>
      set destination-port-min <0-65535>
      set destination-port-max <0-65535>
   next
end
```

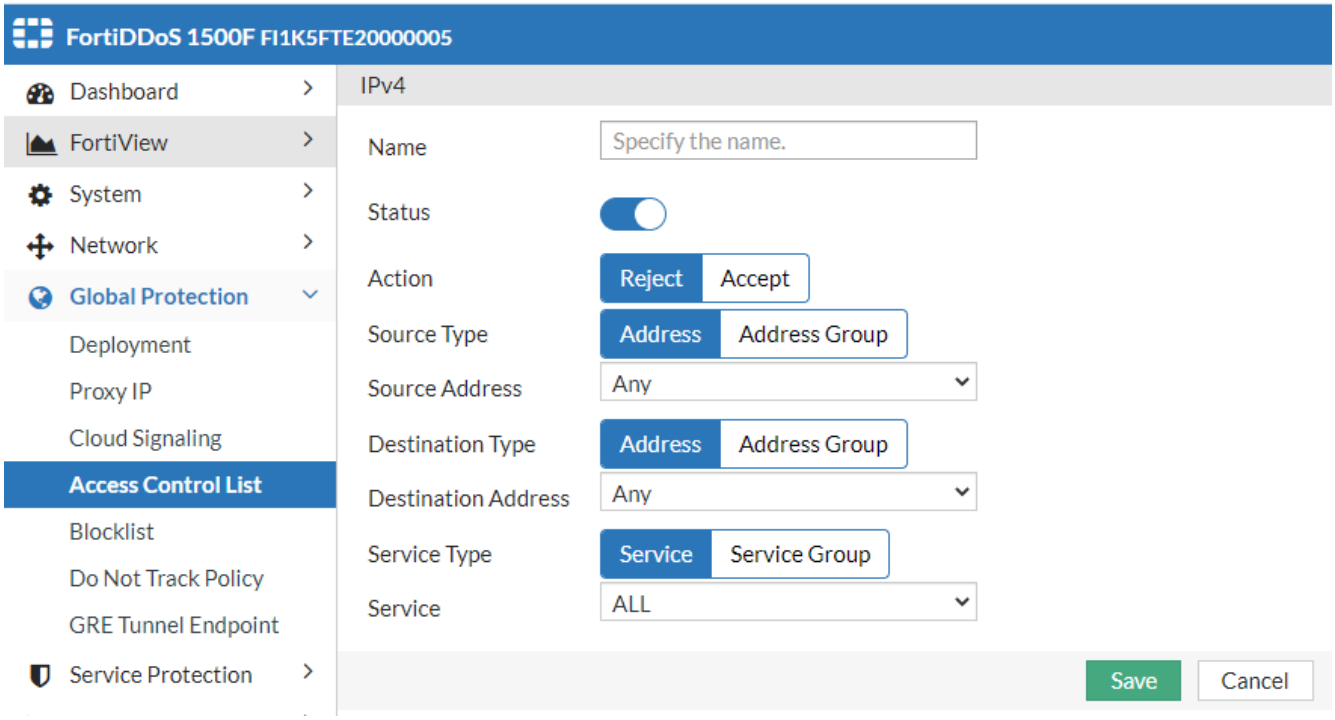


- Service Group
  - Groups Services into a single Object



Define Global Access Control Lists

Define Global ACLs via *Global Protection > Access Control List > IPv4 or IPv6*.



Note:

- Global ACLs are always in Prevention Mode, dropping traffic regardless if the individual Service Protection Profiles are in Detection or Prevention Mode.
- Global ACL drops will always show in the default SPP in 6.1.x versions.
- The Global ACL list is searched top-to-bottom. You many need to re-order the list using the arrow buttons on the right for correct behavior.

ACL Settings

Setting	Description
Name	a-Z,0-9, - , _ only
Status	Enable or disable ACL
Action	Reject = block/drop Accept = process the packet with for all other mitigations. This is not a allow-list indicator. See Do Not Track Policy for Allow-list configuration and behavior
Source Type	Address or Address Group (for IPv4 or IPv6 depending on the menu chosen)
Source Address	Pulldown showing all available System ACL objects
Destination Type	Address or Address Group (for IPv4 or IPv6 depending on the menu chosen)
Destination Address	Pulldown showing all available System ACL objects
Service Type	Service or Service Group
Service	Pulldown showing all available System Service ACL objects

To configure using the CLI:

```
config ddos global {acl | acl6}
   edit <entry_index>
      set source-address <address_name>
      set action {accept | deny}
   next
end
```

Define Do Not Track Policies

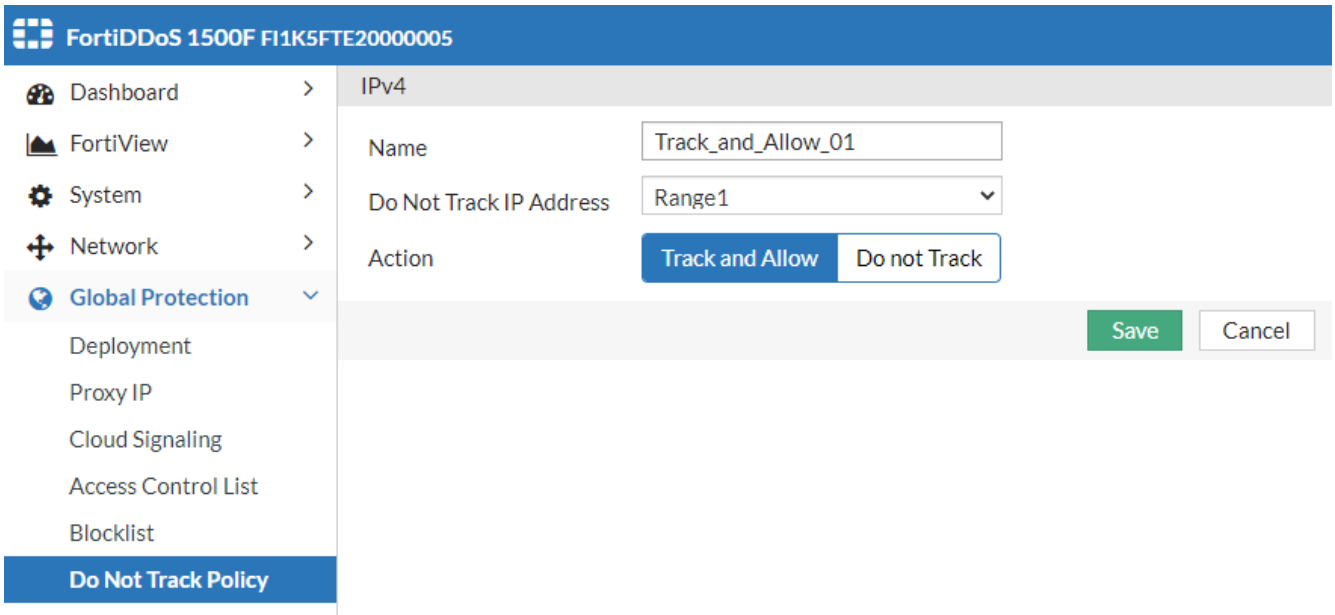
Do Not Track policies define two different types of Allowlists for IPv4 and/or IPv6 addresses, subnets or ranges:

- Do Not Track
  - No traffic nor drops will be reported for this ACL – there is no visibility of any traffic to or from this address
  - Traffic is not used for learned Traffic Statistics
  - Use this very carefully and ever use this for protected IP addresses. If an attacker can discover this IP address, he can launch attacks FortiDDoS will not monitor.
- Track and Allow
  - FortiDDoS processes traffic normally and reports virtual drops a but packets are always allowed to pass. Think of this as a mini-Detection Mode for IP addresses or subnets.
  - Use this ACL with care. While FortiDDoS reports attack traffic, it may not be obvious that the system is allowing the traffic to pass, even when all SPPs are in Prevention Mode.

  Note: Allowlists are relevant whether the IP address is a Source or a Destination.

Define *Do Not Track Policies* via *Global Protection > Do Not Track Policy > IPv4 or IPv6*

1. Use the Do Not Track IP Address dropdown menu to select the System ACL object for the policy.
2. Select *Track and Allow* or *Do not Track*.

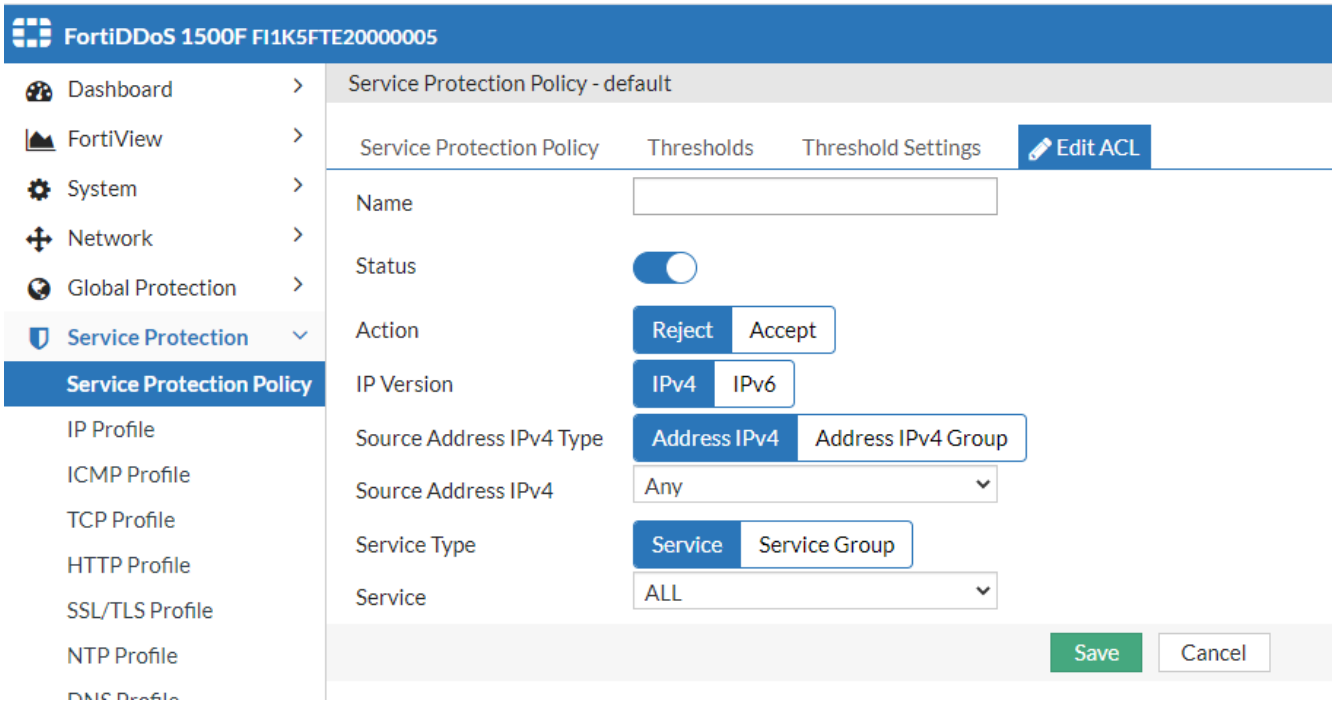


Define SPP Access Control Lists

Define SPP ACLs via *Service Protection* > *Service Protection Policy* > *ACL*.

Note:

- The SPP must be defined first before you can add any ACLs
- ACL Settings and allowable entries are identical to the Global settings above.
- SPP ACLs confirm to SPP Detection/Prevention rules.



To configure using the CLI:

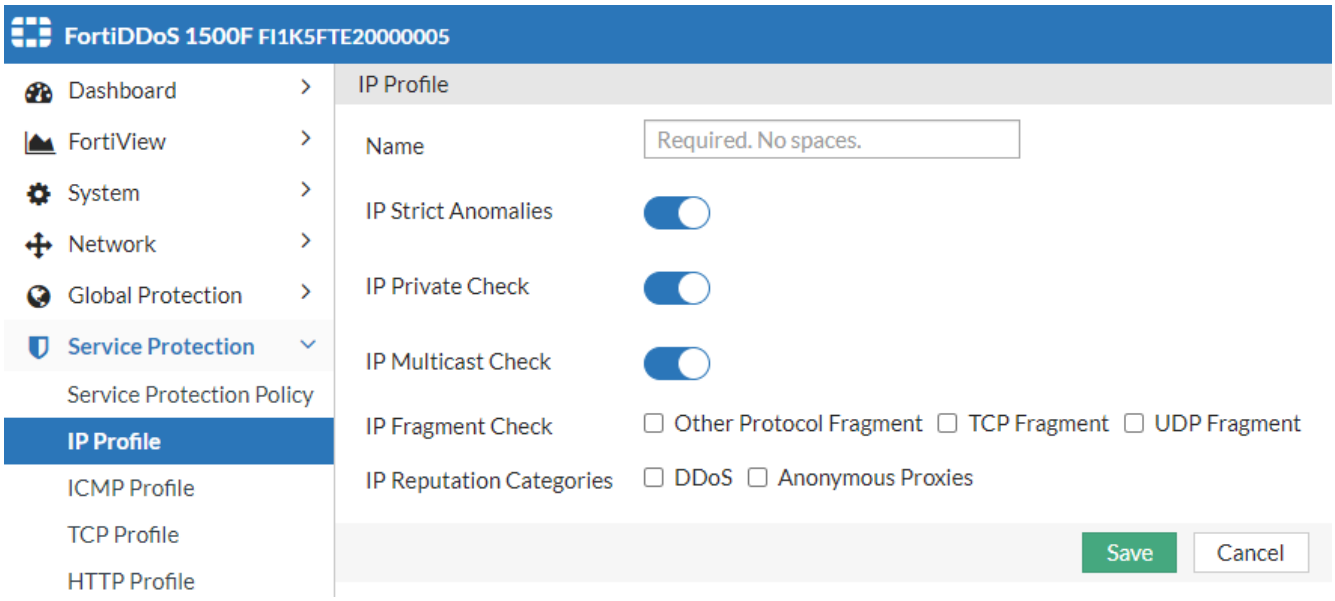
```
config ddos spp rule
   edit <spp_name>
      config acl
         edit <acl_name>
            set status { enable | disable }
            set action { reject | accept }
            set ip-version { IPv4 | IPv6 }
            set source-address4-type { addr4 | addr-grp4 }
            set source-address-v4 <IPv4 Address>
            set source-address-v4-group <IPv4 Address Group>
            set source-address6-type { addr6 | addr-grp6 }
            set source-address-v6 <IPv6 Address>
            set source-address-v6-group <IPv6 Address Group>
            set service-type { service | service-grp}
            set service-id <Service>
            set service-grp-id <Service Group>
         next
      end
   next
end
```

Define Service Protection Profiles

Service Protection Profiles for IP, ICMP, TCP, HTTP, SSL/TLS, DNS and NTP contain feature settings used to define mitigations when the Profiles are assigned to Service Protection Policies. The following Profiles support ACLs:

IP Profile

Some feature selections in the IP Profile are effectively ACLs:



IP Private Check	Drops packets whose Source IP is in private IP ranges like 10.0.0.0/8
IP Multicast Check	Drops packets whose Source IP is in private IP range 224.0.0.0/4
Above options should be enabled for all IP Profiles for any Service Protection Policy	
IP Fragment Check	
Other Protocol Fragment	Drops any fragmented packet for Protocols 0-255, other then TCP (Protocol 6) and UDP (Protocol 17)
TCP Fragment	Drops any fragmented packet for TCP (Protocol 6)
UDP Fragment	Drops any fragmented packet for UDP (Protocol 17)

Unless you have expert understanding, these Fragment ACLs must be disabled for all IP Profiles used in any Service Protection Policy. Instead, use the 3 Fragment Thresholds that FortiDDoS automatically learns.

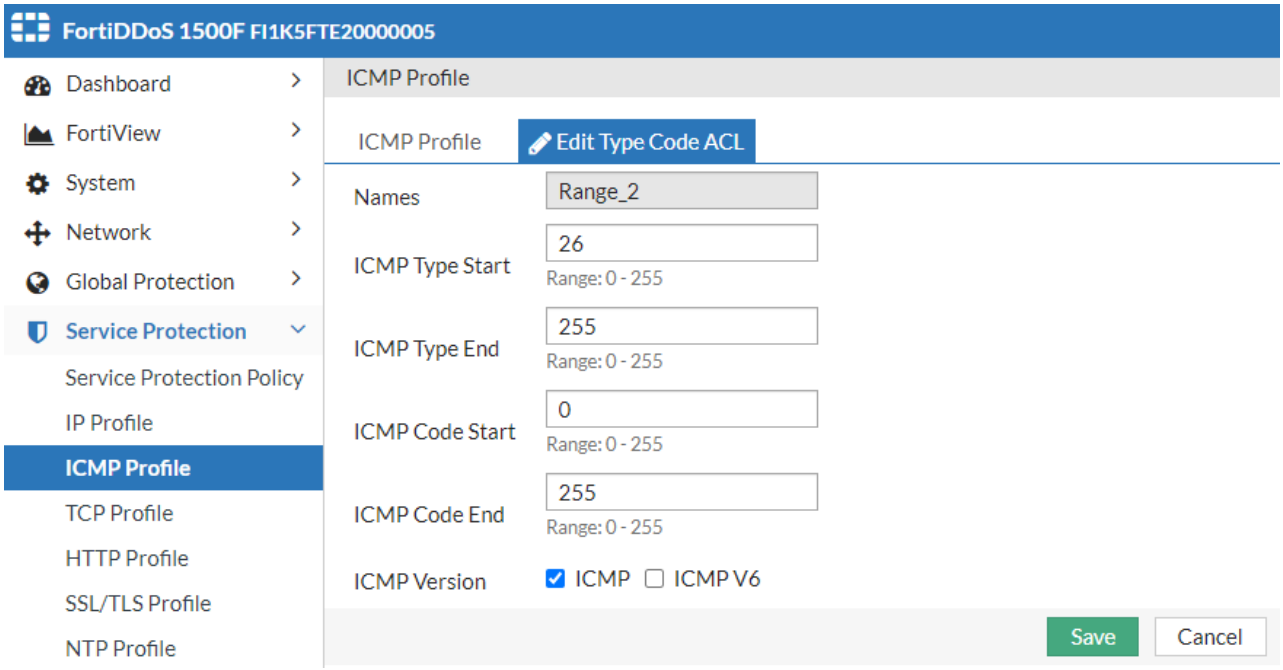
ICMP Profile

After creating a new ICMP Profile you can create ICMP Type/Code ACLs for ICMPv4 and/or ICMPv6.

Note: For non expert-users, enable “ICMP Type Code Anomaly”. This drops all non-IETF/IANA-ratified Types and Codes. Less than 150 Types and codes of 65,536 combinations are ratified.

To create more granular ICMP Type/Code ACLs:

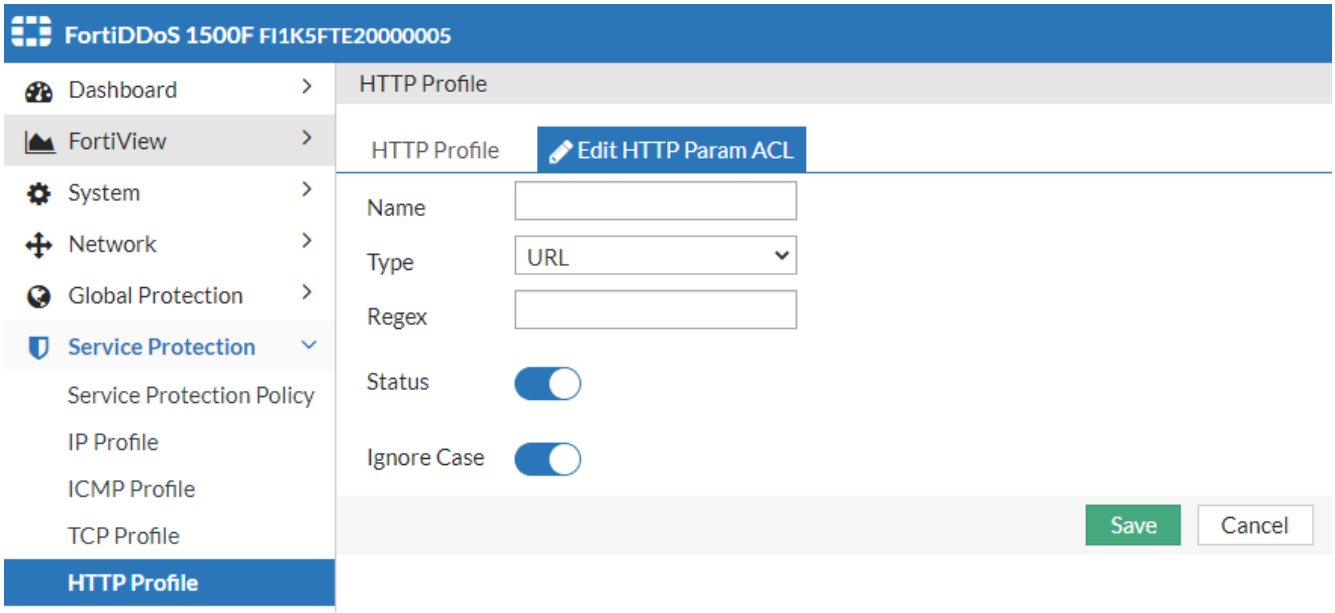
1. Select the ICMP Profile to edit.
2. Enable ICMP Type Code ACL.
3. Create New ACL.



4. Enter Type/Code Ranges. You are allowed to create a total of 8 per ICMP Profile.

HTTP Profile

After creating an HTTP Profile, you can create HTTP Param ACLs for URLs, Hosts, Referers, Cookies and/or User Agents. Regex entries allow wildcard ACLs.

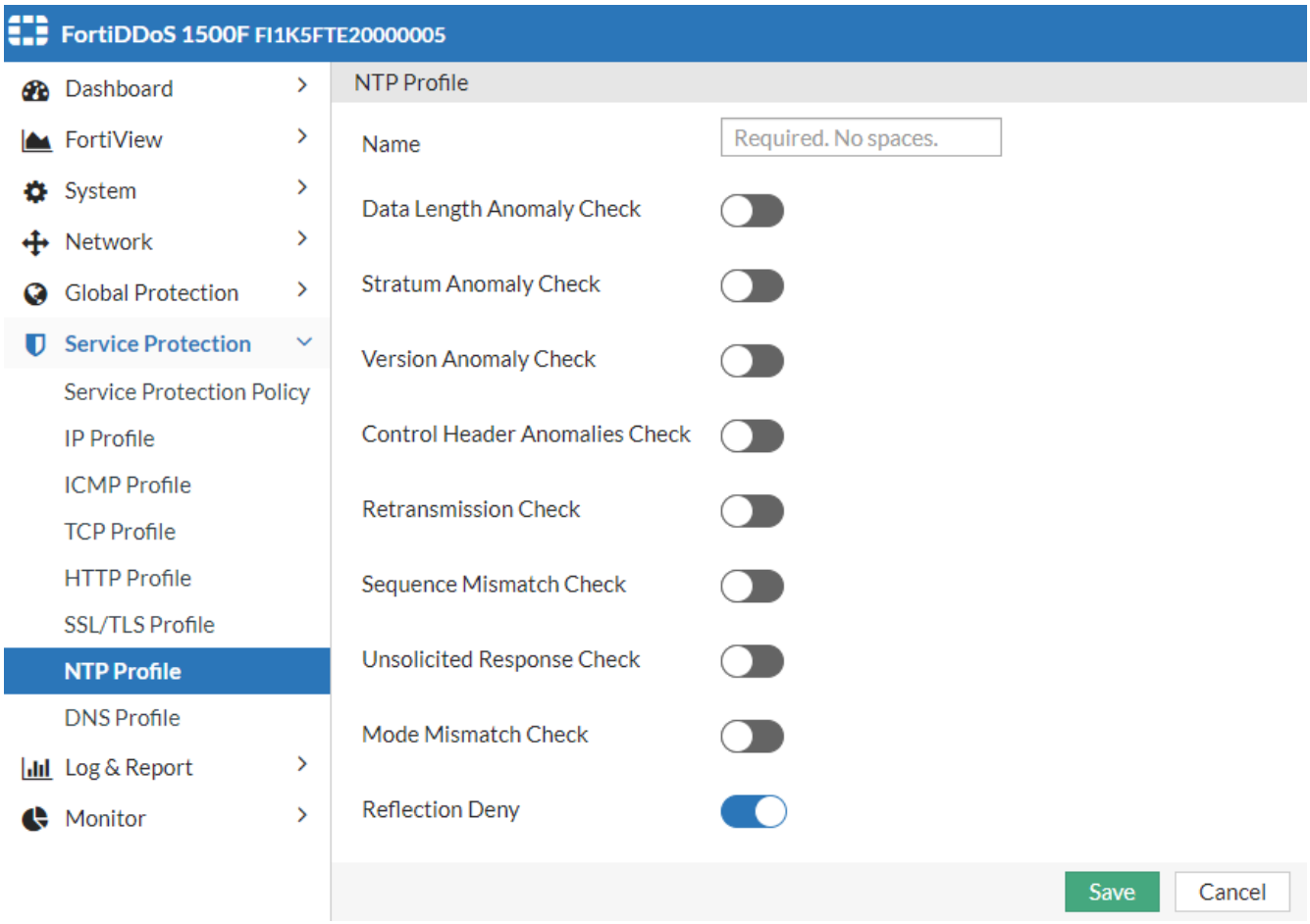


NTP Profile

NTP Reflection Deny is an available option in the NTP Profile. *NTP Reflection Deny* drops any packet where the Mode field is 6 (readvar) or 7 (monlist). These Modes are deprecated and are only used for amplified reflected NTP floods.

Enable this for all NTP Profiles.

Additional NTP Profile settings are discussed in the NTP Profile on page 277.



DNS Profile

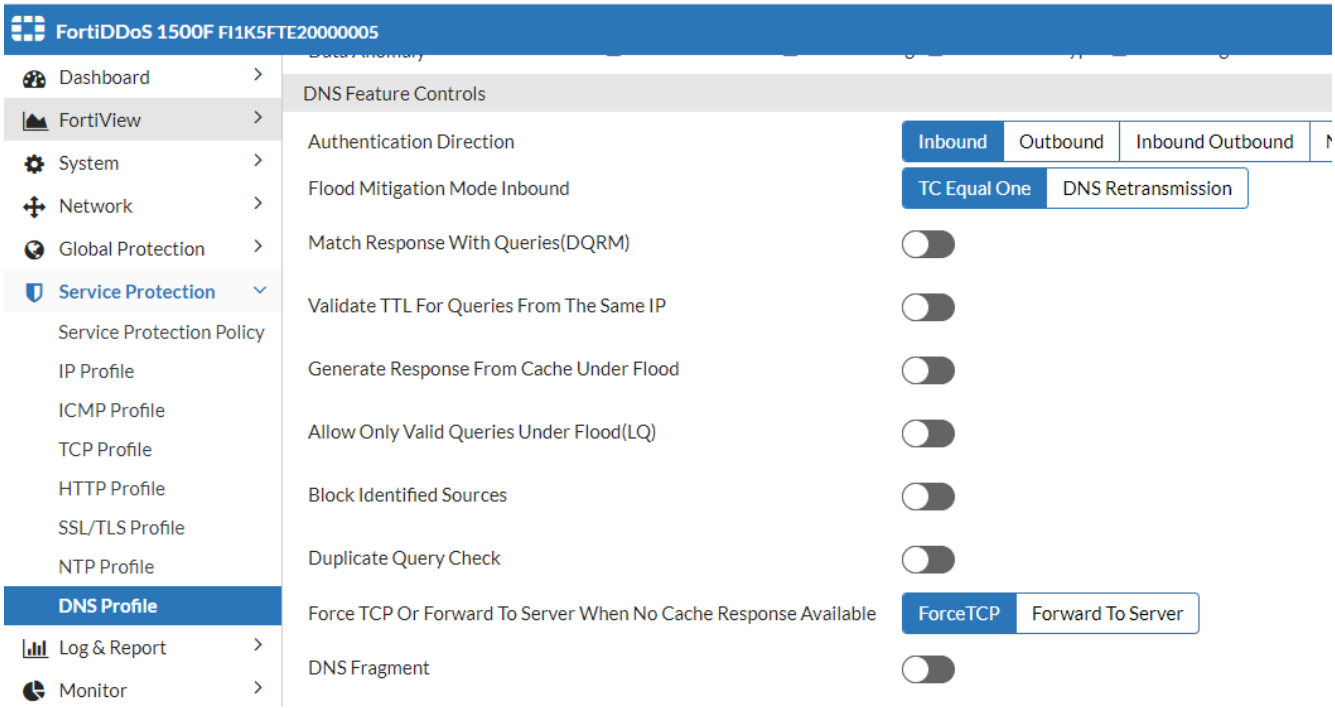
After creating a DNS Profile, you can create *DNS Resource Record Type ACLs*.

1. Edit the DNS Profile
2. Create New DNS Resource Record Type ACL range

DNS expert use only. IETF RFCs allow 65,536 possible DNS Resource Records but only a handful are in current use but they are widely scattered across the full range. Study the RFCs carefully before ACLing Resource Records. FortiDDoS's various Query and Response thresholds and validations will fully protect from any Resource Record used in a DDoS attack.

The DNS Profile also allows you to ACL *DNS Fragments*, which are the first DNS Query or Response packet with the More Fragments bit set (subsequent fragmented packets have no Layer 4 headers to identify them as DNS packets and will be seen as Layer 3 UDP Fragments).

Unless you are an expert user, disable this option. DNS Responses from EDNS0-enabled servers can exceed normal MTUs resulting in fragmented packets. Use the FortiDDoS automatically learned DNS Fragment Threshold to mitigate DNS Fragment (usually Reflected Response) floods.



Understanding FortiDDoS protocol anomaly protection

This section includes the following topics:

- IP/UDP/TCP anomalies
- TCP session state anomalies
- HTTP anomalies
- DNS anomalies

IP/UDP/TCP anomalies

Legitimate traffic conforms with standards set out in Internet Engineering Task Force (IETF) documents known as Requests for Comments (RFC). Traffic that does not conform with RFCs is anomalous. Often, anomalous traffic contains malicious components. In any case, it should be dropped to prevent resource issues.

This section provides detail for all types of anomalies detected and/or removed. Settings to determine processing of these anomalies are contained within the various SPP Profiles detailed later in the document.

The FortiDDoS system drops and logs the following Layer 3 anomalies:

- IP version other than 4 or 6
- Header length less than 5 words
- End of packet (EOP) before 20 bytes of IPv4 Data
- Total length less than 20 bytes
- EOP comes before the length specified by Total length
- End of Header before the data offset (while parsing options)
- Length field in LSRR/SSRR option is other than (3+(n*4)) where n takes value greater than or equal to 1
- Pointer in LSRR/SSRR is other than (n*4) where n takes value greater than or equal to 1
- For IP Options length less than 3
- Reserved flag set
- More fragments
- Source and destination addresses are the same (LAND attack)
- Source or destination address is the same as the localhost (loopback address spoofing)

The FortiDDoS system drops and logs the following Layer 4 anomalies:

- TCP Checksum Error
- UDP Checksum Error
- ICMP Checksum Error
- TCP Invalid Flag Combination
- Invalid ICMP Type/Code (Global option)
- Other header anomalies, such as incomplete packet
- Urgent flag is set then the urgent pointer must be non-zero
- SYN or FIN or RST is set for fragmented packets
- Data offset is less than 5 for a TCP packet
- End of packet is detected before the 20 bytes of TCP header
- EOP before the data offset indicated data offset
- Length field in Window scale option other than 3 in a TCP packet
- Missing UDP payload
- Missing ICMP payload
- SYN with payload (SPP option)

TCP session state anomalies

TCP session state anomalies are a symptom of an attack or invalid junk traffic, but they can also be seen as a by-product of traffic load tools used in test environments. You can use the Protection Profiles > SPP Settings configuration page to enable detection for TCP session state anomalies and to allow for the anomalies that are sometimes triggered by traffic load tools.

The table below summarizes recommended settings for TCP session state for the FortiDDoS deployment modes. In a typical Prevention Mode deployment where FortiDDoS receives both sides of the TCP connection, all settings are available and can be useful. Some settings are not appropriate when FortiDDoS is deployed in Detection Mode or Asymmetric Mode. See Understanding FortiDDoS Detection Mode or Understanding FortiDDoS Asymmetric Mode for TCP for additional information on the guidelines for those modes.

TCP session state anomalies detection options

Setting	Detection Mode	Prevention - Symmetric	Prevention - Asymmetric Inbound SYN Direction
Sequence validation Drops packets with invalid TCP sequence numbers.	Do not enable	Recommended	Do not enable
SYN validation Drops SYNs during a flood if the source has not completed the TCP three-way handshake.	Do not enable	Recommended	Recommended
State transition anomalies validation Drops packets with TCP state transitions that are invalid. For example, if an ACK packet is received when FortiDDoS has not observed a SYN/ACK packet, it is a state transition anomaly.	Do not enable	Recommended	Recommended
Foreign packet validation Drops TCP packets without an existing TCP connection and reports them as a foreign packet. In most cases, the foreign packets validation is useful for filtering out junk.	Do not enable	Recommended	Recommended
Allow tuple reuse Allows tuple reuse. Updates the TCP entry during the closed or close-wait, fin-wait, time-wait states, when the connection is just about to retire.	Recommended	Recommended	Recommended

HTTP anomalies

You can use the *Service Protection > HTTP Profile* to enable detection/ prevention for the following HTTP anomalies:

Anomaly	Description
Known Method Anomaly	There are eight known methods: GET, HEAD, OPTIONS, PUT, POST, CONNECT, DELETE, or TRACE. Drop HTTP traffic if the checkbox of the corresponding method is selected. By default, all methods are disabled.
Unknown Method Anomaly	Drops HTTP traffic that uses a method other than GET, HEAD, OPTIONS, PUT, POST, CONNECT, DELETE, or TRACE. For example, TEST or PROPFIND. The dropped packets will be shown in the Monitor Graphs as well as in the Attack Log.
Invalid HTTP Version Anomaly	Drops HTTP traffic with an HTTP version other than 0.9, 1.0, or 1.1. The dropped packets will be shown in the Monitor Graphs as well as in the Attack Log.
Do Not Parse HTTP 0.9	If enabled, do not parse and check HTTP 0.9 traffic. Disabled by default.

Anomaly	Description
Drop Range Header	Drops packet when the HTTP request includes the HTTP Range header. The Range header can be abused by attackers to exhaust HTTP server resources.
Persistent Transaction	A simple HTTP transaction is one where the client makes a single request for HTTP content within a TCP session. Persistent connections allow the browser / HTTP client to utilize the same connection for different object requests to the same host name. If Persistent HTTP Transactions feature is enabled, FortiDDoS checks for application level conformity in every packet of a TCP connection.

Incomplete HTTP Request	Incomplete HTTP Request Detects HTTP packets that do not end with correct end-of-packet characters.
	This can be a result of attack packets, network fragmentation or large HTTP cookies. Since many web servers use tracking cookies that are getting very large, it is not recommended to enable this function on SPPs containing firewalls, proxies or gateways with outbound sessions. You can enable in Detection Mode on web servers and observe the logs for large and consistent numbers of drops, which would indicate the server is using large cookies. If so, disable before entering Prevention Mode.
	• *Block Incomplete HTTP Requests*: Block Incomplete HTTP Requests drops HTTP requests that do not end in the correct end-of-packet information. There are three reasons for incomplete packets:
	  • Attack traffic
	  • MTU or PMTU settings are incorrect resulting in a network-fragmented HTTP packets
	  • Large Cookies used by your website to identify clients can exceed standard packet lengths and result in HTTP fragments. Do not enable this option if you use large cookies.
	• *Block Sources with Incomplete HTTP Requests*: Block Sources of incomplete HTTP packets for all traffic, based on Global Blocking Periods, as well as dropping the incomplete packets. If enabled, the source of incomplete HTTP packets will be blocked based on *Service Protection Policy> Blocking Period for Identified Sources* (default 60 seconds) and reported as Slow Connection: Source floods. Use this option with care as this may block Firewall, proxy and CDN traffic inbound, most of which is not incomplete HTTP packets.

Aggressive aging feature control	Layer 7 Flood and incomplete HTTP request—Sends a TCP RST to the destination server to reset idle connections when an Incomplete HTTP Request is seen, depending on Incomplete HTTP Request settings.
HTTP Get/Post Mitigation Direction	Enable/disable mitigation when HTTP Get/Post flood is enabled.
HTTP Get flood mitigation	Send redirect packet to client. If the client redirect to the new URL that the source is not spoofed, FortiDDoS allows the connection and adds the source to the legitimate IP address table.

Anomaly	Description
HTTP Post flood mitigation	Send set cookie packet to client. If the client's next request with the set cookie of a source is not spoofed, FortiDDoS allows the connection and adds the source to the legitimate IP address table. This option is recommended if you have enough bandwidth in the reverse direction of the attack.

DNS anomalies

DNS anomalies are packet or session state irregularities known to be exploited by attackers. The table below lists the types of DNS anomalies that can be detected.

Note: DNS Anomalies are disabled by default and should only be enabled with Fortinet assistance.

Many networking devices use encrypted DNS packets but still use UDP 53 as the Query/Response Port. FortiDDoS may see these as anomalous, if these features are enabled and may block legitimate Queries to networking vendors' proprietary web filtering services, for example.

DNS anomaly detection

Group	Anomaly
DNS header anomaly	• Invalid op-code—Invalid value in the OpCode field. • Illegal flag combination—Invalid combination in the flags field. • SP, DP both 53—Normally, all DNS queries are sent from a high-numbered source port (49152 or above) to destination port 53, and responses are sent from source port 53 to a high-numbered destination port. If the header has port 53 for both, it is probably a crafted packet.
DNS query anomaly	• Query bit set—DNS query with the query reply (QR) bit set to 1. In a legitimate query, QR=0. • Null query—DNS query in which the question, answer, additional, and name server counts are 0. • RA bit set—DNS query with the recursion allowed (RA) bit set. The RA bit is set in responses, not queries. • QDCNT not 1 in query—Number of entries in the question section of the DNS packet is normally 1. Otherwise, it might be an exploit attempt.
DNS response anomaly	• QCLASS in reply—DNS response with a resource specifying a CLASS ID reserved for queries only (QCLASS). • QTYPE in reply—DNS response with a resource specifying a TYPE ID reserved for queries only (QTYPE). • Query bit not set—DNS response with the query reply (QR) bit set to 0. In a legitimate response, QR=1. • QDCNT not 1 in response—Number of entries in the question section of the DNS packet is normally 1. Otherwise, it might be an exploit attempt.
DNS buffer overflow	• TCP Message too long—TCP query or response message that exceeds the

Group	Anomaly
anomaly	maximum length specified in the message header. • UDP message too long—UDP query or response message that exceeds the maximum length specified in the message header. • Label length too large—Query or response with a label that exceeds the maximum length (63) specified in the RFC. • Name too long—DNS name that exceeds 255 characters. This can cause problems for some DNS servers.
DNS exploit anomaly	• Pointer loop—DNS message with a pointer that points beyond the end of data (RFC sec4.1.4). This is an exploit attempt. • Zone transfer—An asynchronous Transfer Full Range (AXFR) request (QTYPE=252) from untrusted networks is likely an exploit attempt. • Class is not IN—A query/response in which the question/resource address class is not IN (Internet Address). Although allowed by the RFC, this is rare and might indicate an exploit attempt. • Empty UDP message—An empty message might indicate an exploit attempt. • Message ends prematurely—A message that ends prematurely might indicate an exploit attempt. • TCP Buffer underflow—A query/response with less than two bytes of data specified in the two-byte prefix field.
DNS info anomaly	Type ALL used—Detects a DNS request with request type set to ALL (QTYPE=255). Typical user queries to not request ALL.
DNS data anomaly	• Invalid type, class—A query/response with TYPE or CLASS reserved values. • Extraneous data—A query/response with excess data in the packet after valid DNS data. • TTL too long—TTL value is greater than 7 days (or 604800 seconds). • Name length too short—A query/response with a null DNS name.

NTP Anomalies

For both intentional and unintended reasons, NTP queries and responses may be improperly crafted. FortiDDoS allows you to block any packet with the following anomalies. Anomalies will be displayed in *Attack Logs* and *Monitor* > *Anomaly Drops* > *Layer 7* > *NTP* graph page.

The following Header Anomalies can be enabled/disabled as required. Turn these Anomalies ON during Learning/Detection Mode and evaluate the Outbound drops showing for these anomalies. If you are seeing large outbound drops for a specific anomaly and the Protected IP looks legitimate, disable the anomaly. Note that while Outbound may be in Detection mode if the system “drops” an Outbound Query because of an Anomaly, it will not put this Query in the NRM table and if an Inbound Response is seen it will be dropped as “unsolicited” (see below) which will affect the ability of your devices to reach NTP servers.

Header Anomaly	Description	Usage
Data Length	Each NTP version has a specified maximum data length in the Query or Response. FortiDDoS will match the actual data length to the defined data length for the identified Version and drop any packet that does match correctly.	Normally, this anomaly can be enabled for all conditions.
Stratum	NTP includes Stratum information to describe the accuracy of the server clock. The RFC supports 0-15 “stratum” but the Stratum field allows 256. Any number above 15 is an anomaly and will be dropped. In addition, if the Stratum is 2 or greater a Reference ID must be included in the request and response. If it is not included, it will be dropped.	Normally, this anomaly can be enabled for all conditions.
Version	NTP Version must be between 1 and 4. If the Version is 1, then the Mode must be 0.	Normally, this anomaly can be enabled for all conditions.
Control Header	FortiDDoS monitors 9 different Control header anomalies • Request LEAP INDICATOR as zero • Request with ERROR or MORE bits set • Request with non-zero OFFSET • Request with reserved OPCODE (>7). • Response with COUNT value as 0 • Fragmented error response (E=1 and M=1) • First response with M=1 with non-zero OFFSET • Response with reserved STATUS values(>7)	Normally, this anomaly can be enabled for all conditions. However if you are hosting an NTP server, you many need to disable this option. Enable and monitor during Learning/ Detection and evaluate the number of events and drops in both directions. If unsure contact Fortinet Support.

State Anomaly	Description	Usage
Retransmission Check	If multiple identical Requests are seen before a Response is seen subsequent identical Requests are dropped. **Note:** This feature will not work where there is asymmetric traffic and FortiDDoS may not see all Responses. Disable this feature if FortiDDoS is in Asymmetric Mode.	Normally used on an NTP server seeing Requests.
Sequence Mismatch	Detects header Sequence number errors in Queries and Responses. **Note:** This feature will not work where there is asymmetric traffic and FortiDDoS may not see all Responses.	Disable this feature if FortiDDoS is in Asymmetric Mode.

State Anomaly	Description	Usage
Unsolicited Response Check (NRM)	FortiDDoS records all passing NTP Requests. When a matching NTP Response is seen the record is cleared. If an NTP Response has seen that was not Requested, it is “unsolicited” and dropped immediately. **Note:** This feature mitigates NTP Reflected Response Floods from the first packet, without the requirement for a Response Threshold. However, this feature will not work where there is asymmetric traffic and FortiDDoS may not see all Requests or Responses. If the system is in Asymmetric Mode, disable this feature and use Response Threshold below.	This feature would normally be used where inside protected clients are trying to reach NTP servers outside (internet-side) of the FortiDDoS. This features also works where you are expecting no NTP traffic in either direction, where, for example, you have an NTP server on your network and do not need to access the Internet for time information.
Mode Mismatch	Some Modes must be different in the Client Query and Server Response while some Modes are the same for both. FortiDDoS monitors valid combinations and if any are invalid, that packet will be dropped. The only valid Mode pairs for Requests/Responses are 1/2, 3/4, 6/6 or 7/7. **Note:** Mode Mismatch (MM) is like Unsolicited Response, working only with symmetric traffic. If FortiDDoS is in Asymmetric Mode, disable this feature. MM can be used without it.	See Unsolicited Response (NRM) above.
Reflection Deny	No parameters. If you enable Reflection Deny, FortiDDoS will deny NTP Mode 7 and NTP Mode 6 packets in Queries and Responses. These packets are not needed and are frequently abused to create reflected, amplified NTP DDoS attacks.	

SSL/TLS Anomalies

You can use the *Service Protection* > *SSL/TLS Profile* to enable detection/prevention for the following SSL/TLS anomalies:

Anomaly	Description
Protocol Anomaly	Enable/Disable TLS protocol Anomaly Check. Normal Content types mainly include :changecipherspec, alert, handshake, application_data, heartbeat. Once protocol-anomaly option enabled and DDOS the type in the received message mismatched the above type value, DDOS will take the message as protocol-anomaly message, then log and drop the message.
Version Anomaly	Enable/Disable TLS Version Anomaly Check. Valid version values are SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 which are from 768 to 771 inclusive. Once version-anomaly option enabled, and the version value in the received message is mismatched these values, FortiDDoS will take the message as version-anomaly, then log and drop it.

Anomaly	Description
Cipher Anomaly	Enable/Disable TLS Cipher Anomaly Check. FortiDDoS will verify if the cipher is normal. If not, it will take the message as the cipher-anomaly message, then log and drop it.
Block Incomplete Request	Enable/Disable Block Incomplete TLS Request Slow-connection. When the actual data length of TLS record is less than its length field value or the data length of handshake protocol is less than its length field value, the request is considered as Incomplete Request which will be dropped and logged.
Aggressive Aging Incomplete Request	Enable/Disable switch for send reset to server for incomplete message to release Server resources. When it's enabled, as long as Incomplete Request traffic is detected, FortiDDoS will send reset to server for aging TCP connection.
Block Source with Incomplete Request	Enable/Disable source with Block Incomplete TLS Request to block client. When it's enabled, as long as Incomplete Request traffic is detected, FortiDDoS will block all traffic from the same source address for a block period.
Renegotiation Check	Enable/Disable renegotiation check (Per connection check). Drops the packet if SSL renegotiations exceed Renegotiation Threshold per Renegotiation Aging Time from any Source. • *Renegotiation Aging Time*: The period of checking renegotiation, default value is 1 second. • *Renegotiation Threshold*: Max renegotiation time for client during aging-time, default value is 5 seconds.

Understanding FortiDDoS Detection Mode

In Detection Mode, FortiDDoS logs events and builds traffic statistics for SPPs, but it does not take actions: it does not drop or block traffic, and it does not aggressively age connections. Packets are passed through the system to and from protected subnets. Any logs and reports that show drop or blocking activity are actually simulations of drop or block actions the system would have taken if it were deployed in Prevention Mode.

When you get started with FortiDDoS, you deploy it in Detection Mode for 2-14 days so that the FortiDDoS system can learn the baseline of normal inbound and outbound traffic. The length of the initial learning period depends upon the seasonality of traffic (its predictable or expected variations) and how representative of normal traffic conditions the learning period is. Ensure that there are no attacks during the initial learning period and that it is long enough to be a representative period of activity. If activity is heavier in one part of the week than another, ensure that your initial learning period includes periods of both high and low activity. Weekends alone are an insufficient learning period for businesses that have substantially different traffic during the week. Thus, it is better to start the learning period on a weekday. In most cases, 7 days is sufficient to capture the weekly seasonality in traffic.

At the end of the initial learning period, you can adopt system-recommended thresholds (usually lower than the factory default) and continue to use Detection Mode to review logs for false positives and false negatives. As needed, you repeat the tuning: adjust thresholds and monitor the results.

When you are satisfied with the system settings, change to Prevention Mode. In Prevention Mode, the appliance drops packets and blocks sources that violate ACL rules and DDoS attack detection thresholds.

Important: In Detection Mode, the FortiDDoS system forwards all packets, but a simulated drop might be recorded. TCP session control options depend on the true TCP state, and simulated drops when the appliance is in Detection Mode can lead to unexpected results. For example, if the system records a (simulated) drop for a TCP connection, when subsequent packets arrive for the connection, the system treats them as foreign packets because the state table entry indicates the session has already been closed.

The table below summarizes our guidelines for SYN flood mitigation and TCP session state settings in Detection Mode.

SYN flood mitigation and TCP state anomaly detection settings

Settings	Guidelines
Global Settings > Settings	
SYN Flood Mitigation	The SYN flood mitigation mode settings are not applicable and disregarded. In Detection Mode, the FortiDDoS system does not drop packets, so it cannot test the legitimacy of source IP addresses.
Protection Profiles > SPP Settings > TCP session feature control	
SYN validation	Do not enable. This option enables SYN flood mitigation mode, which is not applicable in Detection Mode.
Sequence validation	Do not enable. Simulated “drops” in Detection Mode lead to incorrect window validations for subsequent session packets.
State transition anomalies validation	Do not enable. Simulated “drops” in Detection Mode lead to faulty tracking of session state.
Foreign packet validation	Do not enable. Simulated “drops” in Detection Mode lead to unexpected foreign packet violations.
Allow tuple reuse	Exception to the rule. Enabled by default to support standard test environments that reuse tuples in quick succession. The setting is valid in Detection Mode. Recommended to avoid unnecessary logging of the event when it is detected.
Allow duplicate SYN-in-SYN-SENT	Exception to the rule. Not enabled by default, but the setting is valid in Detection Mode. Recommended to avoid unnecessary logging.
Allow duplicate SYN-in-SYN-RECV	Do not enable.
Allow SYN anomaly	
Allow SYN-ACK anomaly	
Allow ACK anomaly	
Allow RST anomaly	
Allow FIN anomaly	

Understanding FortiDDoS Prevention Mode

This section includes the following information about attack mitigation features when you deploy FortiDDoS in Prevention Mode:

SYN flood mitigation

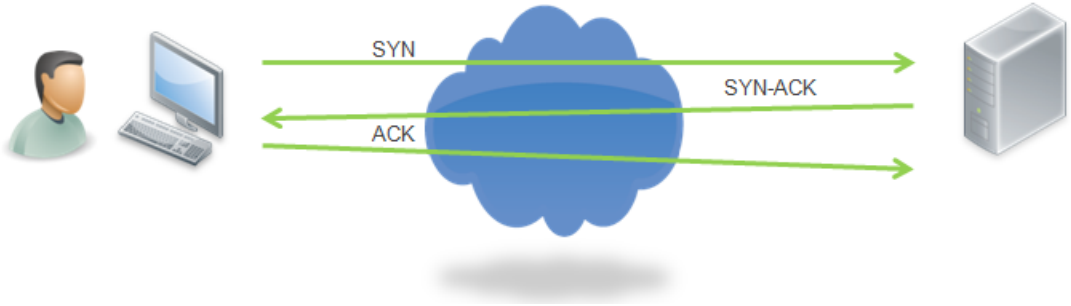
This section includes the following information:

Overview

When a client attempts to start a TCP connection to a server, the client and server perform a three-way handshake:

- The client sends a SYN message to the server to request a connection.
- The server creates an entry for the connection request in the Transmission Control Block (TCB) table with status SYN-RECEIVED, sends an acknowledgment (SYN-ACK) to the client, and waits for a response.
- The client responds with an acknowledgment (ACK), the connection is established, and the server updates the entry in the TCB table to ESTABLISHED.

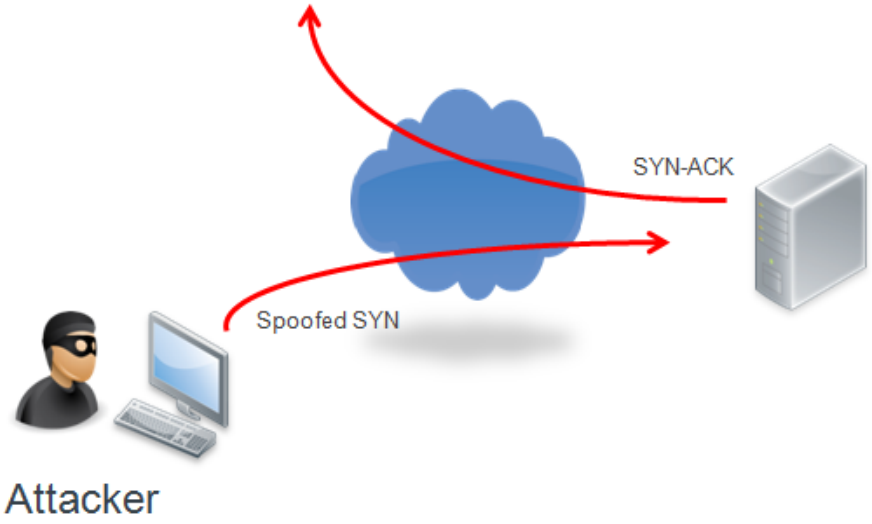
TCP Connection Three-Way Handshake



A SYN flood attack on a server exploits how the server maintains TCP connection state for the three-way handshake in the TCB table. In a spoofed attack, the attacker sends a large number of SYN packets from spoofed IP addresses to the server; or in a zombie attack, the attacker has used a virus to gain control of unwitting clients and sends a large number

of SYN packets from legitimate IP addresses to the server. Each SYN packet that arrives creates an entry in the table. The spoofed addresses make it impossible to resolve the three-way handshake, and the TCP connection state in the TCB table remains 'half-open' instead of completing the cycle. It never transitions to 'established' and ultimately to 'closed'. As a result, TCB table entries are not "cleaned up" by the expected life cycle, resources can be exhausted, and there can be system failure and outages.

Half-Open TCP Connection SYN Flood Attack



To prepare for SYN flood attacks, FortiDDoS maintains a table of IP addresses that have completed a three-way handshake. This is called the legitimate IP address (LIP) table. Entries in the LIP expire after 1 minute.

When FortiDDoS detects a SYN flood attack, it enters SYN flood mitigation mode. In this mode, the system acts as a proxy for TCP connection requests and uses the LIP table to validate new connections:

- New SYN packets coming from addresses in the LIP table are presumed legitimate and are allowed
- FortiDDoS takes a guarded approach to other SYN packets, and they are processed according to the configured SYN flood mitigation mode option:
  - ACK Cookie
  - SYN Cookie (This is the preferred SYN flood mitigation method.)
  - SYN Retransmission

The SYN flood mitigation mode behavior applies only when FortiDDoS has detected a SYN flood with either of the following thresholds:

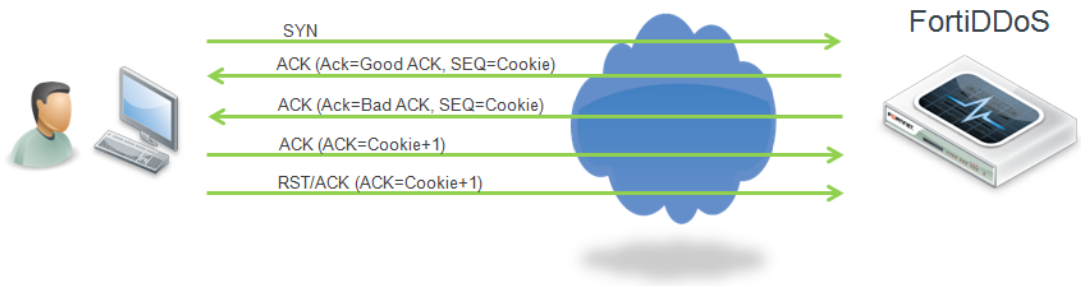
- **syn**: When total SYNs to the subnet exceeds the threshold, the SYN flood mitigation mode tests are applied to all new connection requests.
- **syn-per-dst**: When the per-destination limits are exceeded for a particular destination, the SYN flood mitigation mode tests are applied to all new connection requests to that particular destination. Traffic to other destinations is not subject to the tests.

ACK Cookie

The figure below illustrates the ACK Cookie mitigation mode option. FortiDDoS sends the client two ACK packets: one with a correct ACK number and another with a wrong number. The system determines whether the source is not

spoofed based on the client's response. If the client's response indicates that the source is not spoofed, FortiDDoS-F allows the connection and adds the source to the legitimate IP address table. Fortinet recommends this option if you have enough bandwidth in the reverse direction of the attack. (This method generates 2 responses for every SYN. Thus, a 1 Gbps SYN flood will generate 2 Gbps reverse traffic.)

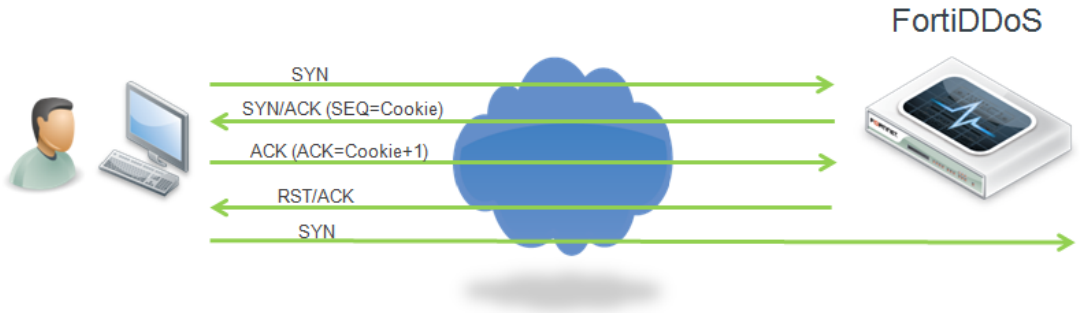
SYN Flood Mitigation Mode—ACK Cookie



SYN Cookie

The figure below illustrates the SYN Cookie mitigation mode option. FortiDDoS sends a SYN/ACK with a cookie value in the TCP sequence field. If it receives an ACK back with the right cookie, a RST/ACK packet is sent and the IP address is added to the LIP table. If the client then retries, it succeeds in making a TCP connection. Fortinet recommends this option if you cannot use ACK Cookie and you anticipate high volume attacks.

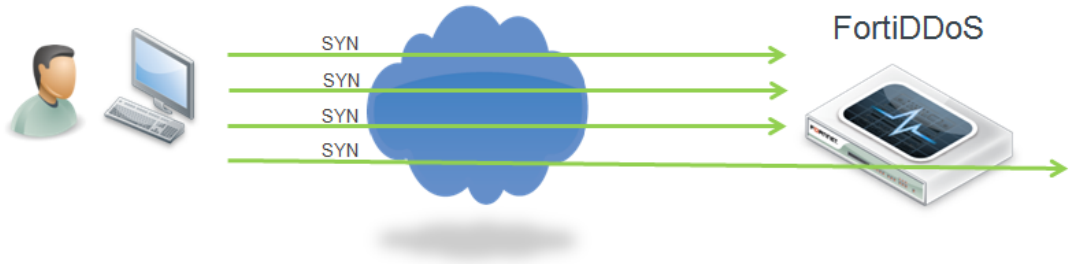
SYN Flood Mitigation Mode—SYN Cookie



SYN Retransmission

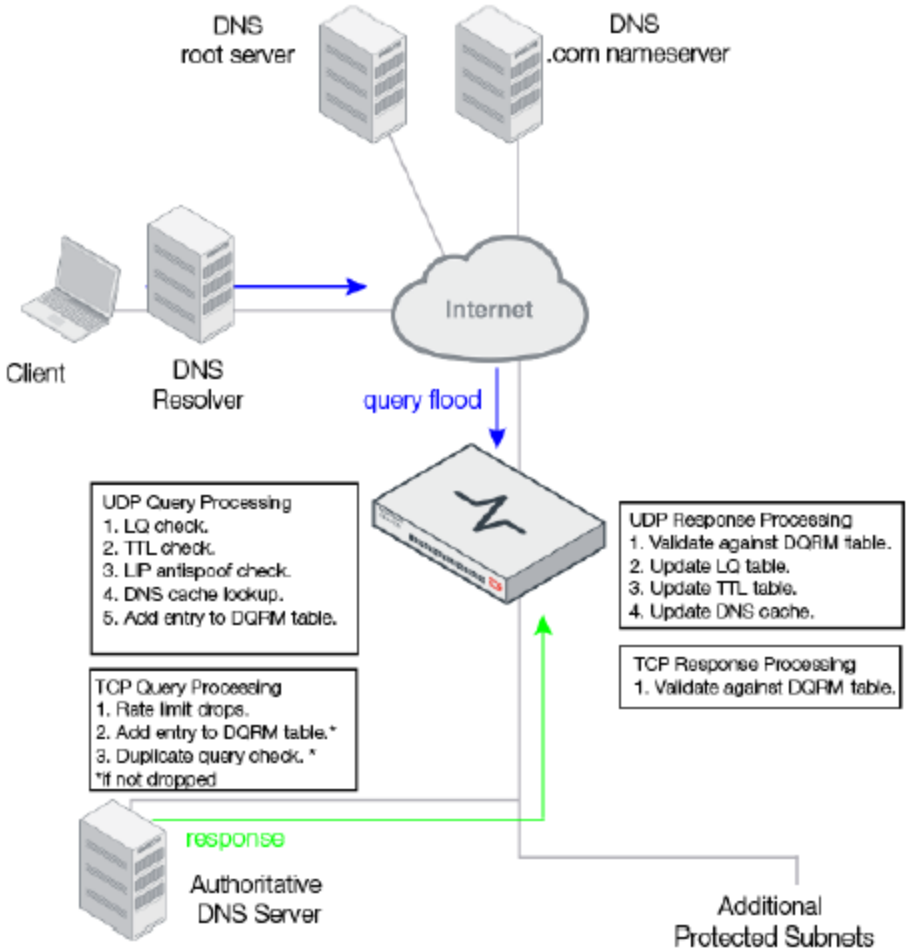
The figure below illustrates the SYN Retransmission mitigation mode option. FortiDDoS drops the initial SYNs to force the client to send a SYN again. If a pre-configured number of retransmitted SYNs arrive within a predefined time period, the FortiDDoS considers the source to be legitimate. It allows the connection to go through and adds the source to the legitimate IP address table. Fortinet recommends this option if you cannot use ACK Cookie and you anticipate low volume attacks.

SYN Flood Mitigation Mode—SYN Retransmission



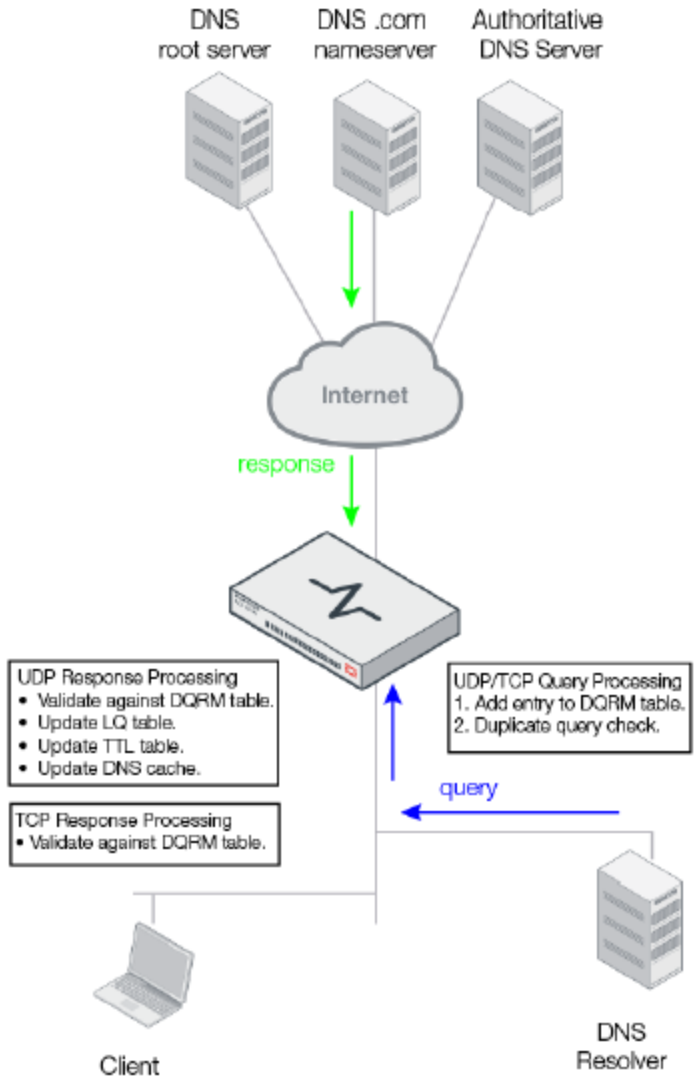
DNS flood mitigation

The following figure shows how FortiDDoS mitigates a DNS query flood. It uses the DNS tables and LIP table to validate queries and responses.



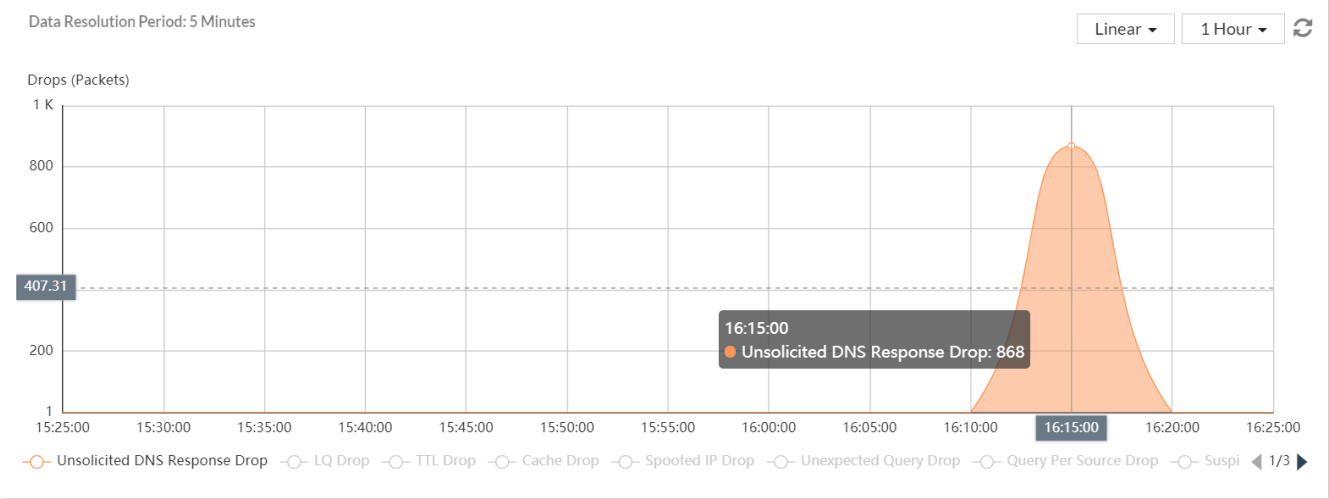
FortiDDoS mitigates DNS threats by applying tests to determine whether responses are legitimate.

These methods minimize illegitimate traffic from reaching protected DNS servers and maximize the availability of DNS services for legitimate queries during a flood.



DNS Query Response Matching (DQRM)

When a DNS query is received, the system stores the DNS transaction details in the DQRM table. It can store up to 1.9 million records. When it receives a response, it searches this table for a matching query. If the response has no matching query, FortiDDoS drops the unmatched response. Drops are reported on the *Monitor* > *Layer 7* > *DNS* > *Unsolicited Response* graph. The table entry is cleared after the matching response is received. The DQRM table response validation prevents attacks that attempt to exploit DNS responses, such as DNS cache poisoning and DNS amplification attacks (also called Distributed Reflective Denial of Service attacks). The DQRM can also be used to throttle repeated queries that would otherwise result in unnecessary server activity. The "Duplicate query check before response" option drops identical queries (same transaction details) that are repeated at a rate of 3/second. Drops are reported on the *Monitor* > *Layer 7* > *DNS* > *Unexpected Query* graph.



DNS Rcode Thresholds

Inbound/Outbound limitation packet rate for the selected RCODE. Invalid range of RCODE and inbound/outbound threshold are configurable.

To improve DNS Response Flood mitigation with asymmetric traffic and/or where encrypted DNS is present, Thresholds can be added in Service Protection/Service Protection Policy/Threshold/DNS RCODE:

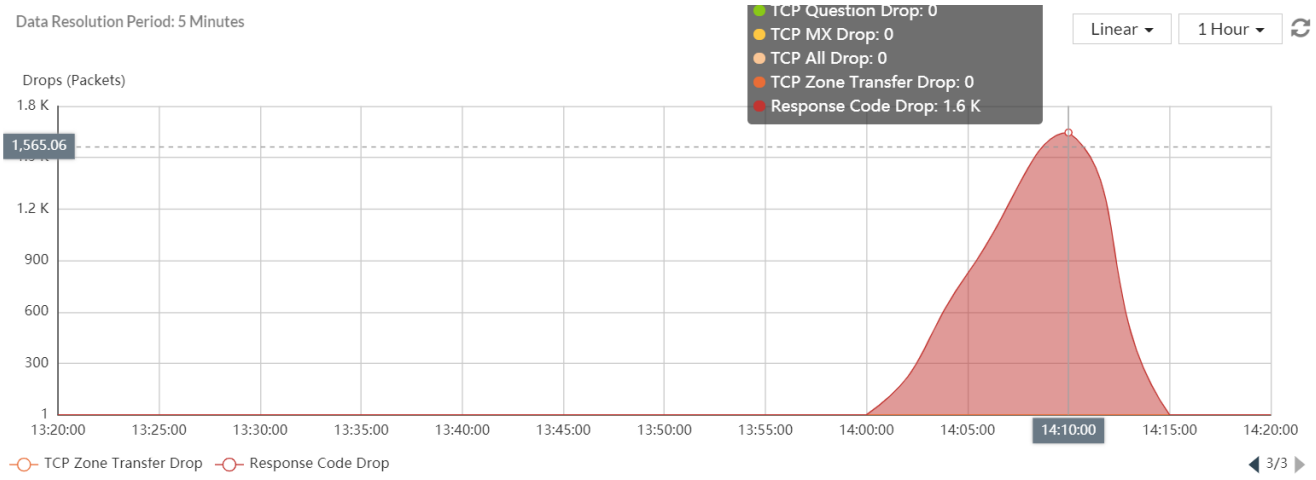
Rcode Start: Threshold applied to DNS R-Code start.

Rcode Stop: Threshold applied to DNS R-Code stop.

Inbound Threshold: Ingress limitation packet rate for the selected RCODE

Outbound Threshold: Outgress limitation packet rate for the selected RCODE

Traffic and Drops for all R-codes is seen in the *Monitor > Drops > L7 >DNS*



NTP flood mitigation

The following shows how FortiDDoS mitigates NTP response flood. It uses reflection check,connection state check and threshold limit check to validate NTP responses.

Reflection Deny

When NTP reflection deny is enabled, FortiDDoS will drop NTP Mode 7 (Monlist) and NTP Mode 6 (Varlist) packets in Queries and Responses. These packets are unnecessary and are frequently abused to create reflected, amplified NTP DDoS attacks. Drops are reported on *Drop Monitor > ACL Drops > Layer7 > NTP> NTP Reflection ACL Drops*.

Unsolicited Response Check

When FortiDDos receives a NTP query, the system stores the NTP transaction details in the NRM table. When it receives a response, it searches this table for a matching query. If the response has no matching query, FortiDDoS drops the unmatched response. Drops are reported on the *Drops Monitor > Anomaly Drops > Layer 7 > NTP graph*. The table entry is cleared after the matching response is received. The NRM table response validation prevents attacks that attempt to exploit NTP responses, such as NTP amplification attacks (also called Distributed Reflective Denial of Service attacks). The NRM can also be used to throttle repeated queries that would otherwise result in unnecessary server activity. When the "Retransmission" option is enabled, if multiple identical Requests are seen before a Response is received, subsequent identical Requests will be dropped. Drops are reported on the *Drops Monitor > Anomaly Drops > Layer 7 > NTP graph*.

NTP Thresholds

FortiDDos supports NTP response per destination threshold, NTP request threshold, NTP response threshold and NTP broadcast threshold to limit different types of NTP traffic rates. Thresholds can be added in *Service Protection > Service Protection Policy > Threshold > Scalars*. Drops are reported on the *Drops Monitor > Flood Drops > Layer 7 > NTP graph*.

Aggressive aging

This section includes the following topics:

- Slow connection detection and aggressive aging
- Rate anomalies and aggressive aging
- Idle connections and aggressive aging

Slow connection detection and aggressive aging

Slow connection attacks are Layer 4-7 attacks that aim to make a service unavailable or increase latency to a service. These attacks are not detected by Layer 4 volumetric detection methods because they create legitimate TCP connections. With these attacks, distinguishing attackers from legitimate users is a complex task.

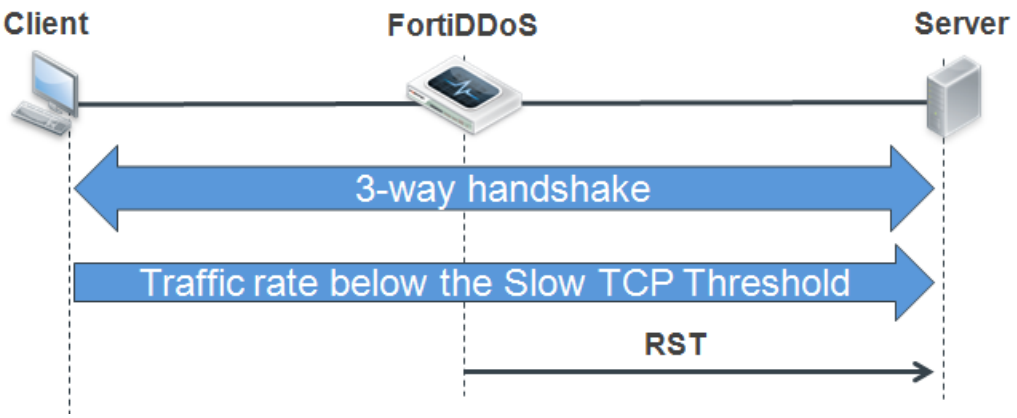
Variations of the Slowloris attack involve opening a legitimate TCP connection and not doing anything at all. Such idle connections fill up the connection tables in firewall and servers.

FortiDDoS can detect slow connection attacks and combat them by 'aggressively aging' slow connections. When slow connection detection is enabled, the system monitors TCP ports 80 by default, and 443 for slow connection anomalies. Monitor ports can be user-configured. If the traffic volume for a connection is below a specified byte threshold during an observation period, the connection is deemed a slow connection attack and the following actions can be taken:

- If the *Service Protection* > *TCP Profile* > *TCP Session Settings* > *Aggressive Aging Feature Control* > ***Slow TCP Connections*** option is enabled, FortiDDoS sends a RST packet to the server so that the server can remove the connection from its connection table.
- If the *Service Protection* > *TCP Profile* > *TCP Packets Validation* > ***Foreign Packet Validation*** option is enabled, the subsequent packets for the connection are treated as foreign packets and dropped. The event is logged as a Foreign Packets (Aggressive Aging and Slow Connections) and then as a State Anomalies: Foreign packet (Out of State) event and drops are reported on the *Drops Monitor* > *Anomaly Drops* > *Layer 4*.
- If **Block Sources with Slow TCP Connections** option is enabled, FortiDDoS applies the 'Blocking Period for Identified Sources' configured on the *Service Protection Policy* > *Blocking Settings* > *Blocking Period For Identified Sources* (in seconds). The drops based on this blocking period action are also logged as 'Slow Connection: Source flood' events and reported on the *Drops Monitors* > *Flood Drops* > *Layer 4* page.

The figure below illustrates how FortiDDoS deployed between the client and server can monitor slow attack threats and take action to aggressively age them.

Slow connection detection and aggressive aging



Note: By default, FortiDDoS uses the MAC address for the management interface (mgmt1) when it sends a TCP reset to aggressively age the connection. To configure a different MAC address for the resets, go to *Global Settings* > *Settings* > *Settings*.

Another slow connection attack, the R U Dead Yet? (RUDY) attack, injects one byte of information into an HTTP POST request. The partial request causes the targeted web server to hang while it waits for the rest of the request. When repeated, multiple simultaneous RUDY connections can fill up a web server's connection table.

When deployed between clients and servers, FortiDDoS can detect HTTP connections that resemble RUDY attacks and 'aggressively age' the connections in the same way it does for slow TCP connection attacks. When a partial request is sent from a client, it can be dropped.

The following actions can be taken:

- If *Service Protection* > *HTTP Profile* > *Incomplete Request Action* setting is set to Drop, the Incomplete HTTP Packet is dropped. The event is logged as a 'Incomplete HTTP Request' event, and drops are reported on Drops Monitors > Anomaly Drops > Layer 7 > HTTP Header page.
- If *Service Protection* > *HTTP Profile* > *Incomplete Request Action* setting is Aggresive Aging, the Incomplete HTTP Packet is also dropped. The session entry in the FortiDDoS TCP state table is timed out and an RST is sent

to the server. The event is logged as an 'Incomplete HTTP Request' event and drops are reported on *Drops Monitor > Anomaly Drops > Layer 7 > HTTP Header* page.

- If the *Service Protection > TCP Profile > TCP Packets Validation > Foreign Packet Validation* is enabled, subsequent packets for the connection are treated as foreign packets and dropped The event is logged as a Foreign Packets (Aggressive Aging and Slow Connections) and then as a 'State Anomalies: Foreign packet (Out of State)' event and drops are reported on *Monitor > Anomaly Drops > TCP State Anomalies* page.
- If the Block Sources with Incomplete HTTP Request setting is enabled, FortiDDoS applies the 'Blocking Period for Identified Sources' configured on the *Service Protection Policy > Blocking Settings* page. The drops based on this blocking period action are also logged as 'Slow Connection: Source flood' events and reported on the *Drops Monitor > Flood Drops > Layer 4* page.

- Track Slow TCP Connections should not be enabled if FortiDDoS is in Asymmetric Mode, since it needs to see both directions of traffic to properly determine Byte counts.
- Large Cookies can also cause Incomplete HTTP Requests. It is recommended that this feature should not be used on SPPs that contain firewalls, gateways, proxies or other devices that originate many outbound sessions to the Internet.

The table below summarizes the predefined thresholds for slow connection detection.

Slow connection detection thresholds

Setting	Moderate	Aggressive	User Defined	None
Slow TCP connection byte threshold	512 Bytes	2048 Bytes	1 – 65535 Bytes	Disabled – ignore entry
Slow TCP connection observation period	30 seconds	15 seconds	1 – 1023 seconds	Disabled – ignore entry

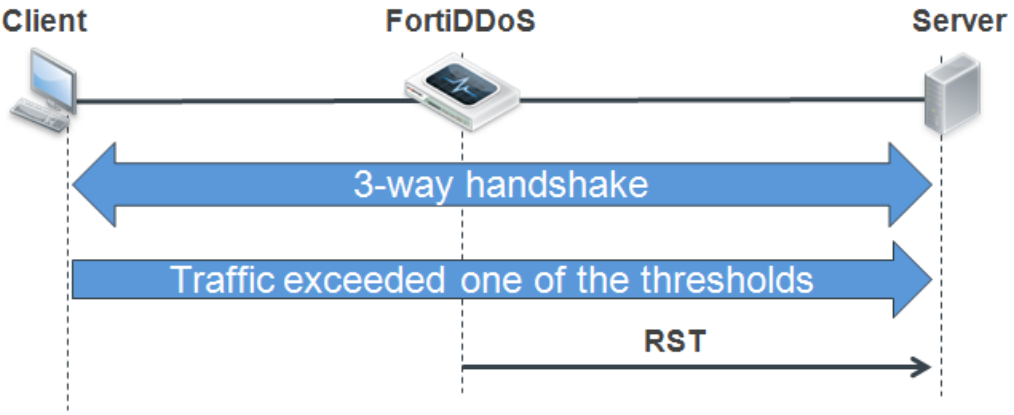
Caution: Source blocking for slow connection detection is disabled by default. Do not enable if it is typical for the SPP to receive traffic with source IP addresses that are proxy IP addresses (for example, a CDN proxy like Akamai). You want to avoid blocking a proxy IP address because the block potentially affects many users that are legitimately using the same proxy IP address.

Rate anomalies and aggressive aging

In addition to the slow connection detection, you can use *Service Protection > TCP Profile > Aggressive Aging Feature Control > High Concurrent Connection per Source* option and *HTTP Profile > Aggressive Aging Flood* option to reset the connection (instead of just dropping the packets) when the high-concurrent-connection-per-source and HTTP rate anomalies are detected.

The figure below illustrates aggressive aging when high concurrent connection or HTTP rate anomalies are detected.

Rate anomalies and aggressive aging



Note: The initial drops resulting from aggressive aging appear in logs and reports as SYN per Source flood drops or HTTP method flood drops, as appropriate. If the TCP session feature control option **foreign-packet-validation** option is also enabled, subsequent packets from these sources are dropped as foreign packet anomalies because the packets are correlated with a connection that has been reset.

Idle connections and aggressive aging

FortiDDoS maintains its own massive TCP connection table. To reserve space in this table for active traffic, FortiDDoS periodically uses aggressive aging to reset inactive connections based on the idle timers configured in *Service Protection > TCP Profile > TCP Session Idle Timeout*.

Rate limiting

FortiDDoS maintains rate meters for packets, connections, and requests. It drops packets that exceed the maximum rates (which are based on history, heuristics, and a multiplier that you specify or based on an absolute limit that you specify).

Rate limiting thresholds are not only a good way to detect attacks, but also an effective method to protect servers. When deployed between client and server traffic, the rate limits ensure that a server is not inundated with more traffic than it can handle.

When FortiDDoS drops packets that exceed the maximum rates, the originating client retransmits the packets. Traffic originating from attackers is likely to be marked by extended blocking periods, while traffic originating from legitimate clients is likely to find itself within the acceptable rates as thresholds are reevaluated.

Blocking

In Prevention Mode, traffic that exceeds protection profile thresholds is blocked for the configured blocking period. When blocking period is over, the threshold is checked again.

The below examples assume that the blocking period has the default value of 15 seconds.

Example 1: Too many packets with a specified protocol

- The system drops incoming packets with the protocol that are destined for a specific network (specified as a subnet) for 15 seconds. It forwards all other packets.
- The system tracks the source of the packets to determine if this is a single-source attack.
- After 15 seconds, the system checks the rate of the packets against the threshold again.

Example 2: Too many mail messages to an SMTP server

- The system drops incoming TCP packets destined for port 25 on the mail server (or the mail server's network) for 15 seconds. It forwards all other packets.
- The system tracks the source of the packets to determine if this is a single-source attack. If there is a single source, the appliance blocks all packets from that source for 15 seconds.
- After 15 seconds, the system checks the rate of the packets against the threshold again.
- Mail clients assume that the network is slowing down because TCP packets are lost. The clients start to send packets at a slower rate. No mail messages are lost.

Example 3: Too many SYN packets to a web server

- The system checks SYN packets destined for a web server. If they come from an IP address in the legitimate IP address table, the system permits them to continue to the web server. The appliance allows these packets as long as their rate is lower than the new-connections threshold (designed to indicate zombie floods). The system forwards all other SYN packets.
- If the IP address does not exist in the legitimate IP address table, and if the SYN flood mitigation method is SYN cookie, the system performs a proxy three-way handshake to validate the IP address.
- After 15 seconds, the system checks the packet rate against the threshold again.

Example 4: Too many concurrent connections from a single source

- If there are too many concurrent TCP connections from a single source, the system blocks new connections until the number of concurrent connections is less than the threshold.
- Once the concurrent connection count goes down, the system allows the source to establish new connections.
- The system tracks the source of the connections to determine if this is a single-source attack. If there is a single source, the appliance blocks all packets for 15 seconds.
- After 15 seconds, the system checks the connection rate against the threshold again.

Reducing false positives

When the FortiDDoS-F system blocks traffic because it exceeds the threshold of a specific traffic parameter, it blocks subsequent traffic with the offending characteristic. As a result, during the blocking period, the system might block traffic from legitimate sources in addition to traffic from a malicious source.

The system uses the following mechanisms to minimize the impact of these false positives:

- Because the blocking period is short (1 to 15 seconds), the system frequently checks to see if the traffic no longer exceeds the threshold that detected the attack.

- The system simultaneously attempts to determine whether the attack is not spoofed and can be attributed to one or a few sources. If it can identify these sources (called source attackers), it applies a “multiplier” to them. The multiplier makes traffic from these source attackers more likely to exceed the most active source threshold, which causes the system to apply a longer blocking period.
- If it identifies attackers, the system can stop blocking traffic from legitimate sources as soon as the standard, shorter blocking period is over, but continue to block traffic from source attackers for a longer period.

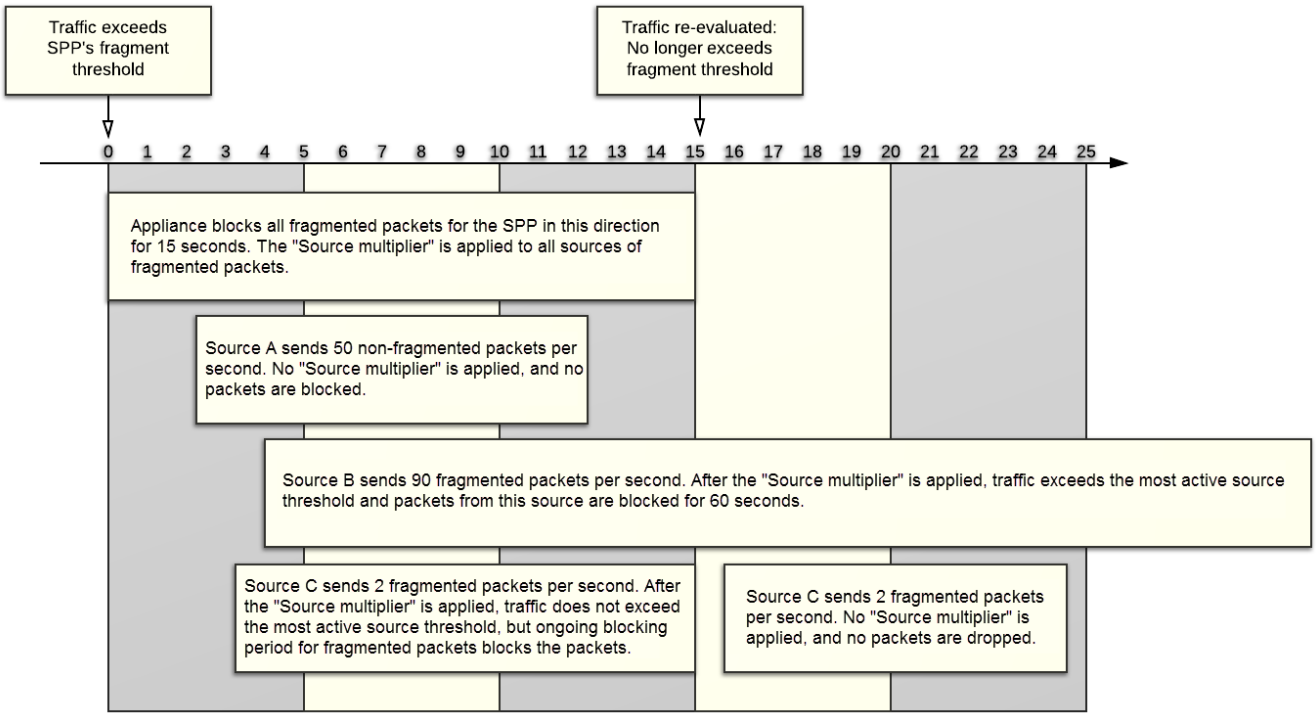
The figure below illustrates how the FortiDDoS system responds immediately to attacks but then adjusts its attack mitigation activity to packets from specific sources only.

In this example, the standard blocking period is 15 seconds and the blocking period for source attackers is 60 seconds (the default value). The multiplier for source attackers is 16, and the most active source threshold is 100 packets per second.

When Source B sends 90 fragmented packets, the calculated rate is 1440 packets per second, which exceeds the most active source threshold. But when Source C sends 2 fragmented packets per second, the calculated rate of 32 packets per second does not exceed the threshold. Thus, the system applies the longer blocking period to Source B only.

Source C, which sends an insignificant number of fragmented of packets, is blocked only for the length of the shorter, standard blocking period.

System attack response timeline



Understanding FortiDDoS Asymmetric Mode for TCP

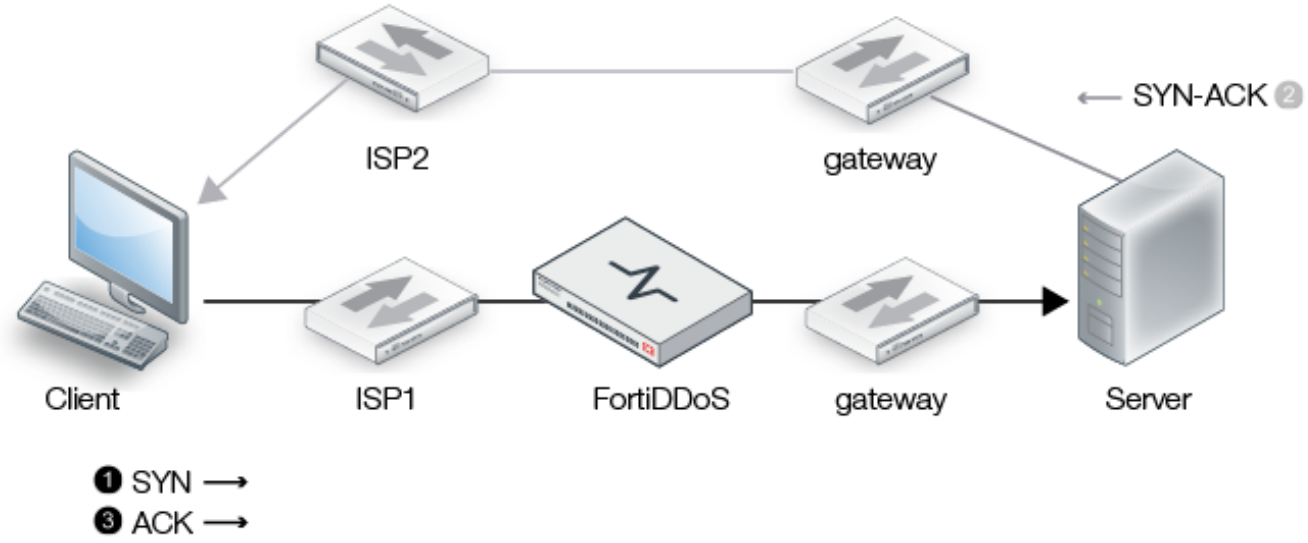
FortiDDoS monitors TCP states. For TCP state monitoring to work fully and properly for all types of related mitigation, bidirectional traffic must pass through FortiDDoS.

When only one direction of traffic passes through the device, from FortiDDoS' perspective, we call it Asymmetric traffic and the appliance must be set in Asymmetric Mode.

Combinations of multiple links and BGP routing tables at the ISPs and the customer can result in inbound and outbound using any combination of the links.

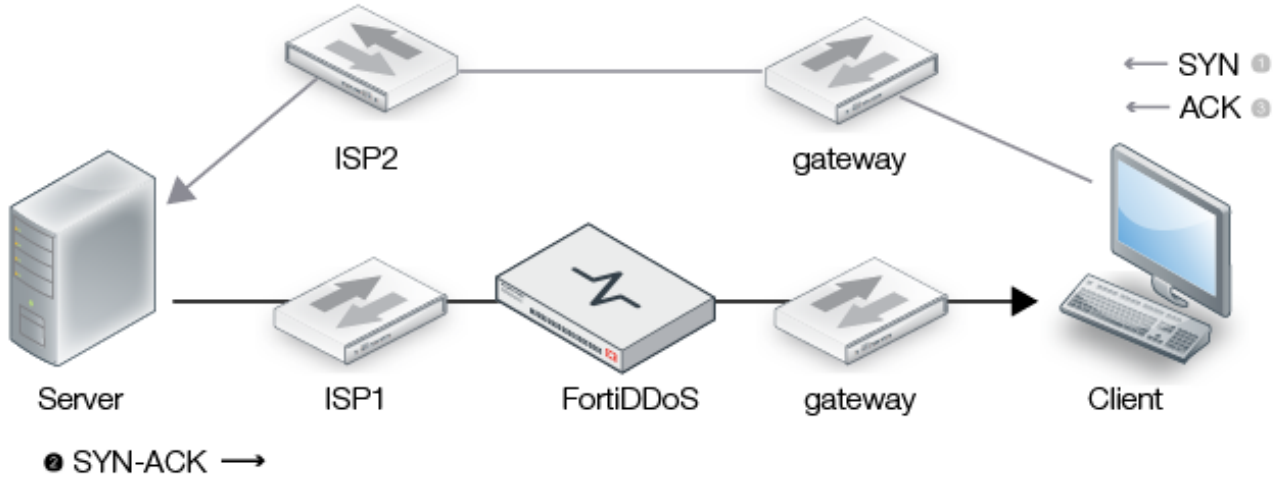
The figure below shows an asymmetric route when an external client initiates the connection, such as a web server request. The initial TCP SYN traverses the network path where FortiDDoS has been deployed, but the SYN-ACK response takes a different route to the client.

Asymmetric route when an external client initiates the connection



The following figure shows an asymmetric route when the internal resource initiates the connection, such as when a backup server initiates a scheduled job. The TCP SYN takes an out-of-path route, and the SYN-ACK packet is the first packet that FortiDDoS sees for the session.

Asymmetric route when an internal server initiates the connection



We have two key recommendations if you plan to deploy the FortiDDoS appliance in a network path where asymmetric routes are possible:

- When feasible, design the network routes so that FortiDDoS sees both sides of the client-server connection. You might be able to do this with the preferred routes, persistence, or active/active synchronization features of the routing devices in your deployment.
- If you cannot avoid asymmetric traffic, enable FortiDDoS Asymmetric Mode. In Asymmetric mode, FortiDDoS can use virtually 100% of its methods to detect abnormal network traffic, with the exception of the parameters noted below. Disabling these parameters results in a very small loss of attack detection capability.

In Asymmetric Mode, the system can parse Layer 4 and Layer 7 headers for most floods and URL-related features. If this feature is off, such floods are not detected when two-way session traffic is not completely seen by the appliance.

You must enable both **Asymmetric Mode** and the **Allow Inbound SYN-ACK** option so the system can properly handle asymmetric TCP traffic. When enabled, the system treats an inbound SYN-ACK as if a SYN, and it creates an entry for it in the TCP connection table. It does not increment the **syn** threshold counter, but it does track **syn-per-src** in order to protect against attacks that might attempt to exploit this behavior.

TCP state anomaly detection depends on tracking a two-way traffic flow, so some feature options on the Protection Profiles > SPP Settings page do not work in Asymmetric Mode. The table below summarizes the configuration guidelines for these feature options.

Recommended TCP state anomaly detection settings in Asymmetric Mode

Settings	Guidelines
SYN validation	Recommended. This option enables SYN flood mitigation mode.
Sequence validation	Do not enable. Depends on tracking a two-way traffic flow.
State transition anomalies validation	Do not enable. Depends on tracking a two-way traffic flow.
Foreign packet validation	Recommended. In Asymmetric Mode, FortiDDoS can still track foreign packets.
Allow tuple reuse	Enabled by default to support standard test environments that reuse

Settings	Guidelines
	tuples in quick succession. The setting is valid in Asymmetric Mode. Recommended to avoid unnecessary logging of the event when it is detected.
Allow duplicate SYN-in-SYN-SENT	Not enabled by default, but the setting is valid in Asymmetric Mode. Recommended when FortiDDoS is in Detection Mode to avoid unnecessary logging of the event when it is detected.
Allow duplicate SYN-in-SYN-RECV	Do not enable.
Allow SYN anomaly	
Allow SYN-ACK anomaly	
Allow ACK anomaly	
Allow RST anomaly	
Allow FIN anomaly	

Workflow for getting started with Asymmetric Mode

1. Go to Global Settings > Settings > Settings > Deployment tab and enable the following settings:
   - Asymmetric Mode
   - Allow inbound SYN/ACK
2. Get started in Detection Mode:
   a. For each SPP, go to Protection Profiles > SPP Settings and ensure that the following TCP state anomaly options are enabled and no other:
      - Syn validation
      - Foreign packet validation
      - Allow tuple reuse
      - Allow duplicate SYN-in-SYN-SENT
   b. Enable Detection Mode.
   c. Establish a baseline of traffic statistics and set thresholds.
3. Change settings to the ones appropriate for Prevention Mode when there is asymmetric traffic:
   a. For each SPP, go to Protection Profiles > SPP Settings and ensure that the following TCP state anomaly options are enabled and no other:
      - SYN validation
      - Foreign packet validation
      - Allow tuple reuse
   b. Enable Prevention Mode.

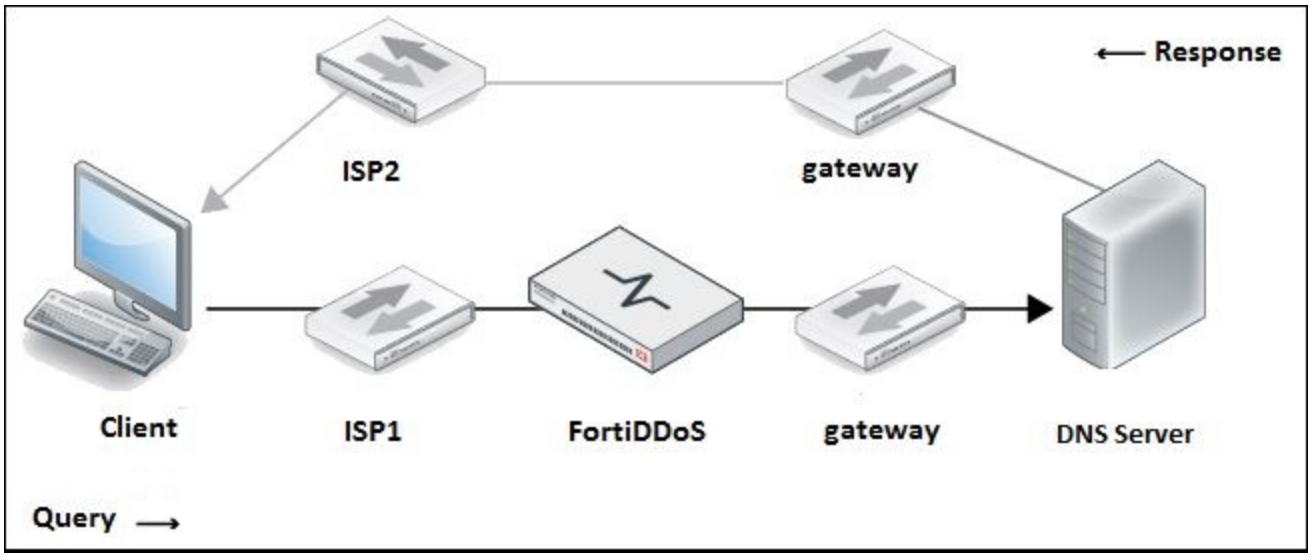
Understanding Asymmetric Mode and DNS

An asymmetric route is one in which the traffic in one direction traverses FortiDDoS system, but traffic in the other direction takes a route that does not go via FortiDDoS. Combinations of multiple links and BGP routing tables at the ISPs and customer can result in inbound and outbound using any combination of the links.

If FortiDDoS is deployed in Asymmetric mode, then most DNS Feature controls must be disabled.

To mitigate many DNS DDoS attacks, FortiDDoS maintains tables for both DNS Queries and Responses. If both Queries and Responses do not go through FortiDDoS, then the functionality must be disabled for the device to work and report attacks properly.

Asymmetric Mode and DNS

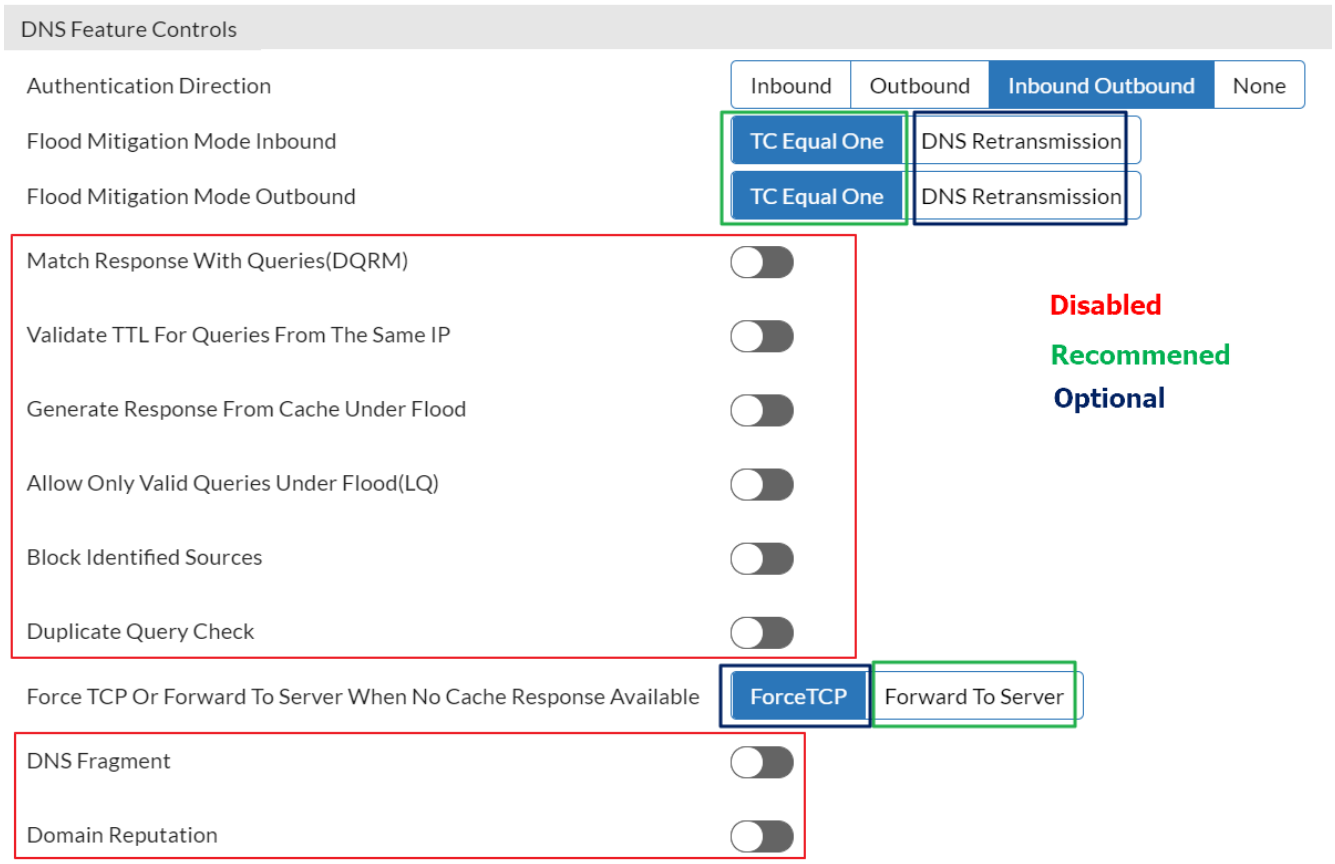


In asymmetric mode, the expectation is that FortiDDoS will only see half of most DNS Query/Response transactions. Since DNS is normally UDP and stateless, FortiDDoS cannot make assumptions of the state and may drop DNS Queries and/or Responses as anomalous.

DNS Anomaly Feature Controls are primarily DNS header anomalies. This can be enforced in Asymmetric mode because they work on packet by packet basis rather than maintaining state across packets.

The following figure shows the allowed DNS Feature Control configuration for use with asymmetric traffic:

DNS Feature Control configuration for asymmetric traffic



Understanding FortiDDoS DNS attack mitigation

This section includes the following information:

- DNS attack vulnerability overview
- FortiDDoS DNS protection module summary
- FortiDDoS DNS flood mitigation overview
- FortiDDoS DNS flood types
- FortiDDoS DNS deployment topologies
- Getting started with DNS mitigation on page 87

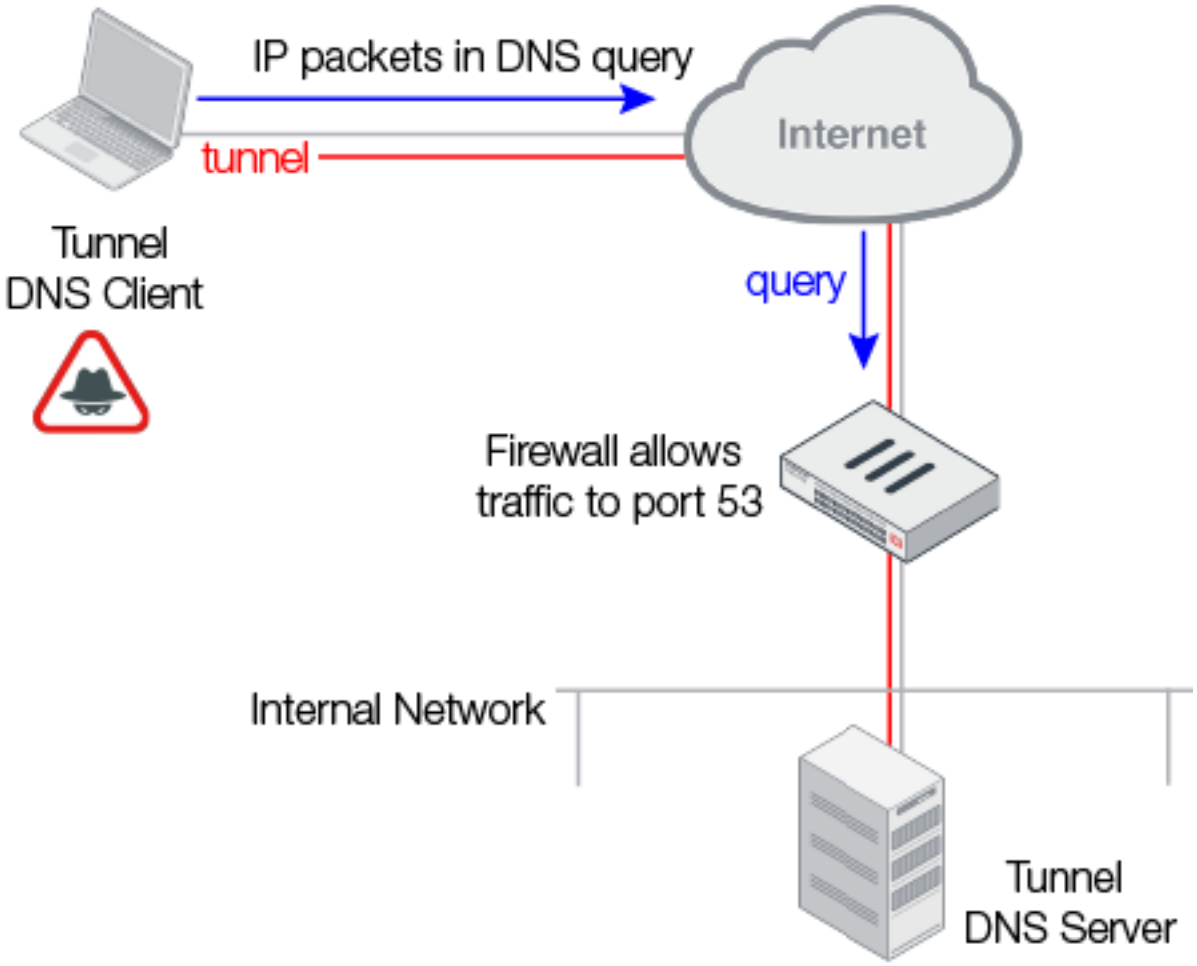
DNS attack vulnerability overview

DNS was designed for robustness and reliability, not security. It is vulnerable to multiple types of attacks that can compromise or take down a network. Some of these attacks are described here.

DNS tunneling

DNS tunneling exploits the fact that firewall administrators must open port 53 in order for DNS authoritative name servers to respond to queries from the Internet. The attacker compromises a host in the internal network and runs a DNS tunnel server on it. A DNS tunnel client outside the internal network can then gain access to the internal network by sending a DNS query to the compromised host that sets up a DNS tunnel.

DNS tunneling attack



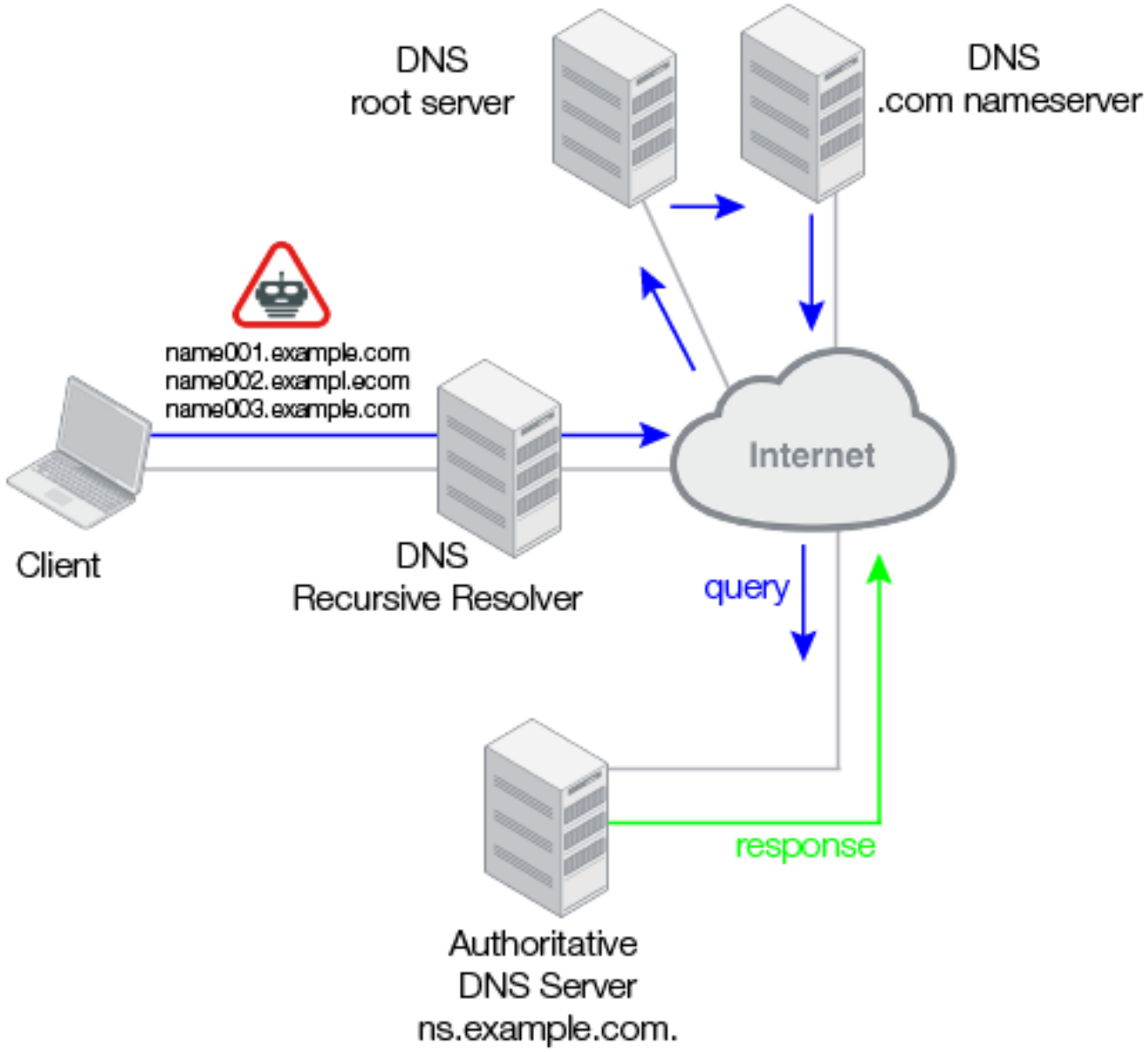
You can use FortiDDoS DNS anomaly detection to drop DNS tunneling attempts if the tunneling attempts do not conform to DNS header syntax.

DNS query floods

A DNS flood is an attempt to create a network outage by flooding critical DNS servers with excessive queries.

Some DNS floods target the authoritative name server for a domain. In these types of attacks, malware bots send a continuous flood of queries for random, nonexistent subdomains of a legitimate domain. All of the DNS servers in the recursive chain consume resources processing and responding to the bogus queries.

DNS slow-drip, random, non-existent subdomain attack

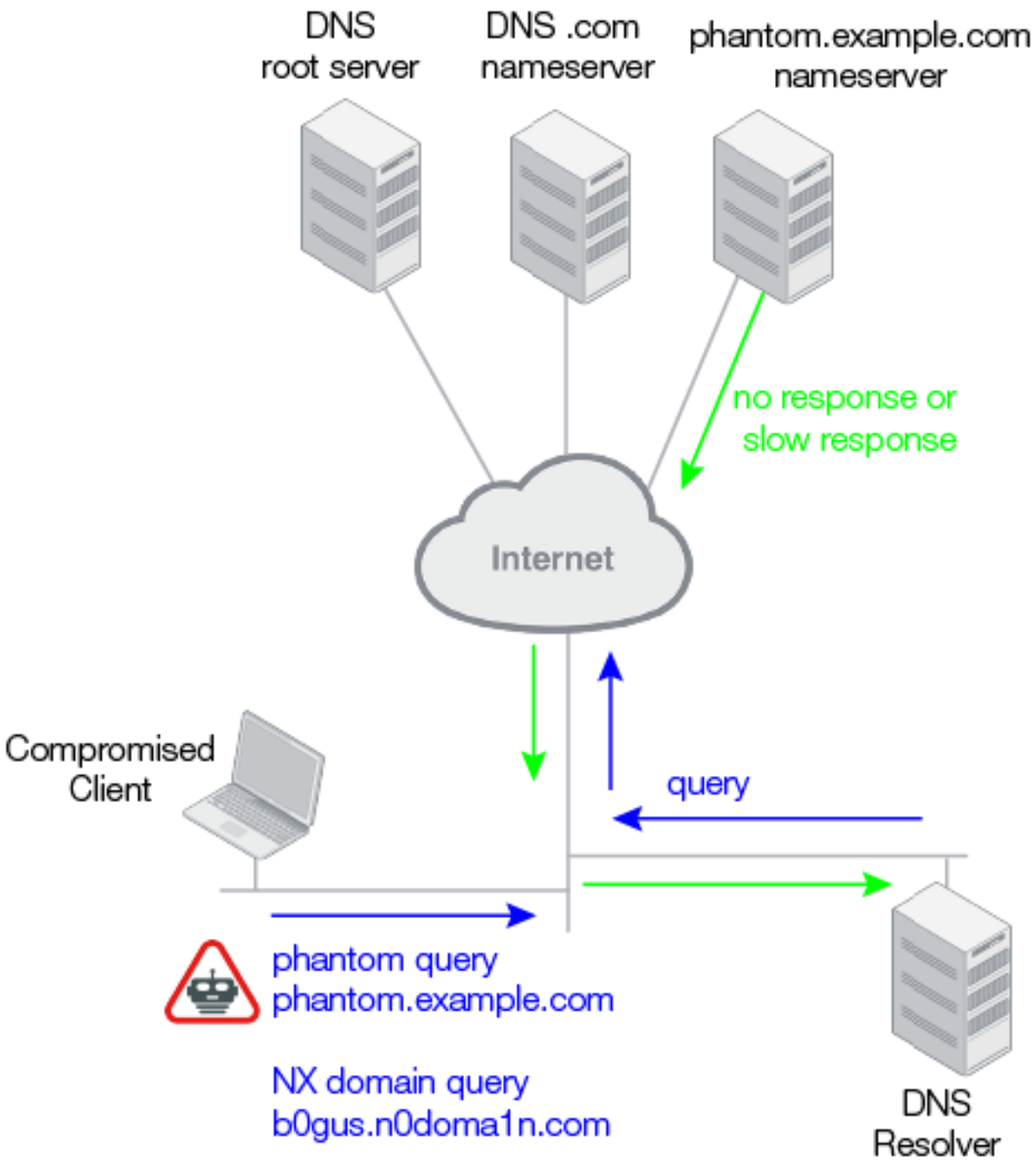


If clients in your internal network have been compromised by malware, your internal DNS resolvers could also be targets of query flood attacks.

In non-existent NX domain (NXDOMAIN) attacks, the clients that have been compromised send queries for domains that do not exist. This uses resources and can fill up the cache.

In phantom domain attacks, the clients that have been compromised send DNS queries for a phantom domain name—a domain server that exists, but it is controlled by an attacker. The attacker might have configured it to send no responses or slow responses. These illegitimate transactions waste resources, and a flood of them can take down the DNS resolver.

DNS NX domain and phantom domain attack

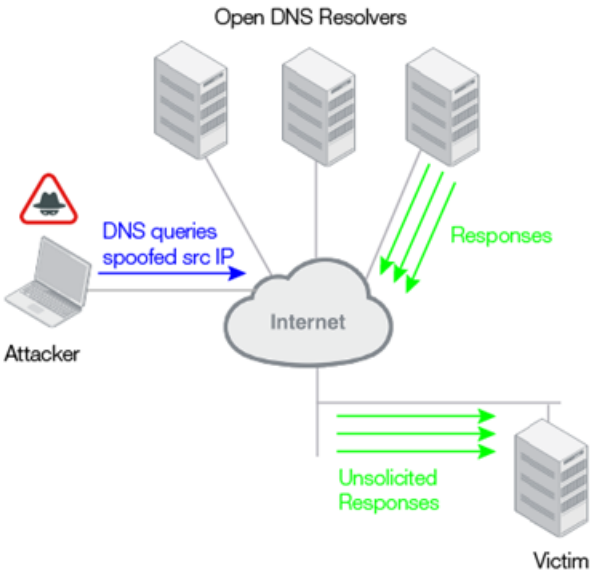


You can use FortiDDoS DNS flood mitigation features to prevent query floods.

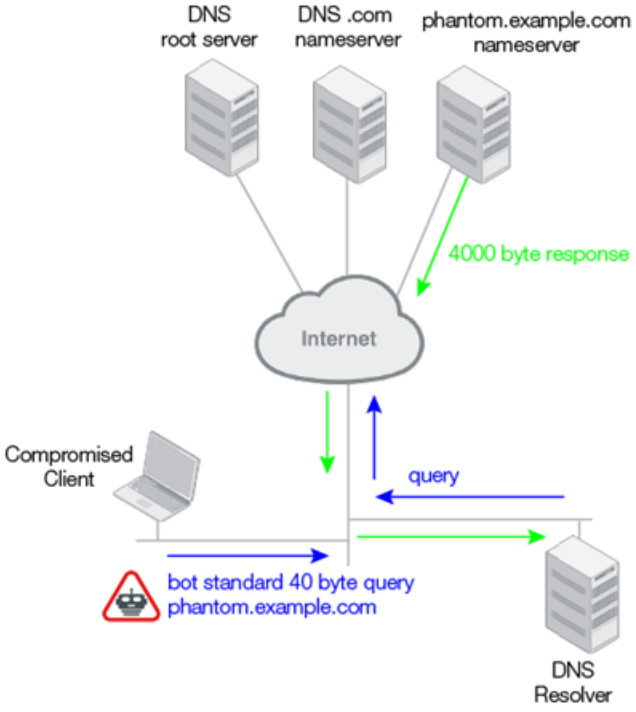
DNS response exploits

There are also many attacks that use DNS responses to do damage. Unsolicited responses are a symptom of DNS Distributed Reflective Denial of Service attacks, DNS amplification attacks, and DNS cache poisoning.

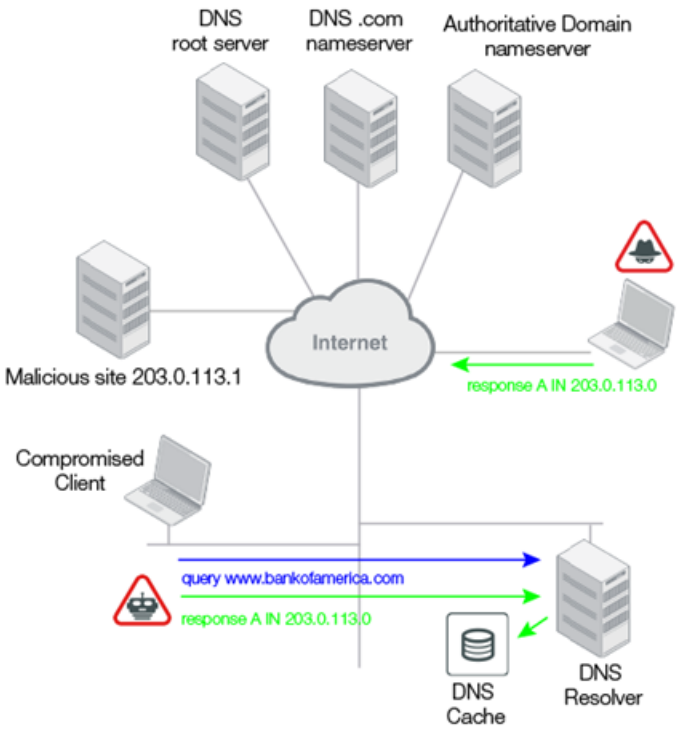
DNS reflection attack



DNS amplification attack



DNS cache poisoning



You can use the FortiDDoS DNS query response matching (DQRM) feature to prevent DNS response exploits.

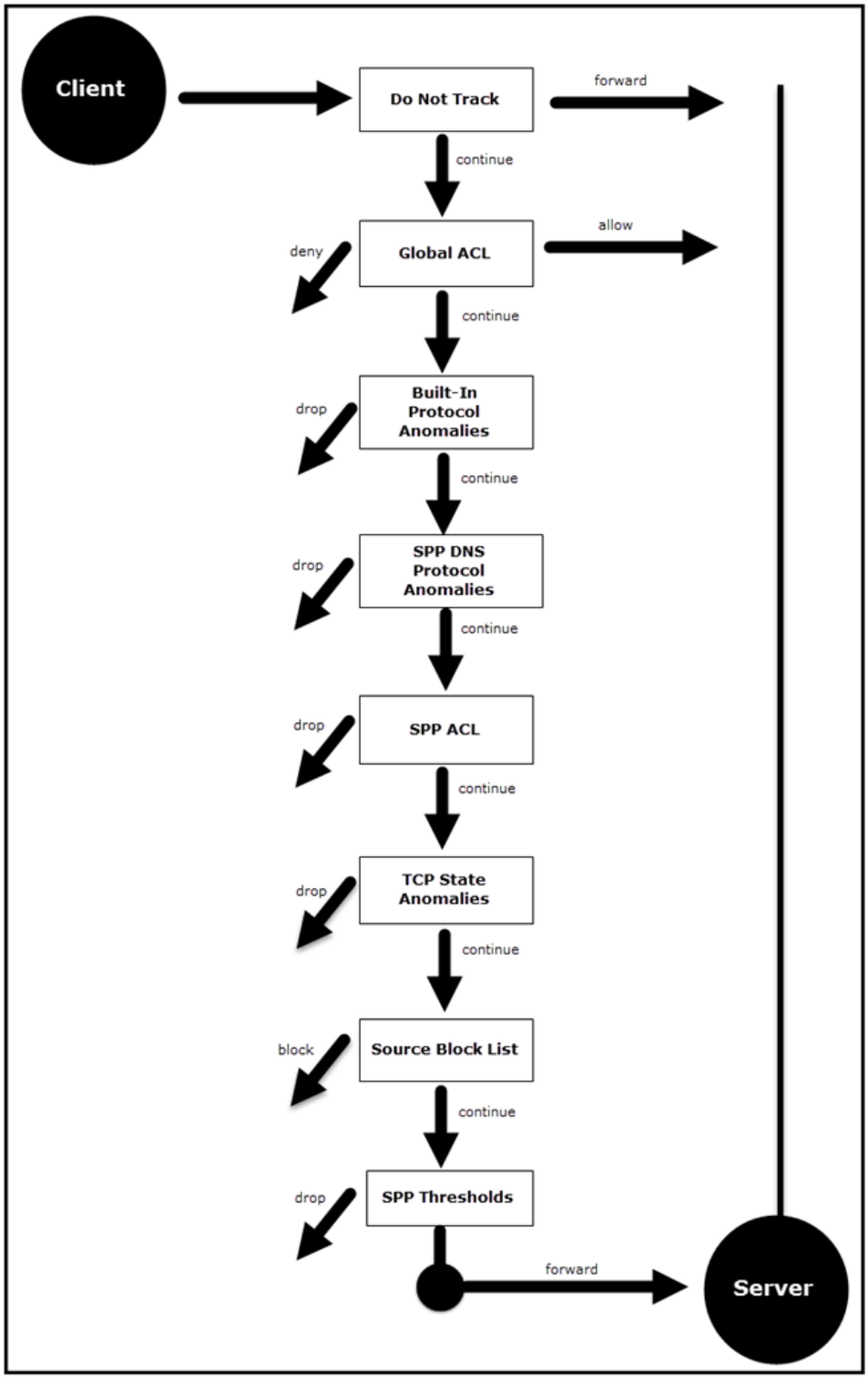
FortiDDoS DNS protection module summary

FortiDDoS has the following protection modules for DNS (transport over TCP or UDP):

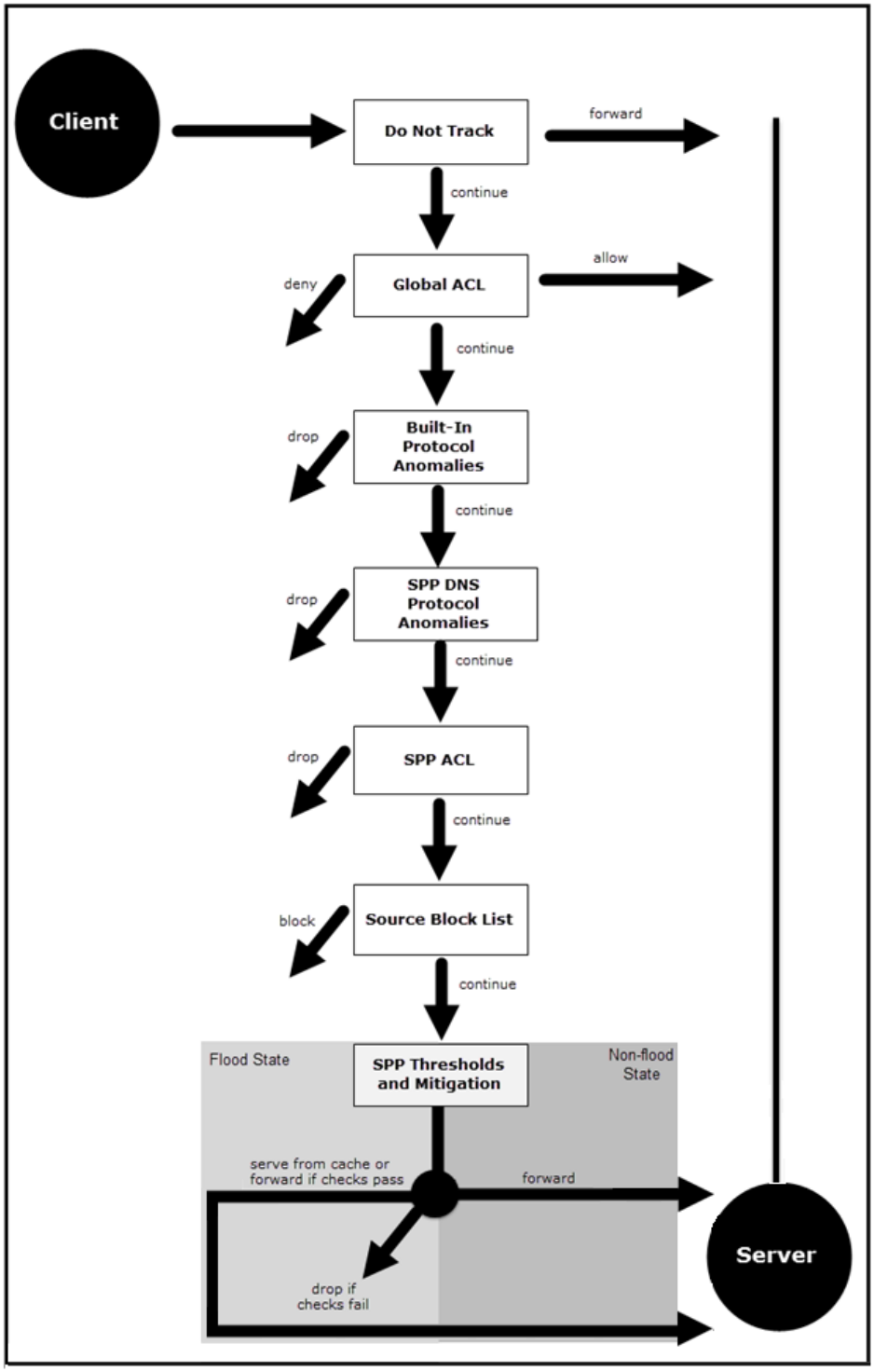
- Protocol anomaly rules
  Built-in and user-enabled rules filter malformed traffic and known protocol exploits. There is a special set of anomalies that can be detected in DNS traffic. For an overview of protocol anomalies, see Understanding FortiDDoS protocol anomaly protection.
- Rate meters and flood mitigation mechanisms
  For TCP, the DNS rate meters enforce rate limits (drops). For UDP, the DNS rate meters trigger flood mitigation responses that drop illegitimate queries but continue DNS services for legitimate user queries. For details, see FortiDDoS DNS flood mitigation overview.
- DNS Query Response Matching (DQRM)
  Blocks unsolicited responses and throttles duplicate queries (regardless of flood state). See FortiDDoS DNS flood mitigation overview.

The following two figures illustrate the order in which FortiDDoS applies its rules and actions for TCP and UDP DNS traffic, respectively.

TCP DNS Drop Precedence



UDP DNS Drop Precedence



FortiDDoS DNS flood mitigation overview

FortiDDoS mitigates DNS threats by applying tests to determine whether queries and responses are legitimate. These methods minimize illegitimate traffic from reaching protected DNS servers and maximize the availability of DNS

services for legitimate queries during a flood.

Under normal conditions (no floods), FortiDDoS builds a baseline of DNS traffic statistics and stores DNS query and response data in tables. At all times, the tables are used to validate response traffic. During UDP floods, the tables are used to test queries and responses. The following table describes the system tables used for DNS attack mitigation.

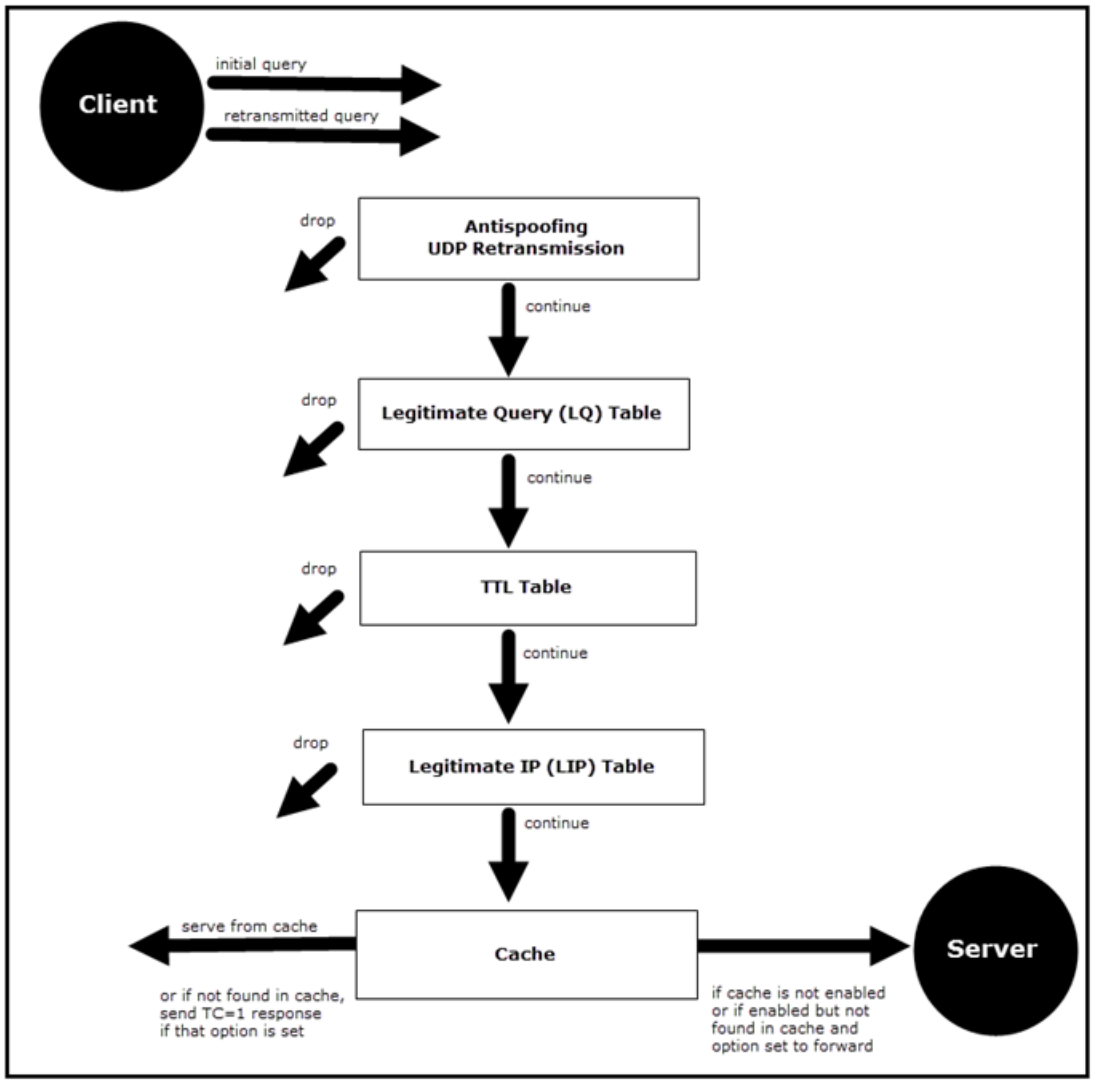
DNS-related system tables

System Table	DNS Flood Mitigation
DNS Query Response Match (DQRM) table	Used for all DNS traffic—UDP or TCP. When it receives a DNS query, the system stores the DNS transaction details in the DQRM table. It can store up to 1.9 million records. When it receives a response, it searches this table for a matching query. If the response has no matching query, FortiDDoS drops the unmatched response. Drops are reported on the Monitor > Layer 7 > DNS > Unsolicited Response graph. The table entry is cleared after the matching response is received. The DQRM table response validation prevents attacks that attempt to exploit DNS responses, such as DNS cache poisoning and DNS amplification attacks (also called Distributed Reflective Denial of Service attacks). The DQRM can also be used to throttle repeated queries that would otherwise result in unnecessary server activity. The "Duplicate query check before response" option drops identical queries (same transaction details) that are repeated at a rate of 3/second. Drops are reported on the Monitor > Layer 7 > DNS > Unexpected Query graph.
Legitimate Query (LQ) table	Used to mitigate UDP floods. When a valid response is received, the query details are stored in the table. It can store 128,000 records. Entries are cleared when the TTL expires. During a flood, the system drops queries that do not have entries in the table. Drops are reported on the Monitor > Layer 7 > DNS > LQ Drop graph.
TTL table	Used to mitigate UDP floods. When a valid response is received, the query details are correlated with the client IP address and stored in the table. It can store 1.5 million records. Entries are cleared when the TTL expires. Responses with TTL=0 are not added to the table. During a flood, the system drops queries that have an entry in the table. It is not expected that a client would send the same query before the TTL expires. Drops are reported on the Monitor > Layer 7 > DNS > TTL Drop graph.
Legitimate IP table	Used to mitigate UDP floods. During DNS query floods, you can leverage the legitimate IP (LIP) table to test whether the source IP address is spoofed. If the source IP address is found in the LIP table, processing continues; if there is no entry, the system can test source IP legitimacy by performing a UDP retransmission test or by sending a response with the TC flag set. The TC flag indicates to the client to retry the request over TCP. When the query is retried over TCP, other flood mitigation mechanisms may be available, such as SYN flood antispoofing features. Drops are reported on the Monitor > Layer 7 > DNS > Spoofed IP Drop graph.
DNS cache	Used to mitigate UDP floods.

System Table	DNS Flood Mitigation
	When a valid response is received, the system caches the response packets. It can store 64,000 records. Entries are cleared when the TTL expires. During a flood, if the query passes the LQ and TTL checks, the response is served from the cache and the query is not forwarded to the DNS server. This enables legitimate clients to get DNS results without adding load to the server that is being attacked. If there is not an entry in the cache, you can configure whether you want the query to be forwarded to the DNS server or have FortiDDoS send a response with the TC flag set. The TC flag indicates to the client to retry the request over TCP. Drops are reported on the Monitor > Layer 7 > DNS > Cache Drop graph.
Source tracking table	Used for source flood tracking—UDP or TCP. Tracks DNS queries per source and suspicious actions per source. It drops packets that exceed the maximum thresholds and applies the blocking period for identified sources. Drops are reported on the Monitor > Layer 7 > DNS Query Per Source and the Monitor > Layer 7 > Suspicious Sources graphs.

Source tracking thresholds and TCP thresholds are rate limits, resulting in drops when the flood rate thresholds are crossed. For UDP, rate thresholds trigger mitigation mechanisms. Drops are based on results of the mitigation checks. The figure below illustrates the packet flow through mitigation mechanisms during a UDP flood.

UDP mitigation process flow


Client
initial query
retransmitted query
drop
Antispoofing
UDP Retransmission
continue
drop
Legitimate Query (LQ) Table
continue
drop
TTL Table
continue
drop
Legitimate IP (LIP) Table
continue
serve from cache
Cache
Server
or if not found in cache,
send TC=1 response
if that option is set
if cache is not enabled
or if enabled but not
found in cache and
option set to forward

FortiDDoS DNS flood types

The following table summarizes the types of DNS floods mitigated by FortiDDoS.

DNS Flood types

DNS Flood Type	Thresholds
Query Flood	Abnormal rate of DNS queries or occurrences of query data. Spikes in DNS queries and fragmented queries are obvious symptoms of an attempt to take down the DNS server. Changes in norms for query data, such as question type and question count, are also symptoms of exploit attempts. Detected by the dns-query, dns-fragment, dns-question-count, dns-mx -count, dns-all-count, and dns-zone-xfer-count thresholds. The Monitor > Layer 7 graphs include packet rate graphs for each key threshold, and the Layer 7 drops graphs show which thresholds were at a flood state when the packets were dropped.
Per Source Flood	Rate limit for DNS queries from a single source. Detected by the dns-query-per-source threshold. The system applies the blocking period for identified sources. The Monitor > Layer 7 graphs include a Query Per Source graph.
Suspicious Sources	Heuristics to track other abnormal activity from a single source. Detected by the dns-packet-track-per-src threshold. This counter is incremented when a query is not found in the DQRM, when there are fragmented packets in the query or response, and when the response has an RCODE other than 0. The system applies the blocking period for identified sources. The Monitor > Layer 7 graphs include a Suspicious Sources graph.

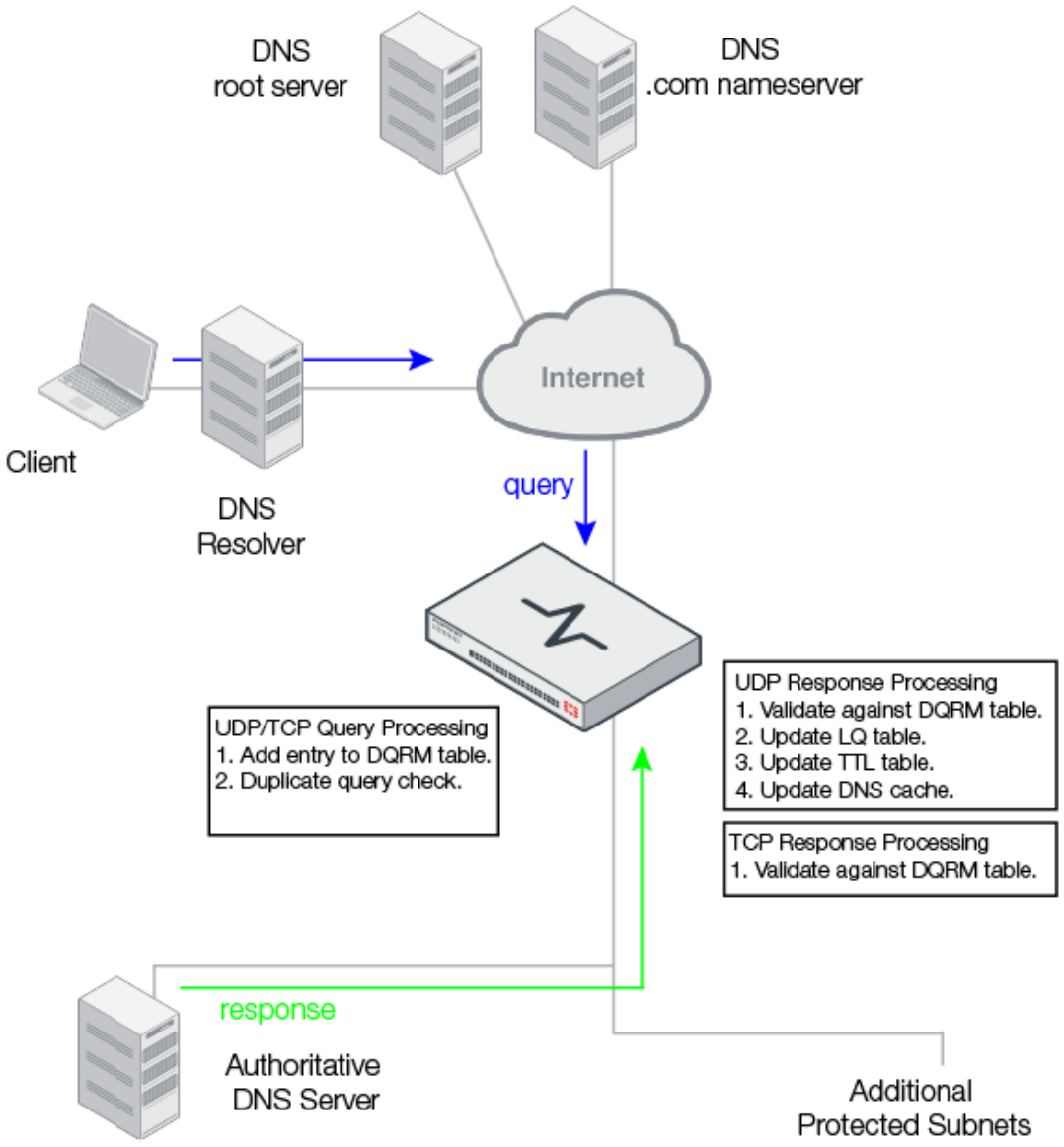
FortiDDoS DNS deployment topologies

FortiDDoS can be deployed to protect:

- Authoritative DNS servers that receive queries from the Internet.
- DNS recursive resolvers that send queries to and receive responses from Internet DNS authorities.

The following figure shows a topology where FortiDDoS is deployed primarily to protect the authoritative DNS server for a domain. Under normal traffic rates, FortiDDoS builds a baseline of DNS traffic statistics and stores DNS query and response data in tables. The tables are used to validate response traffic.

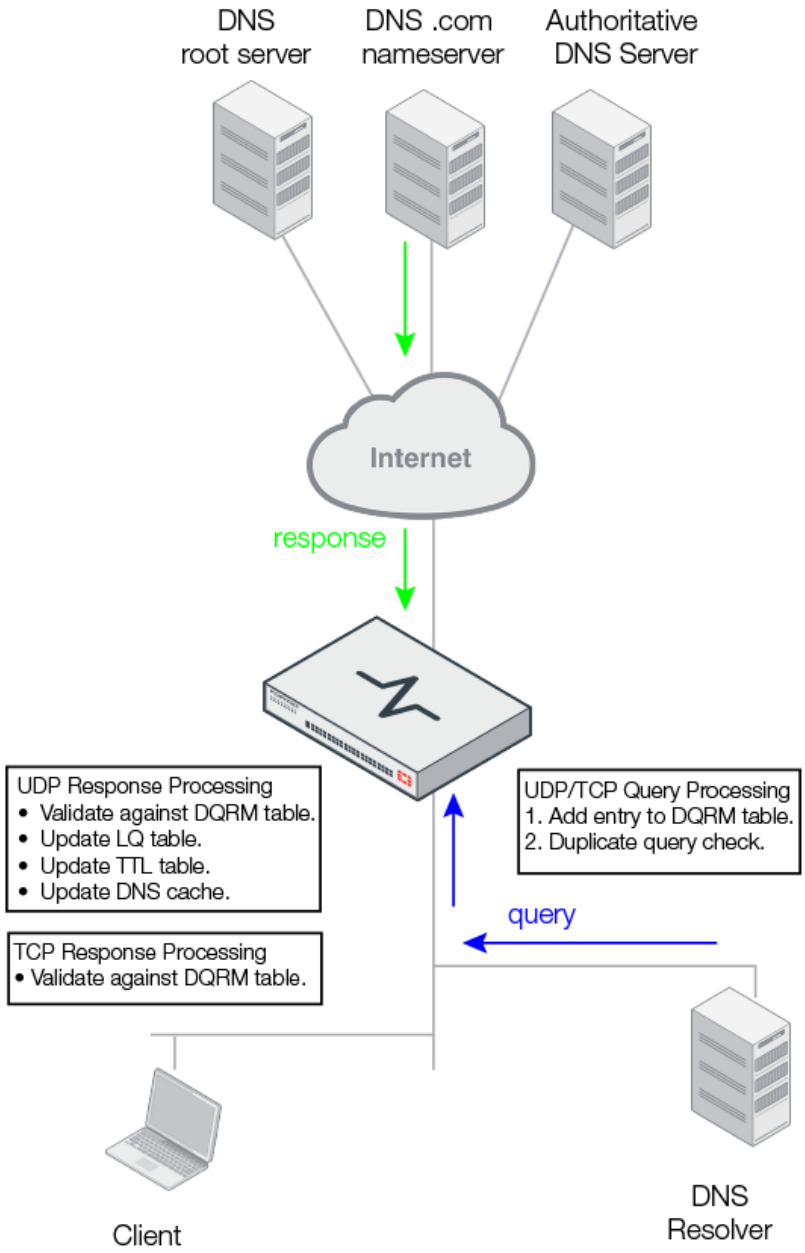
DNS no flood: inbound queries



	Query	Response
UDP	• Adds an entry to the DQRM table. • Performs a duplicate query check to prevent unnecessary queries to the server.	• Validates the response against the DQRM table. If there is an entry, the traffic is forwarded; otherwise, it is dropped. • Updates the LQ table, the TTL table, and the DNS cache.
TCP	• Adds an entry to the DQRM table. • Performs a duplicate query check to prevent unnecessary queries to the server.	Validates the response against the DQRM table. If there is an entry, the traffic is forwarded; otherwise, it is dropped.

The following figure shows a topology where FortiDDoS is deployed in front of an internal DNS resolver that sends queries to and receives responses from the Internet. This type of deployment is useful for open resolvers where the DNS resolver is protected primarily from Internet-originating inbound reflection attacks.

DNS no flood: inbound response traffic

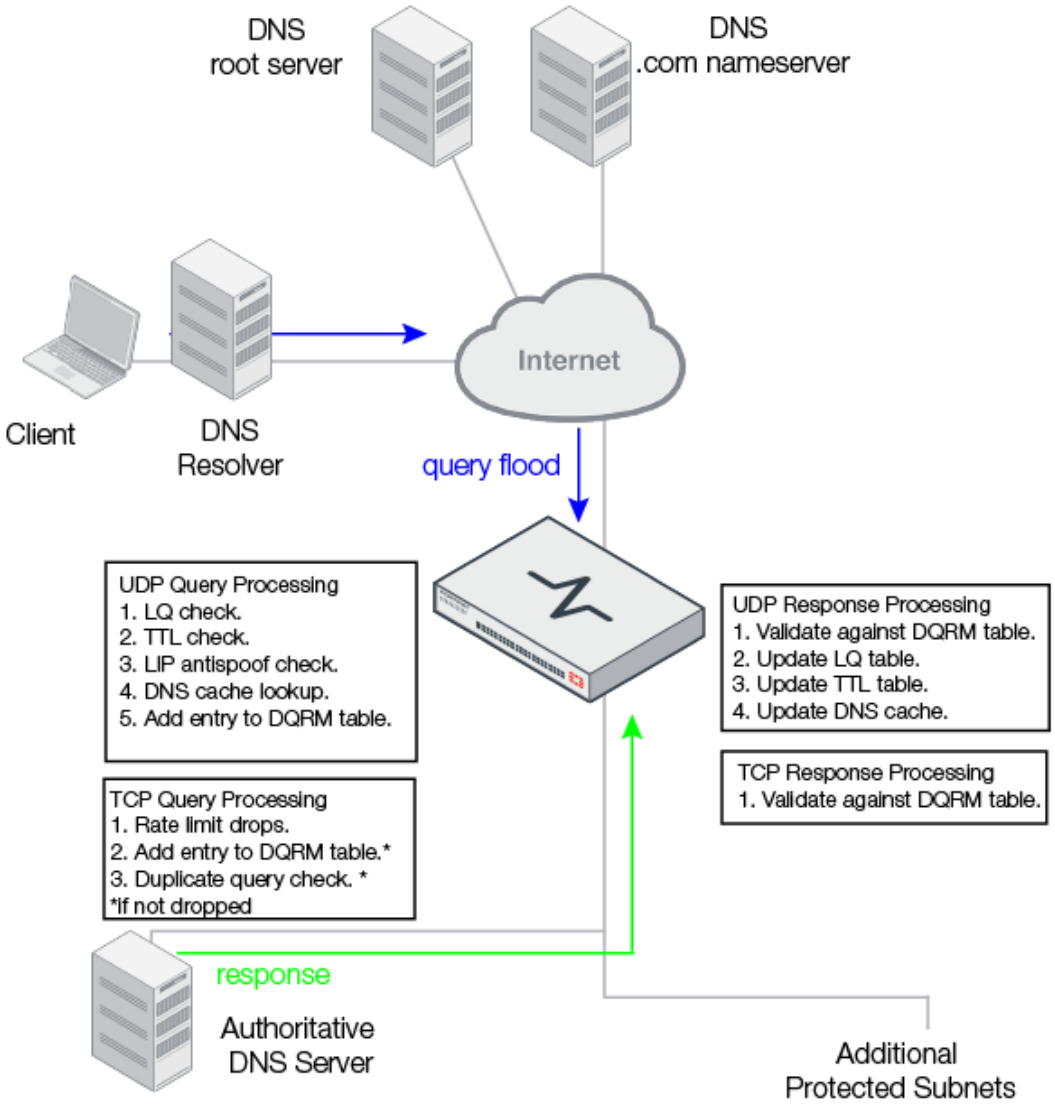


FortiDDoS collects data and validates the inbound responses and outbound requests the same as when queries are inbound. This deployment protects your network against different threats, such as DNS amplification attacks that result in unsolicited DNS response floods to targeted victims and DNS cache poisoning attacks, in which attackers send responses with malicious records to DNS recursive resolvers. In a deployment like this, the unsolicited responses would fail the DQRM check and be dropped.

DNS query flood mitigation

The following shows how FortiDDoS mitigates a DNS query flood. It uses the DNS tables and LIP table to validate queries and responses.

DNS Query Flood



	Query	Response
UDP	1. Validates against the LQ table. Under flood conditions, a query must have an entry in the LQ table or it is dropped. 2. Validates against the TTL table. If a match	• Validates the response against the DQRM table. If there is an entry, the traffic is forwarded; otherwise, it is dropped.

	Query	Response
	is found, the TTL check fails and the packets are dropped. It is not expected that a client would send the same query before the TTL expires. 3. Perform a lookup in the LIP table. If an entry exists, processing continues; otherwise, FortiDDoS drops the packets and tests the legitimacy of the source IP address. You can configure FortiDDoS to do so by performing a UDP retransmission challenge or by sending the requestor a response with the TC flag set. The TC flag indicates to the client to retry the request over TCP. 4. Performs a lookup in the DNS cache. If found, the response to the query is sent from the cache and the query is not forwarded to the protected server. If not found, you can configure whether to forward the query to the server or to send a TC=1 response to force the client to retry using TCP. 5. Adds an entry to the DQRM table.	• Updates the LQ table, the TTL table, and the DNS cache.
TCP	• Drops packets according to thresholds. • Adds an entry to the DQRM table. • Performs a duplicate query check to avoid unnecessary queries to the server.	Validates the response against the DQRM table. If there is an entry, the traffic is forwarded; otherwise, it is dropped.

Getting started with DNS mitigation

We recommend you allocate an SPP exclusively for DNS traffic. It takes a week to establish a baseline of traffic statistics for the SPP.

Steps

1. Go to *Service Protection* > *Service Protection Policy* and create an SPP rule exclusively for DNS traffic.
2. Go to *Service Protection* > *Service Protection Policy*> *{SPP Rule}* > *Service Protection Policy*. Ensure the SPP is in Detection mode.
3. Navigate to *Service Protection* > *DNS Profile* and create a DNS Profile that links the SPP Rule created in step 1.
4. Set *DNS Feature Controls* > *DNS Fragment to Enable* to apply Fragment ACLs (If required/Optional)
5. Add DNS Resource Record Type ACL to same DNS Profile (if required/Optional)
6. We recommend that you enable all anomaly checks under the section DNS Anomaly Feature controls and disable only if you encounter false positives (not expected)

7. We recommend you enable all features under DNS Feature Controls section and leave disabled only features that are not suitable for your deployment.
8. Navigate to *Traffic Monitor* > *Layer 7* > *DNS* and observe the accumulation of traffic statistics for the SPP's DNS counters. After you have established a baseline (a week's worth of traffic), continue on to the next steps to prepare for and switch to prevention mode.
9. Configure thresholds in the following way:
   a. Go to *Service Protection* > *Service Protection Policy* > *Threshold Settings* > *System Recommendation* and generate baseline statistics.
   b. On the same *System Recommendation* page, generate thresholds.
   c. Go to *Service Protection* > *Service Protection Policy* > *Thresholds,* and review the configurations. Make any manual changes if necessary.
10. Create TCP Profile and Enable *TCP Session Feature controls* > *Foreign packet validation*. This feature is useful when there is DNS traffic over TCP and FortiDDoS drops connections due to rate limits. When this setting is enabled, subsequent packets from the same connection are dropped.
11. Navigate to *Service Protection* > *Service Protection Policy* > *{SPP rule}*> *Service Protection Policy*, set Operating mode to *Prevention*.

Using FortiDDoS SPPs

Service Protection Profile (SPP) Rules are used to enable a single FortiDDoS appliance to protect multiple network zones with thresholds appropriate for the traffic in each of those zones.

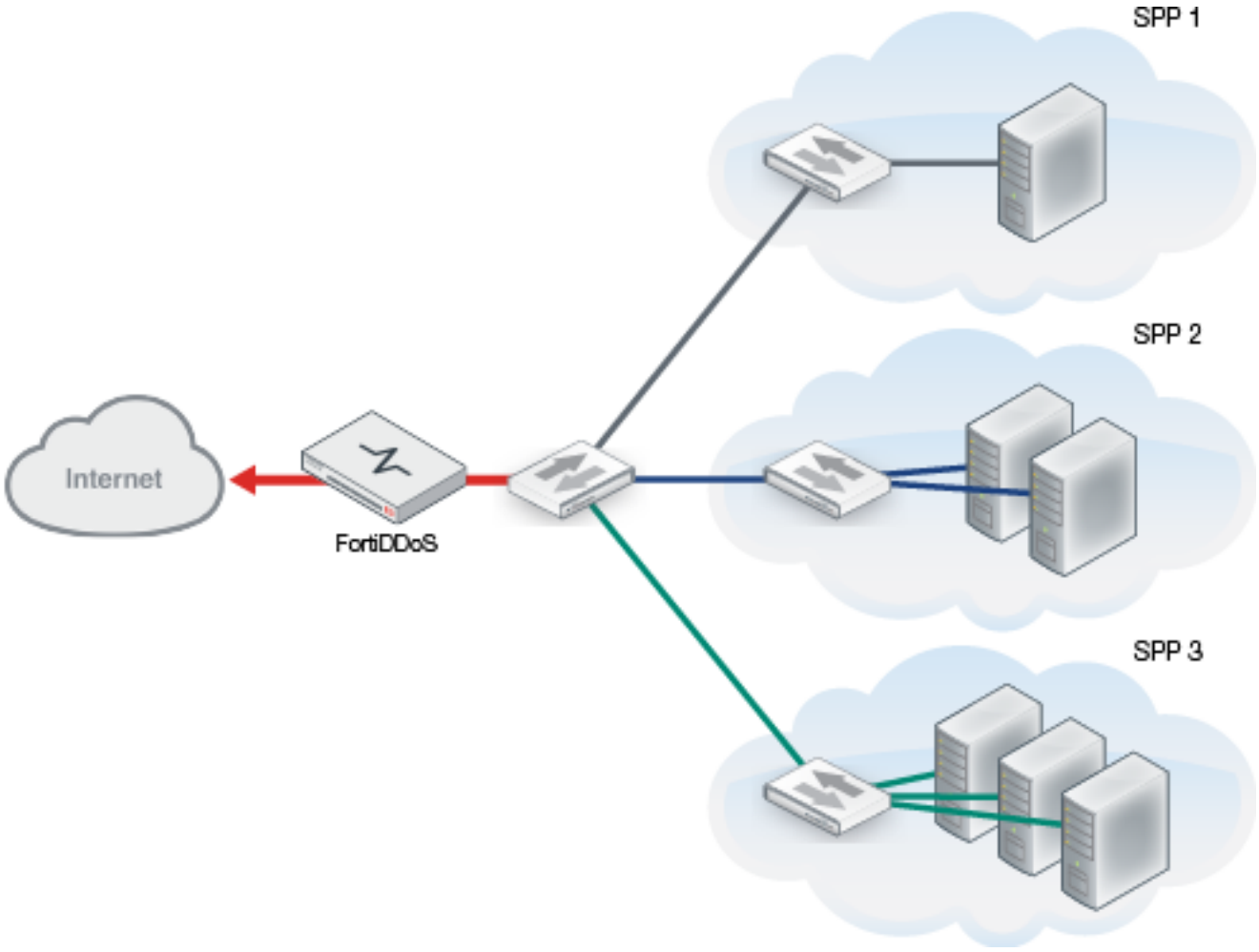
One SPP (default) is designated as the default SPP. You allocate the remaining SPPs to subnets.

In an enterprise deployment, you can configure SPPs for specific departments, geographic locations, or functions within an organization.

In a multi-tenant deployment, you can use SPPs to separate a single physical FortiDDoS device into multiple logical devices. Each SPP has its own configuration and traffic database. The configuration of each SPP can be under the control of a different administrator.

The following figure shows how multiple SPPs are used to protect multiple subnets.

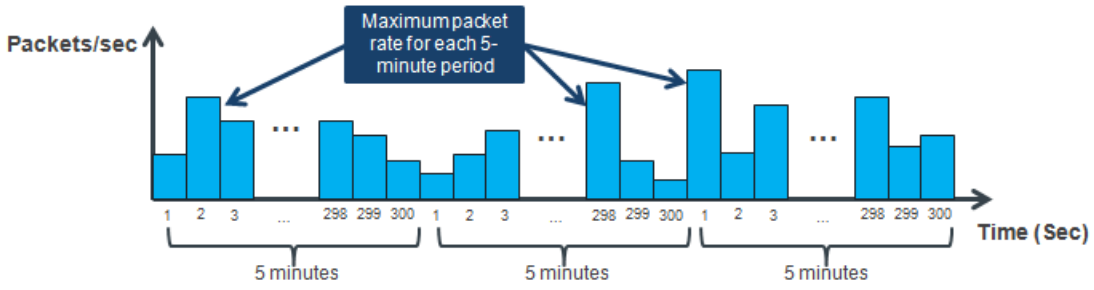
Multiple SPPs, multiple subnets



Working with the FortiDDoS Monitor graphs

The FortiDDoS system records data points for monitored thresholds every five minutes. The data point is the highest rate observed in any one second during the five-minute window.

Maximum values recorded



The FortiDDoS graphs are plots of data points. The reporting framework uses resolution periods to fit data points in time-based graphs. In a graph with a five-minute resolution period, the graph is based on a plot of the rates or counts recorded for the regular five minute window. In a graph with a one hour resolution period, the graph is based on a plot of the rates or counts for the highest rate among the points recorded in a one-hour window—in other words, the highest rate among the twelve five-minute windows reported in the hour.

The following table lists resolution periods used for report periods.

Data resolution periods

Graph Period	Resolution Period
1 hour	5 minutes
8 hours	5 minutes
1 day	5 minutes
1 week	1 hour
1 month	3 hours
1 year	45 hours

Note: The data displayed in a graph is current as of the time the last data point was written. For example, a 1-hour graph with a 5-minute resolution is current as of the time the last 5-minute resolution data point was stored. Traffic in the most recent 0-5 minutes might not have been registered yet. Similarly, for a 1-year graph with a data resolution of 45 hours, data for the last 0-45 hours might not have been registered yet.

Working with the FortiDDoS attack log

The monitoring and reporting framework is designed to maximize the processing resources that are available for preventing attacks, rather than forensics. In order to conserve resources to withstand multi-gigabyte attacks, the system records only data that it can use to improve security, not all possible Layer 3, Layer 4, and Layer 7 data. As a result, reporting tools such as the DDoS attack log do not always include detailed traffic parameter information. Outside of specific scenarios, the system does not report source and destination IP addresses and ports, protocols, and so on, for every dropped or blocked packet.

It is not uncommon for a FortiDDoS-F system that is monitoring a 1 Gbps traffic flow to be the target of a 700 Mbps SYN flood for 8 hours. If the system stored every source and destination IP address, port, and protocol, the logging demands (via hard disk, syslog, or SNMP trap) would soon overwhelm the disk or network.

By concentrating its resources on dropping attack traffic and maintaining service, FortiDDoS-F allows you to focus your attention elsewhere and still provide you with helpful and relevant information when an attack is underway.

A typical workflow for investigating FortiDDoS attack events

Whenever there is an attack, you should investigate until you fully understand why packets were dropped, and you know whether the attack event is a false positive.

A typical FortiDDoS attack investigation includes the following steps:

1. Identify the destination and source.
2. Identify the type of attack.
3. Identify the attack size.
4. Analyze Layer 3, Layer 4, and Layer 7 parameters to understand the attack method.

Step 1: Identifying the destination and source

Most of the statistics graphs identify the SPP and the direction of the attack, so, if there is only one subnet in the attacked SPP, you can easily determine the attack destination.

If the SPP contains more than one subnet, you can use the following reports to determine the attack destinations and sources:

- *Top Attacks* dashboard
- *Log & Report* > *Log Access* > *Logs* > *DDoS Attack Log*

Note: DDoS attacks are often spoofed attacks. Source information is not provided as it is irrelevant.

Step 2: Identifying the type of attack

If the SPP contains more than one subnet, you can use the following reports to determine the attack type:

• *Top Attacks* dashboard

• *Dashboard* > *Status* > *Attack Logs*

• *FortiView* > *SPP* > *{SPP Rule}* > *Attacks* tab

• *Log & Report* > *Log Access* > *Logs* > *DDoS Attack Log*

The following table describes DDoS attack types and identifies the FortiDDoS events to look for.

Types of attacks

Attack	Description	Threshold to configure/adjust	Events to watch
SYN Attack	A spike in packets on a specific TCP port. In most cases, the source address is spoofed.	Layer 3 - TCP protocol (6) Layer 4 - TCP ports on which the server is listening Layer 4 - SYN Layer 4 - New connections	Protocol 6 Flood SYN Flood Zombie Flood TCP Port Flood
Source Flood	A single source sends excessive number of IP Packets	Layer 3 – Most Active Source	Source Flood
Zombie Attack	A spike in TCP packets from Legitimate IP addresses	Layer 3 – TCP protocol (6) Layer 4 – TCP ports on which the server is listening Layer 4 – SYN	Layer 3 Protocol 6 SYN Flood Zombie Flood

Attack	Description	Threshold to configure/adjust	Events to watch
		Layer 4 - SYN per source (syn-per-src) Layer 4 - New connections	Port Flood SYN Flood from Source
Fragment Flood	Excessive number of fragmented packets	Layer 3 – Other Protocols Fragment Layer3 – TCP Fragment Layer 3 – UDP Fragment	Other Protocols Fragment Flood TCP Fragment Flood UDP Fragment Flood Protocol Flood
ICMP Flood	An Excessive number of ICMP Packets	Layer 3 – ICMP protocol (1) Layer 4 – ICMP type and code	Protocol 1 Flood Layer 4 ICMP Flood of a specific type and code
Smurf Attack	Traffic that appears to originate from the target server's own IP address or somewhere on its network. Targeted correctly, it can flood the network with pings and multiple responses.	Layer 3 – ICMP protocol (1) Layer 4 – ICMP type and code combinations that are allowed by the firewall and ACL	Protocol 1 Flood ICMP Flood of Echo-Request/Response Type (Type= 0, Code = 0)
MyDoom Attack	Excessive number of HTTP packets zombies	Layer 3 – TCP protocol (6) Layer 4 – TCP port 80 Layer 4 – SYN Layer 4 – New connections	Protocol 6 Flood SYN Flood Zombie Flood TCP Port Flood
HTTP GET Attack	Excessive number of HTTP GET Method packets	Layer 3 – TCP protocol (6) Layer 4 – TCP ports on which the server is listening Layer 4 – SYN Layer 4 – New connections Layer 4 – Concurrent connections per source Layer 7 – HTTP Methods Layer 7 – URL	Protocol 6 Flood SYN Flood TCP Zombie Flood TCP Port Flood Concurrent Connections per Source Flood HTTP Method Flood URL Flood
Slow Connection Attack	Legitimate IP sources send legitimate TCP connections but do it slowly and remain idle, which fills up the server's connection table memory.	Layer 3 – TCP protocol (6) Layer 4 – TCP ports on which the server is listening Layer 4 – SYN Layer 4 – New connections Layer 4 - Concurrent connections per source	Protocol 6 Flood SYN Flood Zombie Flood TCP Port Flood Concurrent Connections per Source

Attack	Description	Threshold to configure/adjust	Events to watch
UDP Flood Attack	An excessive number of UDP packets.	Layer 3 – UDP protocol (17) Layer 4 – UDP ports on which the server is listening	Protocol 17 Flood UDP Port Flood
Slammer Attack	An excessive number of packets on UDP port 1434	Layer 3 – UDP protocol (17) Layer 4 – UDP ports 1434	Protocol 17 Flood UDP Port 1434 Flood
Fraggle Attack	Spoofed UDP packets to a list of broadcast addresses. Usually the packets are directed to port 7 on the target machines, which is the echo port. Other times, it is directed to the CHARGEN port. Sometimes a hacker is able to set up a loop between the echo and CHARGEN port.	Layer 3 – ICMP protocol (1) Layer 3 – UDP protocol (17) Layer 4 – UDP echo port (7) Layer 4 – Daytime Protocol port (13) Layer 4 – Quote of the Day (QOTD) port (17) Layer 4 – UDP Character Generator protocol (CHARGEN) (19) Layer 4 – ICMP Type/Codes specific to host/port not available	Protocol 1 Flood Protocol 17 Flood UDP Port 7 Flood UDP Port 13 Flood UDP Port 17 Flood UDP Port 19 Flood ICMP Flood of Port Not Available Type, Code (3,3) ICMP Flood of Host Not Available Type, Code (3,1)
DNS Port Flood	An excessive number of packets on UDP port 53	Layer 3 - UDP protocol (17) Layer 4 - UDP port 53	Protocol 17 UDP Flood UDP Port 53 Flood
DNS Query Flood	A spike in DNS queries and occurrences of query data.	Layer 7 - DNS query-related thresholds	DNS Query Flood

Step 3: Identify the attack size

You can use the Monitor graphs and Attack Logs to analyze the dimensions of the attack: increases in throughput and drops.

Step 4: Analyze attack parameters in each OSI layer

You can use the DDoS Attack log or the Monitor graphs to analyze aggregate throughput and drops due to Layer 3, Layer 4, and Layer 7 FortiDDoS rate thresholds or ACL rules.

1. For Drop Monitor Graphs, start using the following graphs to identify the layer at which the attack is happening:
   - Aggregate Flood Drops
   - Aggregate ACL Drops
   - Aggregate Anomaly Drops
   - Out of Memory Drops
2. Drill down further by accessing statistics specific to each layer and attack type.

Getting Started

This section provides the basic work-flow for getting started with a new deployment.

Basic steps:

1. Install the appliance.
2. Configure the management interface.
3. Configure the following basic network settings:
   - Administrator password
   - System date and time
   - Network interfaces
   - DNS
4. Test connectivity.
5. Complete product registration, install your license, and update the firmware.
6. Deploy the system in Detection Mode for 2-7 days.
7. Generate traffic statistics, review them, and set SPP thresholds to the system recommended values.
8. Continue to monitor throughput rates and attacks, and adjust thresholds as needed.
9. Deploy the system in Prevention Mode.
10. Back up this basic configuration so that you have a restore point.

Tips:

- Configuration changes are applied to the running configuration as soon as you save them.
- Configuration objects are saved in a configuration management database. You cannot change the name of a configuration object after you have initially saved it.
- You cannot delete a configuration object that is referenced in another configuration object (for example, you cannot delete an address if it is used in a policy).

Note:
If you are using Internet access links from multiple service providers, and both links do not connect to the same FortiDDoS, BGP will likely create asymmetric traffic where FortiDDoS will only see a portion of TCP handshakes. See Understanding FortiDDoS Asymmetric Mode to configure your FortiDDoS correctly.

Step 1: Install the appliance

This Handbook assumes you have already installed the appliance into a hardware rack and used the appropriate cables to connect the traffic interfaces to your network.

Before continuing with “Getting Started”:

Please refer to the FortiDDoS Model Quick Start Guide BEFORE cabling traffic ports. Several startup operations result in system reboots and these should be done prior to putting the system inline with production traffic.

Summary:

Do NOT cable traffic ports.

Connect laptop to Console or Mgmt1 port and set up Administrator password. From Release 5.2.0, FortiDDoS will not allow a “null” password. You will be redirected from admin/null logon to create a new password. If the system is shipped from the factory with firmware release lower than 5.2.0, you are not required to replace the “null” password but when you upgrade below, you will be required to replace it when you next log in.

Upgrade system to latest GA Release. The upgrade result in a system reboot.

Set Time Zone and NTP (this is critical for system operation). Time Zone change and NTP change may cause a system reboot.

Once above is done, you can cable the traffic ports.

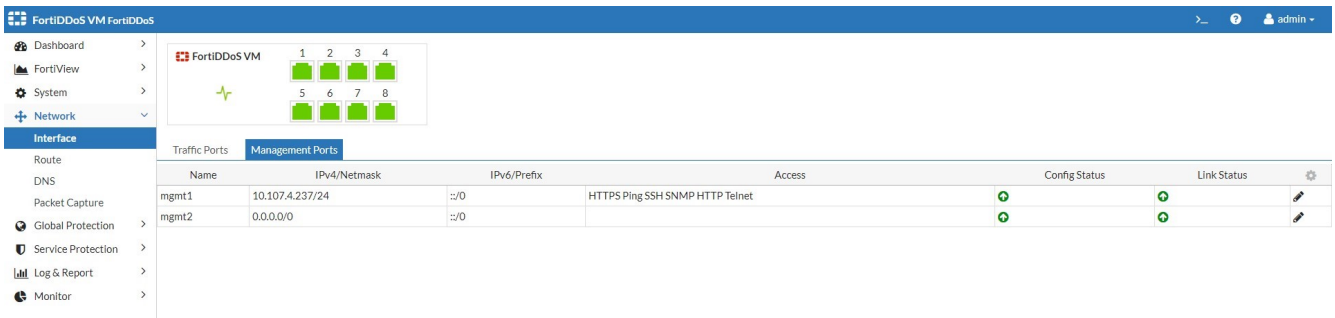
The FortiDDoS system is deployed inline (between the Internet and your local network resources). Consecutively numbered ports belong to port pairs: Use an odd port numbers (1, 3, 5, and so on) for the LAN-side connection and an even port number (2, 4, 6, and so on) for the WAN-side connection. For example, port1 and port2 are a pair. The port1 interface is connected to a switch that connects servers in the local network; the port2 interface is connected to the network path that receives traffic from the Internet.

For information about hardware appliances, refer to the FortiDDoS hardware manuals. For HA installations, refer to High Availability Deployments.

Step 2: Configure the management interface

You use the management port for remote administrator access from the web user interface (web UI) or command line interface (CLI).

Web UI



You configure the following basic settings to get started so that you can access the web UI from a remote location (like your desk):

- Static route—Specify the gateway router for the management subnet so you can access the web UI from a host on your subnet.
- IP address—Assign a static IP address for the management interface. The IP address is the host portion of the web UI URL. For example, the default IP address for the management interface is 192.168.1.99 and the default URL for the web UI is https://192.168.1.99.
- Access—Services for administrative access. We recommend HTTPS, SSH, SNMP, PING.

Before you begin the management interface configuration:

- You must know the IP address for the default gateway of the management subnet and the IP address you plan to assign the management interface.
- For your initial setup, you must have access to the machine room in which the physical appliance has been installed. You must connect a cable to the management port to get started.
- You need a laptop with an RJ-45 Ethernet network port, a crossover Ethernet cable, and a web browser (Microsoft Internet Explorer 8.0 or newer, or Mozilla Firefox 20 or newer). To minimize scrolling, the monitor resolution should be 1280 x 1024 or better.
- Configure the laptop Ethernet port with the static IP address 192.168.1.2 and a netmask of 255.255.255.0. These settings enable you to access the web UI as if from the same subnet as the FortiDDoS in its factory configuration state.
- Use the crossover cable to connect the laptop Ethernet port to the management port.

To connect to the web UI:

1. On your laptop, open the following URL in your web browser:
   https://192.168.1.99/
   The system presents a self-signed security certificate, which it presents to clients whenever they initiate an HTTPS connection to it.
2. Verify and accept the certificate, and acknowledge any warnings about self-signed certificates.
   The system displays the administrator login page.
3. Enter the username **admin** and password **fortinet**.

The system displays the dashboard.

Note: It is not recommended to use Internet Explorer version 9 and 10. If you login to FortiDDoS GUI on Internet Explorer 11 from Windows 10 system, perform the following actions on IE 11 browser settings:

1. Go to Settings > Internet options.
2. Click Settings under Browsing history.
3. Select 'Every time I visit the webpage' option under 'Check for newer versions of stored pages:'.

To configure a static route:

- Go to **System** > **Network** > **Static Route** and follow the instructions under Configuring static routes.

To configure the IP address and access services:

1. Go to **System** > **Network** > **Interface**.
2. Double-click the row for mgmt1 to display the configuration editor.

3. Use CIDR notation to specify the IP address/netmask, and enable services related to administrative access.
4. Save the configuration.

The system processes the update and disconnects your HTTP session because the interface has a new IP address and therefore the web UI has a new URL. At this point, you should be able to connect to the web UI from a host on the management subnet you just configured. You can go back to your desk to verify connectivity by attempting to open the web UI at the new address. You could see the status of configuration and link under Configured Status and Link Status column.

For more details, refer to Configuring network interfaces.

To complete the procedures in this section using the CLI:

1. Use an SSH client such as PuTTY to make an SSH connection to 192.168.1.99 (port 22).
2. Acknowledge any warnings and verify and accept the SSH key.
   The system displays the administrator login prompt.
3. Enter the username **admin** and no password.
4. Use the following command sequence to configure the static route:

```
config system default-gateway
edit 1
set gateway 172.30.153.254
end
```

5. Use the following command sequence to configure the management interface:

```
config system interface
 edit mgmt1
 set ip <address/mask>
 set allowaccess {https ping ssh snmp http telnet sql}
end
```

The system processes the update and disconnects your SSH session because the interface has a new IP address. At this point, you should be able to connect to the CLI from a host on the management subnet you just configured. You can go back to your desk to verify the configuration.

Step 3: Configure basic network settings

The system supports network settings for various environments. To get started, you configure the following basic settings:

- Administrator password—You must change the password for the **admin** account.
- Network interfaces—If necessary. The FortiDDoS appliance is deployed inline. In effect, it is a Layer 2 Bridge, so you do not configure IP addresses for its traffic interfaces. By default, the system is configured to autonegotiate speed/duplex. If desired, you can configure fixed speed/duplex settings.
- DNS—You must specify a primary and secondary server for system DNS lookups.
- System date and time—We recommend you use NTP to maintain the system time.

To change the admin password:

- Go to **System** > **Admin** > **Administrator** tab.
  For details, refer to Managing administrator users.

To configure network interfaces:

- Go to **Network** > **Interface**.
  For details, refer to Configuring network interfaces.

To configure DNS:

- Go to **Network** > **DNS**.
  For details, refer to Configuring DNS.

To configure system time:

- Go to **System** > **Maintenance** > **Time Zone** tab.
  For details, refer to Configuring system time.

To configure with CLI:

Configure management IP address

```
config system interface
   edit mgmt1
      set ip [IPv4 address/net mask]
      set allowaccess https ping ssh snmp http telnet
   next
end
```

Configure default gateway

```
config system default-gateway
   edit 1
      set gateway [gateway]
   next
end
```

Enable L2 Interface pair

```
config system l2-interface-pair
   edit l2-port1-port2
      set status enable
   next
end
```

Step 4: Test connectivity

Use ping and trace route to test connectivity to protected servers.

To test connectivity from the FortiDDoS system to the protected server:

- Run the following commands from the CLI:
  ```
  execute ping <destination_ip4>
  execute traceroute <destination_ipv4>
  ```

To test connectivity from the protected server to the FortiDDoS system:

1. Enable ping on the network interface.
2. Use the ping and trace route utilities available on the protected server to test connectivity to the FortiDDoS network interface IP address.

   For troubleshooting tips, refer to Troubleshooting.

Step 5: Complete product registration, licensing, and upgrades

Your new FortiDDoS-F appliance comes with a factory image of the operating system (firmware). However, if a new version has been released since factory imaging, you might want to install the newer firmware before continuing the system configuration.

Before you begin:

- Register—Registration is required to log into the Fortinet Technical Support site and download firmware upgrade files. For details, go to http://kb.fortinet.com/kb/documentLink.do?externalID=12071.
- Check the installed firmware version—Go to **Dashboard**.
- Check for upgrades—Major releases include new features, enhancements, and bug fixes. Patch releases can include enhancements and bug fixes. Download the release notes at http://docs.fortinet.com/fortiddos/. Download firmware upgrades at https://support.fortinet.com/.

To upgrade the firmware:

- Go to **System** > **Firmware**.
  For details, refer to Updating firmware.

Step 6: Define SPPs and subnets

Service Protection Policies (SPPs) and Protected Subnets are the heart of FortiDDoS protection. SPPs define or contain:

- Protected Subnets
  - Learned Traffic Statistics and Thresholds for over 230,000 parameters for the Protected Subnets
- Specific SPP mitigation features
- Seven Service Protection Profiles assigned to the SPP, each with additional SPP mitigation features for IP, TCP, ICMP, HTTP, SSL/TLS, NTP and DNS traffic
- SPP-specific ACLs
- SPP-specific Cloud Signaling for Cloud DDoS Service partners

SPPs can be individually toggled between Prevention (mitigation) Mode and Detection (monitor) Mode.

All graphing is done per SPP with logs showing SPP and Protected Subnet and Protected IP.

Protected Subnets from an IPv4/32 or IPv6/128 are defined in each SPP. FortiDDoS automatically subnets for you. You can assign a /24 subnet to the “Infrastructure” SPP with a /32 IP address from that /24 to the “Web” SPP and a second /32 to the “Firewall” SPP. FortiDDoS will monitor and learn traffic for each /32 (and SPP containing that /32) separately from the /24.

This Section will focus on creation of SPPs and Protected Subnets so that the system can begin learning traffic parameters as quickly as possible. Other than the configurations shown here, all other settings must remain default. For further configuration of additional SPP Settings and Thresholds please see Service Protection Policy Feature Settings on page 223.

Defining SPPs

For enterprise users, configure SPPs, at a minimum, to protect different services:

- Firewalls, email servers, WiFi gateways, outbound Proxies and other outbound connection originators (and outbound DNS Query originators)
- Web servers
- Authoritative DNS servers
- VPN Servers
- Full subnet(s) (for IP addresses not covered above)

Different types of services require different types of mitigations. Combining different services into a single SPP may result in “lowest-common-denominator” protection.

Conversely, if you have different types of web servers on different IP addresses, particularly if some servers allow client logins, separating the non-login and login servers in two different SPPs can be useful.

Balancing this is the effort to manage Thresholds on multiple SPPs. Initial setup will take longer with more SPPs and while ongoing SPP “maintenance” is minimal, the fewer the better.

For hosting and ISP users, end-user services may not be obvious or most users are residential or mobile. If users are homogeneous, spread the subnets across several SPPs. If there are clear differences like residential/commercial or residential/mobile you can create SPPs for those. In all cases, the “enterprise” services for the hosting provider or ISP should be defined like the enterprise section above.

FortiDDoS models provide differing numbers of SPPs:

Model	VM04	VM08	200F	VM16	1500F
SPPs	4	8	8	16	16

One SPP (default) is always present and cannot be renamed or deleted. The default SPP gathers traffic for subnets that are not defined in other SPPs. If needed, the default SPP can be used for explicit Protected Subnets. If using the default SPP, place the largest subnets you have in this SPP.

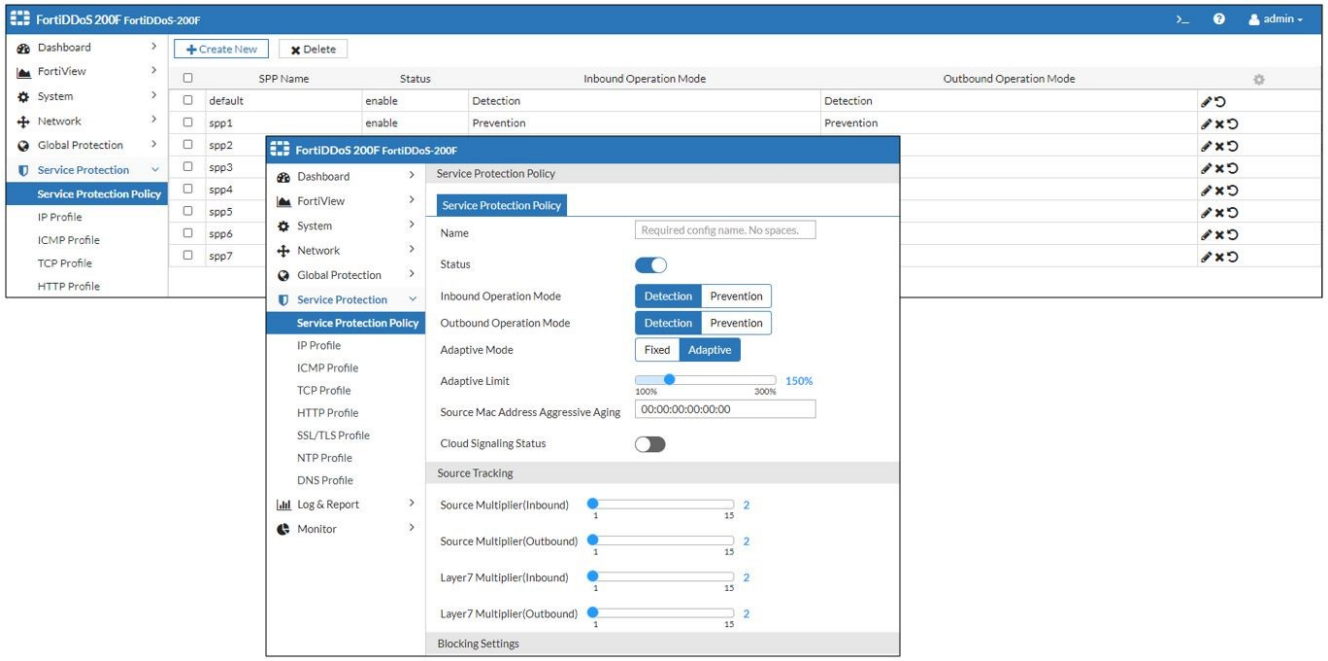
Before you begin:

- You must have a good understanding of the list of SPPs you need to deploy.
- You must have a good understanding of the features you want to enable.
- You must have Read-Write permission for Service Protection settings.

Caution: The name of the SPP cannot be modified once it has been created. Ensure that you are satisfied with the name before you do further SPP configuration. The only way to have a different SPP name is to delete the SPP and create a new one.

Note: Deleting an SPP removes a significant amount of graph and log data. Please see instructions to delete SPPs.

Creating a new Service Protection Policy



1. Go to *Service Protection* > *Service Protection Policy* and click *Create New*.
2. In the SPP configuration window, enter the SPP Name only and click *Save*.
3. Once saved, you can:
   a. Continue with creating additional SPPs
   b. Edit the created SPP and continue with further SPP configuration including Protection Profile Settings, Protection Subnets or ACLs.

Note: Configuring a new SPP requires system configuration of more than 230,0000 Round Robin Databases for that SPP. This can take several minutes, depending on the model but is a one-time action.

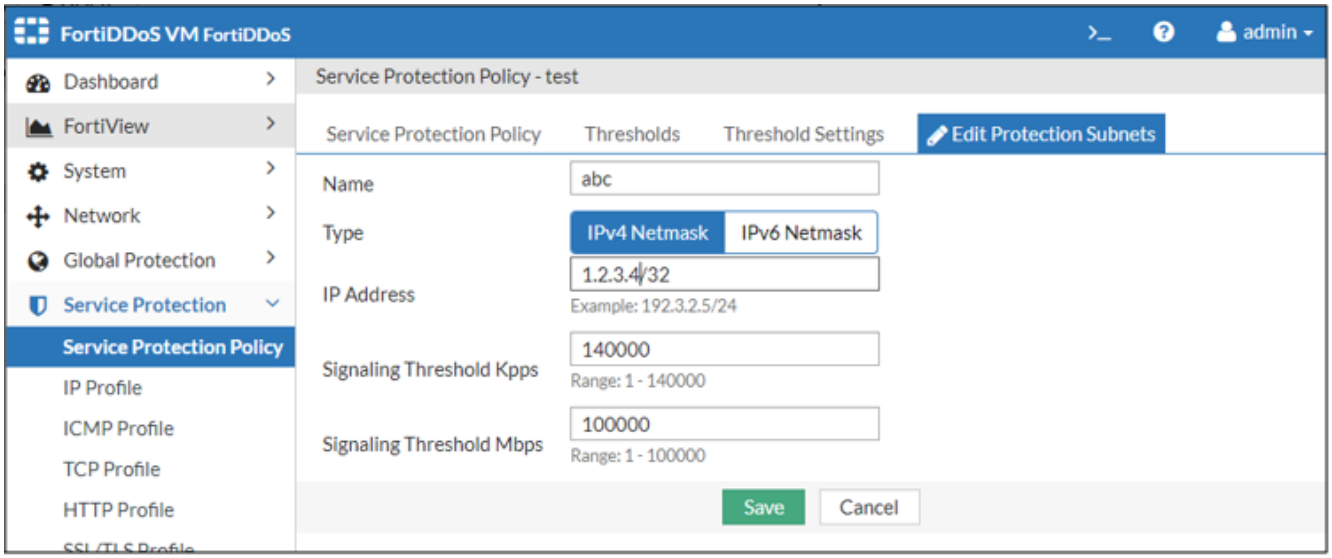
To configure using the CLI:

```
config ddos spp rule
   edit <spp_name>
   next
end
```

Configuring protected subnets

Before you begin:

- You must have a good understanding of the subnets you will be protecting
- You must have Read-Write permission for Service Protection settings.



Configure subnets (from IPv4 /24 or IPv6 /128) protected by an SPPs settings and threshold with the following steps:

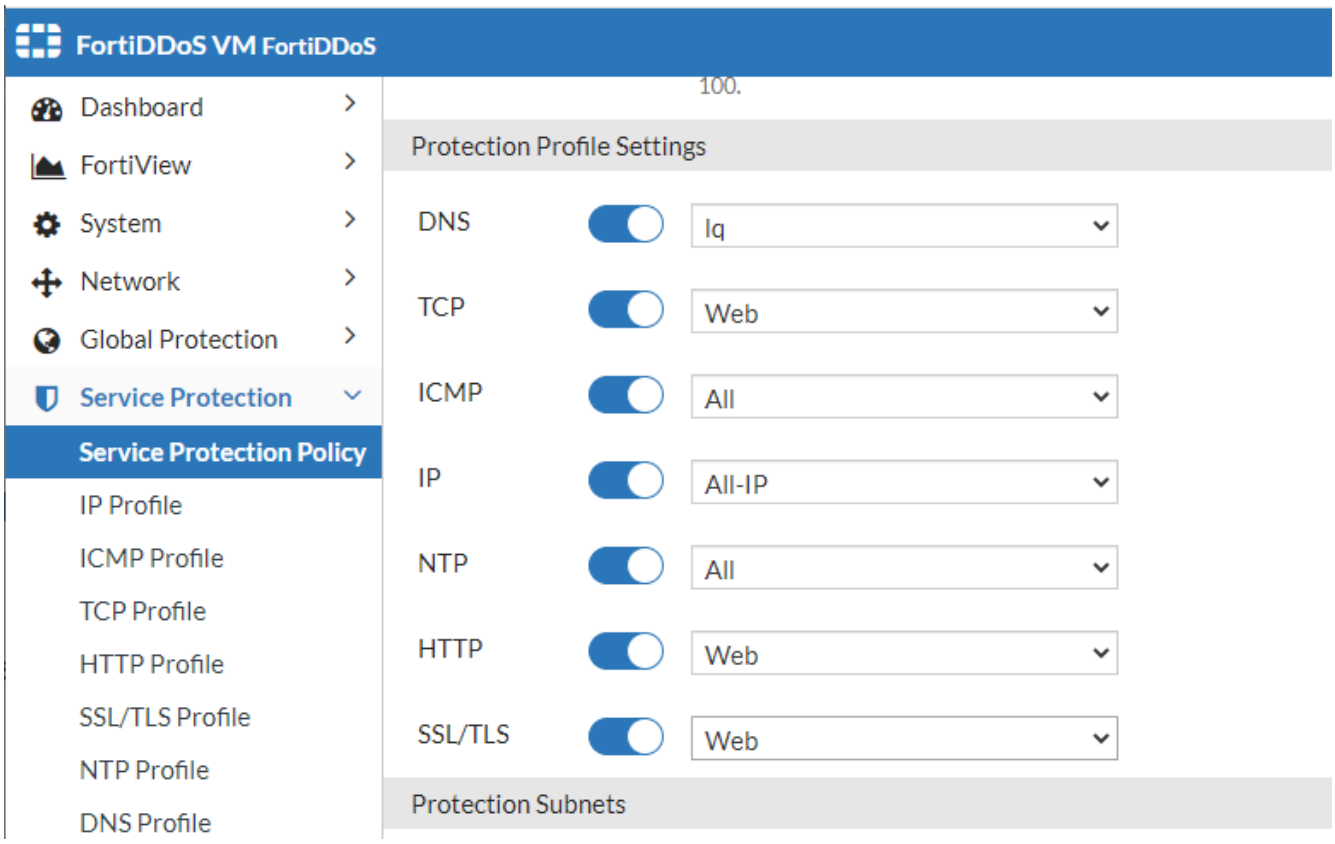
1. Go to *Service Protection* > *Service Protection Policy* and select the Service Protection Policy from the list.
2. Navigate to *Protection Subnets* and click *Create New*
3. Name of the Protected Subnet (Max length = 35 characters, a-Z, 0-9 and "-" or "_" only)
4. Enter the IP/netmask. **Note:** IPv4 and IPv6 subnets can be used in the same SPP
5. Leave all other fields as default and click *Save*
   Note: Once saved, you cannot edit the Name of the Protected Subnet. You must delete it and re-enter the Name and Subnet information.
6. Continue adding additional subnets until finished.
   When finished, clicking Cancel from the Service Protection Policy page will return you to the SPP List where you can edit additional SPPs to add more Protected Subnets

Applying Service Protection Profiles

Before you begin:

- You must have a good understanding of the protection requirements for each SPP.
- You must have Read-Write permission for Service Protection settings.

Note: While preferred, it is not critical that Service Protection Profiles be applied when defining SPPs and Protected Subnets. You can return to the SPP and add them at any time but they must be applied before the SPP is set to Prevention Mode since many mitigations will not be used unless the Profiles are assigned. This section will be repeated in Service Protection Policy Feature Settings on page 223.



There are 7 Service Protection Profiles that must be assigned to each SPP. In some cases one Profile can be used for all SPPs but in other cases each SPP will require a unique profile. Please see SPP Profiles Overview for details on SPP Profiles Overview on page 260.

SPP Profiles	Description
IP profile	Enables/disables ACLs for IP header anomalies, Private address space, multicast address space, fragments and IP Reputation. Normally a single Profile can be used for all SPPs
ICMP profile	Enables/disables ACLs for ICMP anomalies and can ACL all unused ICMP Type/Codes (only about 114 of the available 65k ICMP Types and Codes are ratified by IANA and IETF). Optionally, defines ACLs for specific Types/Codes or ranges of Types/Codes. Use with care. For example Type/Code 3:4 is requires for TCP PathMTU calculation. Most users can use a single Profile for all SPPs.
TCP profile	Enables/disables a significant number of TCP features and mitigations. This Profile is critical for SYN Flood mitigation. Most users can use a single Profile for all SPPs.
HTTP profile	Enables/disables specific HTTP protection features.
SSL/TLS profile	Enables/disables SSL/TLS anomaly and renegotiation protections. Important for HTTPS servers but can be used by all SPPs.
NTP profile	Enables/disables several NTP anomaly checks and 2 important NTP Reflection flood mitigations. Most users can use a single Profile for all SPPs.

SPP Profiles	Description
DNS profile	Enables/disables several DNS anomaly checks as well as several important DNS Flood attack features. Separate DNS Profiles are needed for Authoritative DNS servers; recursive DNS Servers; Firewalls, email servers and other users of outbound DNS Queries; web servers; and other infrastructure. DNS Reflection Floods are used against all infrastructure, not just DNS servers, so appropriate Profiles are required on all SPPs.

Step 7: Deploy the system in Detection Mode

You can initially deploy the system in Detection Mode. In Detection Mode, the system operates with high (factory default) thresholds and does not drop any packets.

The system needs about 2 to 7 days of attack-free learning in Detection Mode to learn typical traffic patterns so it can set the initial thresholds. The length of the initial learning period depends upon the seasonality of traffic (its predictable or expected variations) and how representative of normal traffic conditions the learning period is.

Weekends alone are an insufficient learning period for businesses that have substantially different traffic during the week. Thus, it is better to start the learning period on a weekday. In most cases, 7 days is sufficient to capture the weekly seasonality in traffic.

Basic steps

1. Go to *Service Protection* > *Service Protection Policy* and Add new SPP rules by clicking *Create New*.
2. Go to *Service Protection* > *Service Protection Policy* > *{SPP rule}* > *Protection Subnets* and configure subnets.
3. Go to *Service Protection* > *Service Protection Policy* > *{SPP rule}* > *Service Protection Policy* and ensure SPP rule is deployed in Detection Mode (factory default).

Step 8: Generate traffic statistics and set the configured minimum thresholds

At the end of the initial learning period, you can adopt system-recommended thresholds (usually lower than the factory default).

Basic steps

1. Go to *Service Protection* > *Service Protection Policy* > *{SPP rule}* > *Threshold Settings* > *System Recommendation* and generate statistics for the selected time period.
2. 2. Go to *Service Protection* > *Service Protection Policy* > *{SPP rule}* > *Threshold Settings* > *System Recommendation* and review the maximum packet rates generated for the SPP. The values represent the maximum packet rate observed during the selected period. For example, during each 1-hour period, there are 12, 5-minute observation periods. FortiDDoS captures a maximum rate for each 5-minute interval. The generated threshold is the highest maximum rate that was captured among the 12 observation periods.

3. Go to *Service Protection* > *Service Protection Policy* > *{SPP rule}* > *Threshold Settings* > *System Recommendation* and set the configured minimum thresholds to the system recommended settings.

For each OSI layer you can specify two settings:

- *Percentage*: The configured minimum threshold is the generated baseline rate multiplied by this percentage.
- *Low Traffic Threshold*: The system uses this value instead for the configured minimum threshold if it is higher.

Tip: When you are getting started, we recommend that you accept the defaults for the adjustment percentages and low traffic thresholds.

For details, refer to the following sections:

- Generating baseline traffic statistics
- Displaying baseline traffic statistics
- Modifying thresholds

Step 9: Monitor the system and become familiar with logs and reports

For your initial deployment, continue to use Detection Mode for a day or two during which you review logs for potential false positives and false negatives.

Basic steps

1. Go to *Traffic Monitor and Drop Monitor* and review throughput rates. Start with aggregate graphs and then use the more detailed graphs to drill in on patterns of interest or concern.
2. Go to *Log & Report* > *Log Access* > *Logs* > *DDoS Attack Log* and become familiar with the log table and how to use log filters.
3. Go to *Dashboard* > *Top Attacks* and become familiar with the Top Attack summary for all types of attack information.

For details, refer to the following sections:

- Monitor Graphs
- Using the DDoS Attack Log table
- Using the Executive Summary dashboard
- Using the Attack Graph dashboard

Step 10: Deploy the system in Prevention Mode

After you have set the statistical baseline and evaluated the configured minimum thresholds, you change to Prevention Mode. In Prevention Mode, the system uses the configured minimum threshold in its calculations that determine the estimated thresholds. The estimated thresholds are rate limits that are enforced by packet drops. The estimated thresholds are also the triggers for reporting flood attacks and entering SYN flood attack mitigation mode.

Repeat the tuning as needed: monitor observed throughput, estimated thresholds, and drops; adjust the configured minimum thresholds; monitor; adjust.

For details, refer to Service Protection Policy Overview and Modifying thresholds.

1. Go to *Service Protection* > *Service Protection Policy* > *{SPP rule}* > *Service Protection Policy* and change the configuration to Prevention Mode. Do this for each SPP.
2. Create TCP Profile under *Service Protection* > *TCP Profile*, enable the recommended TCP session state anomalies options.
3. Continue to monitor traffic.
4. Tune the configuration if necessary. Go to *Service Protection* > *Service Protection Policy* > *{SPP rule}* > *Thresholds* to set rates manually or *Service Protection* > *Service Protection Policy* > *{SPP rule}* > *System Recommendation* to adjust percentages applied at OSI layers or to adjust the low traffic threshold.

Step 11: Back up the configuration

Once you have tested your basic installation and verified that it functions correctly, create a backup. This “clean” backup is a reference point that has many benefits, including:

- Troubleshooting—You can use a tools such as a tool such as diff to compare a problematic configuration with this baseline configuration.
- Restarting—You can rapidly restore your system to a simple yet working point.
- Rapid deployment—You can use the configuration file as a template for other FortiDDoS systems to the extent it makes sense to do so. For example, you might use the same network infrastructure configuration (DNS, SNMP, log, syslog), the same general settings, and more or less the same ACL rules, but SPP settings and SPP thresholds are usually appropriate only to the subnet in which the system has been deployed. You can use any text editor to edit the plain text configuration file and import it into another FortiDDoS system. Be sure to change unique identifiers, such as the management IP address and sometimes other local network settings that differ from one deployment to another.

To back up the system configuration:

1. Go to **System** > **Maintenance** > **Backup & Restore** tab.
   For details, refer to Backing up and restoring the configuration of an appliance.

Dashboard

This section includes the following topics:

Status

FortiDDoS Dashboard contains tables or graph summary of system information or system status. You can use the dashboard to check system status at-a-glance or to quickly find system information, like the hardware serial number, firmware version, license status, or interface status. For a deeper look at attack traffic, use the Monitor and Log & Report menus.

Note: The SPP selection from the top-right corner of the UI updates only the Count of Unique Sources graph.

Before you begin:

- You must have Read-Write permission for Log & Report settings.

To display the Dashboard:

- Go to **Dashboard** tab.

The default dashboard setup includes the following tables/graphs:

- System Information on page 108
- License Information on page 108
- High Availability (HA) on page 109
- System Resources on page 109
- Administrators on page 110
- Drops on page 112
- Attack Logs on page 113
- Data Path Resources on page 113
- Cloud Signaling on page 114

For any graph, you can select either Linear or Logarithmic scale link from the top right corner. If there is a range of data where one or a few points are much larger than the bulk of the data, select Logarithmic scale to reduce the skewness towards large values. The graphs are displayed in linear scale by default.

System Information

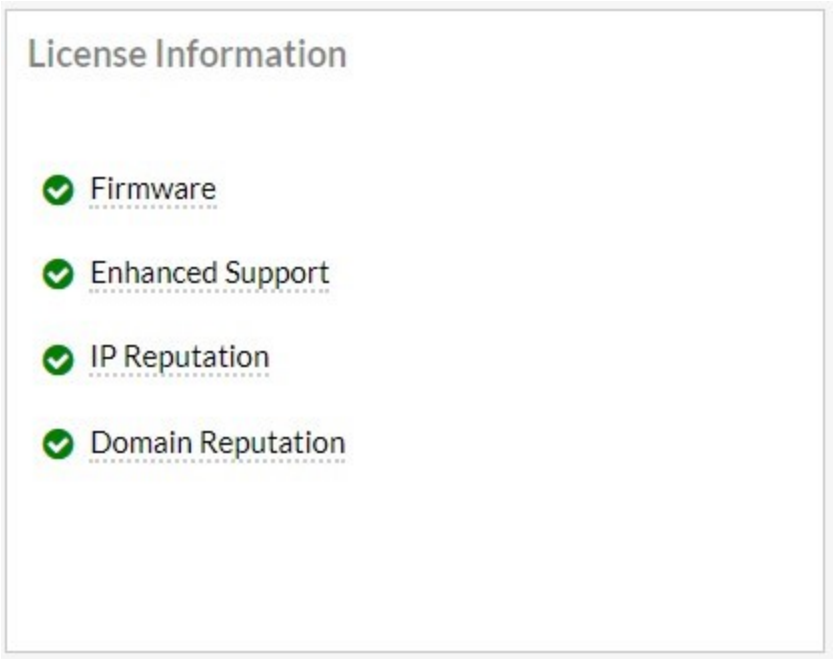
This dashboard displays the basic information, such as firmware version, serial number, host name, system time, system uptime, effective HA mode, user name and ASIC version.

System information dashboard

License Information

This dashboard displays license and registration status, including status for the FortiGuard IP Reputation and Domain Reputation Services. If the system is behind web proxy, set up Tunnel (proxy) under **System > FortiGuard**. These Tunnel settings work for system registration, IP Reputation, Domain Reputation and Signaling.

License Information dashboard



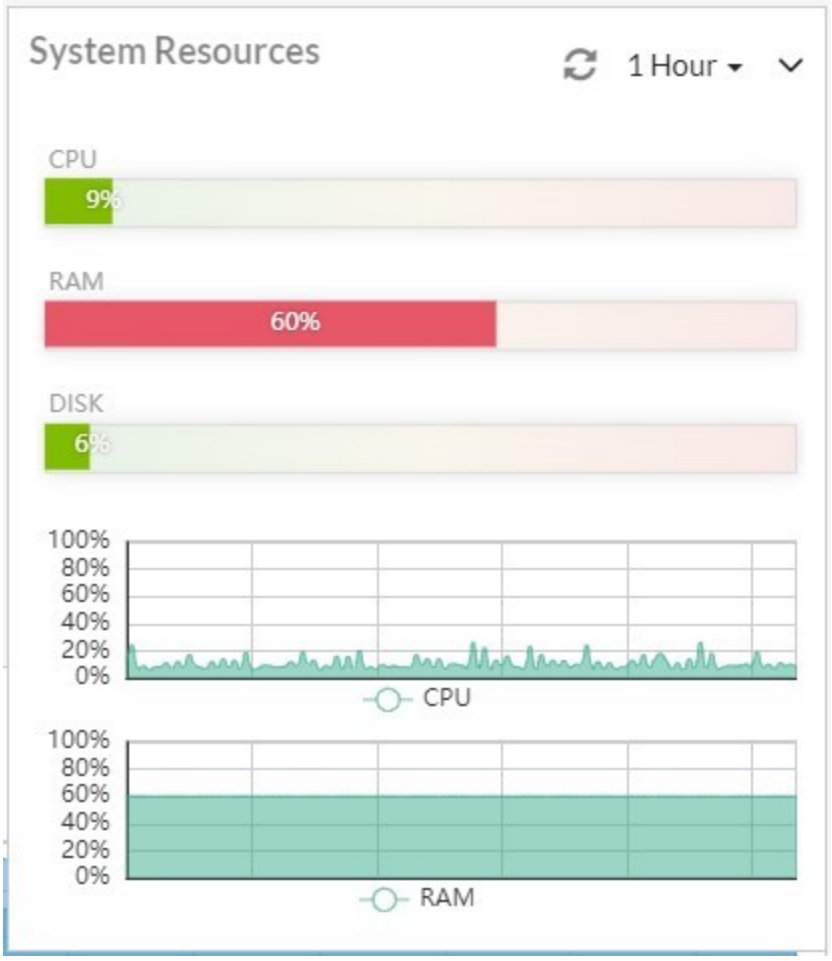
High Availability (HA)

High Availability (HA) configuration allows you to synchronize configuration information between two FortiDDoS appliances to create a secondary appliance that always has an up-to-date configuration.

Mode	Standalone/HA configuration
eMode	on/off
Group	group of appliances configured in HA mode
Override	Enable/disable

System Resources

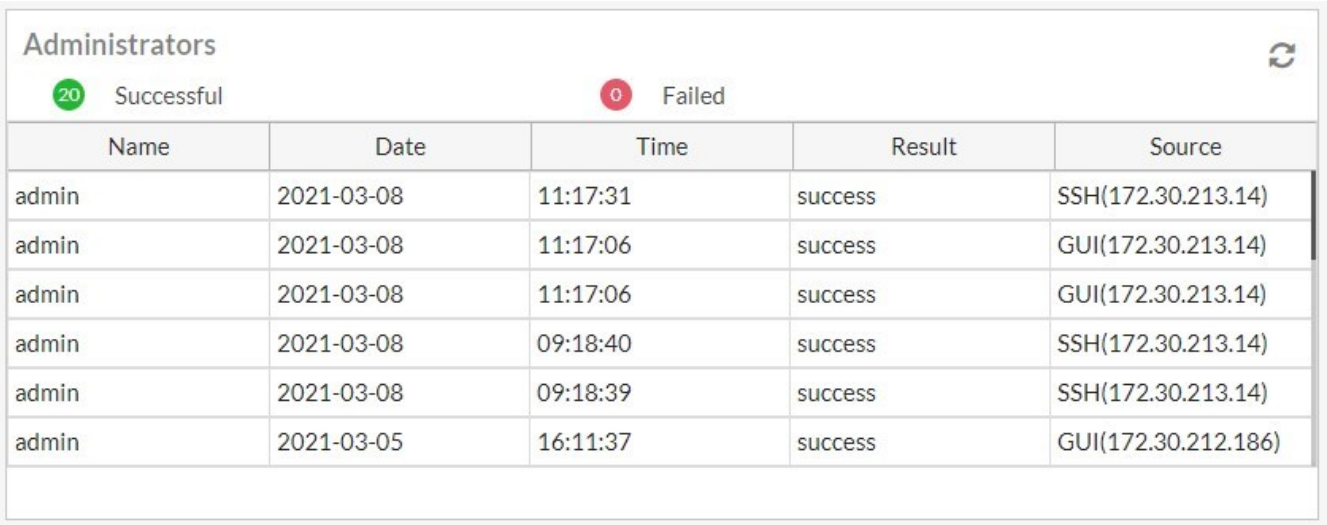
System Resources gauges display CPU, RAM, and disk usage for all processes.



Administrators

The Recent Event Logs help you to track system events, such as administrator logins and firmware changes.

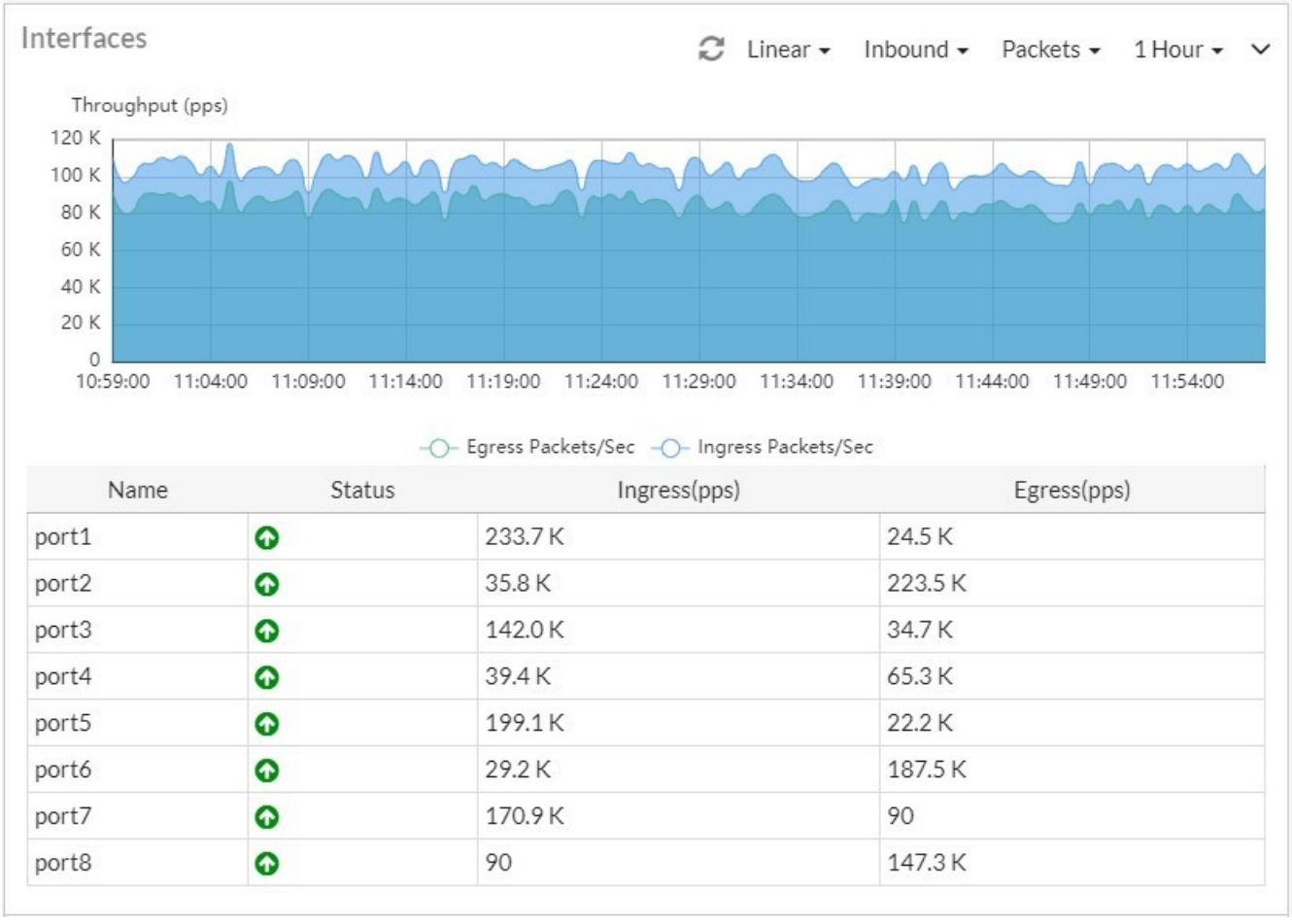
Recent event logs dashboard



Name	Date	Time	Result	Source
admin	2021-03-08	11:17:31	success	SSH(172.30.213.14)
admin	2021-03-08	11:17:06	success	GUI(172.30.213.14)
admin	2021-03-08	11:17:06	success	GUI(172.30.213.14)
admin	2021-03-08	09:18:40	success	SSH(172.30.213.14)
admin	2021-03-08	09:18:39	success	SSH(172.30.213.14)
admin	2021-03-05	16:11:37	success	GUI(172.30.212.186)

Interfaces

The Interfaces dashboard displays traffic through all interfaces ports for both Ingress and Egress directions.



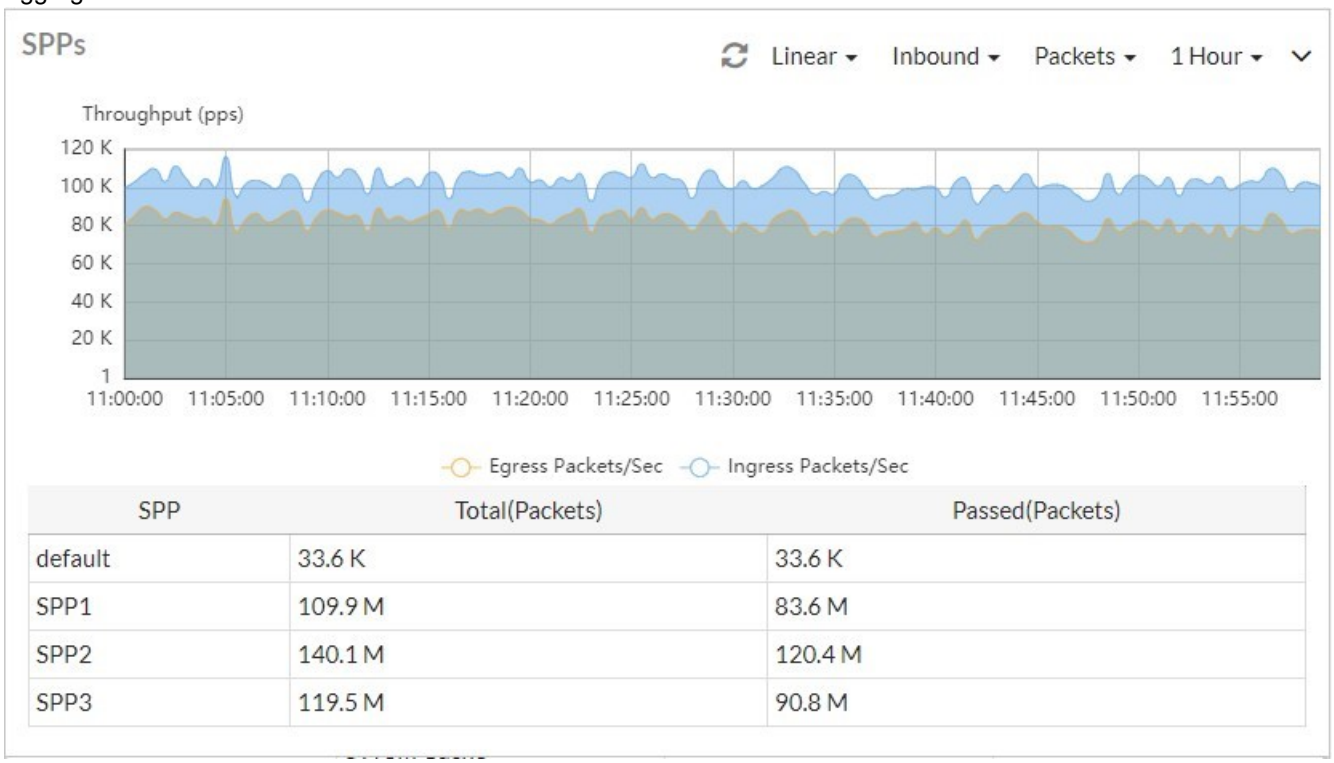
Name	Status	Ingress(pps)	Egress(pps)
port1	↑	233.7 K	24.5 K
port2	↑	35.8 K	223.5 K
port3	↑	142.0 K	34.7 K
port4	↑	39.4 K	65.3 K
port5	↑	199.1 K	22.2 K
port6	↑	29.2 K	187.5 K
port7	↑	170.9 K	90
port8	↑	90	147.3 K

SPP Traffic (SPPs)

This dashboard displays the trend in aggregate throughput over a specific period of time across all SPPs. This graph provides an overview of the traffic pattern.

To display inbound or outbound traffic, select **Inbound** / **Outbound** links on the top-right of the graph.

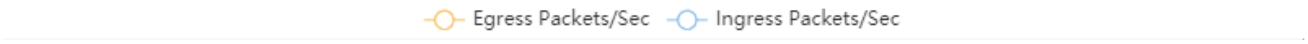
Aggregate SPP Traffic dashboard



SPP	Total(Packets)	Passed(Packets)
default	33.6 K	33.6 K
SPP1	109.9 M	83.6 M
SPP2	140.1 M	120.4 M
SPP3	119.5 M	90.8 M

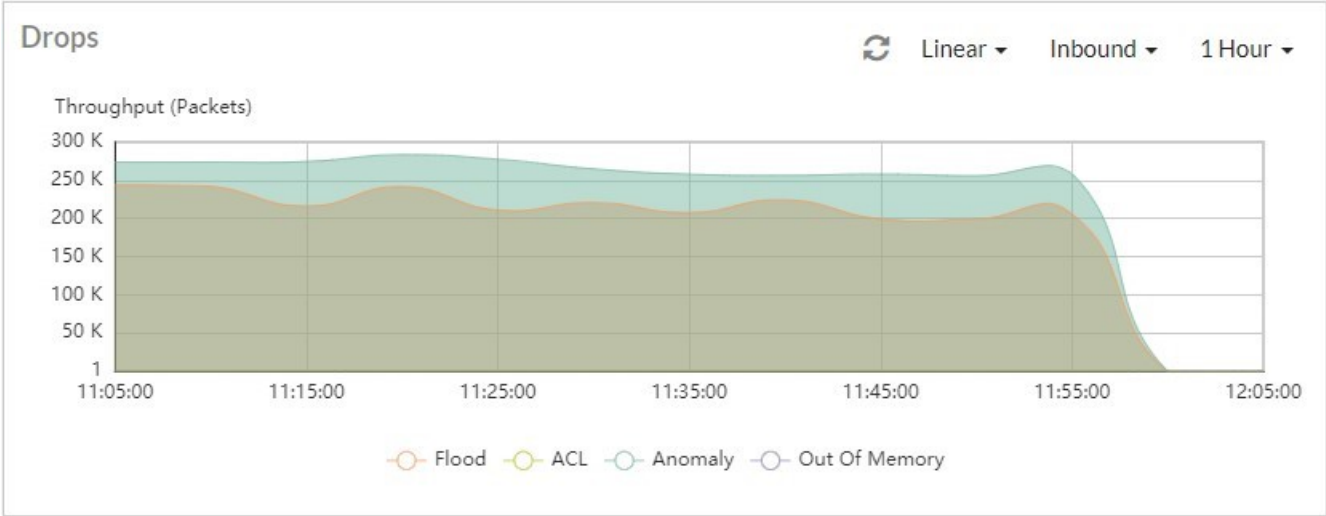
You can hide or display the throughput for Aggregate Ingress or Aggregate Egress traffic by clicking the label.

Aggregate SPP Traffic dashboard - hide/show specific traffic



Drops

The Drops dashboard displays traffic with packets dropped based on types of attack.



Attack Logs

The Attack Logs dashboard displays the table which contains the most recent attack logs by event type, drops count, mode based on timestamp.

Attack Logs

Timestamp	Event Type	Drops	Mode
2021-03-08 12:00:59	DNS Spoofed IP: UDP Question Flood Drop during Retransmission Check	22	Prevention
2021-03-08 12:00:59	DNS Spoofed IP: UDP Qtype All Flood Drop during Retransmission Check	53	Prevention
2021-03-08 12:00:59	DNS Spoofed IP: UDP Query Flood Drop during Retransmi	1,098	Prevention

Data Path Resources

The Data Path Resources table displays the internal table usage statistics.

Data Path Resources

Table Name	Occupancy	Capacity	Percentage Occupancy
Sessions	4,194,304	4,194,304	100.00%
Sources	1,048,576	1,048,576	100.00%
Destinations	1,048,576	1,048,576	100.00%
Non-Spoofed IPs	128,509	1,048,576	12.26%
HTTP Host	1,274	8,192	15.55%
HTTP Referer	1,280	8,192	15.62%

Cloud Signaling

The Cloud Signaling table displays records for devices registered in cloud center.

Cloud Signaling

Device	Status	Last Mitigation Mode	Connection Status
test	disable	registered	

Top Attacks

The DDoS Top Attacks dashboard gives you insight into the attacks that have been thwarted by that SPP's or the entire system's security posture.

The data is filtered by:

- SPP or All SPPs
- Time period of 1 hour to 1 year
- Inbound or Outbound Drops

Available attack reports

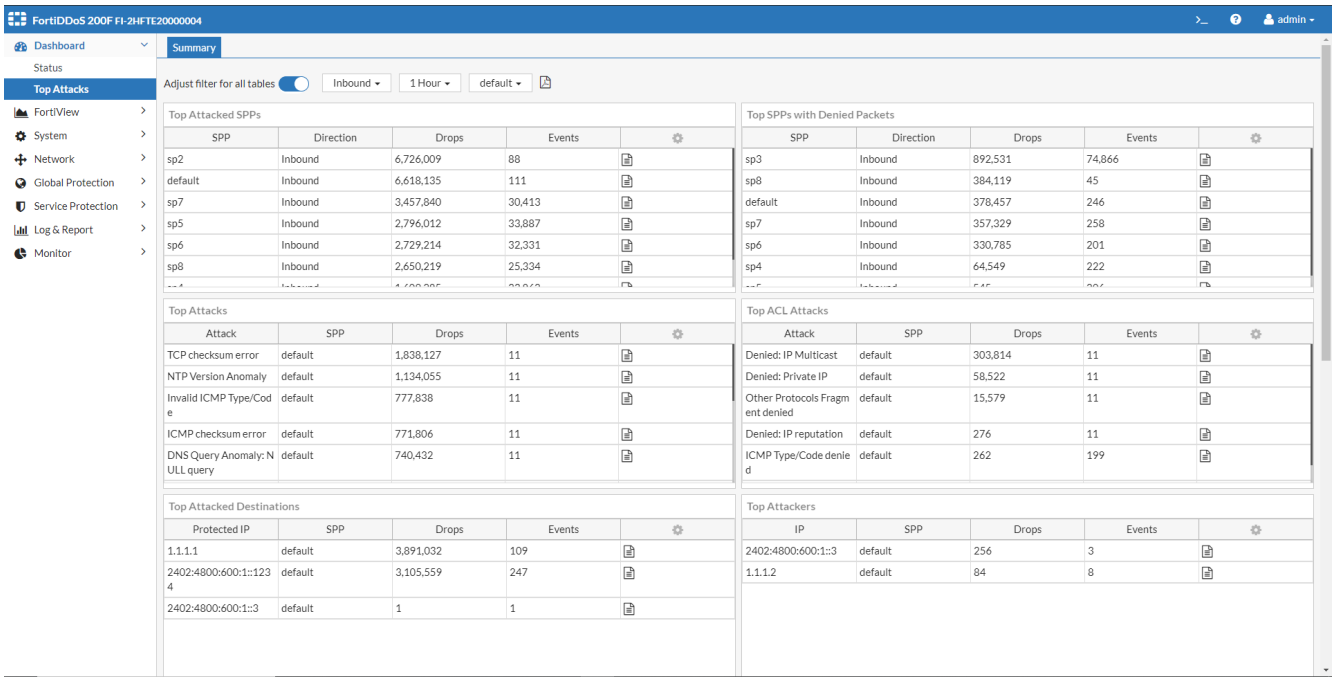
Reports	Description
Top Attacked SPPs	Drop and Event counts by SPP Note: Top Attacked SPPs is shown no matter which SPP or All is selected for display.
Top SPPs with Denied Packets	ACL drop count by SPP

Reports	Description
Top Attacks	Drop count by DDoS attack type
Top ACL Drops	Drop count by ACL rules
Top Attacked Subnets (SPP Policies)	Drop count by SPP Policy Note: If an SPP has more than 1000 attacked subnets, the first 1000 will be shown. All attacked subnets will be displayed in the Attack Logs.
Top Attacked Subnets with Denied Packets	ACL drop count by subnet ID
Top Attacked Destinations	Drop count by Destination IP address
Top Attacked HTTP Servers	Drop count by HTTP server IP address
Top Attackers	Drop count by Source IP address
Top Attacked Protocols	Drop count by protocol Icons in this portal link directly to the attacked Protocol graphs.
Top Attacked TCP Ports	Drop count by TCP port. Icons in this portal link directly to the attacked TCP port graphs.
Top Attacked UDP Ports	Drop count by UDP port Icons in this portal link directly to the attacked UDP Port graphs.
Top Attacked ICMP Type Codes	Drop count by ICMP type/code Icons in this portal link directly to the attacked ICMP type/code graphs.
Top Attacked URLs	Drop count by HTTP URL (hash index) Icons in this portal link directly to the attacked HTTP URL graphs.
Top Attacked HTTP Methods	Drop count by HTTP Method Icons in this portal link directly to the attacked HTTP Method graphs.
Top Attacked HTTP Hosts	Drop count by Host header (hash index) Icons in this portal link directly to the attacked HTTP Hosts graphs.
Top Attacked HTTP User Agents	Drop count by User-Agent header (hash index) Icons in this portal link directly to the attacked HTTP User Agent graphs.
Top Attacked HTTP Referers	Drop count by Referer header (hash index) Icons in this portal link directly to the attacked HTTP Referers graphs.
Top Attacked HTTP Cookies	Drop count by Cookie header (hash index) Icons in this portal links directly to the attacked HTTP Cookie graphs.
Top Attacked DNS Servers	Drop count by DNS server IP address
Top Attacked DNS Anomalies	Drop count by DNS server IP address for packets dropped by DNS anomaly rules

To display the DDoS Top Attacks Log dashboard:

1. Go to *Dashboard* > *Top Attacks*.

2. Select the SPP of interest, time period, and traffic direction from the top left corner.
3. Enable the *Adjust filter for all tables option* toggle if desired



CLI Console

The Console enables you to enter CLI commands through the web UI, without making a separate Telnet, SSH, or local console connection. To use the console, click the **">_"** icon on the FortiDDoS UI header from any page in the GUI. You are logged in as the same admin account you used to access the web UI. To close the console, click the Close (X) button or click on the **">_"** icon again.

Configuring the hostname

You can configure a hostname to facilitate system management. If you use SNMP, for example, the SNMP system name is derived from the configured hostname.

Before you begin:

- You must have Read-Write permission for System settings.

To configure the hostname:

1. Go to *System* > *Admin* > *Settings* > *Hostname* and configure according to the following table.

Hostname configuration

Settings	Guidelines
New Name	The hostname can be up to 35 characters in length. It can include US-ASCII letters, numbers, hyphens, and underscores, but not spaces and special characters. The System Information widget and the `get system status` CLI command display the full hostname. If the hostname is longer than 16 characters, the name is truncated and ends with a tilde (~) to indicate that additional characters exist, but are not displayed.

CLI commands:

```
config system hostname
set hostname <name>
end
```

Rebooting, shutting down, and resetting the system

This section includes the following information:

- Rebooting the system
- Shutting down the system
- Resetting the system

Rebooting the system

To reboot the operating system:

CLI commands:

```
execute reboot
```

Shutting down the system

Always properly shut down the system before unplugging it. This causes it to finish writing any buffered data, and to correctly set the Solid-State-Drives.

Do not unplug or switch off the FortiDDoS-F appliance without first halting the operating system. Failure to do so could cause data loss and hardware problems.

To power off the system:

CLI commands:

```
execute shutdown
```

When shutdown is complete:

- Data traffic will be blocked or bypassed depending on the Interface (Copper, SFP or Optical Bypass, depending on mode) and fail-open/fail-closed configuration. In fail-close mode, the traffic is not bypassed and in fail-open mode, traffic gets bypassed.
- System cooling fans stop operating. Note that power supply cooling fans may still be operating and the power supplies themselves are still powered.
- You will have no GUI or Console access to the system in shutdown. The only way to regain access is full power off (unplug) and restart (see below).

To completely power off:

- Remove power cable(s) from the power supplie(s). Turn off power switch.

Resetting the system

The following table summarizes 'factory reset' options.

Factory reset options

Task	Menu
Reset the threshold configuration for an SPP	*Protection Profiles* > *Thresholds Settings* > *Factory Defaults*
Reset the threshold configuration and clear traffic history for an SPP	*Protection Profiles* > *Reset*
Reset the system to its factory state. All SPPs, statistics, and logs will be deleted	See below.

To reset the system to its factory state:

Use both the commands below:

- `# execute factoryreset`: Deletes all the configuration without deleting any data.
- `# execute formatlogdisk`: Deletes all the data, including MySQL database (attack log, event log) and RRDs (graphs). This does not delete the configuration, but that has already been deleted by the command above.

FortiView

FortiView provides a real-time Threat map view of attacks with historical drop count data. Since 99% of DDoS attacks use spoofed Source IPs, which cannot be validated, the Threat Map provides little useful forensic information. It can be useful as an overview of attacks over a long period. Also, see the Drops Monitor graphs.

With FortiView you can view details of SPP information, including:

- SPP List with summary information
- SPP View including
  - Overview information
  - SPP Traffic graph
  - Top Countries, Attacks and Protocols graph

This section includes details on the following features:

Threat Map

FortiView Threat Map displays a map view of attacks based on FortiDDoS logs, including source and destination geo-locations (when identifiable) with a single day view of information.

The attacks can be from various geo-locations:

- **Internal** - Identified Public Source IPs from the same country geolocation as the FortiDDoS Protected IPs.
- **Identified** - Identified Public Source IP from other geo-locations.
- **Unknown**- Spoofed or otherwise unidentifiable Source IPs

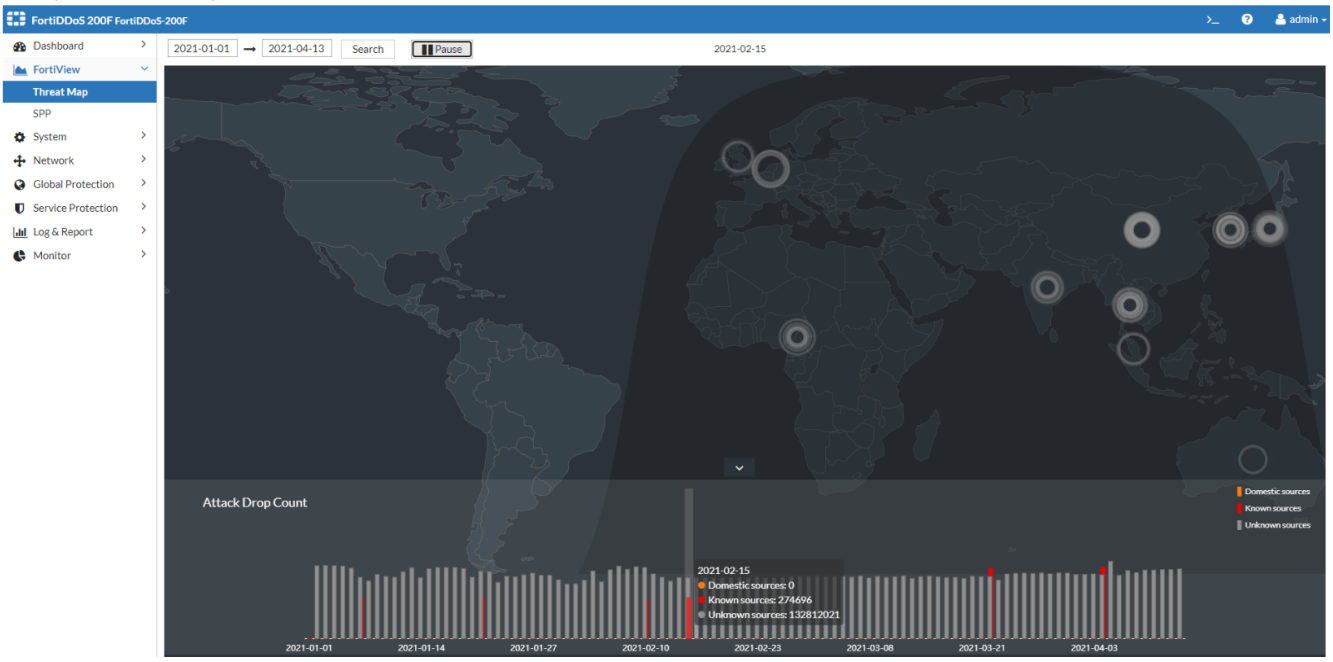
Note: Identifiable Source IPs normally make up less than 10% of DDoS attacks

To view the Threat Map:

1. Go to **FortiView** > **Threat Map**.
2. Select the required SPP from the top-right corner of the GUI. To view the attacks for all SPPs on Threat Map, select **All**.
3. Choose the required date from the above parameters to view the attack details.
   The graph below the map displays an overview of the aggregate drops over the selected range. You can click any specific date from this graph to view the attack details on the map.

- The initial view of Threat Map shows attack information for the current day.
- If Source or Destination IP address are private IPs, they will not be displayed on the Threat Map.
- Threat Map is optimized for Chrome and Firefox browsers.

Sample Threat Map



SPP

SPP Overview

FortiView SPP displays a summary view of traffic and attacks based on FortiDDoS RRDs data, including source geolocations (when identifiable), attack types, and protocol types.

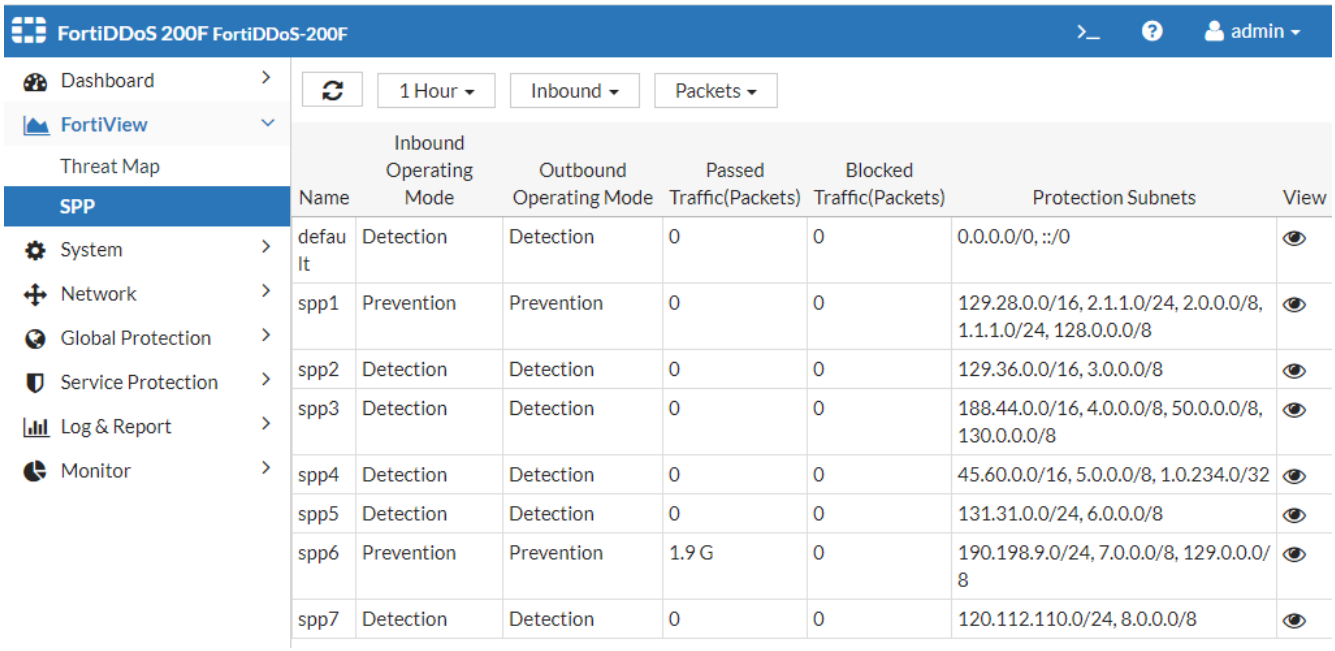
FortiView SPP provides a list view of all configured SPPs with the following information:

Name	Configured SPP Name. “default” SPP always present
Inbound Operating Mode	Detection or Prevention
Outbound Operating Mode	Detection or Prevention
Passed Traffic	Summary of passed traffic in Packet or bits over a time period, depending on modifier settings below
Blocked Traffic	Dropped Packets or or bits over a time period, depending on modifier settings below
Protection Subnets	Summary of all Protection Subnets configured in this SPP
View icon	Icon to select SPP View mode

You can adjust the display using the following parameters:

- Time period (1 hour, 1 day, 1 week, or 1 month)
- Inbound or Outbound Traffic and Drops
- Bits or Packets Traffic and Drops

Sample SPP list view



Name	Inbound Operating Mode	Outbound Operating Mode	Passed Traffic(Packets)	Blocked Traffic(Packets)	Protection Subnets	View
default	Detection	Detection	0	0	0.0.0.0/0, ::/0	
spp1	Prevention	Prevention	0	0	129.28.0.0/16, 2.1.1.0/24, 2.0.0.0/8, 1.1.1.0/24, 128.0.0.0/8	
spp2	Detection	Detection	0	0	129.36.0.0/16, 3.0.0.0/8	
spp3	Detection	Detection	0	0	188.44.0.0/16, 4.0.0.0/8, 50.0.0.0/8, 130.0.0.0/8	
spp4	Detection	Detection	0	0	45.60.0.0/16, 5.0.0.0/8, 1.0.234.0/32	
spp5	Detection	Detection	0	0	131.31.0.0/24, 6.0.0.0/8	
spp6	Prevention	Prevention	1.9 G	0	190.198.9.0/24, 7.0.0.0/8, 129.0.0.0/8	
spp7	Detection	Detection	0	0	120.112.110.0/24, 8.0.0.0/8	

SPP Summary View

The SPP Summary View displays a top-level view of SPP information, the SPP traffic chart, and SPP Countries/Attacks/Protocols.

The SPP Summary vView page has 2 global modifiers:

- Time period (1 hour, 1 day, 1 week, or 1 month)
- Inbound or Outbound Traffic and Drops

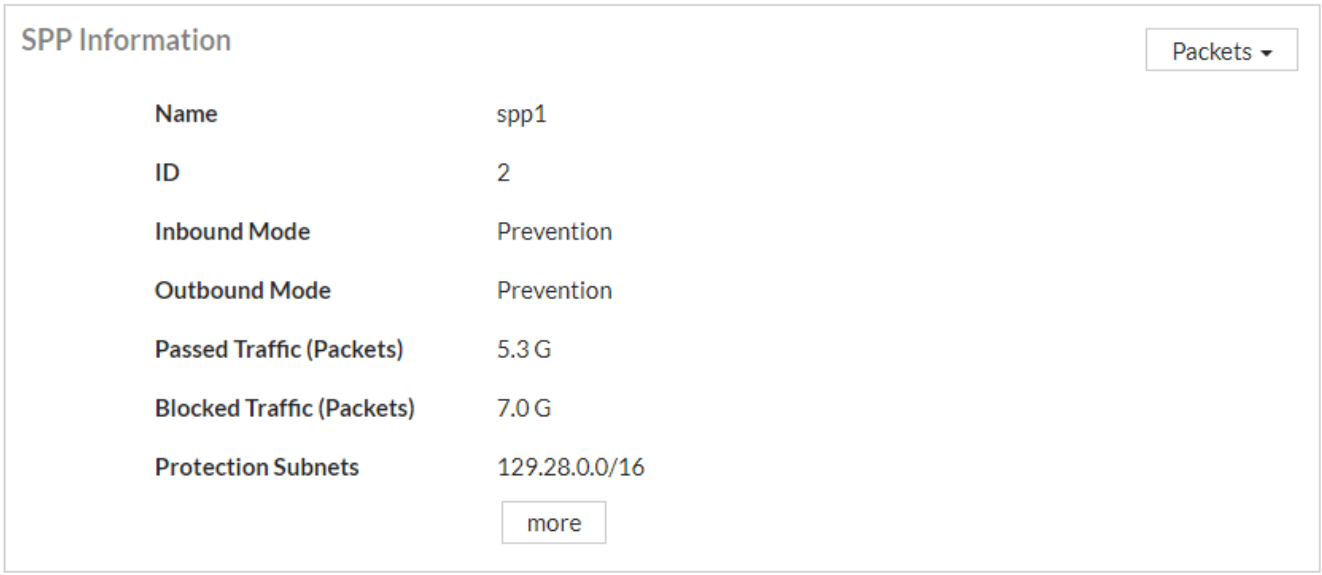
SPP Information

SPP Information panel provides similar SPP summary information as the SPP list view:

- SPP configured Name
- SPP Number (system-generated)
- Inbound Mode (Detection | Prevention)
- Outbound Mode (Detection | Prevention)
- Passed Traffic (total for the time period) (Packets | Bits)
- Blocked Traffic (total for the time period) (Packets | Bits)
- Protection Subnets – Only 1 subnet appears. The More button displays all configured Protection Subnets.

SPP Information has a single modifier selection for Packets or Bits.

SPP Information



SPP Traffic Chart

The SPP Traffic Chart displays Ingress and Egress traffic based on the global modifiers for Time Period and Direction.

Note: FortiDDoS displays Ingress and Egress traffic differently than most networking products.

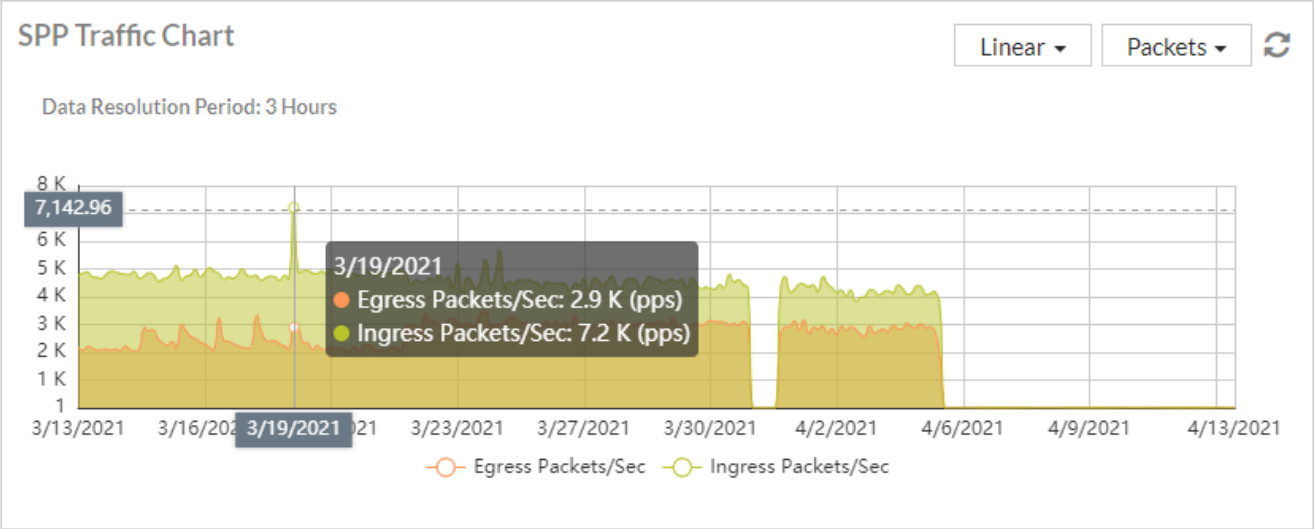
- Inbound Ingress traffic is from the Internet to FortiDDoS. Inbound Egress traffic is from FortiDDoS to your local network.
- Conversely, Outbound Ingress is from your local network to FortiDDoS and Outbound Egress traffic is from FortiDDoS to the Internet.

This allows instant recognition of dropped packets as the traffic traverses FortiDDoS. In the screenshot below, it is obvious that the orange Egress traffic is lower than the green Ingress traffic. This shows that FortiDDoS dropped attack traffic as it passed through the system / SPP.

On the chart, you can:

• Select Linear or Logarithmic Y-axis views. Logarithmic view allows you to see both Ingress and Egress graphs if there is a very large differential between them.

- Select Packets (pps) or Bits (bps)
- Roll the cursor over the graph to reveal a tool tip with precise Ingress/Egress traffic details.
- Refresh the graph. Most FortiDDoS graphs do not auto-refresh
- Toggle either Ingress or Egress graphs off or on by selecting the graph icon beside the X-axis labels.



Countries Graph

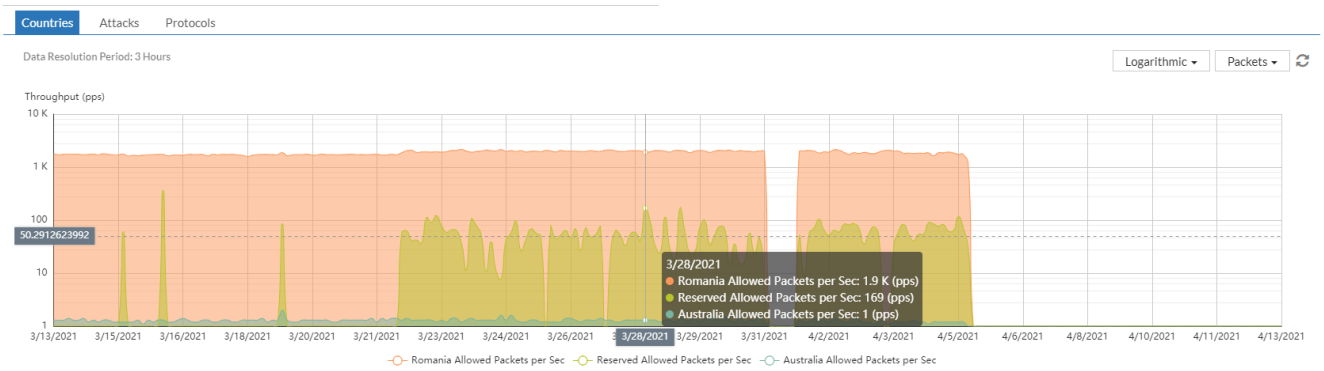
The Countries graph and table provides geolocation information for the top Source countries of passed (Egress) traffic based on the global page modifiers for Time Period and Direction.

The Countries graph includes the following modifiers:

- Select Linear or Logarithmic Y-axis views. Logarithmic selection allows a better view if there is a very large differential between the various graph parameters.
- Select Packets (pps) or Bits (bps)
- Roll the cursor over the graph to reveal a tool tip with precise traffic details for any point on the graph.
- Refresh the graph. Most FortiDDoS graphs do not auto-refresh
- Toggle the various Country sub-graphs off or on by selecting the graph icon beside the X-axis labels.

The Countries table provides a top Countries summary with Passed and Blocked packets (total) and rates (pps).

The Countries graph/table should not be used exclusively for geolocation ACL decisions. FortiDDoS attempts to geolocate the Source IP of any passed packet. UDP and ICMP packets, for example (and any non-TCP Protocol), cannot be source-validated. Under-threshold packets may still use Spoofed IPs. While the Countries graph is interesting to look at, it has little forensic value.



Country	Passed Traffic(Packets)	Pass Rate(pps)	Blocked Traffic(Packets)	Block Rate(pps)
Macao	5350240.9 T	2.0 T	0	0
Antigua and Barbuda	1631429.0 T	624.2 G	0	90.2 T
Romania	3.6 G	1.4 K	0	0
Reserved	70.9 M	27	56.6 K	0
Australia	2.5 M	1	4.8 G	1.8 K

Attack Graph

The Attacks graph and table provides top Attack (drops) information based on the global page modifiers for Time Period and Direction.

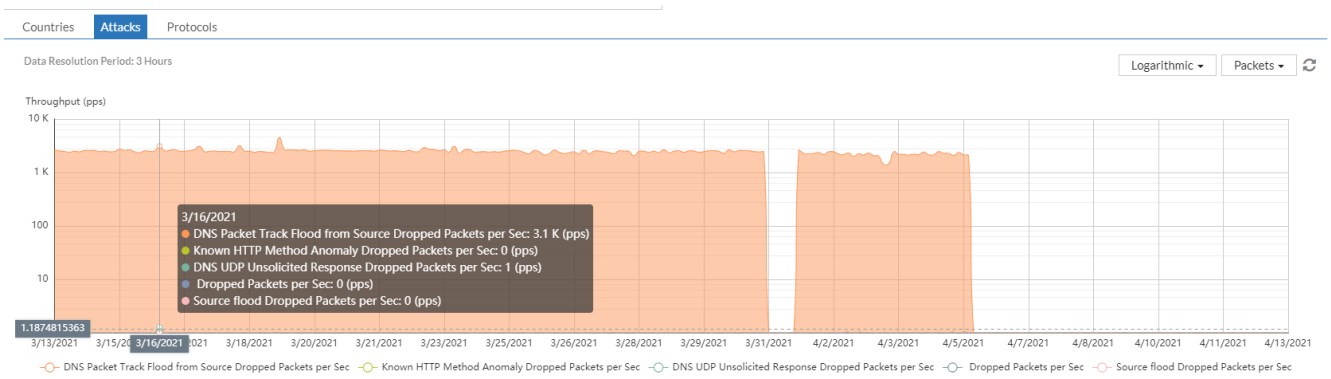
The Attacks graph includes the following modifiers:

- Select Linear or Logarithmic Y-axis views. Logarithmic selection allows a better view if there is a very large differential between the various graph parameters.
- Select Packets (dropped) or Bits (dropped)
- Roll the cursor over the graph to reveal a tool tip with precise drop details for any point on the graph.
- Refresh the graph. Most FortiDDoS graphs do not auto-refresh
- Toggle the various Drop sub-graphs off or on by selecting the graph icon beside the X-axis labels.

The Attacks table shows the following information for the global time-period selected:

- Total Blocked traffic (bits/packets)
- Peak Blocked rate (bps/pps)

Note: The attacks shown and listed may be different for Packets and Bits. SYN Floods use 64 Byte packets while DNS Reflection Floods often use 1500 Byte packets. Thus a DNS Reflection flood may be in the top “Bits” list while a SYN Flood may be in the top “Packets” list.



Attack Type	Blocked Traffic(Packets)	Block Rate(pps)
Most Active Destination	1479432.5 T	566.1 G
DNS Packet Track Flood from Source	4.8 G	1.8 K
DNS UDP Unsolicited Response	20.5 K	0

Protocols Graph

The Protocols graph and table provides top Protocols information based on the global page modifiers for Time Period and Direction. Protocols graphs shows “allowed” or Egress traffic only.

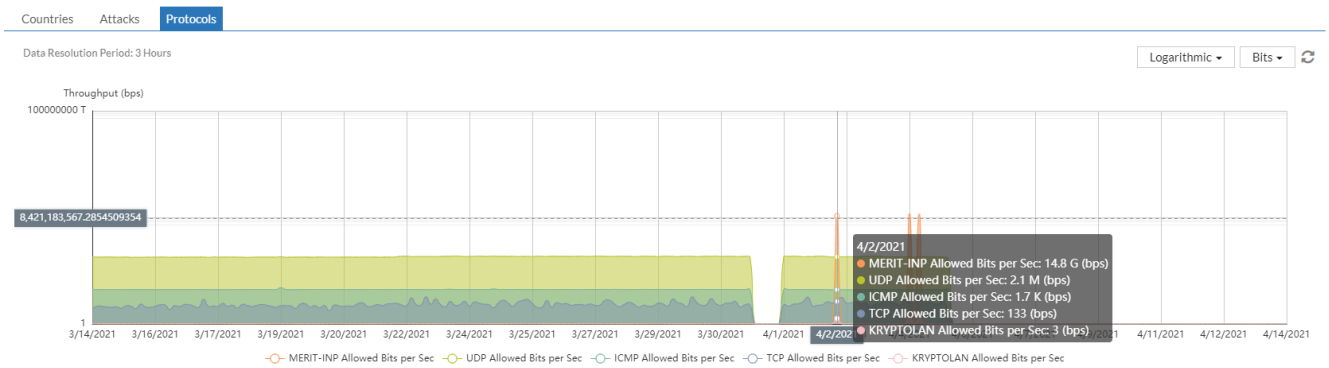
The Protocols graph includes the following modifiers:

- Select Linear or Logarithmic Y-axis views. Logarithmic selection allows a better view of Egress graphs if there is a very large differential between the various graph parameters.
- Select Packets or Bits
- Roll the cursor over the graph to reveal a tool tip with precise Protocol egress traffic details.
- Refresh the graph. Most FortiDDoS graphs do not auto-refresh
- Toggle the various Protocol sub-graphs off or on by selecting the graph icon beside the X-axis labels.

The Protocols table shows the following information for the global time-period selected:

- Total passed traffic (bits/ packets)
- Peak pass rate (bps/pps)
- Total blocked traffic (bits/ packets)
- Peak blocked rate (bps/pps)

Note: The Protocols shown and listed may be different for Packets and Bits depending on the packet sizes seen.



Protocol	Passed Traffic(Bits)	Pass Rate(bps)	Blocked Traffic(Bits)	Block Rate(bps)
MERIT-INP	588.3 T	225.1 M	0	0
UDP	3.8 T	1.5 M	5.0 T	1.9 M
ICMP	3.2 G	1.2 K	6.7 M	3
TCP	159.2 M	61	108.7 M	42
KRYPTOLAN	132.0 K	0	0	0

System Management

This section includes the following topics:

High Availability Deployments

HA feature overview

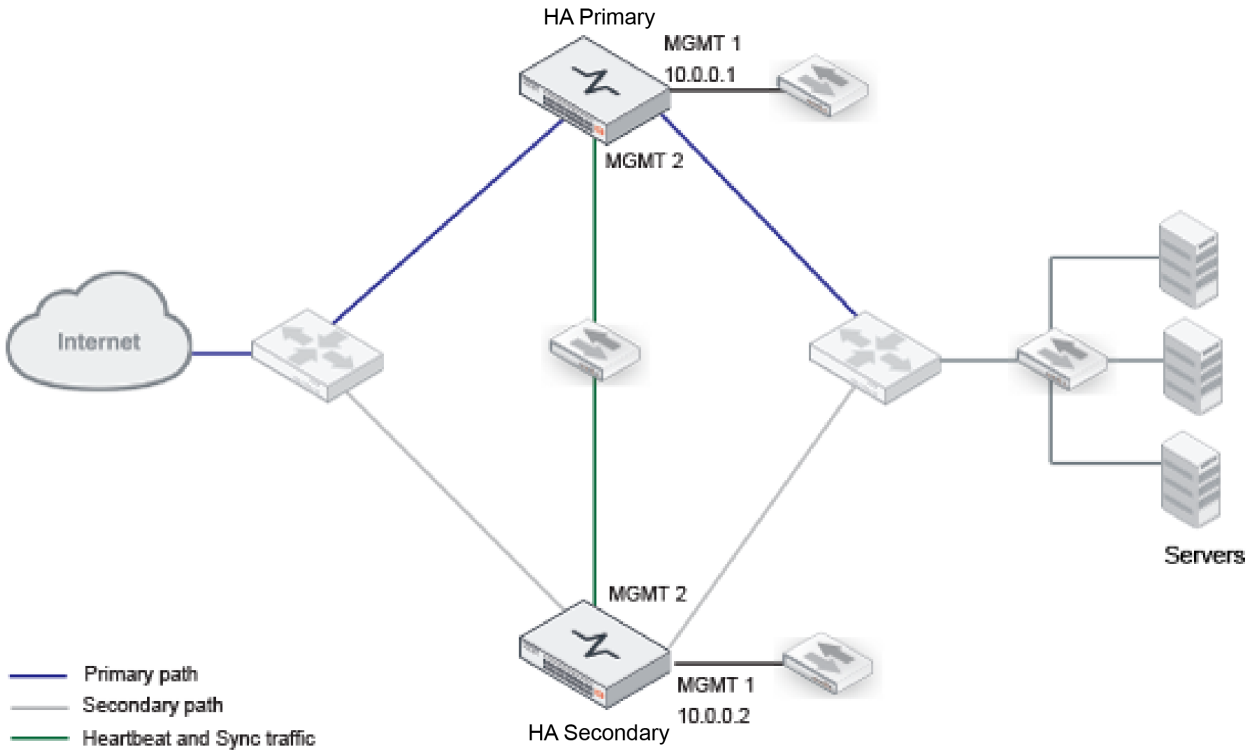
FortiDDoS-F appliances can be deployed as standalone appliances or as members of a high availability (HA) pair. FortiDDoS supports *active-passive* cluster pairs. In an HA pair, one node is the *primary node*, and the other is called the *secondary node*.

The figure below shows an active-passive deployment. The cluster uses the connection of MGMT2 ports for two types of HA communication:

- *Heartbeats*. A cluster node indicates to other nodes in the cluster that it is up and available. The absence of heartbeat traffic indicates the node is not up and is unavailable.
- *Synchronization*. During initialization and periodically thereafter, the primary node pushes its configuration (with noted exceptions) to the secondary nodes.

You can log into the management interface (MGMT1) of either node, but you actively manage the configuration of the primary node only.

Active-passive cluster



Although one appliance is deemed active (the primary) and one passive (the secondary), the ports are not turned off on the passive node. It can receive traffic, mitigate attacks and forward it.

You should use the adjacent routers to ensure that traffic is forwarded through only the active path. For example, you can set a path priority or costing to set a high priority (low cost) path that goes through the primary node, ignoring the secondary, even if it can pass traffic. If the primary fails, its interfaces can be configured to 'fail closed'; the router can detect this and switch to the alternative path.

If that secondary node fails as well (double failure) and you do not want the traffic to fail, configure the secondary system to 'fail open' (For appliances only. VM not supported).

In some applications, you can utilize the ability to pass traffic on the passive node to your advantage. For example, your can create a multi-link LACP and allow the traffic to be distributed between FortiDDoS appliances, doubling the available bandwidth for mitigation. Since traffic is evenly distributed, the thresholds learned and implemented in the Primary system will work equally well in the Secondary system. However, each system graphs data, logs and creates reports independently. These logs can be aggregated by FortiAnalyzer or FortiSIEM.

HA system requirements

- Two identical appliances (the same hardware model and same firmware version).
- By default, you use MGMT2 port to connect the HA appliances directly or through a Layer 2 switch. The HA port can be changed but be aware of the settings on the System > Network > Interface page before changing from default.

- Heartbeat and synchronization traffic between cluster nodes occur over the physical network ports you specify. If switches are used to connect heartbeat interfaces between nodes, the heartbeat interfaces must be reachable by Layer 2 multicast. HA traffic uses multicast UDP on port numbers 6065 (heartbeat) and 6056 (synchronization). The HA multicast IP address is 239.0.0.1; it is hard-coded, and cannot be configured.

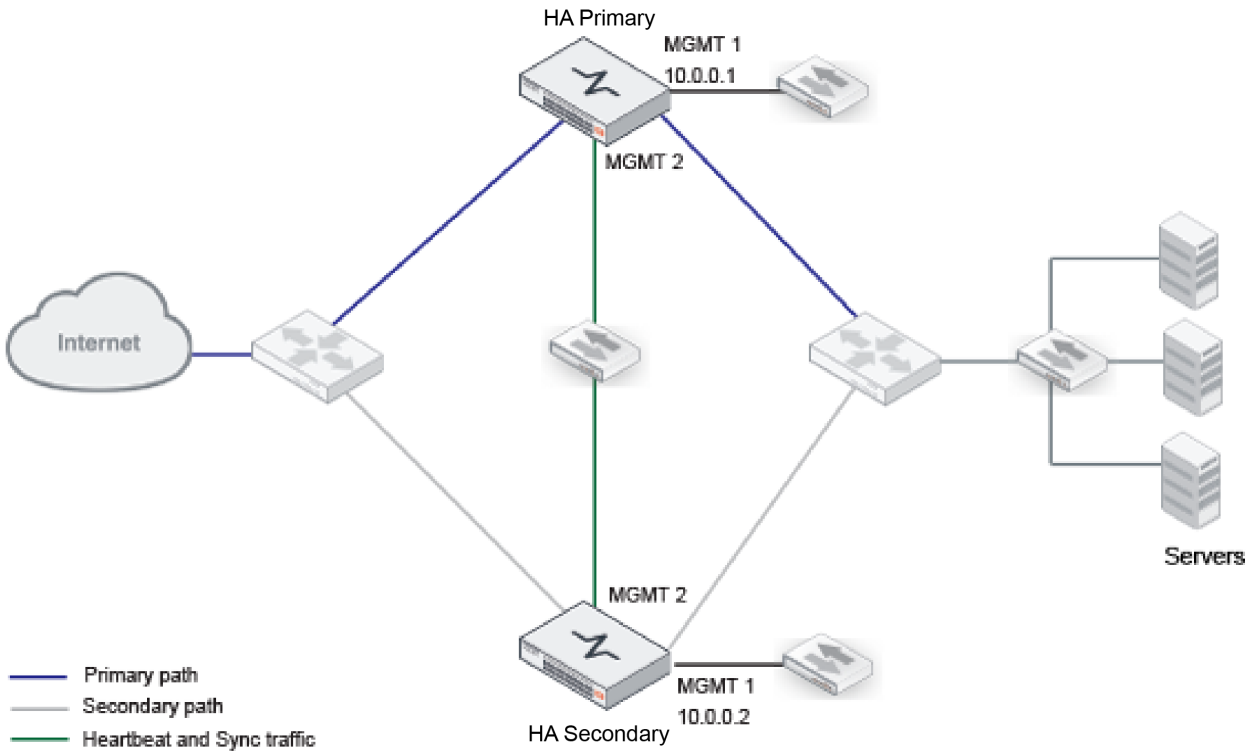
Deploying an active-passive cluster

This topic includes the following information:

Overview

The following figure shows an active-passive deployment. When HA is enabled, the system sends heartbeat packets between the pair to monitor availability, and the primary node pushes its configuration to the secondary node.

Active-passive cluster



When the primary node goes down, the secondary becomes the primary node. When the primary node comes back online, the system selects the primary based on the following criteria:

- Lowest device priority number (1 has greater priority than 2)
- Highest up-time value
  - **Note:** Before you configure HA Settings, familiarize yourself on how FortiDDoS High Availability works.

Basic steps

To deploy an active-passive cluster:

1. License all FortiDDoS-F appliances in the HA cluster, and register them, including FortiGuard services, with the Fortinet Technologies Inc. Technical Support website: https://support.fortinet.com/
2. Physically link the FortiDDoS-F appliances that make up the HA cluster.
   You must link at least one of their ports (for example, mgmt2 to mgmt2) for heartbeat and synchronization traffic between members of the cluster. You can do either of the following:
   - Connect the two appliances directly with an Ethernet cable.
   - Link the appliances through a switch. If connected through a switch, the HA interfaces must be reachable by Layer 2 multicast.
3. Configure the secondary node:
   a. Log into the secondary appliance as the **admin** user.
   b. Go to Global Settings > Settings and set the Power Failure Bypass Mode to **Fail Open** or **Fail Closed**, according to your preference on how to handle traffic when both nodes fail. If you use an external bypass unit, you configure **Fail Closed**.
   c. Complete the HA settings as described in Configuring HA settings.

   Important: Set the Device Priority to a higher number than the primary appliance; for example, set Device Priority to 2.
4. Configure the primary node:
   a. Log into the primary appliance as the **admin** user.
   b. Go to Global Settings > Settings and set the Power Failure Bypass Mode to **Fail Closed**.
   c. Complete the configuration for all features, as well as the HA configuration.

   Important: Set the Device Priority to a lower number than the secondary appliance; for example, set Device Priority to 1.

Note: After you have saved the HA configuration changes, cluster members might join or rejoin the cluster. After you have saved configuration changes on the primary node, it automatically pushes its Global Settings and Protection Profiles configuration to the secondary node.

HA synchronization

The Primary node pushes the following configuration elements to the Secondary node. This is known as synchronization.

Setting	Synced (Yes/No)	Editable on Secondary in Active/Passive Mode (Yes/No)
System		
High Availability	No	Yes
Admin		
• Administrator	Yes	No

Setting	Synced (Yes/No)	Editable on Secondary in Active/Passive Mode (Yes/No)
• Profile	Yes	No
• Settings	Yes	No
• Host Name	No	No
Authentication		
• RADIUS	Yes	No
• LDAP	Yes	No
• TACACS+	Yes	No
SNMP		
• System Information	No	Yes
• Thresholds	Yes	No
• Community	Yes	No
• User	Yes	No
Certificate	No	Yes
Maintenance		
• Backup & Restore	Backup/Restore Allowed	Backup/Restore Allowed
• Date & Time (including NTP)	Yes	No
• Time Zone	Yes	No
• Daily Config Backup	No	Yes
FortiGuard	Yes	No
Address and Service		
• Address IPv4	Yes	No
• Address IPv4 Group	Yes	No
• Address IPv6	Yes	No
• Address IPv6 Group	Yes	No
• Service	Yes	No
• Service Group	Yes	No
Network		
Interface		
• Traffic Ports	No	Yes

Setting	Synced (Yes/No)	Editable on Secondary in Active/Passive Mode (Yes/No)
• Management Ports	No	Yes
Route	No	Yes
DNS	No	Yes
Packet Capture	No	Yes
Global Settings		
Deployment		
• Deployment	No	Yes
• Bypass MAC	Yes	No
Proxy IP		
• Proxy IP Detection	Yes	No
• Proxy IP List	Yes	No
Cloud Signaling	No	Yes
Access Control List		
• Access Control List	Yes	No
• Access Control List IPv6	Yes	No
Blocklist		
• Blocklisted IPv4 Address	No	Yes
• Blocklisted Domains	No	Yes
Do Not Track Policy		
• IPv4	Yes	No
• IPv6	Yes	No
GRE Tunnel Endpoint	Yes	No
Service Protection		
Service Protection Profiles		
• Service Protection Policy	Yes	No
• Source Tracking	Yes	No
• Blocking Settings	Yes	No
• Service Ports Setting	Yes	No
• Protection Profile Settings	Yes	No

Setting	Synced (Yes/No)	Editable on Secondary in Active/Passive Mode (Yes/No)
• Protection Subnets	Yes	No
• ACL	Yes	No
• Thresholds	Yes	No
DNS Protection Profile	Yes	No
TCP Protection Profile	Yes	No
IP Protection Profile	Yes	No
ICMP Protection Profile	Yes	No
NTP Protection Profile	Yes	No
HTTP Protection Profile	Yes	No
SSL/TLS Protection Profile	Yes	No
Log & Report		
Log configuration	No - all settings and Reports are independent.	
• Local Log Settings	No	Yes
• Event Log Remote	No	Yes
• DDoS Attack Log Remote	No	Yes
• Alert Email Settings	No	Yes
• Log Purge Settings	No	Yes
• SNMP Trap Receivers	No	Yes
• Remote Log Settings	No	Yes
Log Access		
• Logs	No	Not Applicable Logs are displayed independently on each appliance
• Log Backup	No	Yes
Report Configuration	No	Yes
Report Purge	No	Yes
Report Browse	No	Yes
Flowspec	No	Yes
Monitor		

Setting	Synced (Yes/No)	Editable on Secondary in Active/Passive Mode (Yes/No)
All Graphs	No	Not Applicable All graphing is independent to each appliance. There are no configuration options in Monitor graphs.

Synchronization occurs immediately when an appliance joins the cluster, and thereafter every 30 seconds. In an active-passive cluster, any synchronized settings (Yes in the 'Synced' column above) are read-only on the Secondary node.

All other system configuration, network and interface configuration, HA configuration, and log/report configuration (Yes in the 'Editable' column above) are not synchronized but may be edited on the Secondary even when it is in Active-Passive Mode.

Note the following:

- It is not recommended to perform the below actions on a Primary node when it is in HA Active-Passive mode. You need to switch to standalone mode to modify these settings:
  - Configuration restore - this is likely to cause Secondary system reboots. It is better to put the systems in standalone mode and restore to each system, then place in Active-Passive mode, unless Secondary rebooting is acceptable.
  - TAP mode change
- HA Secondary does not synchronize time/date from HA Primary.
- HA settings are read-write on all nodes in all modes so that you can switch from HA to standalone mode as needed.

Collected data is also *not* synchronized. The following data is not synchronized:

- **Session data**—It does not synchronize session information or any other element of the data traffic.
- **Estimated thresholds**—Configured thresholds are part of the configuration and are synchronized, but estimated thresholds that are shown in Monitor graphs are based on the history of traffic processed by the local system.
- **Log messages**—These describe events that happened on that specific appliance. After a failover, you might notice that there is a gap in the original active appliance's log files that corresponds to the period of its down time. Log messages created during the time when the standby was acting as the active appliance (if you have configured local log storage) are stored there, on the original standby appliance.
- **Generated reports**—Like the log messages that they are based upon, PDF, HTML, RTF, and plain text reports also describe events that happened on that specific appliance. As such, report settings are synchronized, but report output is not.

Configuring HA settings

Before you begin:

- You must have Read-Write permission to items in the System category.
- Before you configure HA Settings, familiarize yourself on how FortiDDoS High Availability works, here.

To configure HA settings:

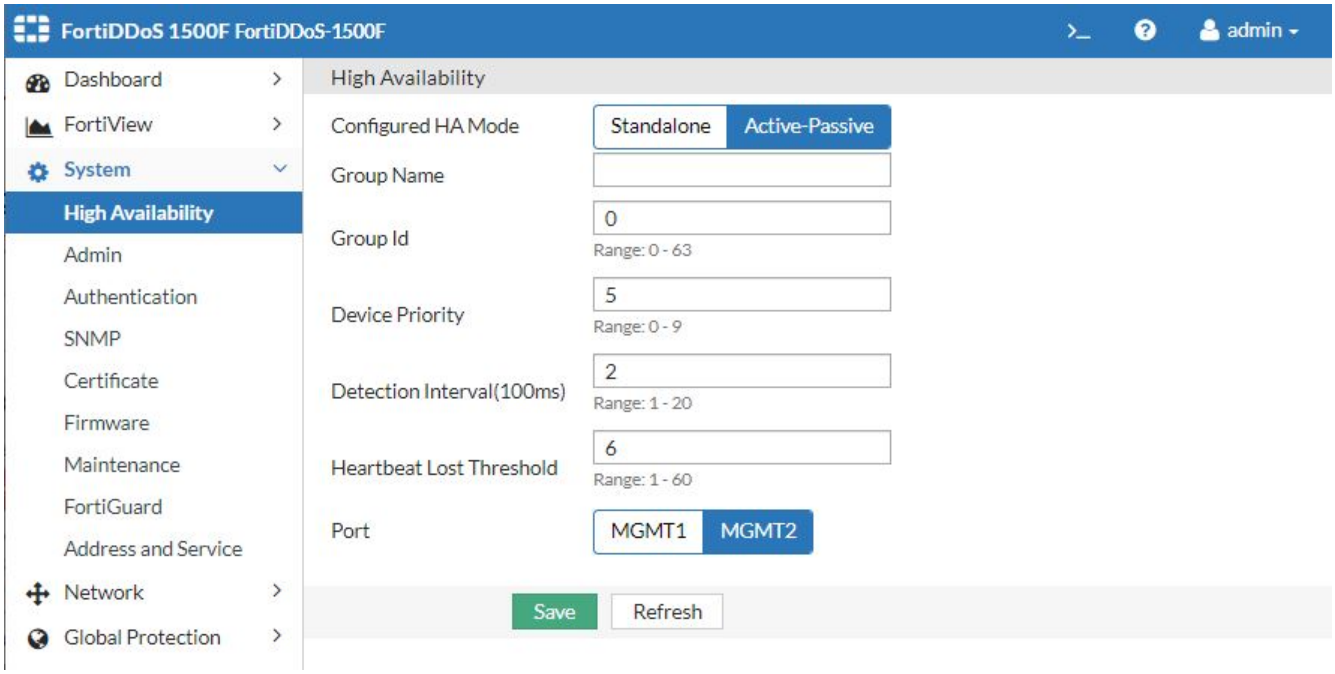
1. Go to **System** > **High Availability**.
2. Complete the configuration as described in the table below.

3. Save the configuration.

After you have saved the configuration, cluster members begin to send heartbeat traffic to each other. Members with the same Group ID join the cluster. They send synchronization traffic directly through the HA connection.

NOTE: If you change the HA Mode from Active-Passive to Standalone, HA settings will be reset to Default. Before you change to Standalone, take a screenshot or otherwise record the Active-Passive settings so you can restore them when you return to Active-Passive Mode.

High availability page



High availability settings

Settings	Guidelines
Configured HA Mode	• Standalone • Active-passive This setting should only be changed after other non-synchronized settings are complete, although this is not mandatory. See **HA synchronization** for settings that are not synchronized between devices. When changed to active-passive, all synchronized parameters on the Secondary device will be replaced with data from the primary device and made read-only. Non-synchronized parameters may be modified on the Secondary device, as required, while it is in Active-Passive mode.
Group Name	Name to identify the HA cluster if you have more than one. This setting is optional, and does not affect HA function. The maximum length is 35 characters (no special characters or spaces are allowed).
Device Priority	Number indicating priority of the member node when electing the cluster primary node. The smaller the number, the higher the priority. It is mandatory to set this correctly. The valid

Settings	Guidelines
	range is 0 to 9 and the default is 5.
Group ID	Number that identifies the HA cluster. Nodes with the same group ID join the cluster. If you have more than one HA cluster on the same network, each cluster must have a different group ID. The valid range is 0 to 63. The default is 0.
Detection Interval	Number of 100-millisecond intervals at which heartbeat packets are sent. This is also the interval at which a node expects to receive heartbeat packets. These numbers must match on Primary and Secondary. The valid range is 1 to 20 (that is, between 100 and 2,000 milliseconds). The default is 2.
Heartbeat Lost Threshold	Number of times a node retries the heartbeat and waits to receive HA heartbeat packets from the other node before concluding the other node is down. The valid range is from 1 to 60. The default is 6.
Port	Mark the check boxes for the network interface to be used for port monitoring and heartbeat packets. Use the same port number for both systems. For example, if you select mgmt2 on the primary node, select mgmt2 as the heartbeat interface on the other node. The standard practice is to use mgmt2 for port monitoring and heartbeat packets with a dedicated cable between the devices. However, the HA multicast traffic can share a management port that has an IP address for system GUI/CLI access. If not directly connected, ensure that the two HA ports/systems have Layer 2 multicast connectivity between them.

CLI commands:

```
config system ha
set mode <standalone | active-passive>
set group-name <group_name_str>
set priority <priority_int>
set group-id <group_id_integer>
set hb-interval <hb_interval_int>
set hb-lost-threshold <hb_lost_thresh_int>
set hbdev <mgmt1 | mgmt2>
end
```

Operational tasks

Monitoring an HA cluster

You can use SNMP, log messages, and alert email to monitor HA events, such as when failover has occurred. The system logs HA node status changes as follows:

- When a member joins a group: `Member (FI-2HFTE20000005) join to the HA group`
- When the HA configuration is changed from standalone to an active-passive: `HA device into Secondary mode`
- When HA synchronization is initialized: `HA device Init`

Note: SNMP logging and email alerts are independently set on each device. They can be identical but must be entered separately.

Updating firmware on an HA cluster

Note the following before upgrade:

- Upgrading FortiDDoS requires at least one reboot of each appliance and can be disruptive of network traffic depending on fail-open/closed conditions and RSTP/BGP settings of surrounding switches. This procedure assumes production traffic on the Primary appliance with an upgrade of the Secondary appliance first. This procedure can be reversed – move traffic to the Secondary, upgrade the primary, revert traffic and upgrade the Secondary.
- If both devices are carrying production traffic (each appliance is on one leg of an asymmetric traffic environment), ensure both devices support fail-open and perform in a maintenance window.
- Do not modify any configuration settings when systems are in Standalone Mode. Any configuration changes may cause the Seondary unit to reboot when returning to the HA pair.

To update the firmware of an HA cluster:

1. Verify that the cluster node members are powered on and available.
2. Log into the web UI of the primary node with an account whose access profile contains **Read** and **Write** permissions in the Maintenance and HA category.
3. Backup the Primary configuration.
4. Go to System > High Availability and note the number in the **Device Priority** field. The Primary Device Priority must be higher than Secondary Device Priority. (1 is a higher priority than 5, for example). If this is not true, note the error to be corrected during upgrade.
5. Change the HA mode from Active-Passive to Standalone.
6. Repeat steps 2-4 on the Secondary system.
   Note: Having both systems in Standalone mode is important for this procedure.
7. Follow the upgrade procedure as instructed in the Release Notes on Secondary system. (This assumes that the traffic is currently on the Primary system.).
8. Once the Secondary system is upgraded, leave the Secondary in Standalone Mode and move traffic to the Secondary.
9. Follow the upgrade procedure on Primary System as instructed in the Release Notes.
10. On the Primary System > High Availability: Confirm or set the device priority to a higher priority (lower number) than the Secondary system and then change **Configured HA Mode** to 'Active-Passive'.
11. Revert traffic to the Primary system.
12. On the Secondary System > High Availability: Confirm or set the device priority to a lower priority (lower number) than the primary system and then change **Configured HA Mode** to 'Active-Passive'.

Modifying system or report settings on HA Secondary

Follow the steps below to modify system or report settings on an HA Secondary:

1. Log in to the Secondary device using credentials with Read-Write permissions.
2. Proceed to the **System** or **Log & Report** menus and make the required changes.

Managing administrator users

This topic includes the following information:

Administrator user overview

In its factory default configuration, FortiDDoS-F has one administrator account named **admin**. This administrator has permissions that grant Read-Write access to all system functions.

Unlike other administrator accounts, the administrator account named admin exists by default and cannot be deleted. The **admin** account is similar to a root administrator account. This account always has full permission to view and change all system configuration options, including viewing and changing *all* other administrator accounts. Its name and permissions cannot be changed. It is the only administrator account that can reset another administrator's password without being required to enter that administrator's existing password.

To prevent accidental changes to the configuration, it is best if only network administrators—and if possible, only a single person—use the **admin** account. You can use the **admin** account to configure more administrator accounts for other people. Accounts can be made with different scopes of access. You can associate each of these accounts with either all SPPs or a single SPP, and you can specify the type of profile settings that each account can access. If you require such role-based access control (RBAC) restrictions, or if you simply want to harden security or prevent inadvertent changes to other administrators' areas, you can do so with access profiles. For example, you can create an account for a security auditor who must only be able to view the configuration and logs, but *not* change them.

Basic steps

1. Configure profiles to provision permissions to roles.
2. Optional. Create RADIUS or LDAP server configurations if you want to use a RADIUS or LDAP server to authenticate administrators. Otherwise, you can use local authentication.
3. Create administrator user accounts with permissions provisioned by the profiles.

Configuring access profiles

Access profiles provision permissions to roles. The following permissions can be assigned:

- Read (view access)
- Read-Write (view, change, and execute access)
- No access

When a profile includes only read access to a category, the user can access the web UI page for that category, and can use the `get` and `show` CLI command for that category, but cannot make changes to the configuration.

When a profile includes no categories with read-write permissions, the user can log into the web UI but not the CLI.

In larger companies where multiple administrators share the workload, access profiles often reflect the specific job that each administrator does ("role"), such as account creation or log auditing. Access profiles can limit each administrator account to their assigned role. This is sometimes called role-based access control (RBAC).

The table below lists the administrative areas that can be provisioned. If you provision read access, the role can view the web UI menu (or issue a CLI get command). If you provision read-write access, the role can save configuration changes (or issue a CLI set command).

For complete access to *all* commands and abilities, you must log in with the administrator account named **admin**.

Areas of control in access profiles

Web UI Menus	CLI Commands

System	`config system ...`
	`show full-configuration`
	`diagnose ...`
	`execute ...`

Global Settings	`config ddos global ...`
Protection Profiles	`config spp ...`

Monitor	`get system status`
	`get system performance`
	`show system status`
	`show system performance`
	`show full-configuration`

Log & Report	`config log ...` `config system`

***** For each `config` command, there is an equivalent `get`/`show` command, unless otherwise noted. `config` commands require write permission. `get`/`show` commands require read permission.

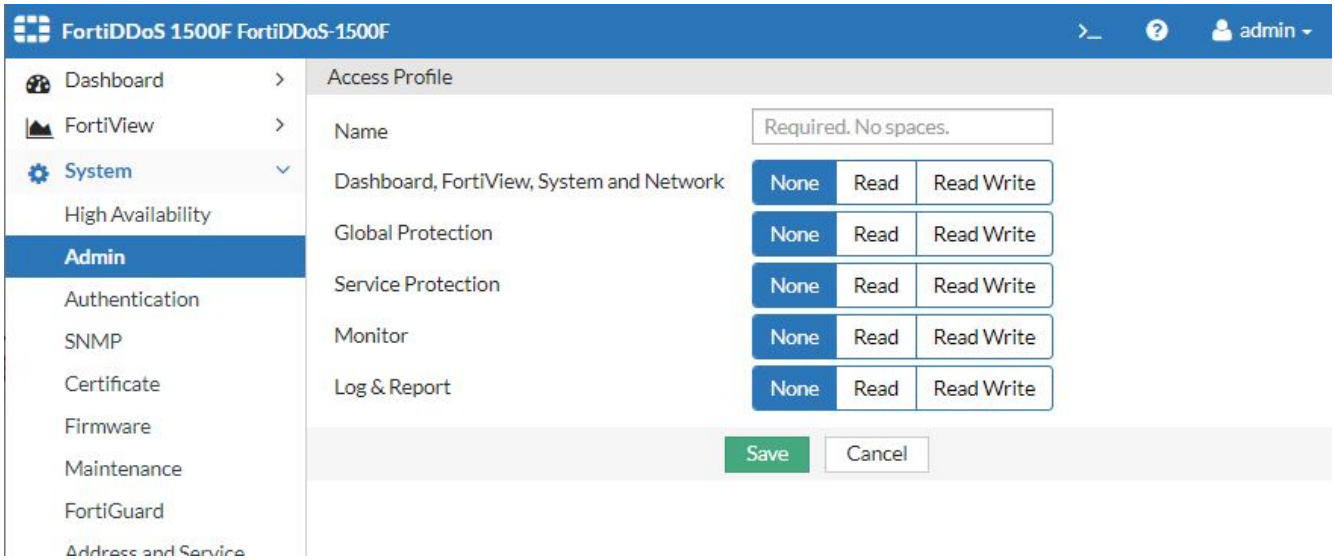
Before you begin:

- You must have Read-Write permission for System settings.

To configure administrator profiles:

1. Go to **System** > **Admin** > **Access Profile**.
2. Click **Add** to display the configuration editor.
3. Complete the configuration as described in the table below.
4. Save the configuration.

Admin profile configuration page



Admin profile configuration guidelines

Settings	Guidelines
Profile name	Unique name. No spaces or special characters.
Access Control	• None—Do not provision access for the menu. • Read Only—Provision ready-only access. • Read-Write—Enable the role to make changes to the configuration.

The **super_admin_prof** access profile, a special access profile assigned to the **admin** account and required by it, appears in the list of access profiles. It exists by default and cannot be changed or deleted. The profile has permissions similar to the UNIX root account.

Creating administrator users

We recommend that only network administrators—and if possible, only a single person—use the **admin** account. You can configure accounts that provision different scopes of access. For example, you can create an account for a security auditor who must only be able to view the configuration and logs, but *not* change them.

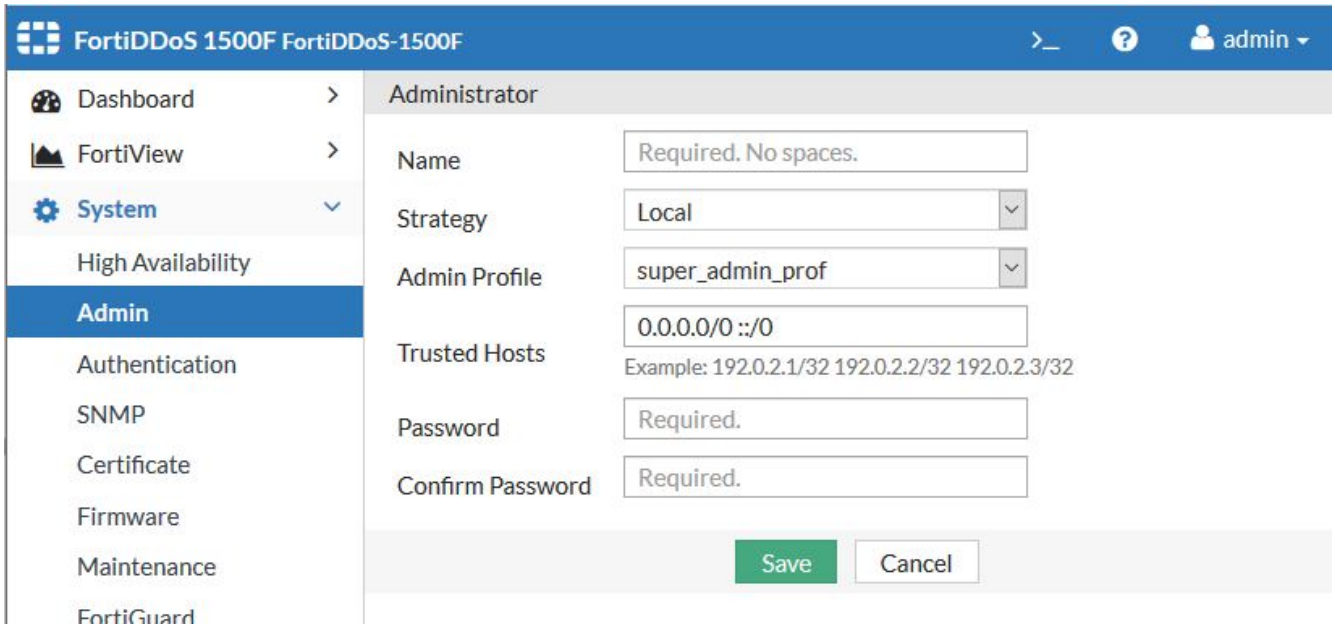
Before you begin:

- You must have Read-Write permission for System settings.

To create administrator users:

1. Go to **System** > **Admin** > **Administrator**.
2. Click **Add** to display the configuration editor.
3. Complete the configuration as described in the table below.
4. Save the configuration.

Administrator user configuration page



Administrator user configuration guidelines

Settings	Guidelines
Name	Name of the administrator account, such as `admin1` or `admin@example.com`, that can be referenced in other parts of the configuration. Do not use spaces or special characters except the 'at' symbol (`@`). The maximum length is 35 characters. If you use LDAP or RADIUS authentication, this is the username stored in the LDAP or RADIUS authentication server. **Note:** This is the user name that the administrator must provide when logging in to the CLI or web UI. If using an external authentication server such as RADIUS or Active Directory, this name will be passed to the server via the remote authentication query.
System Admin	If the user is regarded as a System Administrator with access to all SPPs, select

Settings	Guidelines
	Yes or else click **No**.
Allow API Access	This option will only display if the user is a 'System Admin'. The option allows users to authenticate REST API instructions sent to FortiDDoS. For example, to access Security Fabric information from FortiOS on FortiGate, a matching user/password must exist in both FortiDDoS and FortiGate Security Fabric access.
SPP Admin	**Yes**—Administrator for all SPPs. **No**—Administrator for selected SPPs only. You must have SPPs configured before you can make this selection.
SPP Policy Group	If the user is not a System or SPP Admin, select the **SPP Policy Group** from the drop-down. You must have SPP Polices (subnets) and SPP Policy Groups configured before you can make this selection.
Service Protection Profile	If the user is an SPP Admin, select the SPP profile that the SPP Admin manages.
Strategy	• **Local**—Use the local authentication server. When you use the local authentication server, you also configure a password. • **LDAP**—Authenticate against an LDAP server. When you use LDAP, you do not configure a password. The system authenticates against the username and password stored in the LDAP server. • **RADIUS**—Authenticate against a RADIUS server. When you use RADIUS, you do not configure a password. The system authenticates against the username and password stored in the RADIUS server. • **TACACS+**—Authenticate against a TACACS+ server. When you use TACACS+, you do not configure a password. The system authenticates against the username and password stored in the TACACS+ server.
Admin Profile	Select a user-defined or predefined profile. The predefined profile named **super_admin_prof** is a special access profile used by the **admin** account. However, selecting this access profile will *not* confer all permissions of the **admin** account. For example, the new administrator would not be able to reset lost administrator passwords. **Note**: This option does not appear for the **admin** administrator account, which by definition always uses the **super_admin_prof** access profile.
Password	Type a password for the administrator account. Passwords may have a maximum of 16 characters, may include numbers, upper and lowercase characters, and the following special characters: % ^ & ! @ # $ * _ - < > ( ) = | : ; , / ? **Notes**: • " ? " is not allowed as a special character in the CLI so "?" should not be used for passwords that may be needed for CLI access. • " \ " is not allowed as a special character

Settings	Guidelines
Confirm Password	Type the password again to confirm its spelling.
Trusted Hosts	Source IP address and netmask from which the administrator is allowed to log in. For multiple addresses, separate each entry with a space. You can specify up to three trusted areas. They can be single hosts, subnets, or a mixture. Configuring trusted hosts hardens the security of the system. In addition to knowing the password, an administrator can connect only from the computer or subnets you specify. Trusted host definitions apply both to the web UI and to the CLI when accessed through Telnet, SSH, or the CLI console widget. Local console access is *not* affected by trusted hosts, as the local console is by definition not remote, and does not occur through the network. If ping is enabled, the address you specify here is also a source IP address to which the system will respond when it receives a ping or traceroute signal. To allow logins only from *one* computer, enter only its IP address and 32- or 128-bit netmask:`192.0.2.2/32` `2001:0db8:85a3:::8a2e:0370:7334/128` To allow login attempts from any IP address (not recommended), enter:`0.0.0.0/0.0.0.0`. **Caution:** If you restrict trusted hosts, do so for *all* administrator accounts. Failure to do so means that all accounts are still exposed to the risk of brute force login attacks. This is because if you leave even *one* administrator account unrestricted (i.e. `0.0.0.0/0`), the system must allow login attempts on all network interfaces where remote administrative protocols are enabled, and wait until *after* a login attempt has been received in order to check that user name's trusted hosts list. **Tip:** If you allow login from the Internet, set a longer and more complex password, and enable only secure administrative access protocols. We also recommend that you restrict trusted hosts to IPs in your administrator's geographical area. **Tip:** For improved security, restrict all trusted host addresses to single IP addresses of computer(s) from which *only* this administrator will log in.

CLI commands:

```
config system admin
edit admin
set access-profile super_admin_prof
next
edit admin-spp1
set is-system-admin no
set domain SPP-1
set password ENC $1$0b721b38$vk7GoO147JXXqy5B3ag8z/
set access-profile admin
end
```

Changing user passwords

By default, this administrator account has the password `fortinet`. Set a strong password for the `admin` administrator account. Change the password regularly.

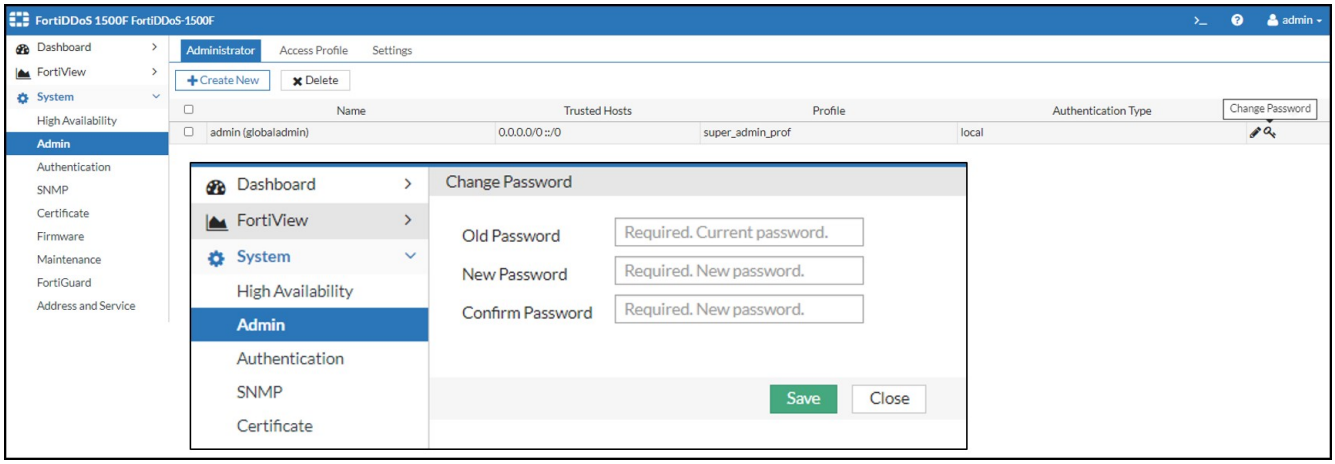
Before you begin:

- You must have Read-Write permission for System settings.

To change the password:

1. Go to **System** > **Admin** > **Administrator**.
2. Click **Change Password** icon.
3. Complete the configuration as described in the table below.
4. Save the configuration.

Administrator settings page



Password configuration

Settings	Guidelines
Old Password	Type the current password.
New Password	Type a password for the administrator account. Passwords may have a maximum of 16 characters, may include numbers, upper and lowercase characters, and the following special characters: _ (underscore), - (hyphen), !, @, #, $, %, ^, &, *
Confirm Password	Type the password again to confirm its spelling.

CLI commands:

```
config system admin
edit <any-username>
set password <new-password_str>
end
```

Configuring administration settings

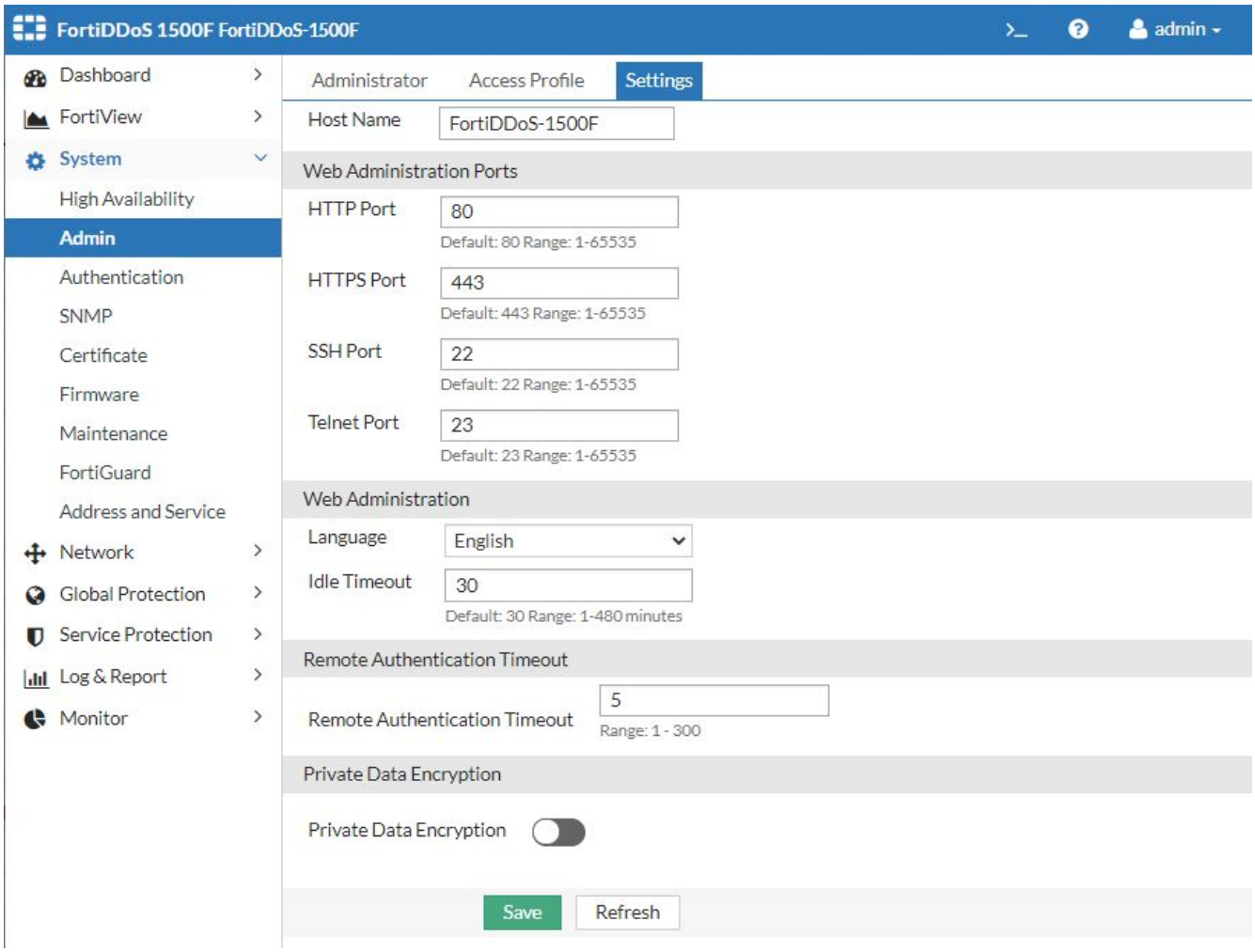
Before you begin:

- You must have Read-Write permission for System settings.

To change the administration settings:

1. Go to **System** > **Admin** > **Settings**.
2. Complete the configuration as described in the table below.
3. Save the configuration.

Administration settings page



Administration settings guidelines

Settings	Guidelines
Web Administration Ports	
HTTP Port	**HTTP is not supported. Any traffic directed to the HTTP Port set here or to HTTP Port 80 will be redirected to the HTTPS port.**
Telnet Port	Specify the port for the Telnet service. Usually, Telnet uses port 23.
SSH Port	Specify the port for the SSH service. Usually, SSH uses port 22.
Web Administration	
Language	Language of the web UI. • English • Simplified Chinese

Settings	Guidelines
	• Korean • Japanese • Spanish • Portuguese List of languages are not fully supported in 6.x.x. Fuller translations will be added in the future. **Note:** This setting does *not* affect the display of the CLI.
Idle Timeout	Number of minutes that a web UI connection can be idle before the administrator must log in again. The maximum is 480 minutes (8 hours). The default is 30 minutes.
Remote Authentication Timeout	When using slow servers or authentication proxies, it may be necessary to lengthen the time FortiDDoS waits for a response. Default is 5 seconds with range of 1 – 300 seconds.
Private Data Encryption	The FortiDDoS Administrator can create a private encryption Key to replace the default static key used by Fortinet for external API credentials like RADIUS and REST API. If after creating and using the Key, the Administrator disables it, the system will re-encrypt credentials with its default key. **Note**: This key will not be seen in the Configuration File. **HA Deployments:** Private Key on Primary and Secondary should be exactly same. It will not be synced automatically. Any Changes to Private Key Encryption should be done in standalone mode. To create this key: Enable Private Data Encryption Enter a 32-character hexadecimal number (0-9, a-f?) in the Private Data Encryption Key field Save the page

Login lockout

To protect from intrusion attempts, the system temporarily blocks the Source IP of any user who makes five failed login attempts. The login page will display 'IP has been blocked'. The user may try to login again in few minutes.

Configuring RADIUS authentication

You can configure administrator authentication using a Remote Authentication Dial-In User Service (RADIUS) server.

After you complete the RADIUS server configuration and enable it, you can select it when you create an administrator user on the System > Admin > Administrator page. When RADIUS is selected, no local password option is available. You also specify the SPP or SPP Policy Group assignment, trusted host list, and access profile for that user.

If RADIUS is enabled, when a user logs in, an authentication request is made to the remote RADIUS server. If authentication succeeds, and the user has a configuration on the System > Admin > Administrator page, the SPP or SPP Policy Group assignment, trusted host list, and access profile are applied. If the user does not have a configuration on the System > Admin > Administrator page, these assignments are obtained from the Default Access Strategy settings described below.

If your RADIUS server supports Two-Factor Authentication (2FA), from Release 5.1.0, FortiDDoS will display a field for entry of the 2FA token, after your credentials have been entered.

You may adjust the time FortiDDoS waits for a response from your RADIUS server or authentication proxy in System > Admin > Settings tab.

Before you begin:

- You must have Read-Write permission for System settings.

To configure a RADIUS server:

1. Go to **System** > **Authentication** > **RADIUS**.
2. Complete the configuration as described in the table below.
3. Save the configuration.

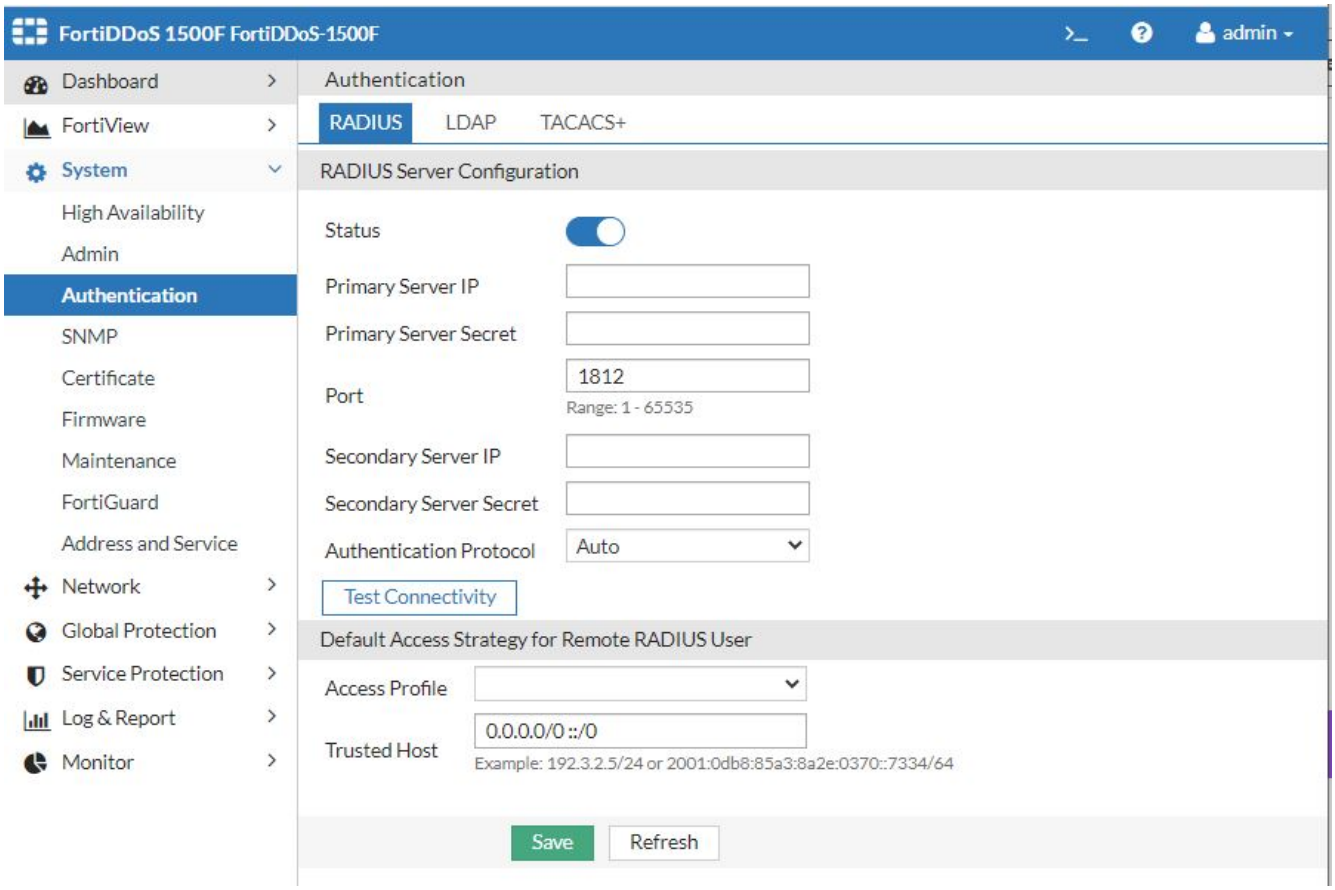
RADIUS server settings

Settings	Guidelines
Status	Select to enable RADIUS server configuration or deselect to disable.
Primary Server Name/IP	IP address or FQDN of the primary RADIUS server.
Primary Server Secret	RADIUS server shared secret – maximum 116 characters (special characters are allowed).
Secondary Server Name/IP	Optional. IP address or FQDN of a backup RADIUS server.
Secondary Server Secret	Optional. RADIUS server shared secret – maximum 116 characters (special characters are allowed).
Port	RADIUS port. Usually, this is 1812.
Authentication Protocol	• Auto—If you leave this default value, the system uses MSCHAP2. • PAP—Password Authentication Protocol • CHAP—Challenge Handshake Authentication Protocol (defined in RFC 1994) • MSCHAP—Microsoft CHAP (defined in RFC 2433) • MSCHAP2—Microsoft CHAP version 2 (defined in RFC 2759)
Test Connectivity	
Test Connectivity	Select to test connectivity using a test username and password specified next. Click the **Test** button before you save the configuration.

Settings	Guidelines
Username	Username for the connectivity test.
Password	Corresponding password.
Default Access Strategy for remote RADIUS user	
Is System Admin	If the user is regarded as a System Administrator with access to all SPPs, select **Yes** or else click **No**.
Is SPP Admin	This option is available only if **Is System Admin** is set to 'No'. **Yes** - Administrator for only one SPP. **No** - Neither system admin nor admin to SPP. Administrator for specific policy group.
Default SPP Policy Group	If the user is not a System or SPP Admin, select the **Default SPP Policy Group** from the drop-down. You must have SPP Polices (subnets) and SPP Policy Groups configured before you can make this selection.
Service Protection Profile	If the user is an SPP Admin, select the SPP profile that the SPP Admin manages.
Trusted Hosts	Source IP address and netmask from which the administrator is allowed to log in. For multiple addresses, separate each entry with a space. You can specify up to three trusted areas. They can be single hosts, subnets, or a mixture. Configuring trusted hosts hardens the security of the system. In addition to knowing the password, an administrator can connect only from the computer or subnets you specify. Trusted host definitions apply both to the web UI and to the CLI when accessed through Telnet, SSH, or the CLI console widget. Local console access is *not* affected by trusted hosts, as the local console is by definition not remote, and does not occur through the network. If ping is enabled, the address you specify here is also a source IP address to which the system will respond when it receives a ping or traceroute signal. To allow logins only from *one* computer, enter only its IP address and 32- or 128-bit netmask:`192.0.2.2/32` `2001:0db8:85a3:::8a2e:0370:7334/128` To allow login attempts from any IP address (not recommended), enter:`0.0.0.0/0.0.0.0`. **Caution:** If you restrict trusted hosts, do so for *all* administrator accounts. Failure to do so means that all accounts are still exposed to the risk of brute force login attacks. This is because if you leave even *one* administrator account unrestricted (i.e. `0.0.0.0/0`), the system must allow login attempts on all network interfaces where remote administrative protocols are enabled, and wait until *after* a login attempt has been received in order to check that user name's trusted hosts list. **Tip:** If you allow login from the Internet, set a longer and more complex password, and enable only secure administrative access protocols. We also recommend that you restrict

Settings	Guidelines
	trusted hosts to IPs in your administrator's geographical area. **Tip:** For improved security, restrict all trusted host addresses to single IP addresses of computer(s) from which *only* this administrator will log in.
Access Profile	Select a user-defined or predefined profile. The predefined profile named **super_admin_prof** is a special access profile used by the **admin** account. However, selecting this access profile will *not* confer all permissions of the **admin** account. For example, the new administrator would not be able to reset lost administrator passwords. **Note**: This option does not appear for the **admin** administrator account, which by definition always uses the **super_admin_prof** access profile.

RADIUS server configuration page



RADIUS server configuration guidelines

```
config system authentication radius
  set state {enable|disable}
  set primary-server <ip|domain>
  set primary-secret <string>
  set backup-server <ip|domain>
  set backup-secret <string>
  set port <port>
  set authprot {auto|chap|mschap|mschapv|pap}
  set is-system-admin {yes|no}
  set is-spp-admin {yes|no}
  set dft-domain <SPP>
  set dft-accprofile <profile>
  set dft-trusted-hosts <CIDR list>
end
```

FortiDDoS Vendor Specific Attributes (VSA)

Release 4.5.0 onwards includes the following VSAs for MSSP feature. Release 4.4.2 and earlier included the first three VSAs.

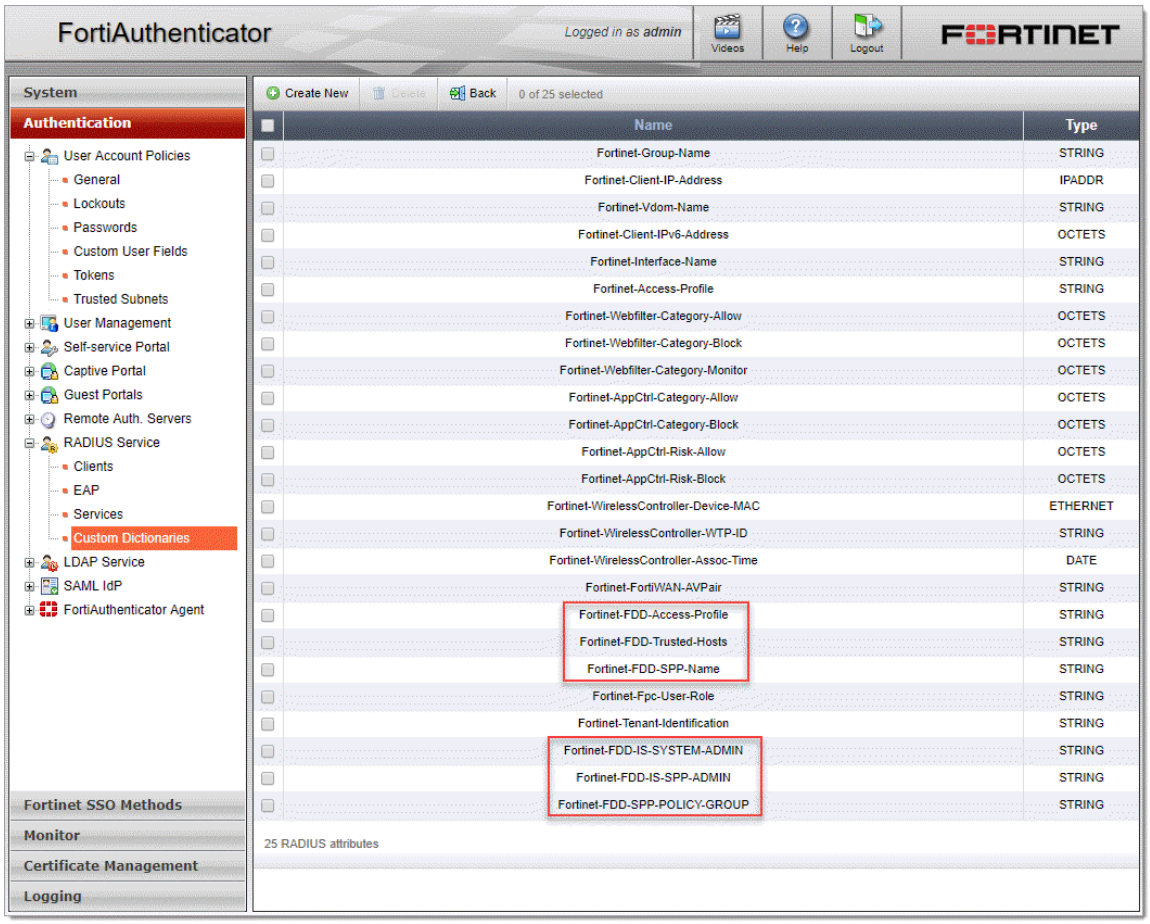
VSA	Number	Value
ATTRIBUTE Fortinet-FDD-Access-Profile	30	User-defined or predefined profile.
ATTRIBUTE Fortinet-FDD-Trusted-Hosts	31	The Source IP address and netmask from which the administrator is allowed to log in.
ATTRIBUTE Fortinet-FDD-SPP-Name	32	Name of the SPP profile that the SPP Admin manages.
ATTRIBUTE Fortinet-FDD-IS-SYSTEM-ADMIN	33	System Administrator with access to all SPPs.
ATTRIBUTE Fortinet-FDD-IS-SPP-ADMIN	34	Administrator for all SPPs or else Administrator for selected SPPs only.
ATTRIBUTE Fortinet-FDD-SPP-POLICY-GROUP	35	User profile with access to the graphs and reports specific to a SPP policy group.

Configuring FortiAuthenticator for FDDoS Radius Authentication

Follow the steps below to configure FortiAuthenticator for FDDoS Radius Authentication:

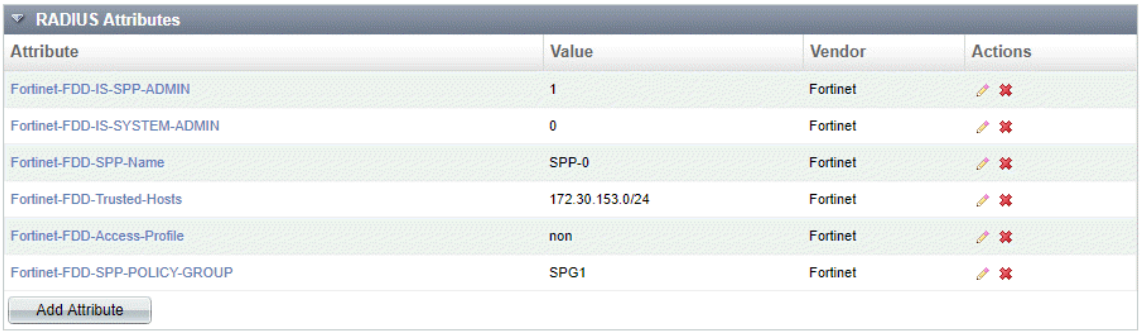
1. Log in to FortiAuthenticator.
2. Go to Authentication > RADIUS Service > Clients.
3. Click **Create New**.
4. Enter the following information:
   a. **Name** - Radius client name
   b. **Client address** - IP/Hostname, Subnet or Range of the client
   c. **Secret** - secret code for authentication between FortiAuthenticator and FortiDDoS

5. Click **OK**.
6. Go to Authentication > RADIUS Service > Custom Dictionaries and click **FortiDDoS**.
7. Ensure that all FortiDDoS VSAs are available in the list.



8. Go to Authentication > User Management > Local Users.
9. Click **Create New** to create a new local user.
   a. Enter a **username**.
   b. Select a **Password creation** from the available options:
      - Set and email a random password
      - No password, FortiToken authentication only
10. Select **Allow RADIUS authentication** and click **OK**.
11. Select the **RADIUS Attributes** drop-down and click **Add Attribute** to create new user RADIUS attributes.
12. Enter the following information to add each FortiDDoS VSA:
    a. **Vendor**: Select **Fortinet** from the drop-down.
    b. **Attribute ID**: Select the FortiDDoS VSA from the drop-down.
    c. **Value**: Enter the value based on the FortiDDoS VSA selected.

13. Repeat Step 11 until all FortiDDoS VSAs are added.



14. Click **OK**.

Configuring LDAP authentication

You can configure administrator authentication against a Lightweight Directory Access Protocol (LDAP) server.

After you have completed the LDAP server configuration and enabled it, you can select it when you create an administrator user on the **System** > **Admin** > **Administrators** page. On that page, you can specify the username but not the password. You can also specify the SPP assignment, trusted host list, and access profile for that user.

If LDAP is enabled, when a user logs in, an authentication request is made to the remote LDAP server. If authentication succeeds, and the user has a configuration on the **System** > **Admin** > **Administrators** page, the SPP assignment, trusted host list, and access profile are applied. If the user does not have a configuration on the **System** > **Admin** > **Administrators** page, these assignments are obtained from the **Default Access Strategy** settings described in LDAP server configuration guidelines table.

Before you begin:

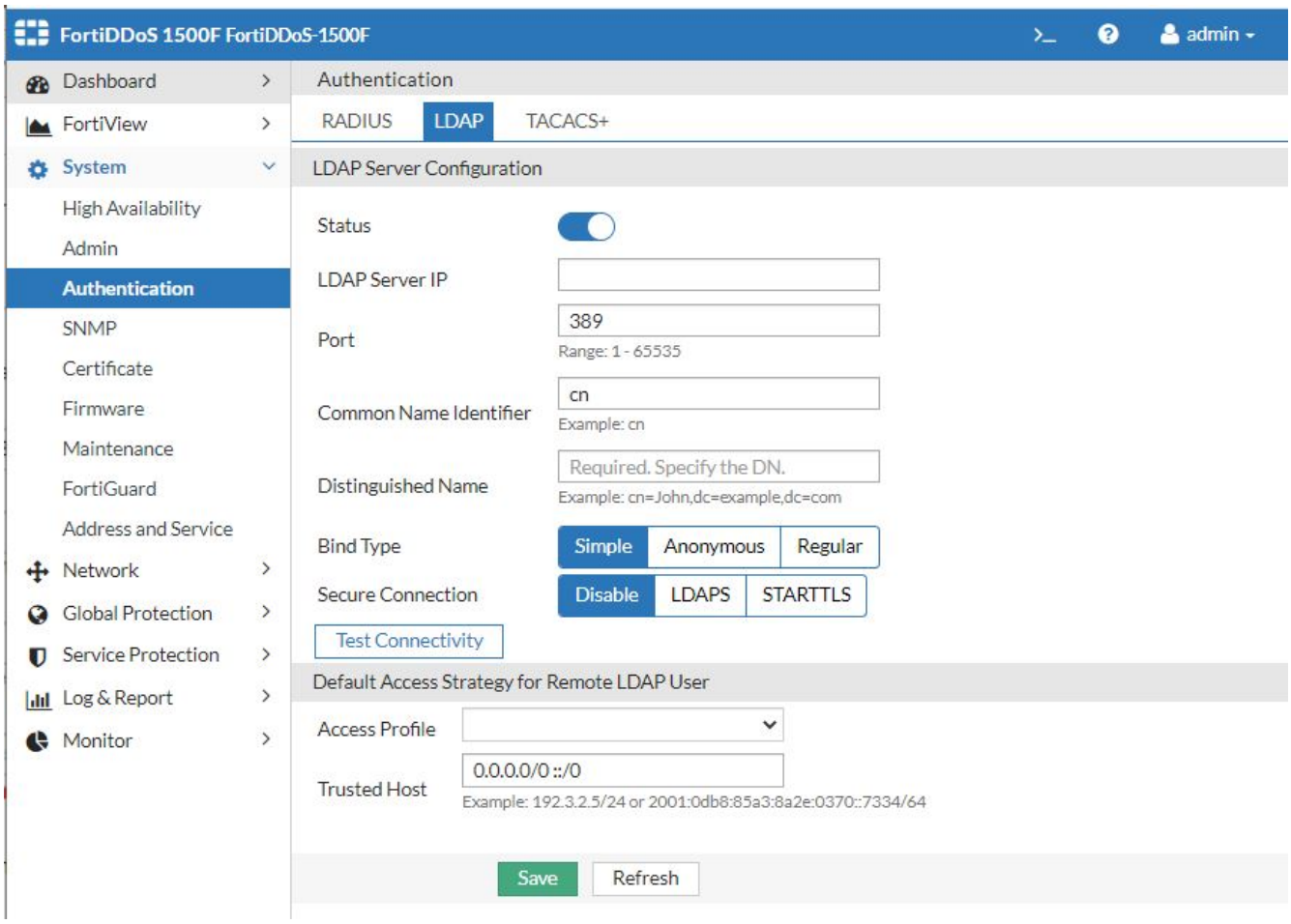
- You must have Read-Write permission for System settings.
- You must work with your LDAP administrator to determine an appropriate DN for FortiDDoS access. The LDAP administrator might need to provision a special group.

To configure an LDAP server:

1. Go to **System** > **Authentication** > **LDAP**.
2. Complete the configuration as described in the table below.
3. Save the configuration.

Note: Using the **Test Connectivity** button with incorrectly-configured LDAP settings will result in a long period without a response. Configure LDAP carefully.

LDAP server configuration page



LDAP configuration guidelines

Settings	Guidelines
Enable	Unique name. No spaces or special characters.
LDAP Server Name/IP	IP address of the LDAP server.
Port	LDAP port. Default is TCP 389 for LDAP and STARTTLS, and TCP 636 for LDAPS. **Note**: FortiDDoS does not support CLDAP over UDP.
Common Name Identifier	Common name (cn) attribute for the LDAP record. For example: `cn` or `uid`.
Distinguished Name	Distinguished name (dn) attribute for the LDAP record. The dn uniquely identifies a user in the LDAP directory. For example: `cn=John%20Doe,dc=example,dc=com` Most likely, you must work with your LDAP administrator to know the appropriate DN to use for FortiDDoS access. The LDAP administrator might need to provision a special group.

Settings	Guidelines
Bind Type	Select the Bind Type: • **Simple** - bind without user search. It can be used only if all the users belong to the same 'branch'. • **Anonymous** - bind with user search. It can be used when users are in different 'branches' and only if the server allows 'anonymous search'. • **Regular** - bind with user search. It can be used when users are in different 'branches' and the server does not allow 'anonymous search'.
User DN	Enter the user Distinguished Name. (Available only when Bind Type is 'Regular'.)
Password	Enter the password for the user. (Available only when Bind Type is 'Regular'.)
Secure	Select the Secure type: • Disable • LDAPS • STARTTLS LDAP over SSL (LDAPS) and StartTLS are used to encrypt LDAP messages in the authentication process. LDAPS is a mechanism for establishing an encrypted SSL/TLS connection for LDAP. It requires the use of a separate port, commonly 636. StartTLS extended operation is LDAPv3 standard mechanism for enabling TLS (SSL) data confidentiality protection. The mechanism uses an LDAPv3 extended operation to establish an encrypted SSL/TLS connection within an already established LDAP connection.

Settings	Guidelines
Trusted Hosts	Source IP address and netmask from which the administrator is allowed to log in. For multiple addresses, separate each entry with a space. You can specify up to three trusted areas. They can be single hosts, subnets, or a mixture. Configuring trusted hosts hardens the security of the system. In addition to knowing the password, an administrator can connect only from the computer or subnets you specify. Trusted host definitions apply both to the web UI and to the CLI when accessed through Telnet, SSH, or the CLI console widget. Local console access is *not* affected by trusted hosts, as the local console is by definition not remote, and does not occur through the network. If ping is enabled, the address you specify here is also a source IP address to which the system will respond when it receives a ping or traceroute signal. To allow logins only from *one* computer, enter only its IP address and 32- or 128-bit netmask:`192.0.2.2/32` and/or `2001:0db8:85a3:::8a2e:0370:7334/128` To allow login attempts from any IP address (not recommended), enter `0.0.0.0/0` and/or `::/0` **Caution:** If you restrict trusted hosts, do so for *all* administrator accounts. Failure to do so means that all accounts are still exposed to the risk of brute force login attacks. This is because if you leave even *one* administrator account unrestricted (i.e. `0.0.0.0/0`), the system must allow login attempts on all network interfaces where remote administrative protocols are enabled, and wait until *after* a login attempt has been received in order to check that user name's trusted hosts list. **Tip:** If you allow login from the Internet, set a longer and more complex password, and enable only secure administrative access protocols. We also recommend that you restrict trusted hosts to IPs in your administrator's geographical area. **Tip:** For improved security, restrict all trusted host addresses to single IP addresses of computer(s) from which *only* this administrator will log in.
Access Profile	Select a user-defined or predefined profile. The predefined profile named **super_admin_prof** is a special access profile used by the **admin** account. However, selecting this access profile will *not* confer all permissions of the **admin** account. For example, the new administrator would not be able to reset lost administrator passwords. **Note**: This option does not appear for the **admin** administrator account, which by definition always uses the **super_admin_prof** access profile.
Test Connectivity	
Test Connectivity	Select to test connectivity using a test username and password specified next. Click the **Test** button after you have saved the configuration.

Settings	Guidelines
Username	Username for the connectivity test.
Password	Corresponding password.

Note: FortiDDoS GUI may become unresponsive if any of the above configuration values (LDAP Server Configuration or Test Connectivity) are incorrect. In this case, refresh the browser to reconnect to the GUI.

To configure LDAP authentication using the CLI:

```
config system central authentication LDAP
  set state enable
  set server 172.30.153.101
  set cnid uid
  set dn ou=users,dc=fddos,dc=com
  set is-system-admin yes
  set dft-accprofile super_admin_prof
  set bind-type regular
  set User-DN cn=admin,dc=fddos,dc=com
  set password ENC
bfLKhxF2uEdh/uTVjeFaBHd5HuPxBLzeAdPW8yuziQd2lSL3ii2+tKae3P9HGACj9CxAbw9jR/h4QI+x4K
gCDcpsFWf9LlOZRmIIMSbCIipQo
end
```

If you initially set is-system-admin to 'no', but later want to change, you must first change dft-domain to SPP-0 and commit it. Then configure the system admin setting.
For example:

```
config system authentication LDAP
  set dft-domain SPP-0
end
config system authentication LDAP
  set is-system-admin yes
end
```

Configuring TACACS+ authentication

You can configure administrator authentication using a Terminal Access Controller Access-Control System Plus (TACACS+) server.

Once you complete the TACACS+ server configuration, create an administrator user under System > Admin > Administrator page and select 'TACACS+' as the **Strategy**. When 'TACACS+' is selected, no local password option is available. You can also specify the SPP or SPP Policy Group assignment, access profile and trusted host list for that user. For more details about creating a user profile, see here.

If TACACS+ is enabled, when a user logs in, an authentication request is made to the remote TACACS+ server.

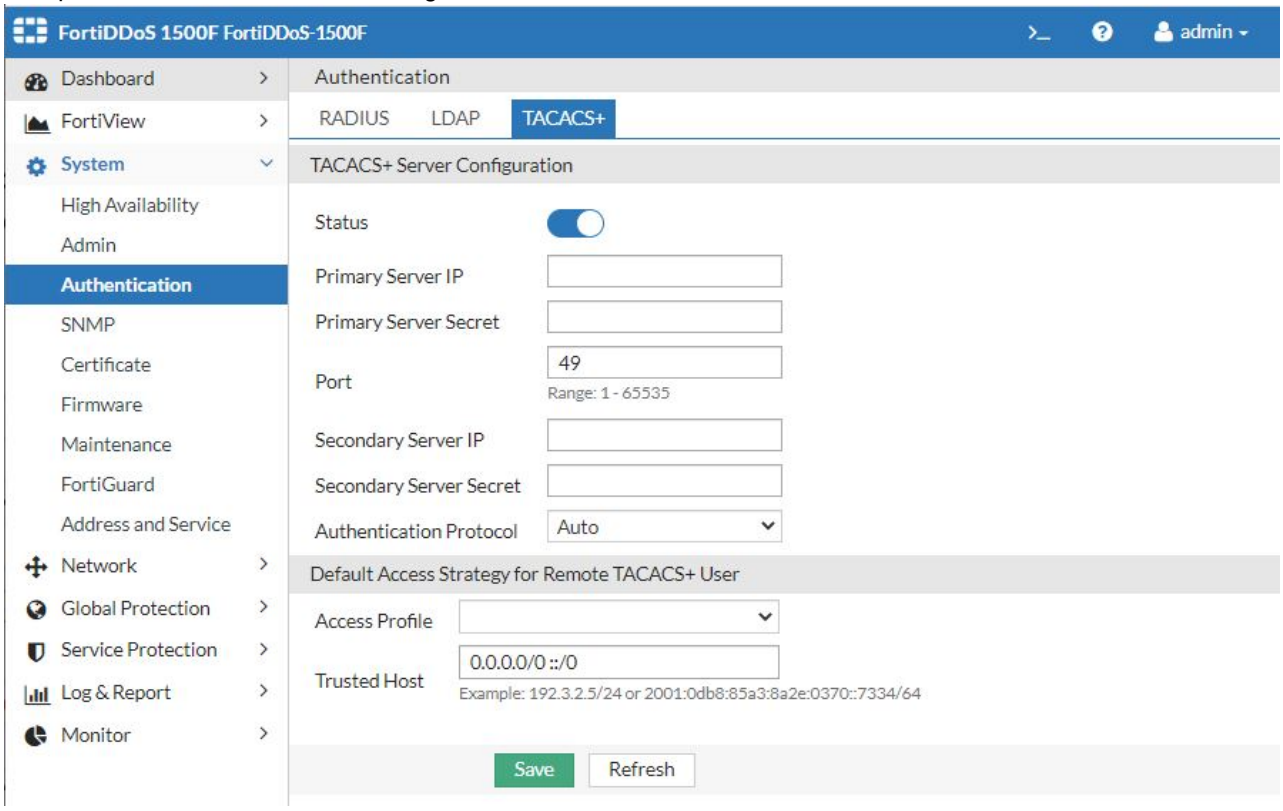
If authentication succeeds, and the user has a configuration on the System > Admin > Administrator page, the SPP or SPP Policy Group assignment, access profile and trusted host list are applied. If the user does not have a configuration on the Administrator page, an authorization request will be sent to TACACS+ server. If the Authorization response contains attribute value pairs except 'service=fortiddos', user will be logged in as per the policy defined in attribute value pairs, otherwise the user will be logged in as per assignments obtained from the 'Default Access Strategy' settings described in Step 3.

Before you begin:

- You must have Read-Write permission for System settings.

To configure FortiDDoS for TACACS+ authentication:

1. Go to **System** > **Authentication** > **TACACS+**.
2. Complete the 'TACACS+ Server Configuration'



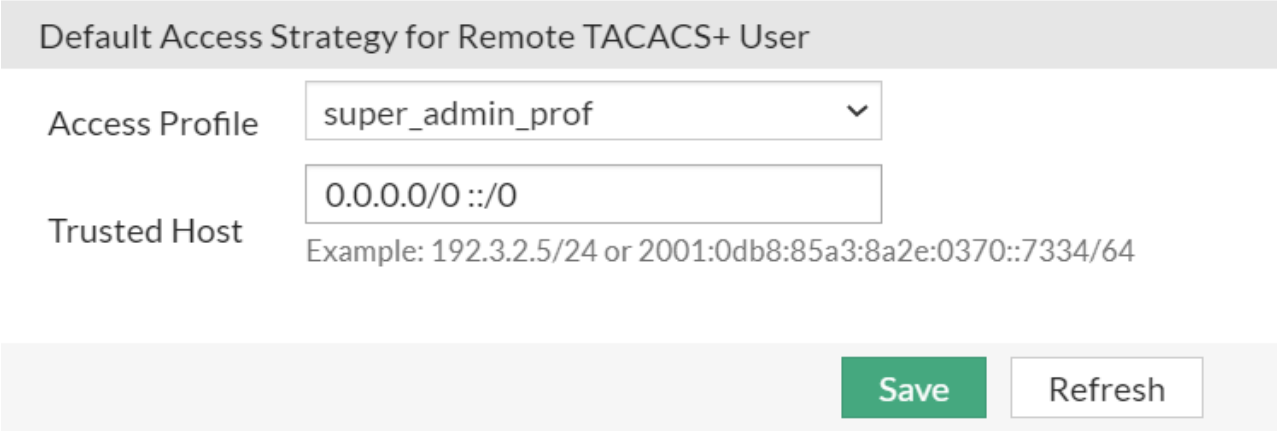
Settings	Guidelines
Status	Select to enable TACACS+ server configuration or deselect to disable.
Primary Server IP	IP address or FQDN of the primary TACACS+ server.
Primary Server Secret	TACACS+ server shared secret – maximum 116 characters (special characters are allowed).
Port	TACACS+ port number in the range: 1 - 65535. The default value is 49.

Settings	Guidelines
Secondary Server IP	(Optional) IP address or FQDN of a backup TACACS+ server.
Secondary Server Secret	(Optional) TACACS+ server shared secret – maximum 116 characters (special characters are allowed).
Authentication Protocol	• PAP - Password Authentication Protocol • CHAP - Challenge Handshake Authentication Protocol (defined in RFC 1994) • ASCII • Auto - Automatically selects one of the above protocols.

Settings	Guidelines
Trusted Hosts	Source IP address and netmask from which the administrator is allowed to log in. For multiple addresses, separate each entry with a space. You can specify up to three trusted areas. They can be single hosts, subnets, or a mixture. Configuring trusted hosts hardens the security of the system. In addition to knowing the password, an administrator can connect only from the computer or subnets you specify. Trusted host definitions apply both to the web UI and to the CLI when accessed through Telnet, SSH, or the CLI console widget. Local console access is *not* affected by trusted hosts, as the local console is by definition not remote, and does not occur through the network. If ping is enabled, the address you specify here is also a source IP address to which the system will respond when it receives a ping or traceroute signal. To allow logins only from *one* computer, enter only its IP address and 32- or 128-bit netmask:`192.0.2.2/32` `2001:0db8:85a3:::8a2e:0370:7334/128` To allow login attempts from any IP address (not recommended), enter:`0.0.0.0/0.0.0.0`. **Caution:** If you restrict trusted hosts, do so for *all* administrator accounts. Failure to do so means that all accounts are still exposed to the risk of brute force login attacks. This is because if you leave even *one* administrator account unrestricted (i.e. `0.0.0.0/0`), the system must allow login attempts on all network interfaces where remote administrative protocols are enabled, and wait until *after* a login attempt has been received in order to check that user name's trusted hosts list. **Tip:** If you allow login from the Internet, set a longer and more complex password, and enable only secure administrative access protocols. We also recommend that you restrict trusted hosts to IPs in your administrator's geographical area. **Tip:** For improved security, restrict all trusted host addresses to single IP addresses of computer(s) from which *only* this administrator will log in.

Settings	Guidelines
Access profile	Select a user-defined or predefined profile. The predefined profile named **super_admin_prof** is a special access profile used by the **admin** account. However, selecting this access profile will *not* confer all permissions of the **admin** account. For example, the new administrator would not be able to reset lost administrator passwords. **Note**: This option does not appear for the **admin** administrator account, which by definition always uses the **super_admin_prof** access profile.
Test Connectivity	
Test Connectivity	Select to test connectivity using a test username and password specified next. Click the **Test** button after you have saved the configuration.
Username	User name for the connectivity test.
Password	Corresponding password.

3. Complete the 'Default Access Strategy for remote TACACS+ user' with reference to the figure/table below.



4. Save the configuration.

CLI commands:

```
config system authentication tacacs+
  set state {enable|disable}
  set primary-server <ip|domain>
  set primary-secret <string>
  set port <port>
  set backup-server <ip|domain>
  set backup-secret <string>
  set authprot {pap|chap|ascii|auto}
  set is-system-admin {yes|no}
  set is-spp-admin {yes|no}
  set dft-domain <SPP>
  set dft-accprofile <profile>
  set dft-trusted-hosts <CIDR list>
end
```

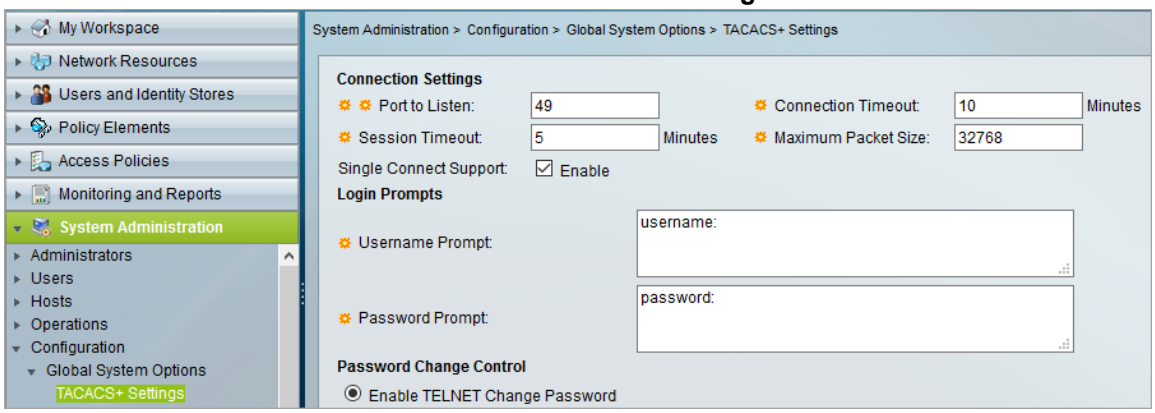
Configuring Cisco Secure ACS for FortiDDoS TACACS+ authentication

Log in to Cisco Secure Access Control System and follow the steps below.

Note: For more information about the settings under each tab, click **Help** on the top-right corner of the UI.

Step 1: Verify TACACS+ Configuration

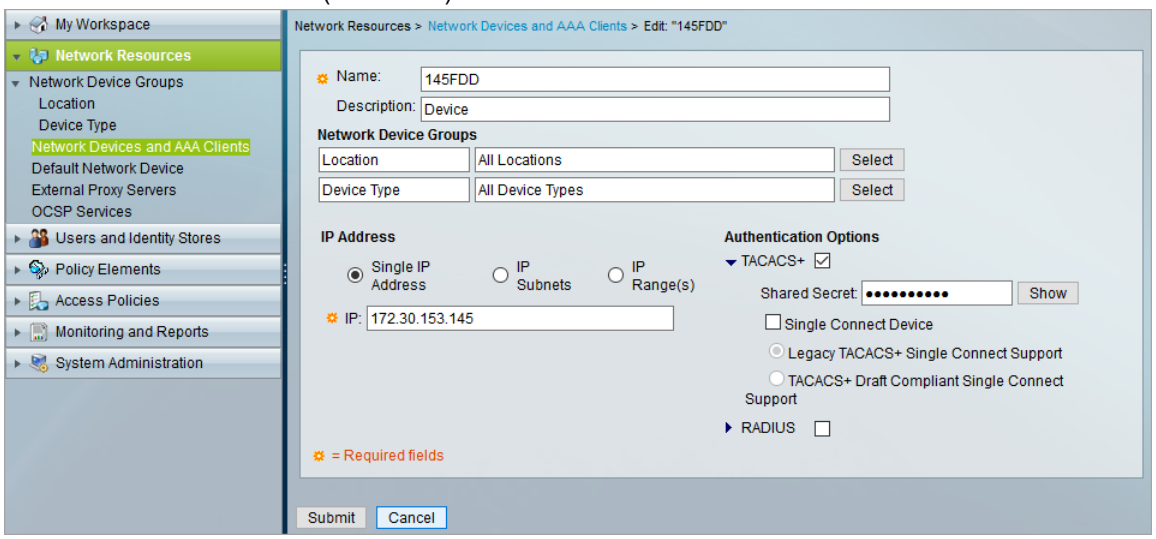
1. Go to **System Administration** > **Configuration** > **Global System Options** > **TACACS+ Settings**.
2. Check whether the **Port to Listen** field under **Connection Settings** is set to '49'.



Step 2: Add the Client (FortiDDoS)

1. Go to **Network Resources** > **Network Devices and AAA Clients**.

2. Click **Create** to add TACACS+ clients (FortiDDoS).
   FortiDDoS is a client to ACS (TACACS+) server.

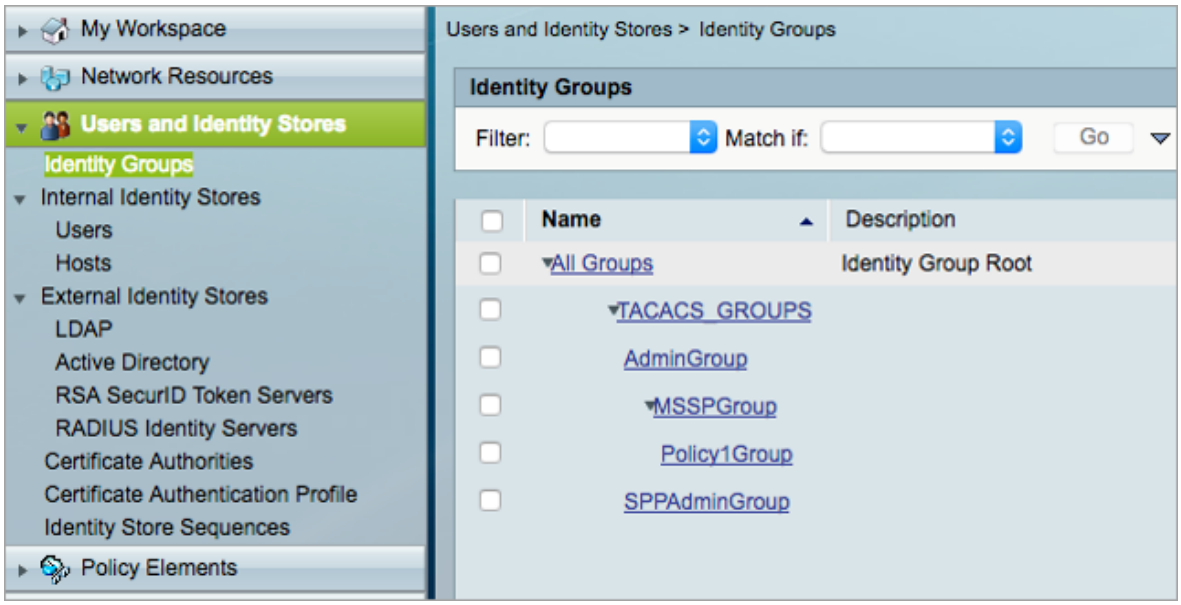


3. Enter the **Name**, **Description**, **Network Device Groups** and **IP Address** of FortiDDoS device.
4. Select 'TACACS+' under **Authentication Options** and enter a **Shared Secret**.
5. Click **Submit**.

Step 3: Create User Groups

User groups are created to associate a group of users to certain TACACS+ VSA policies.

1. Go to **Users and Identity Stores** > **Identity Groups**.
2. Click **Create** and create the user groups.

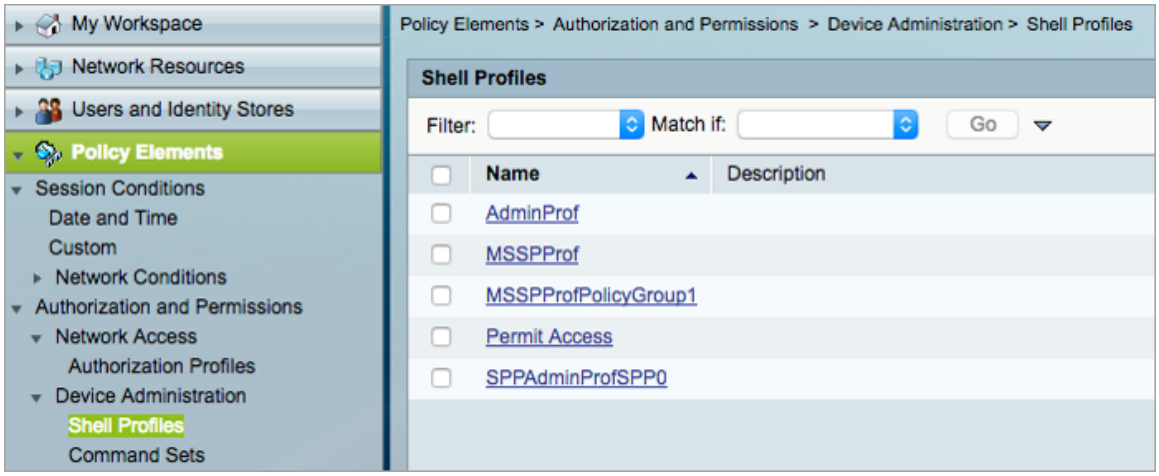


3. Click **Submit**.

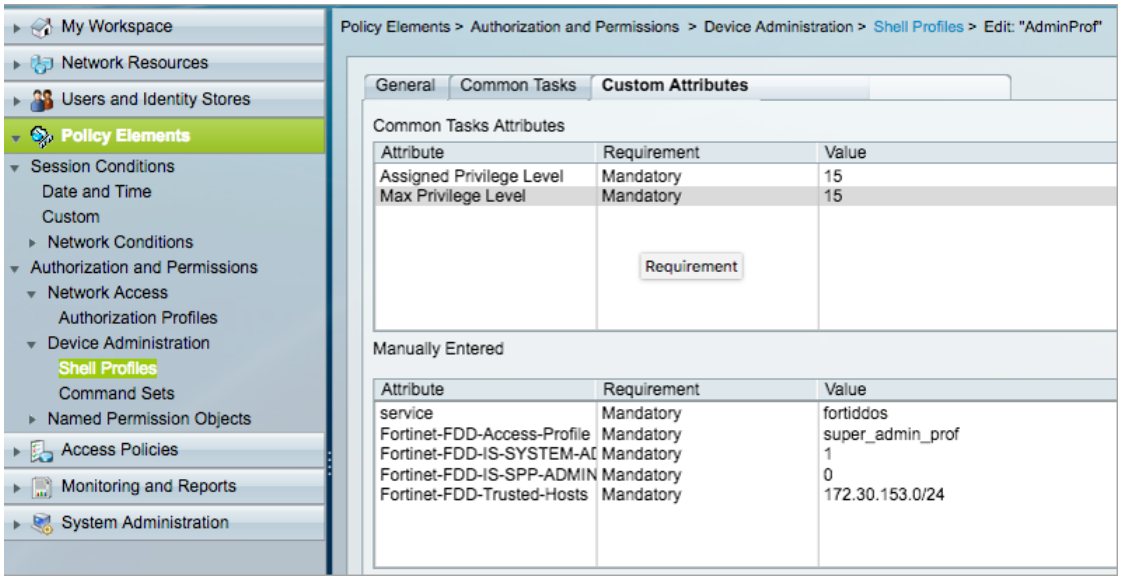
Step 4: Create ACS Shell Profiles

Shell profiles are configured to hold certain VSAs which the Administrator wants to associate with a user or group of users.

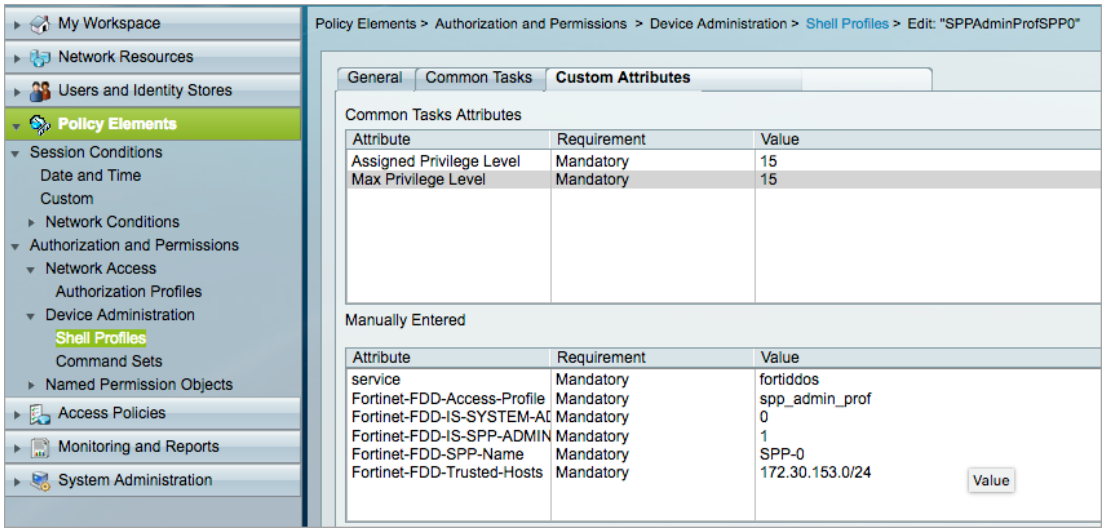
1. Go to **Policy Elements** > **Authorization and Permissions** > **Device Administration** > **Shell Profiles**.
2. Click **Create** to create Shell profiles corresponding to the user groups created in Step 3.
3. Under **General** tab, enter the **Name** and **Description** of the Shell profile.



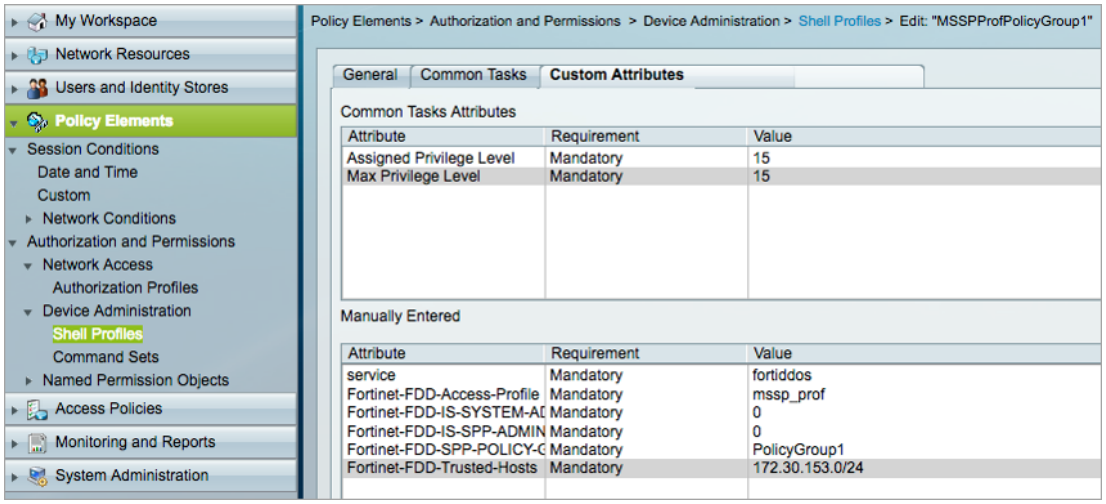
4. Under **Custom Attributes** tab, add the custom attributes based on the Shell profile.
   - **AdminProf**:
     - Fortinet-FDD-Access-Profile: super_admin_prof
     - Fortinet-FDD-IS-SYSTEM-ADMIN: 1
     - Fortinet-FDD-IS-SPP-ADMIN: 0
     - Fortinet-FDD-Trusted-Hosts: 172.30.153.0/24



- **SPPAdminProfSPP0**:
  - Fortinet-FDD-Access-Profile: spp_admin_prof
  - Fortinet-FDD-IS-SYSTEM-ADMIN: 0
  - Fortinet-FDD-IS-SPP-ADMIN: 1
  - Fortinet-FDD-SPP-NAME: SPP-0
  - Fortinet-FDD-Trusted-Hosts: 172.30.153.0/24

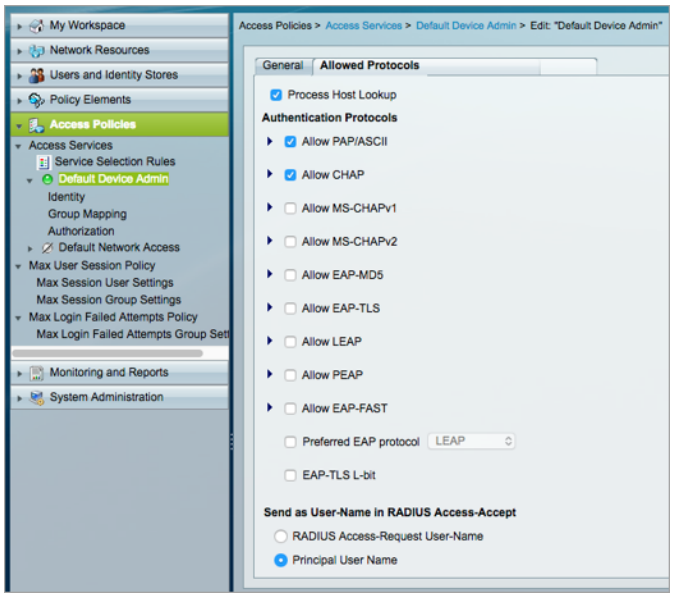


- **MSSPProfPolicyGroup1**:
  - Fortinet-FDD-Access-Profile: mssp_prof
  - Fortinet-FDD-IS-SYSTEM-ADMIN: 0
  - Fortinet-FDD-IS-SPP-ADMIN: 0
  - Fortinet-FDD-SPP-POLICY-GROUP: PolicyGroup1
  - Fortinet-FDD-Trusted-Hosts: 172.30.153.0/24



Step 5: Select the Authentication Protocols

1. Go to **Access Policies** > **Default Network Access** > **Allowed Protocol** tab.
2. Select the Authentication Protocol(s) by checking **Allow PAP/ASCII** and/or **Allow CHAP**. FortiDDoS supports PAP, CHAP and ASCII Protocols.

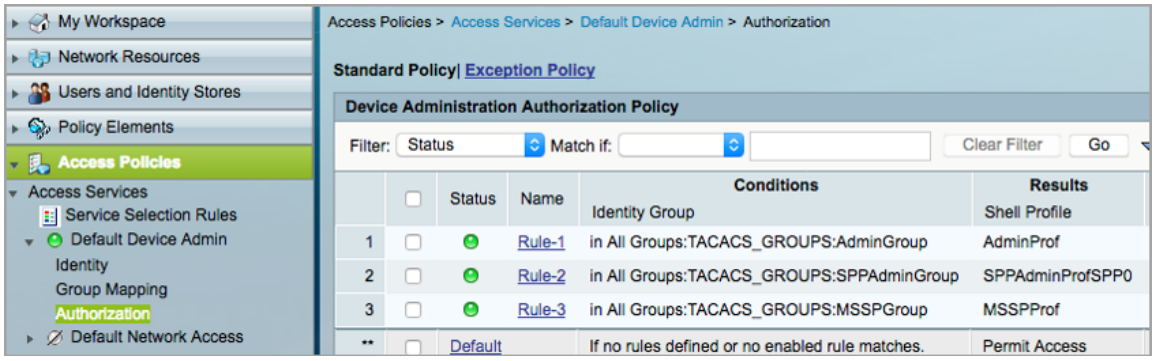


3. Click **Submit**.

Step 6: Associate groups with Shell Profiles

Associating groups with Shell Profiles is an important step providing clear and useful access management technique for Administrators.

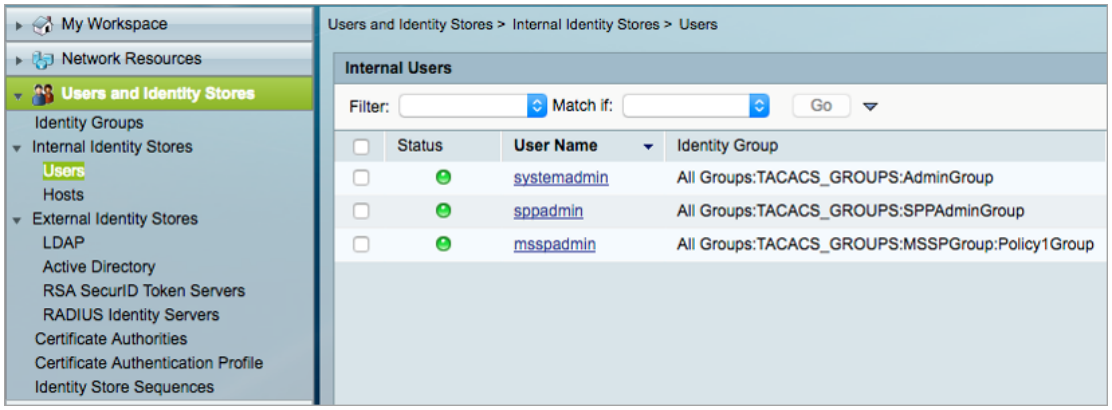
1. Go to **Access Profile** > **Access Services** > **Default Device Admin** > **Authorization** and verify the associated groups.



Step 7: Create users

Create users and add them under certain groups as per their access control decided by the Administrator.

1. Go to **Users and Identity Stores** > **Internal Identity Stores** > **Users**.
2. Click **Create** to add users for Admin group, SPP Admin group and MSSP Admin group.
   - 'systemadmin' for AdminGroup
   - 'sppadmin' for SPPAdminGroup
   - 'msspadmin' for MSSPGroup



You will now be able to log on to the FortiDDoS appliance and get the appropriate authorizations.

Configuring SNMP for remote alarm event trap reporting and MIB queries

An SNMP community is a grouping of equipment for network monitoring purposes. The FortiDDoS-F SNMP agent does not respond to SNMP managers whose query packets do not contain a matching community name. Similarly, trap packets from the FortiDDoS-F agent include community name, and an SNMP manager might not accept the trap if its community name does not match.

Fortinet Technologies Inc. strongly recommends that you do *not* add FortiDDoS-F to the community named `public`. This popular default name is well-known, and attackers that gain access to your network will often try this name first.

This page describes setup of the FortiDDoS SNMP agent for SNMP MIB Queries and alarm Traps. Refer to the list of SNMP traps and conditions.

For setup of Attack Log traps, please refer to **Configuring SNMP trap receivers for remote DDoS attack reporting**.

Test both traps and queries (assuming you have enabled both). Traps and queries typically occur on different port numbers, and therefore verifying one does not necessarily verify that the other is also functional.

To test queries, from your SNMP manager, query the FortiDDoS appliance. To test traps, cause one of the events that should trigger a trap.

Basic steps:

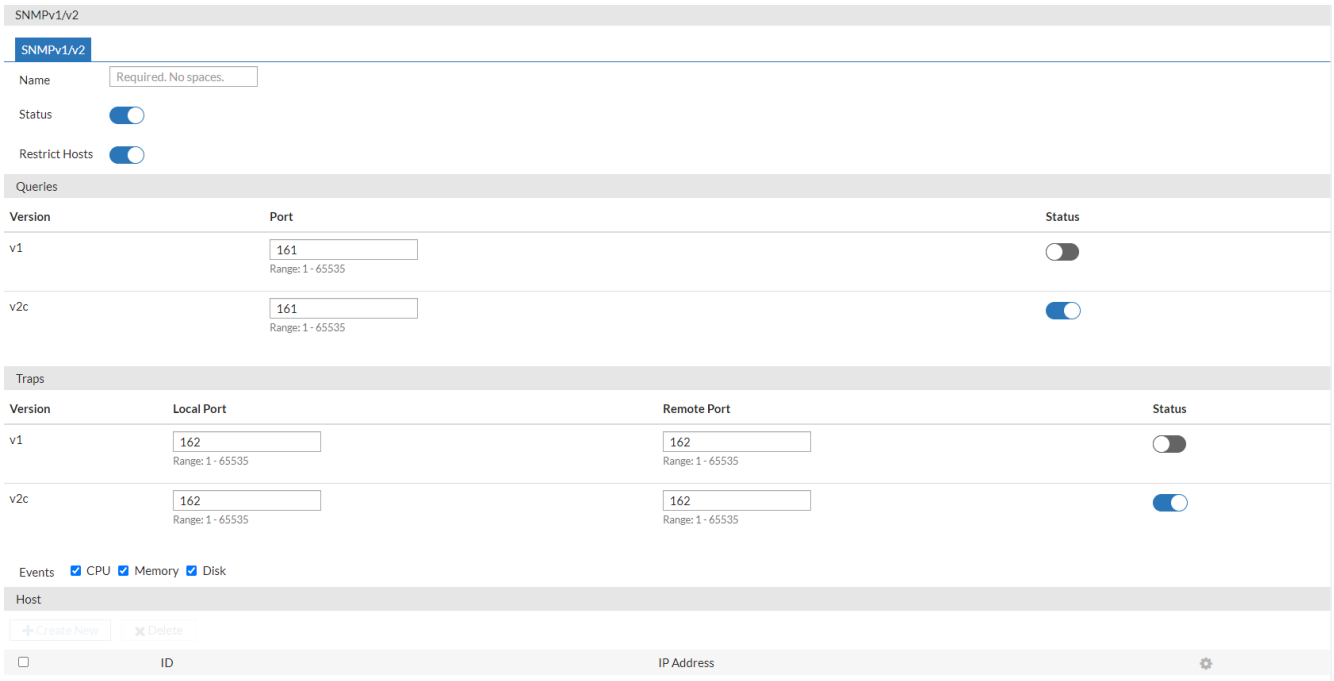
1. Add the Fortinet and FortiDDoS MIBs to your SNMP manager.
   See Appendix C: Management Information Base (MIB).
2. Go to *System* > *SNMP* and configure the SNMP agent and traps for system events.

Before you begin:

- On the SNMP manager, you must verify that the SNMP manager is a member of the community to which the FortiDDoS-F system belongs, and compile the necessary Fortinet Technologies Inc.-proprietary management information blocks (MIBs) and Fortinet Technologies Inc.-supported standard MIBs.
- In the FortiDDoS interface settings, you must enable SNMP access on the network interface through which the SNMP manager connects.
- You must have Read-Write permission for System settings.

To configure SNMP system information:

1. Go to *System* > *SNMP* > *Config* > *Threshold/ SNMPv1v2/SNMPv3*.
2. Complete the configuration as described in the following tables.
3. Save the configuration.



SNMP Threshold settings for system event reporting

Settings	Guidelines
CPU	The system records CPU utilization at the Sample Frequency (default, every 30 seconds) and creates an Alert if the Utilization is over the Trigger threshold (default, 80%) the number of times determined by the Threshold (default, 3 times) within the Sample Period (default 600 seconds) • Trigger—The default is 80% utilization. Minimum = 1% / Maximum = 100%. • Threshold—The default is 3, meaning the event is reported when the condition has been triggered 3 times over the sampling period. Minimum = 1 / Maximum = 960. • Sample Period—The default is 600 seconds. Minimum = 30 seconds / Maximum = 28800 seconds. • Sample Frequency—The default is 30 seconds. Minimum = 30 seconds / Maximum = 100 seconds. **Note**: CPU utilization is for the Management and Reporting Plane CPUs only. All Data Plane processing is done via the TP2 Security Processing Units. TP2 are designed to work to the maximum packet and data rates that can presented on 2x10GE links. The Capacity can be seen on the Dashboard > Data Path Resources table. There are currently no threshold traps for Data Path Resources. In the unlikely event of memory problems Out of Memory attack events will be seen in the Attack Logs.
Memory	The system records Memory utilization at the Sample Frequency (default, every 30 seconds) and creates an Alert if the Utilization is over the Trigger threshold (default, 80%) the number of times

Settings	Guidelines
	determined by the Threshold (default, 3 times) within the Sample Period (default 600 seconds) • Trigger—The default is 80% utilization. Minimum = 1% / Maximum = 100%. • Threshold—The default is 3, meaning the event is reported when the condition has been triggered 3 times over the sampling period. • Sample Period—The default is 600 seconds. Minimum = 30 seconds / Maximum = 28800 seconds. • Sample Frequency—The default is 30 seconds. Minimum = 30 seconds / Maximum = 100 seconds. **Note**: Memory utilization is for the Management and Reporting Plane only. All Data Plane memory is contained in the TP2 Security Processing Units. TP2 are designed to work to the maximum table sizes seen in the Dashboard > Data Path Resources table. There are currently no threshold traps for Data Path Resources. In the unlikely event of memory problems Out of Memory attack events will be seen in the Attack Logs.
Disk (Log disk usage)	The system records Log Disk utilization at the Sample Frequency (default, every 3600 seconds) and creates an Alert if the Utilization is over the Trigger threshold (default, 90%) the number of times determined by the Threshold (default, once) within the Sample Period (default 3600 seconds) • Trigger—The default is 90% utilization. Minimum = 1% / Maximum = 100%. • Threshold—The default is 1, meaning the event is reported each time the condition is triggered. Minimum = 1 / Maximum = 8. • Sample Period—The default is 7200 seconds. Minimum = 3600 seconds / Maximum = 28800 seconds. • Sample Frequency—The default is 3600 seconds. Minimum = 3600 seconds / Maximum = 7200 seconds.

Use similar CLI commands to configure SNMP thresholds:

```
config system snmp threshold
     set cpu 1 1 30 30
     set mem 1 3 30 30
end
```

SNMP Community settings for system event reporting

Settings	Guidelines
Name	Name of the SNMP community to which the FortiDDoS-F system and at least one SNMP manager belongs, such as `management`. You must configure the FortiDDoS-F system to belong to at least one SNMP community so that community's SNMP managers can query system information and receive SNMP traps. You can add up to three SNMP communities. Each community can have a different configuration for queries and traps, and the set of events that

Settings	Guidelines
	trigger a trap. You can also add the IP addresses of up to eight SNMP managers to each community to designate the destination of traps and which IP addresses are permitted to query the FortiDDoS-F system. Name can be up to 35 characters long and contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_).
Status	Select to enable the configuration.
Queries	Port number on which the system listens for SNMP queries from the SNMP managers in this community. The default is 161. Enable queries for SNMP v1, SNMP v2c, or both. SNMP v3 Query settings are available under **User** tab.
Traps	Source (**Local**) port number and destination (**Remote**) port number for trap packets sent to SNMP managers in this community. The default is 162. SNMP v3 Trap settings are available under **User** tab. Enable traps for SNMP v1, SNMP v2c, or both. See SNMP traps and conditions.
SNMP Event	Select to enable SNMP event reporting for the following thresholds: • CPU—CPU usage has exceeded the Threshold set above (default 80%). • Memory—Memory (RAM) usage has exceeded the Threshold set above. • Disk—Disk space usage for the log partition or disk has exceeded the Threshold set above.
Hosts	IP address of the SNMP manager to receive traps and be permitted to query the FortiDDoS system. SNMP managers have read-only access. You can add up to 8 SNMP managers to each community. **Caution:** The system sends security-sensitive traps, which should be sent only over a trusted network, and only to administrative equipment.

To configure SNMPv1/v2 with CLI:

```
config system snmp community
    edit 1
        set name public
        set status enable
        set queryv1-status enable
        set trapv1-status enable
        config host
            edit 1
                set ip <ip address>
            next
            edit 2
                set ip <ip address>
            next
        end
    next
end
```

SNMP v3 User settings for system event reporting

Settings	Guidelines
Name	User name that the SNMP Manager uses to communicate with the SNMP Agent. After you initially save the configuration, you cannot edit the name. Name can be up to 35 characters long and contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_).
Status	Enable/disable the configuration.
Security Level	• No Auth And No Privacy—Do not require authentication or encryption. • Auth But No Privacy—Authentication based on MD5 or SHA algorithms. Select an algorithm and specify a password. • Auth And Privacy—Authentication based on MD5 or SHA algorithms, and encryption based on AES or DES algorithms. Select an Auth Algorithm and specify an Auth Password; and select a Private Algorithm and specify a Private Password.
Query	Port number on which the system listens for SNMP v3 queries from the SNMP managers for this user. The default is 161. Enable queries for SNMP v3.
Traps	Source (Local) port number and destination (Remote) port number for SNMP v3 trap packets sent to SNMP managers for this user. The default is 162. Enable traps for SNMP v3. See SNMP traps and conditions.
Events	Select to enable SNMP event reporting for the following thresholds: • CPU—CPU usage has exceeded the Threshold set above (default 80%).

Settings	Guidelines
	• Memory—Memory (RAM) usage has exceeded the Threshold set above. • Disk—Disk space usage for the log partition or disk has exceeded the Threshold set above.
Hosts	IP Address—Subnet address for the SNMP manager to receive traps and be permitted to query the FortiDDoS system. SNMP managers have read-only access. You can add up to 8 SNMP managers to each community. **Caution:** The system sends security-sensitive traps, which should be sent only over a trusted network, and only to administrative equipment.

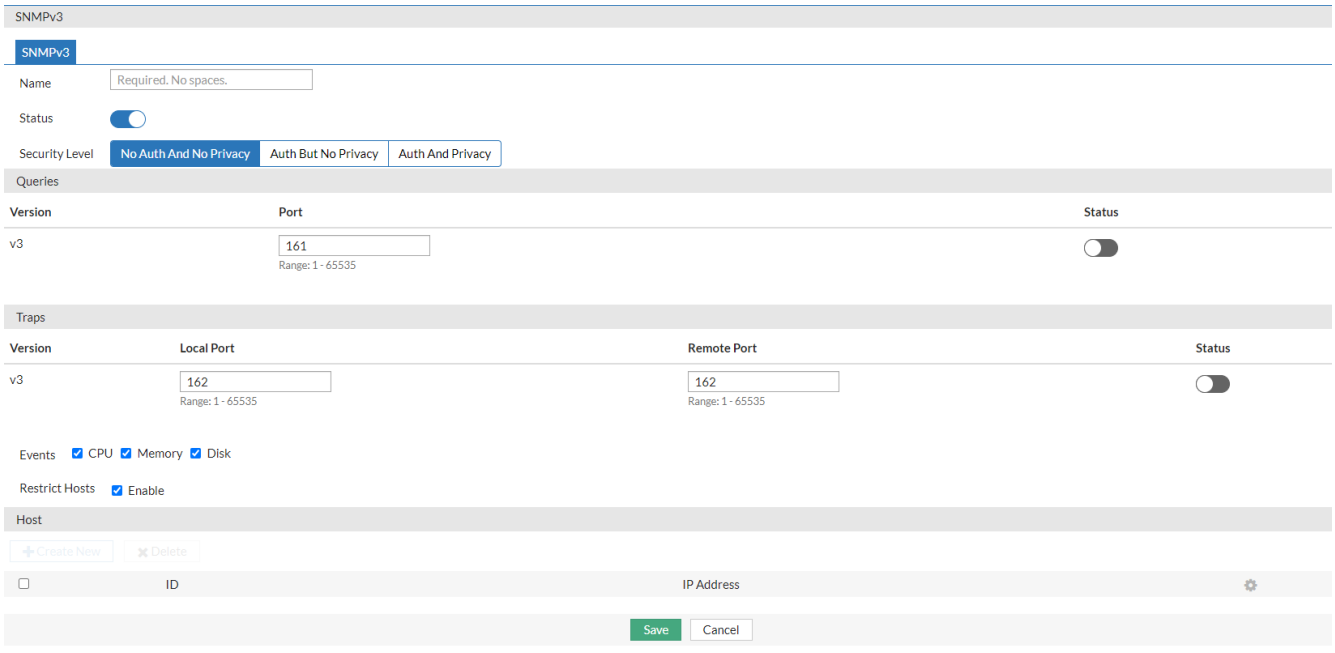
Restrict Hosts Checkbox	Host Configured	Host SNMP Query Restrictions	Trap Receivers	Comments
Enabled	No	No restrictions (any host)	None	
	Yes	Restricted to configured hosts (up to 8)	Sent to configured Hosts (up to 8)	Managers and Trap receivers must be shared
Disabled	No	No restrictions	None	
	Yes	No restrictions	Sent to configured Hosts (up to 8)	

System SNMP traps and conditions

SNMP traps	Conditions
Power supply failure	In dual power supply systems, one supply has failed.
Cold restart	System reboots due to power supply cycle.
Warm restart	User reboots the system.
Link down	Data port goes down.
Link UP	Data port comes up.
IP change	Management port IP is changed.
CPU usage	CPU usage goes above the configured threshold. See SNMP Thresholds above.
Memory usage	Memory usage goes above the configured threshold. See SNMP Thresholds above.
Disk usage	Disk usage goes above the configured threshold. See SNMP Thresholds above.

Use similar CLI commands to configure SNMP user:

```
config system snmp user
    edit 1
        set name bob
        set status enable
        set security-level authnopriv
        set auth-proto sha1
        set auth-pwd <password>
        set query-status enable
        set trap-status enable
        config host
            edit 1
                set ip <ip address>
            next
            edit 2
                set ip <ip address>
            next
        end
    next
end
```



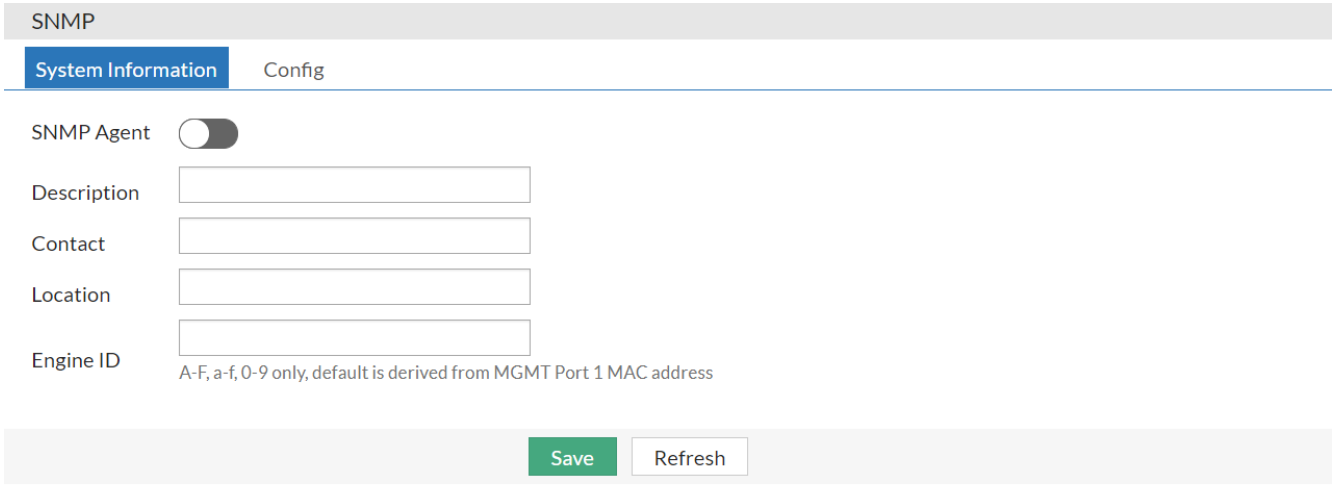
Configuring SNMP system information

Before you begin:

- You must have Read-Write permission for System settings.

To configure SNMP system information:

1. Go to *System* > *SNMP* > *System Information*.
2. Complete the configuration as described in the following tables.
3. Save the configuration.
4. Verify the SNMP configuration and network connectivity between your SNMP manager and this system.



SNMP system information settings for system event reporting

Settings	Guidelines
SNMP Agent	Enable to activate the SNMP agent, so that the system can send traps and receive queries.
Description	A description or comment about the system, such as `dont-reboot`. The description can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_).
Contact	Contact information for the administrator or other person responsible for this system, such as a phone number (`555-5555`) or name (`jdoe`). The contact information can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens (-), 'at' symbol (@) in email address and underscores (_).
Location	Physical location of the appliance, such as `floor2`. The location can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_).
Engine ID	ID that uniquely identifies the SNMP agent. If the Engine ID is not entered by the user,

Settings	Guidelines
	the MAC address of the management port is used to generate the Engine ID. For example, if the MAC address is: 08:5b:0e:9f:05:f0, the Engine ID will be: 8000304403085b0e9f05f0 which is the concatenation of the MAC address and Fortinet's IANA-registered Private Enterprise Number (12356) and additional information defined in RFC3411: 8000304404. To see the default or user-entered Engine ID, use the CLI command `get snmp engine-id`. The MAC address can be obtained using the CLI command `get system interface mgmt1` which displays information about the management port. Engine ID formats are defined by RFC3411. If you intend to use your own Engine ID, ensure conformance with the RFC since SNMP managers may reject non-conforming Engine IDs.

Use similar CLI commands to configure SNMP system information:

```
config system snmp sysinfo
      set status enable
      set description test
      set location HQ
      set contact a@b.com
      set engine-id 8000304404085b0e9f05f0
end
```

Managing local certificates

This section includes the following information:

- Overview
- Generating a Certificate Signing Request (CSR)
- Importing certificates
- Using certificates
- Viewing certificates

Overview

While requesting secure administrator access to a FortiDDoS device via HTTPS, the device uses SSL protocol to ensure that all communication between the device and the HTTP browser is secure no matter which client application is used. Regarding basic authentication made by an HTTP client, the device will use its self-signed security certificate to allow authentication whenever HTTPS is initiated by the client.

Note: The self-signed certificate proposal is the default setting on the device.

The HTTP browser notices the following discrepancies:

- The 'issuer' of the certificate offered by the device is unknown.
- The 'subject' of the certificate doesn't match the FQDN of the HTTP request a.b.c.d.

To avoid the triggering of these messages in the scenario where you don't require your HTTP browser to 'Permanently store this exception':

- Always ensure that the certificate of the CA signed by the device certificate is stored in the browser repository.
- Always ensure that the device is accessed with a correct FQDN.

Once the security exception is confirmed, the login page will be displayed. All the data sent to the device is encrypted and a HTTPS connection is created without reading the self-signed certificate proposal. Once the HTTP browser has permanently stored this exception, the exception prompt is not shown again. If the HTTP client declines the certificate, then the device does not allow the connection.

If you want to avoid these warnings and have a custom certificate, you must assign a host name to the appliance, generate a key pair and certificate request and import the certificate from a signing authority.

NOTE: The factory security certificate is not intended for long term use and as such may have weak security. You MUST secure the system by:

Assigning a host name to the appliance

Generating a key pair and certificate request

Importing the certificate from a valid signing authority.

Generating a Certificate Signing Request (CSR)

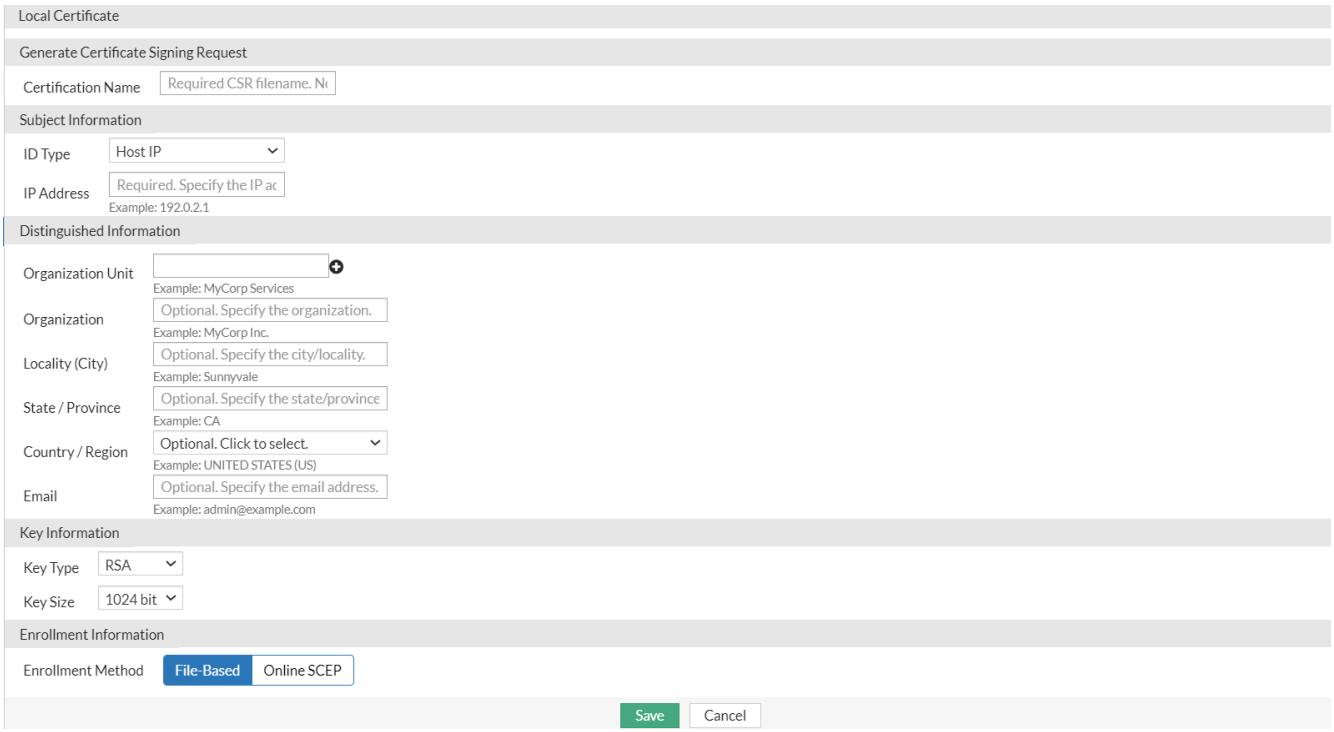
FortiDDoS allows you to generate CSRs that you can send to a CA to sign and give you a signed certificate. FortiDDoS creates a key pair that it keeps in a protected storage and is later used for SSL.

Before you begin:

• You must have Read-Write permission for System settings.

To generate a certificate request:

1. Go to **System** > **Certificate** > **Generate and Import**.
2. Click **Generate** to display the configuration editor.
3. Complete the configuration as described in the table below.
4. Save the configuration.
   The system creates a private and public key pair. The generated request includes the public key of the FortiDDoS appliance and information such as the IP address, domain name, or email address. The FortiDDoS appliance private key remains confidential in the FortiDDoS appliance. The Status column of the new CSR entry is Pending.
5. Select the row that corresponds to the certificate request.
6. Click **Download**.
   Standard dialogs appear with buttons to save the file to the location you select. Your web browser downloads the certificate request (.csr) file.
7. Upload the certificate request to your CA.
   After you submit the request to a CA, the CA will verify the information in the certificate, give it a serial number, an expiration date, and sign it with the public key of the CA.
8. If you are not using a commercial CA whose root certificate is already installed by default on web browsers, download your CA's root certificate, then install it on all computers that will be connecting to your appliance. (If you do not install these, those computers might not trust your new certificate.)
9. When you receive the signed certificate from the CA, you can import the certificate into the FortiDDoS system.



CSR configuration

Settings	Guidelines
Generate Certificate Signing Request	
Certification Name	Configuration name. Valid characters are A-Z,a-z,0-9,_, and -. No spaces. The maximum length is 35 characters. **Note**: This is the name of the CSR file, not the host name/IP contained in the certificate's Subject: line.
Subject Information	
ID Type	Select the type of identifier to use in the certificate to identify the virtual server: • Host IP—The static public IP address of the FortiDDoS virtual server in the **IP Address** field. If the FortiDDoS appliance does not have a static public IP address, use the email or domain name options instead. **Note**: If your network has a dynamic public IP address, you should not use this option. An "Unable to verify certificate" or similar error message will be displayed by users' browsers when your public IP address changes. • Domain Name—The fully qualified domain name (FQDN) of the FortiDDoS virtual server, such as www.example.com. This does not require that the IP address be static, and may be useful if, for example, your network has a dynamic public IP address and therefore clients connect to it via dynamic DNS. Do not include the protocol specification (http://) or any port number or path names. • Email—The email address of the owner of the FortiDDoS virtual server. Use this if

Settings	Guidelines
	the virtual server does not require either a static IP address or a domain name. Depending on your choice for **ID Type**, related options appear.
IP Address	Type the static IP address of the FortiDDoS appliance, such as 10.0.0.1.The IP address should be the one that is visible to clients. Usually, this should be its public IP address on the Internet, or a virtual IP that you use NAT to map to the appliance's IP address on your private network. This option appears only if **ID Type** is **Host IP**.
Domain Name	Type the FQDN of the FortiDDoS appliance, such as www.example.com. The domain name must resolve to the IP address of the FortiDDoS appliance or backend server according to the DNS server used by clients. (If it does not, the clients' browsers will display a Host name mismatch or similar error message.) This option appears only if **ID Type** is **Domain Name**.
E-mail	Type the email address of the owner of the FortiDDoS appliance, such as admin@example.com. This option appears only if **ID Type** is **E-Mail.**
Distinguished Information	
Organization Unit	Name of organizational unit (OU), such as the name of your department. This is optional. To enter more than one OU name, click the + icon, and enter each OU separately in each field
Organization	Legal name of your organization.
Locality (City)	City or town where the FortiDDoS appliance is located.
State/Province	State or province where the FortiDDoS appliance is located.
Country/Region	Country where the FortiDDoS appliance is located.
Email	Email address that may be used for contact purposes, such as admin@example.com.
Key Information	
Key Type	RSA
Key Size	Select a secure key size. Larger keys use more computing resources, but provide better security. For RSA, select one of the following: • 1024 Bit • 1536 Bit • 2048 Bit
Enrollment Information	

Settings	Guidelines
Enrollment Method	File Based—You must manually download and submit the resulting certificate request file to a CA for signing. Once signed, upload the local certificate. Online SCEP—The FortiDDoS appliance automatically uses HTTP to submit the request to the simple certificate enrollment protocol (SCEP) server of a CA, which will validate and sign the certificate. For this selection, two options appear. Enter the **CA Server URL** and the **Challenge Password**.

Importing certificates

Importing Certificates to an appliance using FortiDDoS-CM is not available. If you need to import a Certificate, login directly to the FortiDDoS appliance GUI. See the instructions under http://help.fortinet.com/fddos/4-7-0/index.htm#cshid=manage_local_certificate.

You can import or upload the following types of server certificates and private keys to the FortiDDoS system:

- local
- PKCS12
- certificate

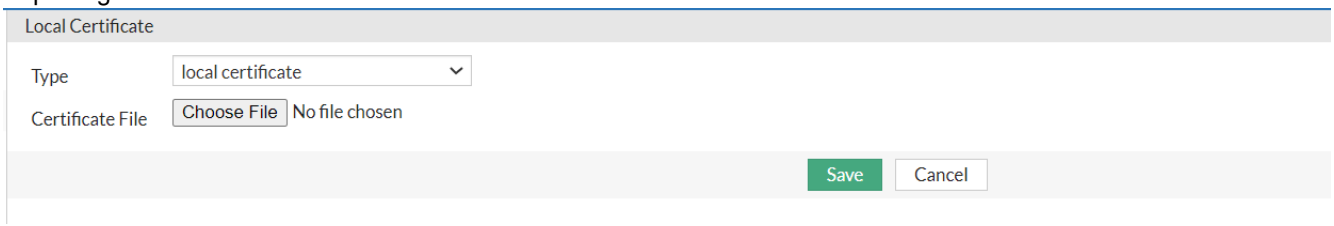
Before you begin:

- You must have Read-Write permission for System settings.
- You must have downloaded the certificate and key files to browse and upload.

To import a local certificate:

1. Go to **System** > **Certificate** > **Generate and Import**.
2. Click **Import** to display the configuration editor.
3. Complete the configuration based on the certificate **Type** selection, as described in the table below.
4. Save the configuration.

Importing a local certificate



Local certificate import configuration

Settings	Guidelines
Type	• Local Certificate: An unencrypted certificate in PEM format. • PKCS12 Certificate: A PKCS #12 password-encrypted certificate with key in the same file. • Certificate: An unencrypted certificate in PEM format. The key is in a separate file. Additional fields are displayed depending on your selection.

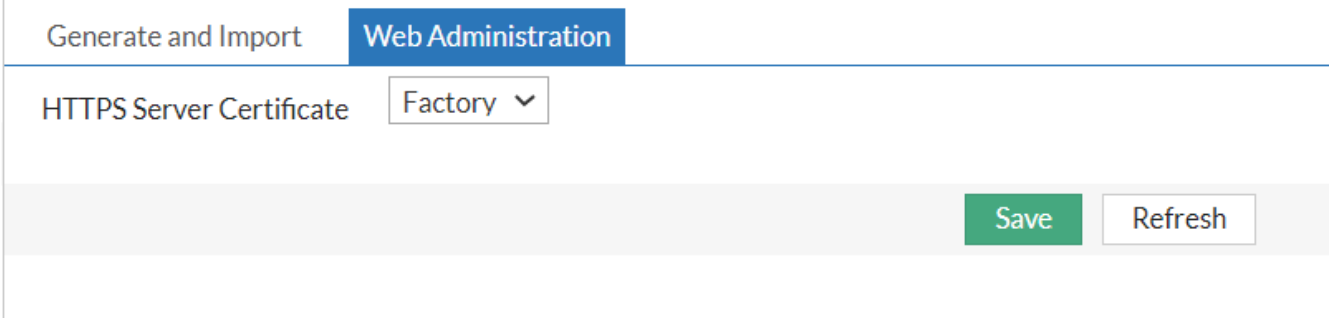
Settings	Guidelines
Local Certificate	
Certificate File	Browse and locate the certificate file that you want to upload.
PKCS12 Certificate	
Certificate Name	Name that can be referenced by other parts of the configuration, such as `www_example_com`. • Do not use spaces or special characters. • Maximum length is 35 characters.
Certificate File	Browse and locate the certificate file that you want to upload.
Password	Password to encrypt the file in local storage.
Certificate	
Certificate Name	Name that can be referenced by other parts of the configuration, such as `www_example_com`. • Do not use spaces or special characters. • Maximum length is 35 characters.
Certificate File	Browse and locate the certificate file that you want to upload.
Password	Password to encrypt the files in local storage.

After the certificate is imported, status shows OK.

Using certificates

1. Go to **System** > **Certificate** > **Web Administration** tab.
2. Select the desired certificate from the **HTTPS Server Certificate** (default: Factory) drop-down.
3. Save the configuration.

Certificate selection page



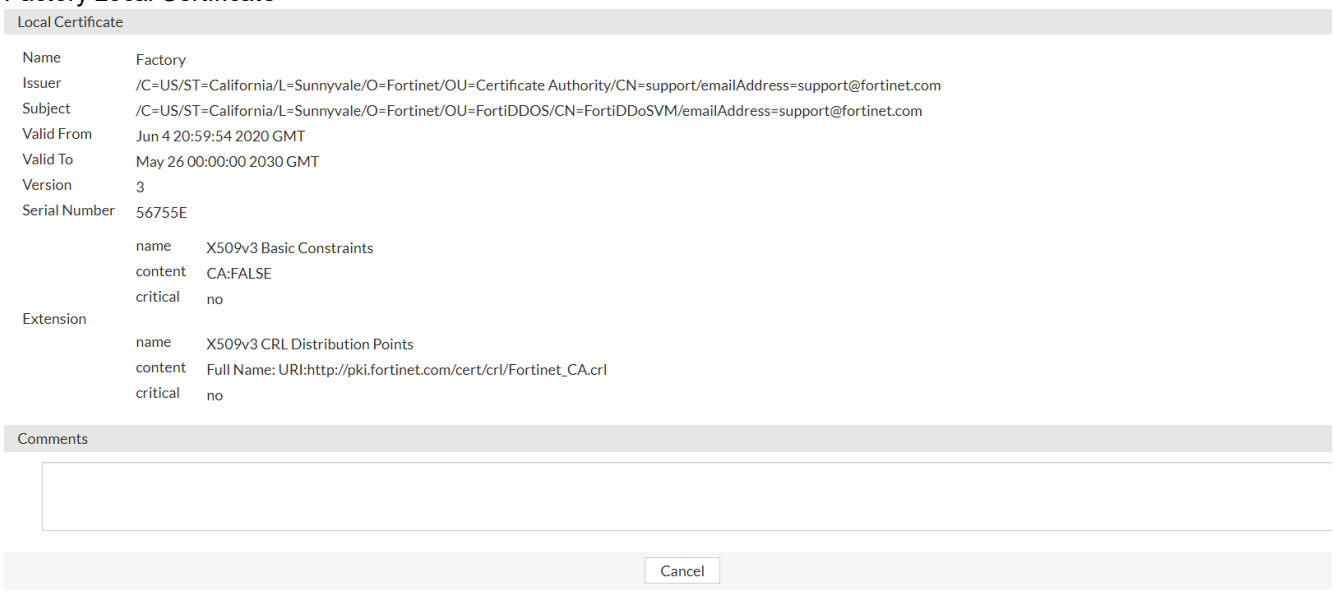
Viewing certificates

The system has its own default 'Factory' certificate that it presents to establish secure connections with the administrator client computer.

To view the local certificate:

1. Go to **System** > **Certificate** > **Generate and Import** tab.
2. Double-click the row corresponding to the **Factory Certificate.**

Factory Local Certificate

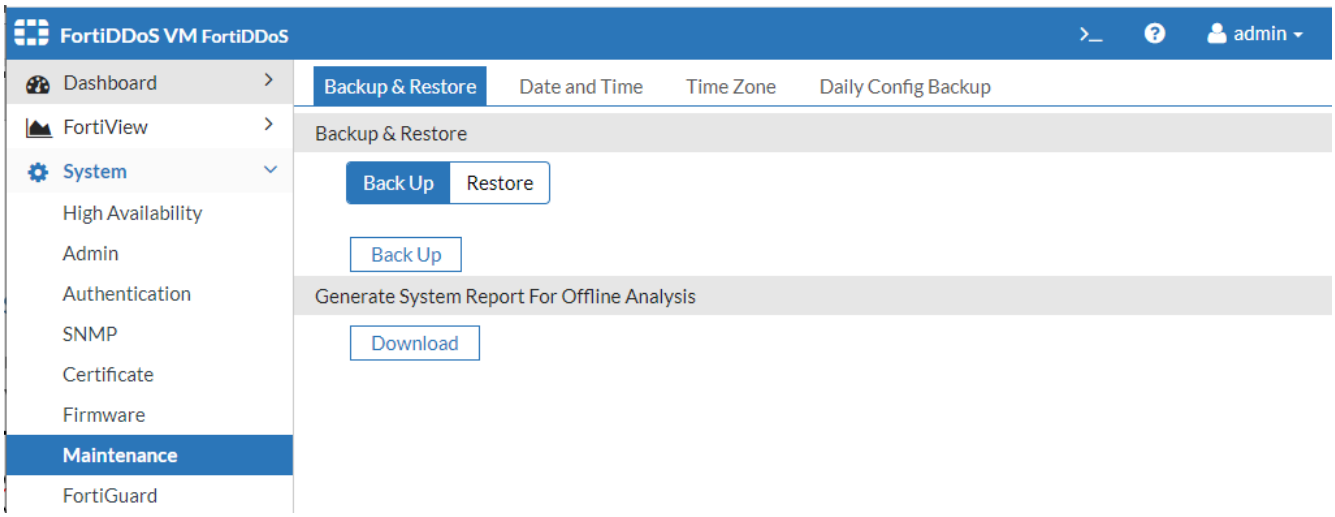


Generating system reports for offline analysis

When requesting support from FortiCare, it can be useful to add an Offline Analysis file to the TAC ticket from FortiDDoS.

To download system reports:

1. Go to *System* > *Maintenance* > *Backup & Restore*
2. Click *Download* under *Generate system reports for offline analysis*



At a minimum, this gzipped file contains the system configuration and debug files if present. Later firmware releases will expand the content of this file.

Updating firmware

This topic includes the following information:

- Upgrade considerations
- Updating firmware using the web UI
- Updating firmware using the CLI
- Downgrading firmware

Upgrade considerations

The following considerations help you determine whether to follow a standard or non-standard upgrade procedure:

- HA—Updating firmware on an HA cluster requires some additions to the usual steps for a standalone appliance. See Updating firmware on an HA cluster
- Downgrades—Special guidelines apply when you downgrade firmware to an earlier version. See Downgrading firmware. In some cases, the downgrade path requires reimaging. Take care to study the release notes for each version in your downgrade path.

Important: Read the Release notes for release-specific upgrade considerations.

Updating firmware using the web UI

Before you begin:

- Download the firmware file from the Fortinet Technical Support website.
- Read the release notes for the version you plan to install.

- **Important**: Back up your configuration before beginning this procedure. If you revert to an earlier firmware version, the running configuration is erased, and you must restore a saved configuration. We recommend you restore a configuration you knew to be working effectively on the firmware version you revert to.
- You must have super user permission (user **admin)** to upgrade firmware.

To install firmware:

1. Go to *System/Firmware*.
2. Under *Upload Firmware*, click *Choose File* and select the firmware file that you want to install. Then click the Update and Reboot icon.

Clear the cache of your web browser and restart it to ensure that it reloads the web UI.

Updating firmware using the CLI

This procedure is provided for CLI users.

Before you begin:

- Read the release notes for the version you plan to install. If information in the release notes is different from this documentation, follow the instructions in the release notes.
- You must be able to use FTP/TFTP to transfer the firmware file to the FortiDDoS system. If you do not have a TFTP server, download and install one, like `tftpd`, on a server located on the same subnet as the FortiDDoS system.
- Download the firmware file from the Fortinet Technical Support website.
- Copy the firmware image file to the root directory of the FTP/TFTP server.
- Back up your configuration before beginning this procedure. Reverting to an earlier firmware version could reset settings that are not compatible with the new firmware.
- Make a note of configurations that are disabled in your active configuration. Configurations that are not enabled are not preserved in the upgrade. For example, if a custom HTTP service port, log remote port, or event log port have been configured and then disabled in 4.1.11, the port information is not preserved in the upgrade to 4.2.1.
- You must have super user permission (user **admin)** to upgrade firmware.

To install firmware via the CLI:

1. Connect your management computer to the FortiDDoS-F console port using an RJ-45-to-DB-9 serial cable or a null-modem cable.
2. Initiate a connection to the CLI and log in as the user **admin**.
3. Use an Ethernet cable to connect FortiDDoS-F port1 to the FTP/TFTP server directly, or connect it to the same subnet as the FTP/TFTP server.
4. If necessary, start the FTP/TFTP server.
5. Enter the following command to transfer the firmware image to the FortiDDoS system:
   `execute restore image tftp <filename_str> <tftp_ipv4>`

where <filename_str> is the name of the firmware image file and <tftp_ipv4> is the IP address of the TFTP server. For example, if the firmware image file name is image.out and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image tftp image.out 192.168.1.168
```

One of the following message appears:

This operation will replace the current firmware version!

Do you want to continue? (y/n)

or:

Get image from tftp server OK.

Check image OK.

This operation will downgrade the current firmware version!

Do you want to continue? (y/n)

6. Type `y`.The system installs the firmware and restarts:

```
MAC:00219B8F0D94
##########################
Total 28385179 bytes data downloaded.
Verifying the integrity of the firmware image.
Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?
```

7. To verify that the firmware was successfully installed, use the following command:`get system status`
The firmware version number is displayed.

If the download fails after the integrity check with the error message `invalid compressed format (err=1`, but the firmware matches the integrity checksum on the Fortinet Technical Support website, try a different FTP/TFTP server.

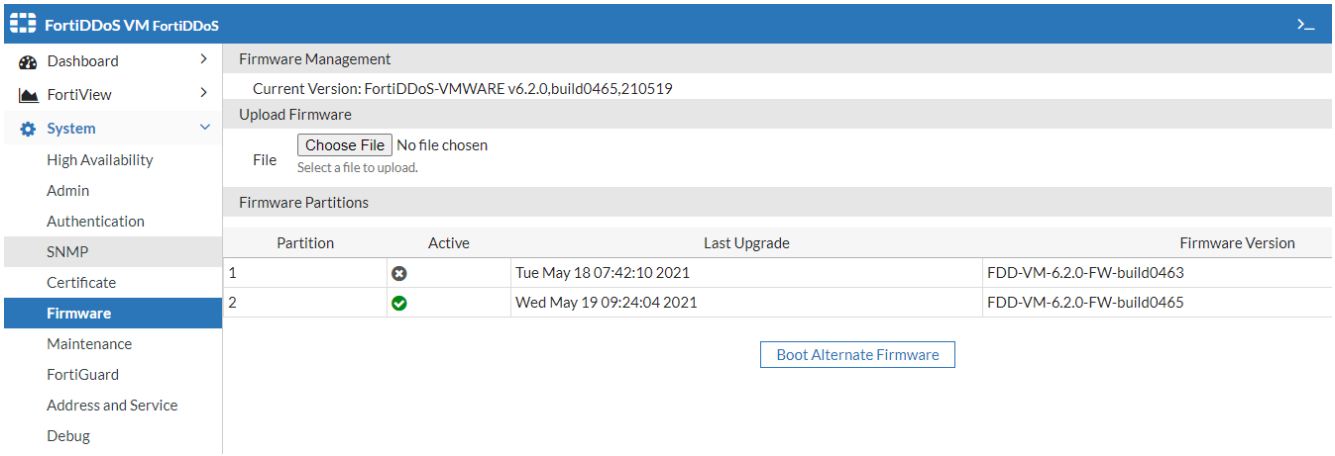
TFTP is not secure, and it does not support authentication. You should run it only on trusted administrator-only networks, and never on computers directly connected to the Internet. Turn off tftpd immediately after completing this procedure.

Downgrading firmware

You can use the web UI or CLI to downgrade to a previous software image. The commands are the same as for upgrading. However, special guidelines apply:

- Always keep a back up of the configuration before you change the software image (upgrade or downgrade).
- FortiDDoS F-Series maintains 2 Firmware images and the configurations associated with those images. Use *System* > *Firmware* > *Boot Alternate Firmware* to downgrade to the most recent previous version and revert to its configuration.
  - Be aware that all configuration changes (including Threshold changes) made in the latest firmware version will be reverted to the previous firmware configuration.

- To Boot Alternate Firmware from CLI:
  ```
  execute restore image alternative
  ```



- Downgrading below the previous most recent firmware version is not recommended since it will result in the erasure of all configuration settings, including the management IP address.
  - You must use a console port connection to reconfigure the management interface.
  - After you have configured the management interface, you can restore the earlier configuration. We recommend you restore a configuration you knew to be working effectively on the firmware version you installed.
  - After restoring the configuration, the system reboots, and the restored configuration will be in effect.

Backing up and restoring the configuration of an appliance

You can use the backup procedure to save a copy of the configuration. The backup file created by the web UI is a text file with the following naming convention: `FDD-<serialnumber>-<YYYY-MM-DD>[-SPP<No>]`. If you use the CLI to create a backup, you specify the filename.

The backup feature has few basic uses:

- Restoring the system to a known functional configuration.
- Saving the configuration as CLI commands that a co-worker or Fortinet support can use to help you resolve issues with misconfiguration.

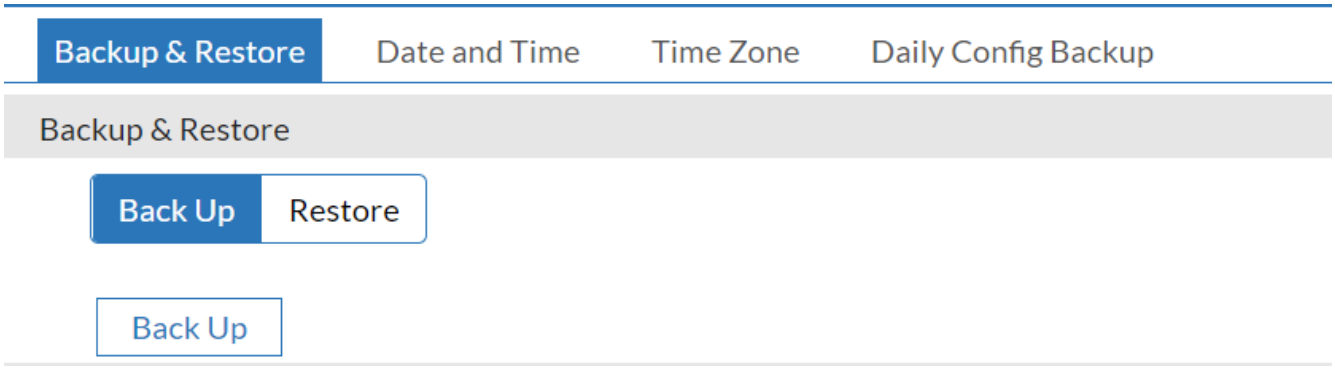
Before you begin:

- If you are restoring a system configuration, you must know its management interface configuration in order to access the web UI after the restore procedure is completed. Open the configuration file and make note of the IP address and network requirements for the management interface. You also must know the administrator user name and password.
- You must have Read-Write permission for System settings.

To backup the system configuration:

1. Go to **System** > **Maintenance** > **Backup & Restore**.
2. Follow the instructions in the table below to complete the configuration.
3. Save the configuration.

Backup and restore configuration page



Backup configuration guidelines

Actions	Guidelines
Backup	
Backup (button)	Click the **Backup** button to start the backup.
Restore	
From File	Type the path and backup file name or click **Browse** to locate the file.
Restore (button)	Click the Restore button to start the restore procedure. Your web browser uploads the configuration file and the system reboots with the new configuration. The time required to restore varies by the size of the file and the speed of your network connection. Your web UI session is terminated when the system reboots. To continue using the web UI, refresh the web page and log in again. If the restored system has a different management interface configuration than the previous configuration, you must access the web UI using the new management interface IP address. **WARNING**: Restoring a configuration (full system) results in a system REBOOT which can interrupt traffic if your traffic links do not have fail-open capability. NOTE: Configuration errors that are present in a backup file will be skipped when that file is restored. After restoring a configuration file, always • Use the CLI to run “get system restore-status” which will display any issues with the configuration restore • Check the Event Log to see if any configuration error messages are present. If you see errors, contact Fortinet Support.

To back up the configuration using the CLI to a TFTP server:

1. If necessary, start your TFTP server.
2. Log into the CLI as the `admin` administrator using either the local console, the **CLI Console** widget in the web UI, or an SSH or Telnet connection. Other administrator accounts do not have the required permissions.

3. Use the following command: `execute backup config tftp <filename> <ipaddress> [spp_name]`

`<filename>`	Name of the file to be used for the backup file, such as `Backup.conf`.
`<ipaddress>`	IP address of the TFTP server.
`[spp_name]`	Optional. SPP configuration name, for example, SPP-0 or SPP-1. Use this option to back up only the SPP configuration. If you do not specify this option, a backup is created for the complete system configuration.

To restore a configuration:

execute restore config tftp <filename> <ipaddress> [spp_name]

`filename>`	Name of the file, such as `Backup.conf`.
`<ipaddress>`	IP address of the TFTP server.

For example: execute restore config tftp Backup-SPP-1.conf 192.0.2.1 SPP-1

TFTP is not secure, and it does not support authentication. You should run it only on trusted administrator-only networks, and never on computers directly connected to the Internet. Turn off tftpd off immediately after completing this procedure.

Configuring system time

Accurate system time is critical to the correct FortiDDoS operation including all graphs, logs, and scheduling.

Changing the time of a system that is operational may have extreme consequences for the data already collected by the system. All saved traffic graphs, drop data and logs may be lost.

We strongly recommend that you use Network Time Protocol (NTP) to maintain the system time and that you configure date and time NTP settings before you do any other configurations.

As an alternative when NTP is not available or is impractical, you can set the system time manually, but this time will drift and changing times later can have serious consequences on existing data and mitigation.

You can change the system time with the web UI or the CLI.

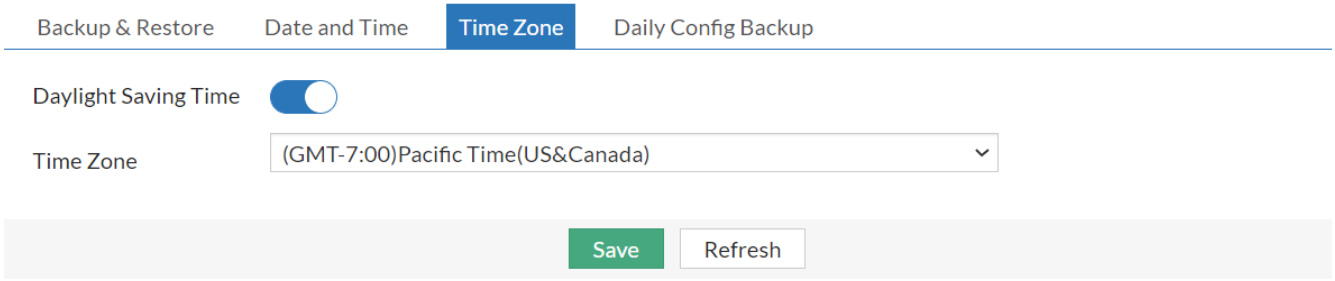
Before you begin:

- You must have Read-Write permission for System settings.
- Ensure you have:
  - DNS settings set in *Network* > *DNS*.
  - Gateway settings so that NTP queries can exit the network: *Network* > *Route*
  - Verify that your firewalls or routers do not block or proxy UDP port 123 (NTP).
- We recommend that — before you change system time settings —If the system is new or has already been factory reset, proceed with the instructions below.
- If the system has saved Traffic Statistics for SPPs and/or graphs and logs from existing traffic:
  - If you need to set the time ahead (from 8 am to 9 am, for example):
    - You may proceed with the instructions below.
  - If you need to set the time back (from 9 am to 8 am, for example):
    - You must perform command execute `formatlogdisk` to clear data that already exists within the time period that will be overwritten. This removes ALL graph, drop and log data from the system.

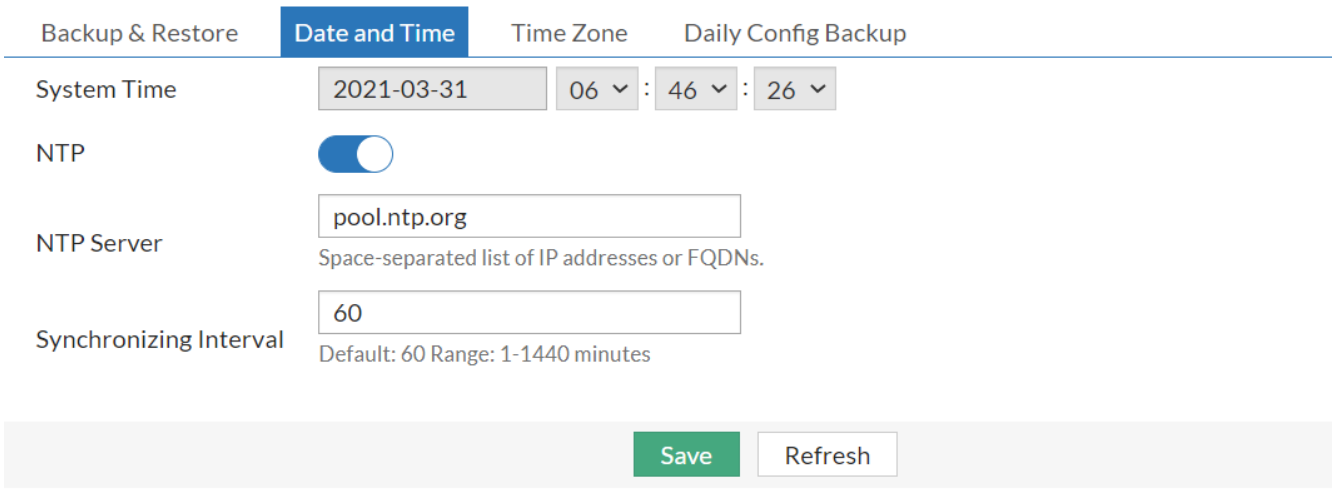
To configure the system time:

1. Navigate to the system time settings page in one of the following ways:
   - Go to **System** > **Maintenance** > **Time Zone**.
2. Complete the configuration as described in the table below.
   Important: You can change settings for only one group at a time: Time Zone or Time Setting. You must save your changes after each group before making changes in the next.
3. Save your changes. The system will reboot.
4. Change tabs to **Date and Time**.
5. Complete NTP or manual time settings.
6. Save your changes. The system will reboot.
   - Success — If you manually configured the system time, or if you enabled NTP and the NTP query for the current time succeeds, the new clock time appears in the System Time field at the top of the page shown in the figure below. If the NTP query reply is slow, you might need to wait a couple of seconds, and then click **Refresh** to update the time displayed in the System Time field.
   - Failure — If the NTP query fails, the system clock continues without adjustment. For example, if the system time had been 3 hours late, the system time is still 3 hours late. To troubleshoot the issue, check settings for your DNS server IP addresses, your NTP server IP address or name, and routing addresses; verify that your firewalls or routers do not block or proxy UDP port 123.

Time zone settings



Date and time settings



System time configuration

Setting	Guidelines
Time Zone	
Time zone	1. Ensure the 'Daylight Saving Time' checkbox is unchecked. 2. Select the time zone where the appliance is located. Check that the GMT offset is correct for the location. In recent years, Time Zone changes have been frequent. If the City/Country-Time Zone pair is inaccurate, use the correct GMT offset and ignore the text information.
Automatically adjust clock for daylight saving changes	Enable if you want the system to adjust its own clock when its time zone changes between daylight saving time (DST) and standard time. When enabled, you will see that the Time Zone GMT offset immediately changes, no matter if you are in DST or not. This is for display only and will not affect the system time.
Synchronize with NTP Server	
Server	Specify the IP address or domain name of an NTP server or pool, such as `pool.ntp.org`. To find an NTP server, go to http://www.ntp.org. You may enter more than one IP address or domain name with a space between them.
Sync Interval	Specify how often the system should synchronize its time with the NTP server, in minutes. For example, to synchronize once a day, type 1440.
OR	
Set Time	
Hour, Minute, Second, Date	This is not required if you have set NTP. Use the controls to set the time manually. The clock is initialized with the time you specified when you click **Save**. **NOTE: Manual time setting is NOT recommended.**

To configure NTP using the CLI:

config system time ntp
set ntpsync enable
set ntpserver {<server_fqdn> | <server_ipv4>}
set syncinterval <minutes_int>
end

To configure the system time manually:

```
config system time ntp
set ntpsync disable
end
config system time manual
set zone <timezone_index>
set daylight-saving-time {enable | disable}
end
```

execute date <mm:dd:yyyy> <hh:mm:ss>

Setting configuration auto-backup

FortiDDoS supports automated daily configuration backup on an FTP or TFTP server.

Note: The configuration backup is done daily at a fixed time UTC 0:00.

To configure daily backup:

1. Go to **System > Maintenance > Daily Config Backup**.
2. Complete the configuration as described in the table below.
3. Save the configuration.

Configuration backup settings

Settings	Guidelines
Status	Select the check-box to enable backup.
Server	IP address or subdomain of the server to back-up the configuration. **NOTE: FortiDDoS does not support folder selection in the address field. For example, "1.2.3.4/FortiDDoS" does not work. Only "1.2.3.4" or "backup.server.com" can be used. Most FTP servers can be set up to assign uploads to folders based on the IP address of the sender.**

Settings	Guidelines
Server Type	Select the server type: • TFTP • FTP
Settings for FTP Server Type	
Port	Port number ranging between 0-65535
User name/Password	User name and password

CLI commands:

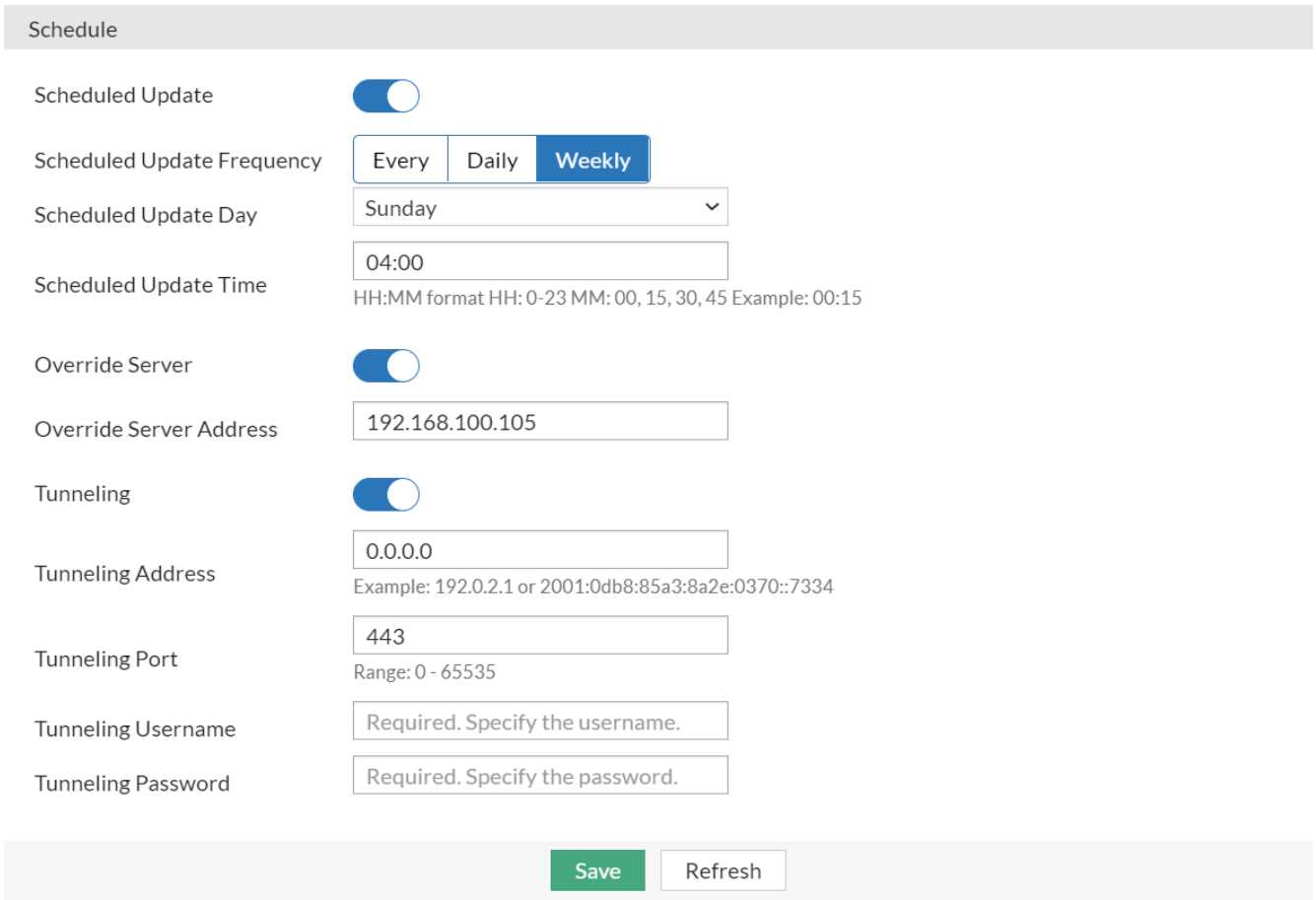
```
config system daily-config-backup
  set status {enable | disable}
  set server ftp.xyz.com
  set server-type {ftp | tftp}
  [set ftp-username <new-username_str>]
  [set ftp-password <new-password_str>]
end
```

FortiGuard

The FortiGuard Domain Reputation service is a licensed subscription that maintains a database of DNS Domain Names that pose a threat to your network and clients.

To configure Fortiguard:

1. Go to *System/FortiGuard*. This dashboard displays license and registration status, including status for the FortiGuard IP Reputation and Domain Reputation Services.
2. Click *Upload License* to import a license file.



FortiGuard update schedule settings

Setting	Description
Scheduled Update	Enable/disable FortiGuard scheduled updating
Scheduled Update Frequency	Every - every available update as they come Daily - daily scheduled updates Weekly - update will occur weekly, every 7 days on the scheduled update day that you set
Scheduled Update Day	Use when Scheduled Update Frequency is *Weekly*. The day of the week when the update will occur.
Scheduled Update Time	HH:MM. The time of day when the update will occur.
Override Server	Enable/disable. Disable to use the default FQDN of FortiGuard. Enable to set FQDN of FortiGuard.
Override Server Address	Set the address of the override server.
Tunneling	Enable to use a web proxy server IP address.
Tunneling IP Address	Web proxy server IP address.

Setting	Description
Tunneling Port	Port for the web proxy server.
Tunneling Username	Administrator user name for the web proxy server.
Tunneling Password	Password for the web proxy server.

To configure using the CLI:

```
config system fortiguard
   set scheduled-update-status {enable|disable}
   set scheduled-update-frequency {daily|weekly}
   set scheduled-update-day
        {Sunday|Monday|Tuesday|Wednesday|Thursday|Friday|Saturday}
   set scheduled-update-time <HH:MM>
   set override-server-status {enable|disable}
   set override-server-address <IP address>
   set tunneling-status {enable|disable}
   set tunneling-address <IP address>
   set tunneling-port <0-65535>
   set tunneling-username <string>
   set tunneling-password <string>
end
```

Address and Service

Address IPv4

You can create address objects to identify IPv4 addresses and subnets that you want to match in the following policy rule bases:

- Global ACL
- Do Not Track
- SPP ACL
- TCP Session Extended Source Address IPv4

Before you begin:

- You must have Read-Write permission for Global Settings.

To configure IPv4 addresses:

1. Go to *System > Address and Service> Address IPv4*.
2. Click *Add* to display the configuration editor.
3. Complete the configuration as described in the following table.
4. Save the configuration.

Setting	Description
Name	Configuration name. Must not contain spaces.
Type	*Address Netmask*- Create an entry for a subnet using an IP address/mask notation. *Address Range* - Create an entry for a address range with “Address Range From” and “To” . *Geo* - Create an entry for an address list belonging to a country or area.

Note: In the Global ACL for IPv4 addresses, you can add “deny rules” based on specified IP addresses or IP netmask configuration objects; you can add “allow rules” based on IP address configuration objects only.

To configure using the CLI:

```
config system address4
   edit addr1
      set type {ip-netmask|ip-range|geo}
      set ip-netmask <ip/mask>
      set ip-max <ip>
      set ip-min <ip>
      set country <string>
   next
end
```

Address IPv4 Group

Create an address group to include one or more address objects.

To configure IPv4 Address Group:

1. Go to *System > Address and Service> Address IPv4 Group*.
2. Click *Add* to display the configuration editor.
3. Complete the configuration and click *Save*.

To configure using the CLI:

```
config system addressgrp
   edit <name>
      set member-list <address1> <address2> …
   next
end
```

Address IPv6

You create address objects to identify IPv6 addresses and subnets that you want to match in the following policy rule bases:

- Global ACL
- Do Not Track
- SPP ACL

Before you begin:

- You must have Read-Write permission for Global Settings.

To configure IPv6 addresses:

1. Go to *Global System > Address and Service> Address IPv6*.
2. Click *Add* to display the configuration editor.
3. Complete the configuration and click *Save*.

To configure using the CLI:

```
config system addressgrp
   edit <name>
      set member-list <address1> <address2> …
   next
end
```

Address IPv6 Group

To configure IPv6 Address Group:

1. Go to *System > Address and Service> Address IPv4 Group*.
2. Click *Add* to display the configuration editor.
3. Complete the configuration and click *Save*.

To configure using the CLI:

```
config system addressgrp6
   edit <name>
      set member-list <address ipv6> <address ipv6> …
   next
end
```

Service

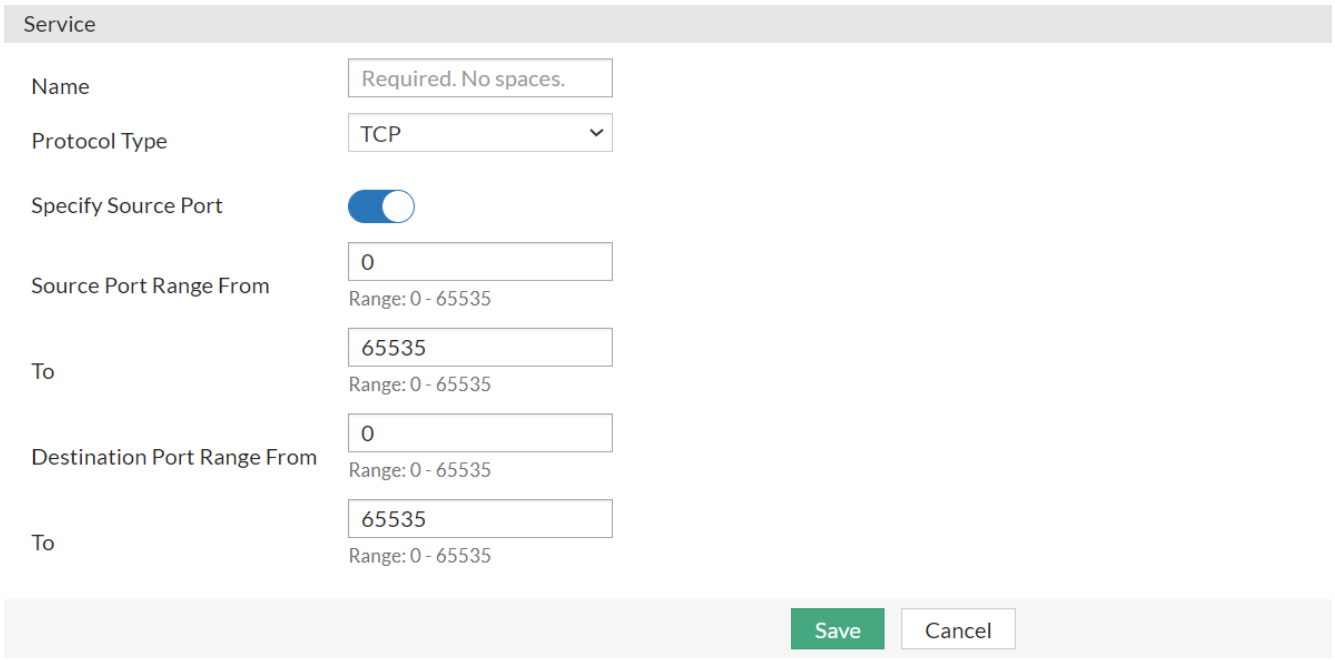
You configure service objects to identify the services that you want to match in SPP ACL or Global ACL policies.

Before you begin:

- You must have Read-Write permission for Protection Profile settings.

To configure service objects:

1. Go to *System > Address and Service> Service*.
2. View all build-in service.
3. Click *Add* to display the configuration editor.
4. Select Protocol type and set protocol ID.
5. Complete the configuration and click *Save*.



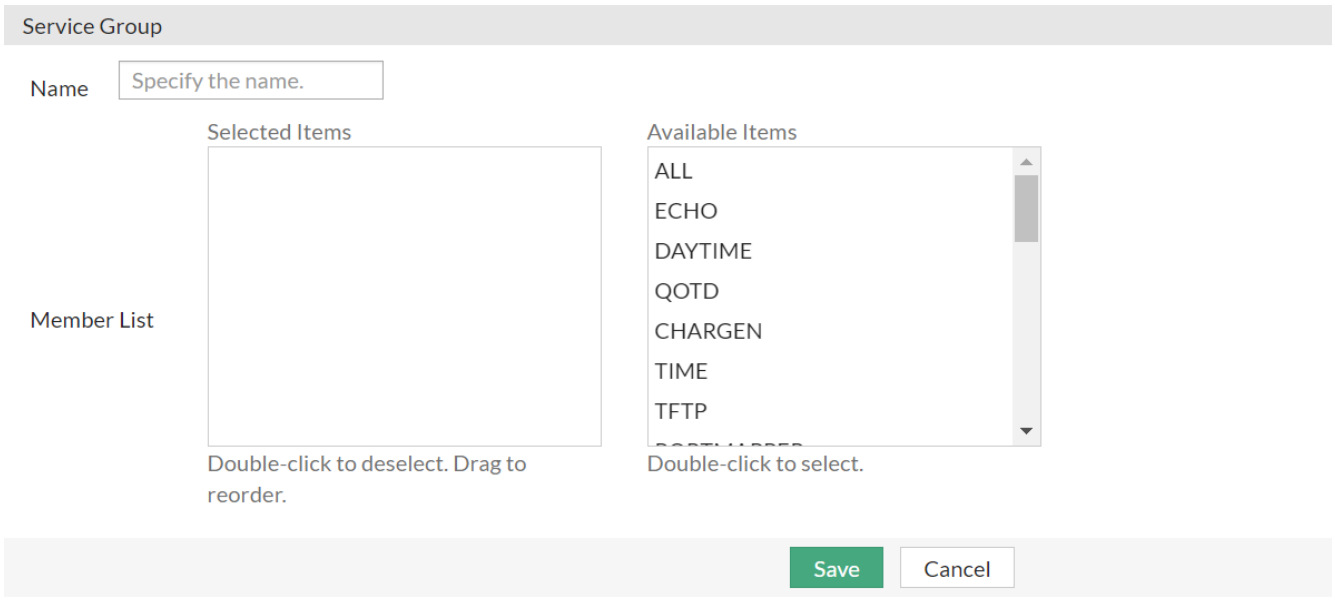
To configure using the CLI:

```
config system service
   edit <name>
      set protocol-type {ip|icmp|tcp|udp|tcp-and-udp}
      set specify-source-port {enable|disable}
      set source-port-min <0-65535>
      set source-port-max <0-65535>
      set destination-port-min <0-65535>
      set destination-port-max <0-65535>
   next
end
```

Service Group

To configure Service Group:

1. Go to *System* > *Address and Service*> *Service Group*.
2. Click *Add* to display the configuration editor.
3. Complete the configuration and click *Save*.



To configure using the CLI:

```
config system servicegrp
   edit <name>
      set member-list <service1> <service2> …
   next
end
```

Network

This section includes the following topics:

[placement content]

Configuring network interfaces

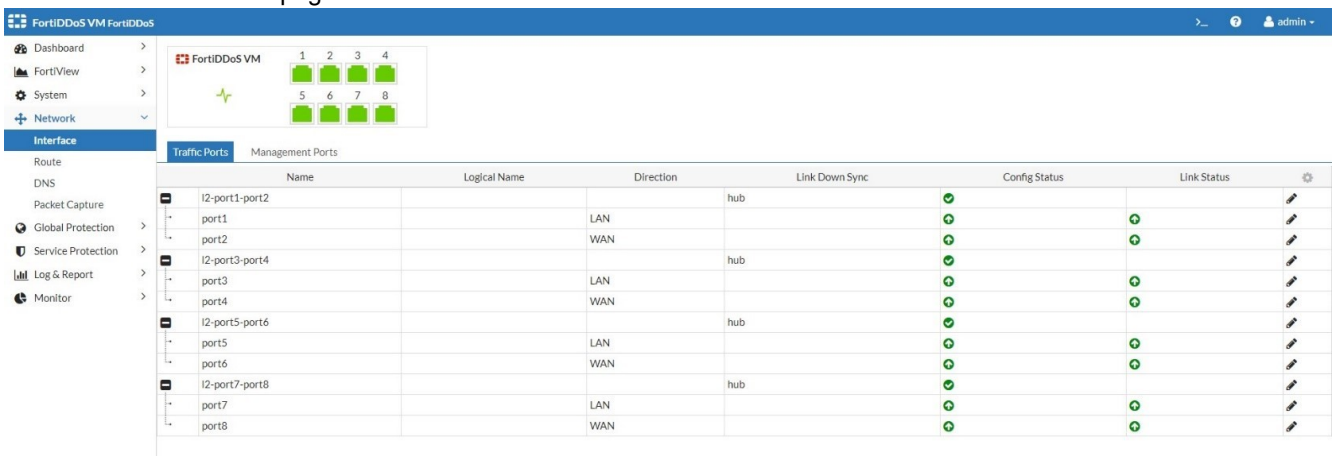
The network interfaces that are bound to physical ports have three uses:

- **Management**—Ports mgmt1 and mgmt2 are management interfaces. Management interfaces are used for administrator connections and to send management traffic, like syslog and SNMP traffic. Typically, administrators use mgmt1 for the management interface.
- **HA**—If you plan to deploy HA, you must select a physical port for HA heartbeat and synchronization traffic. Typically, administrators use mgmt2 for the HA interface.
- **Traffic**—The remaining physical ports can be used for your target traffic—these are your “traffic interfaces.” The FortiDDoS system is deployed inline (between the Internet and your local network resources). Consecutively numbered ports belong to port pairs: Use an odd port numbers (1, 3, 5, and so on) for the LAN-side connection and an even port number (2, 4, 6, and so on) for the WAN-side connection. For example, port1 and port2 are a pair. The port1 interface is connected to a switch that connects servers in the local network; the port2 interface is connected to the network path that receives traffic from the Internet.

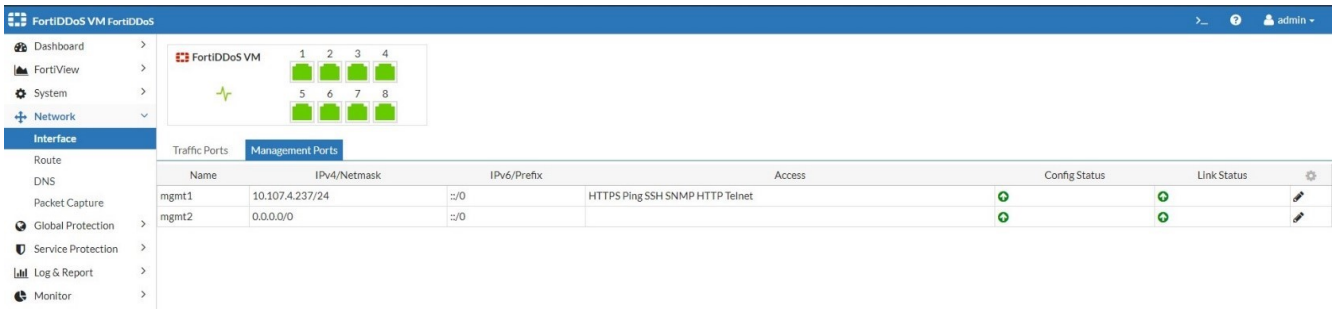
By default, 1000Base-T copper ports use auto-negotiation to determine the connection speed.

See Appendix G: SFP Compatibility Reference for more information.

Network interface status page



Management interfaces settings page



Network interface configuration guidelines

Settings	Guidelines
Name	Network interface name (assigned by system – non-editable)
Speed	Auto only.
Logical Name	Any description (maximum 15 characters) which provides more information about the network interface.
IPv4/Netmask	Management interfaces only. Specify the IP address and CIDR-formatted subnet mask, separated by a forward slash (/), such as 192.0.2.5/24. Dotted quad formatted subnet masks are not accepted.
IPv6/Prefix	Management interfaces only. Specify the IP address and CIDR-formatted subnet mask, separated by a forward slash (/), such as 2001:0db8:85a3:::8a2e:0370:7334/64. Dotted quad formatted subnet masks are not accepted.
Administrative Access	Management interfaces only. Allow inbound service traffic. Select from the following options: • HTTPS—Enables secure connections to the web UI. • Ping—Enables ping and traceroute to be received on this network interface. When it receives an ECHO_REQUEST (“ping”), the FortiDDoS system replies with ICMP type 0 (ECHO_RESPONSE or “pong”). • SSH—Enables SSH connections to the CLI. We recommend this option instead of Telnet. • SNMP—Enables SNMP queries to this network interface. • HTTP— HTTP is no longer supported. HTTP access will be referred to HTTPS. • TELNET—Enables Telnet connections to the CLI. We recommend this option only for network interfaces connected to a trusted private network, or directly to your management computer.

Settings	Guidelines
	Note: We recommend you to enable administrative access only on network interfaces connected to trusted private networks or directly to your management computer. SNMP, Telnet and SQL should be used with care.
Configured Status	This indicator displays Port Configured State up/down as set by the user. This state can only be changed via CLI.
Link Status	The Link Status indicators on the Interface Configuration page display the connectivity status. A green indicator means that the link is connected and negotiation was successful. A red indicator means that the link is not connected or is down.

Note: Settings for speed, duplex, etc. cannot be changed for mgmt1 and mgmt2.
The only settings allowed to be changed are:

- allow access with the interface
- IP address of interface
- IP6 IPv6 address of interface
- Logical Name
- hardware address
- static or dhcp mode
- maximum transportation unit

CLI commands for management ports

Modifying settings:

```
config system interface
    edit {mgmt1|mgmt2}
        set speed
{auto|10half|10full|100half|100full|1000half|1000full}
        set status {up|down}
        set ip <address_ipv4> <netmask_ipv4mask>
        set ipv6 <address_ipv6> <netmask_ipv6mask>
        set logicalname {string - 16 characters a-Z, 0-9, "-",
"_"}
        set allowaccess {https ping ssh snmp http telnet sql}
        set mode {static|dhcp}
        set mtu
    end
```

Confirming settings:

```
    config system interface
       edit {mgmt1|mgmt2}
       show
    end
```

CLI commands for data ports

Modifying settings:

```
config system interface
   edit {portX} (X=1-8|1-16 depending on model)
        set logicalname {string - 16 characters a-Z, 0-9, "-",
"_"}
        set status {up|down}
end
```

Confirming settings:

```
config system interface
   edit {portX} (X=1-8|1-16 depending on model)
   show
end
```

Configuring static routes

You configure a static route to enable you to connect to the web UI and CLI from a remote location, like your desk.

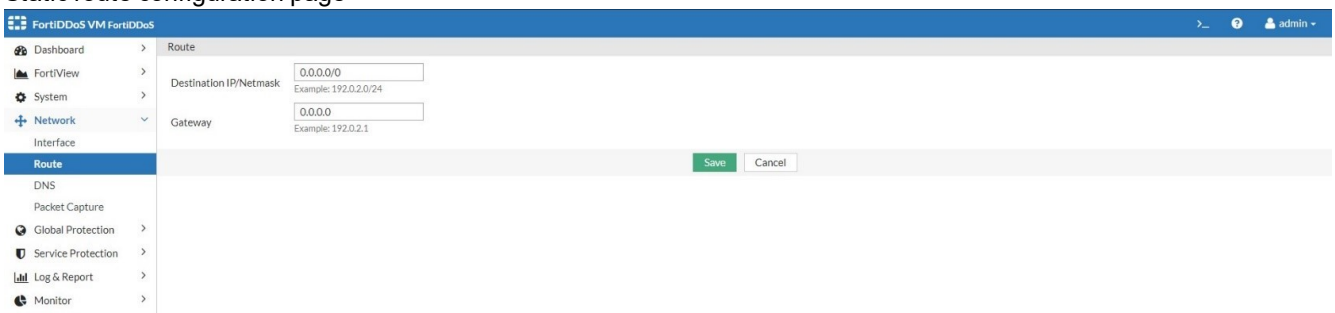
Before you begin:

- You must have Read-Write permission for System settings.

To configure a static route:

1. Go to **System** > **Network** > **Static Route**.
2. Click **Add** to display the configuration editor.
3. Complete the configuration as described in the figure/table below.
4. Save the configuration.

Static route configuration page



Static route configuration guidelines

Settings	Guidelines
Interface	Select the network interface that uses the static route.
Destination IP/mask	Destination IP address and network mask of packets that use this static route, separated by a slash (/) or space. The value `0.0.0.0/0` is a default route, which matches all packets
Gateway	IP address of the next-hop router for the FortiDDoS-F management computer.

To configure a static route using the CLI:

```
config system default-gateway
   edit <route_number>
      set destination <destination_ipv4/mask>
      set gateway <gateway_ipv4>
      set interface {mgmt1 | mgmt2}
end
```

Configuring DNS

The system must be able to contact DNS servers to resolve IP addresses and fully qualified domain names.

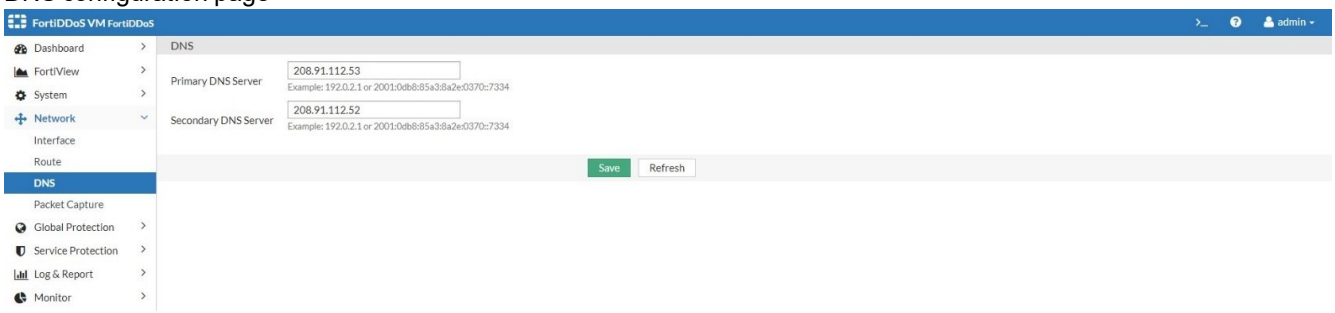
Before you begin:

- You must know the IP addresses of the DNS servers used in your network.
- Your Internet service provider (ISP) might supply IP addresses of DNS servers, or you might want to use the IP addresses of your own DNS servers. You must provide unicast, non-local addresses for your DNS servers. Local host and broadcast addresses are not accepted.
- Incorrect DNS settings or unreliable DNS connectivity can cause issues with other features, such as FortiGuard services and NTP system time.
- You must have Read-Write permission for System settings.

To configure DNS:

1. Go to **System** > **Network** > **DNS**.
2. Complete the configuration as described in the table below.
3. Save the configuration.

DNS configuration page



DNS configuration guidelines

Settings	Guidelines
Primary DNS Server	IPv4/IPv6 address of the primary DNS server. For best performance, use a DNS server on your local network.
Secondary DNS Server	IPv4/IPv6 address of the secondary DNS server for your local network.

CLI commands:

```
config system dns
set primary <ipv4/ipv6 address>
set secondary <ipv4/ipv6 address>
end
```

To verify DNS:

```
execute traceroute <server_fqdn>
```

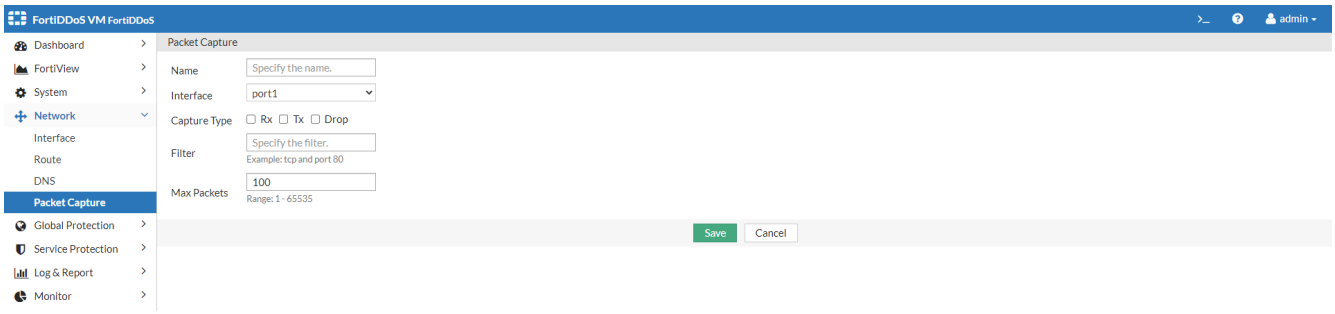
where `<server_fqdn>` is a domain name such as www.example.com.

Packet Capture

FortiDDoS allows you to send dropped packets from selected events to a front panel port for recording by a laptop or other capture device for offline review of dropped packet information.

To configure Packet Capture:

1. Go to *Network* > *Packet Capture*.
2. Click *Create New* to add new *Packet Capture* configuration
3. Save the configuration.



Setting	Description
Name	Any name up to 15 characters (a-Z, 0-9, and special characters -#_*/+|)
Interface	Select the front panel port used for “exporting” the dropped packets from Interface drop down menu.
Capture Type	Select *Rx* for capturing Receive packets. Select *Tx* for capturing Transmit packets. Select *Drop* for capturing drop packets.
Filter	To filter packets through specific protocols and port numbers
Max Packets	Maximum packets number allowed for capturing.

Operation

Many system graphs that display drop information will allow you to select an icon at the end of the graph label to start capture of the drops related to that label. Some graphs have a single drop label and some have many.

Note: Only one type of drop capture can be done at a time.

The Start and Stop buttons are on the right most column.

Global Settings

This section includes the following topics:

Deployment

You can use the deployment settings to configure where in the network the FortiDDoS appliance has to be deployed. You can set Asymmetric, tap mode, Bypass Mode and Bypass MAC list.

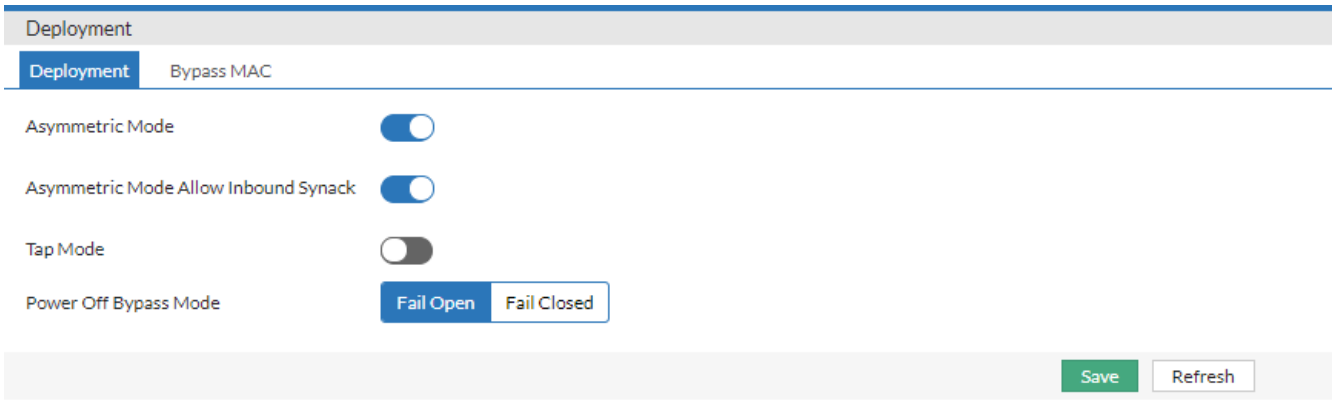
Before you begin:

- You must have Read-Write permission for Global Settings.

Deployment

To configure deployment settings:

1. Go to *Global Protection* > *Deployment* > *Deployment*.
2. Configure the deployment settings according to the table below.
3. Save the configuration.



Deployment settings

Settings	Guidelines
Asymmetric Mode	Enable when deployed in a network segment where traffic can take asymmetric routes. This option is not enabled by default. Special considerations and configuration changes are required. See Understanding FortiDDoS Asymmetric Mode for TCP on page 68.
Allow Inbound SYN/ACK	Enable only when you enable Asymmetric Mode. When there is asymmetric traffic, the system might receive inbound SYN/ACK packets. When this option is enabled, these packets are treated as if there is a valid connection on which to accept data (if the connection does not already exist).
Tap Mode	Enable when deployed out-of-path in conjunction with a bypass bridge appliance. This option is not enabled by default. Note: The system is rebooted when you change this setting. Special considerations and configuration changes are required. See Tap Mode deployments on page 372.
Power Fail Bypass Mode	*Fail Open*— *Fail Open* is default Setting. 200F has bypass ports 1-8 and 13-16 and 1500F has bypass ports 5-8. See Built-in fail-open bypass on page 370. *Fail Closed*—Use with an external bypass unit or (usually) for the primary node in an HA active-passive deployment. When the interfaces are Fail Closed, they do not pass traffic. The external bypass system can detect the outage and forward traffic around the FortiDDoS. As above, 200F ports 9-12 and 1500F ports 1-4 are ONLY 'Fail Closed'. See Built-in fail-open bypass on page 370.

To configure using the CLI:

```
config ddos global deployment
   set asymmetric-mode {enable|disable}
   set asymmetric-mode-allow-inbound-synack {enable|disable}
   set tap-mode {enable|disable}
   set power-fail-bypass-mode {fail-open|fail-closed}
end
```

Bypass MAC

In a deployment with a bypass bridge, the bridge passes heartbeat packets to test the health of the FortiDDoS traffic interfaces. If the heartbeats packets are not passed, bypass mode is triggered.

In most cases, the bypass bridge will expose the MAC addresses of its Monitor ports that are sending the heartbeat packets. It is recommended that these MAC addresses be entered in FortiDDoS Bypass MAC address list to ensure that packets from these MAC addresses are never blocked by FortiDDoS.

Each FortiDDoS model supports the following number of Bypass MAC addresses:

- VM04/VM08/VM16/200F/1500F– 8

Bypass MAC is used only when you are using an external Bypass Bridge that generates heartbeats between its Monitor interfaces to determine the FortiDDoS appliance health.

Do not enter the MAC addresses of connected Switches or Routers. It is unnecessary and results in all traffic bypassing the FortiDDoS mitigation systems.

Before you begin:

- You must know the MAC addresses for the bypass switch.
- You must have Read-Write permission for Global Settings.

To configure a bypass MAC address list:

1. Go to Global Protection > Deployment > Bypass MAC.
2. Click Add to display the configuration editor.
3. Complete the configuration as described in the following table.
4. Save the configuration.

Bypass MAC address list configuration

Settings	Guidelines
Name	Configuration name. Must not contain spaces.
MAC address	Specify the MAC address. Note: You can view MAC addresses of the bypass switch on its status page. If the bypass switches are from the same vendor, the most significant 24-bits of their MAC addresses are the same.

To configure using the CLI:

```
config ddos global bypass-mac
   edit <name>
      set mac <address>
end
```

Proxy IP

This section includes the following topics:

Proxy IP Detection

FortiDDoS can take account of the possibility that a source IP address might be a proxy IP address, and adjust the threshold triggers accordingly. If a source IP address is determined to be a proxy IP address, the system adjusts thresholds for Most Active Source, SYN per source, Concurrent Connections per source, HTTP Method per source and DNS query per source by a multiplier that you specify.

You can configure either or both of the following methods to determine whether source IP address is a proxy IP address:

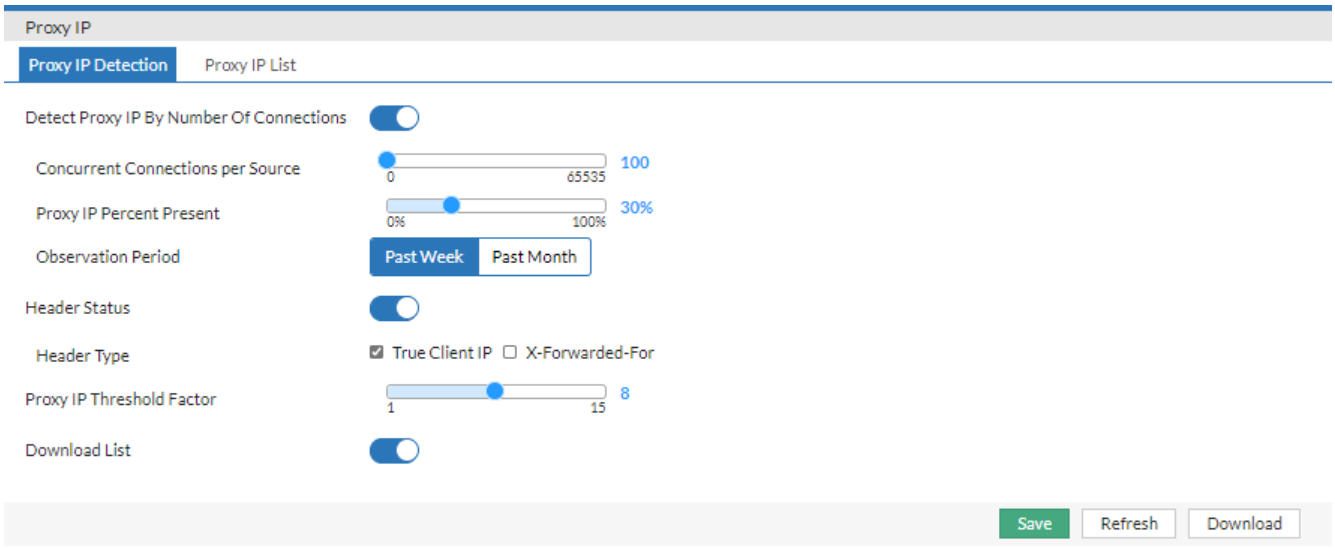
- Concurrent connection count—Used when there are many users behind a web proxy or NAT device like an enterprise firewall.
- HTTP headers—Used when there are many users behind a Content Delivery Network (CDN), such as Akamai.

Before you begin:

• You must have Read-Write permission for Global Settings.

To configure proxy IP settings:

1. Go to *Global Protection* > *Proxy IP* > *Proxy IP Detection*.
2. Complete the configuration as described in the table below.
3. Save the configuration.



Proxy IP configuration

Settings	Guidelines
Detect proxy IP by number of connections	Enable/Disable
Concurrent connections per source	Every 5 minutes, the system records the IP addresses of sources with more than this number of concurrent connections to test whether those sources might be using a proxy IP address. The default is 100 concurrent connections.
Proxy IP Percent present	Threshold that determines whether the source IP address is regarded as a proxy IP address. For example, the default is 30. After the observation period, the IPs whose numbers of concurrent connections have been 30% of the time above 100 are identified as proxy IPs.
Observation period	• Past Week—Uses data from the past week to determine whether a source IP address is a proxy IP address. • Past Month—Uses data from the past month.
Header Status	Enable/Disable
Header Type	Select HTTP headers that indicate a proxy address might be in use: • true-client-IP • x-forwarded-for (selecting this option also enables parsing of x-true-client-ip and x-real-ip headers)
Proxy IP threshold factor	Specify a multiplier when the source IP address is identified as a proxy IP address. For example, if you specify 32, and the Most Active Source threshold is 1000, then the Most Active Source threshold applied to proxy IP addresses is 32 * 1000 or 32,000. The default is 128. The maximum is 32,768. **Note:** The Proxy IP Threshold Factor is set and displayed differently in the GUI and CLI. The actual Threshold Factor is set by the slider on the GUI and shown in orange (default 128). If set from the CLI, the factor must be set as an exponent of 2. For example, if you want to set the factor as '1024', you must enter '10' (2^10=1024). If you check the threshold factor via CLI, it shows the exponent value '10' whereas the GUI shows '1024'.
Download List	Enable/disable downloading proxy log.

To configure using the CLI:

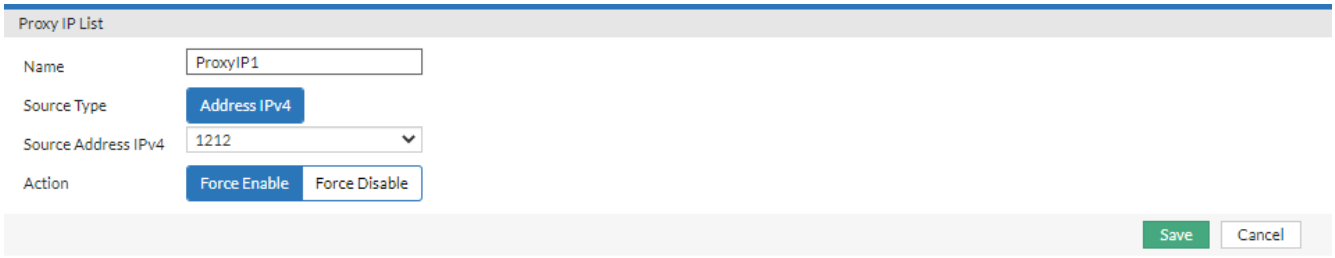
```
config ddos global proxy-ip-setting
   set auto_status {enable | disable}
   set percent <integer>
   set period {past-week | past-month}
   set header_status {enable | disable}
   set header_type {true-client-ip X-Forwarded-For}
   set traffic_coefficient <integer>
end
```

Proxy IP List

FortiDDoS allows you to manually assign a source IP address as proxy IP address through the GUI or CLI. If a source IP is assigned as proxy IP, the system adjusts the thresholds for Most Active Source, SYN per source, Concurrent Connections per source, HTTP Method per source and DNS query per source by a multiplier that you specify.

To configure proxy IP settings:

1. Go to *Global Protection* > *Proxy IP* > *Proxy IP List*.
2. Click *Add*.
3. Complete the configuration as described in the following table.
4. Save the configuration.



Settings	Guidelines
Name	Proxy IP policy name
Source Type	Address IPv4
Source Address IPv4	Proxy IP policy address
Proxy IP Action	Select from the following options: • *force-disable*: To disable automatically detected proxies ensuring that these IPs do not get the elevated treatment for thresholds. • *force-enable*: To force enable certain IPs as proxies ensuring that these IPs get elevated treatment even if it is not detected so by the automatic scheme.

To configure using the CLI:

```
config ddos global proxy-policy
   edit <name>
      set source-type addr4
      set proxy-IP-address <datasource>
      set action <force-enable/ force-disable>
   next
end
```

Best practices

The following recommended best practices:

- Do not set the bypass bridge Tap Mode manually. Set it up as the action on failure for the bypass bridge Inline Mode and then force a failure of the out-of-path segment by turning on FortiDDoS Tap Mode.

- In a FortiDDoS Tap Mode deployment, you can set SPPs in Detection Mode or Prevention Mode. Set it to whichever mode you want enabled when you toggle off Tap Mode and put FortiDDoS inline.

Cloud Signaling

The Service Provider Signaling feature enables small/medium businesses and enterprises to work with participating service providers to route traffic through a "scrubbing station" in the service provider network (SP) before it is forwarded through the WAN link to the customer premises network (CP).

For details on deployments with signaling between FortiDDoS devices, see Service Protection on page 221.

For information on deployments with signaling to 3rd-party Cloud DDoS Mitigation services, please contact your local sales team or Fortinet TAC.

Note: You must use mgmt1 port for signaling. If FortiDDoS is behind a web proxy, configure Tunneling settings under IP Reputation.

Before you begin:

- You must have Read-Write permission for Global Settings.
- Please make sure the following settings are configured in SPP rule:
  - Cloud signaling status is enabled under *Service Protection* > *Service Protection Policy* > *{SPP Rule}* > *Service Protection Policy*
  - Configure Signaling Threshold (KPPS or Mbps or both) for selected subnet under *Service Protection* > *Service Protection Policy* > *{SPP Rule}* > *Service Protection Policy* > *Protection Subnets*

To configure service provider signaling:

1. Go to Global Protection > Cloud Signaling.
2. Click Add to display the configuration editor.
3. Complete the configuration as described in the following table.
4. Save the configuration.

Settings	Guidelines
Cloud Signaling Mode	Customer Premises Service Provider
Signaling Timeout	Timeout after which System will re-investigate if traffic is passed Signaling Threshold
Customer Premises FDD	
Status	Enable or Disable
Name	Configuration name. Must not contain spaces.
Device Type	FortiDDoS—If the service provider uses FortiDDoS, select this option and complete the fields described next. Third Party—If the service provider has a cloud mitigation service, select this option and specify the account ID, shared secret, and URL expected by the third party.

Settings	Guidelines
Serial Number	Serial number of the FortiDDoS in the service provider network. The serial number configuration is case sensitive. Be careful to enter the serial number exactly as it is provided to you.
Shared Secret	Must match the string configured on the SP FortiDDoS. (Allowed characters are a-Z and 0-9) **Note:** Once entered, the Shared Secret/API Key is not displayed on GUI nor in CLI and cannot be recovered. If forgotten, a new matching key must be entered for the paired devices.
Address Type	IPv4 or IPv6
Service Provider IP address	IP address of the SP FortiDDoS management interface.
Service Provider FDD	
Name	Configuration name. Must not contain spaces.
Customer Premises FDD Serial Number	Serial number of the FortiDDoS in the customer premises network. The serial number configuration is case sensitive. Be careful to enter the serial number exactly as it is provided to you.
Shared Secret	Must match the string configured on the CP FortiDDoS. (Allowed characters are a-A and 0-9)
Customer Premises FDD IP Version	IPv4 or IPv6
Customer Premises IP address	IP address of the CP FortiDDoS management interface.
Cloud Signaling/Third Party mitigation	
Name	Configuration name. Must not contain spaces.
Device Type	Third Party
Shared Secret	Obtain from the Cloud Mitigation provider. Allowed characters: A-Z, a-z, 0-9, no spaces. Max 19 characters.
Account ID	User account provided by the Cloud Mitigation provider
SP URL	Listening Signaling URL provided by the Cloud Mitigation provider

To configure using the CLI:

```
config ddos global cloud-signaling
   set mode { customer-premises | service-provider }
   set timeout <integer>
   config devices
      edit <device_name>
         set enable { enable | disable }
         set device-type { FortiDDoS | Third-Party }
         set serial-number <string>
         set shared-secret <passwd>
         set address-type { ipv4 | ipv6 }
         set ipv4-address <ipv4_addr>
         set ipv6-address <ipv6_addr>
         set account-id <string>
         set url <string>
      next
   end
end
```

Configuring blocklisted IPv4 addresses

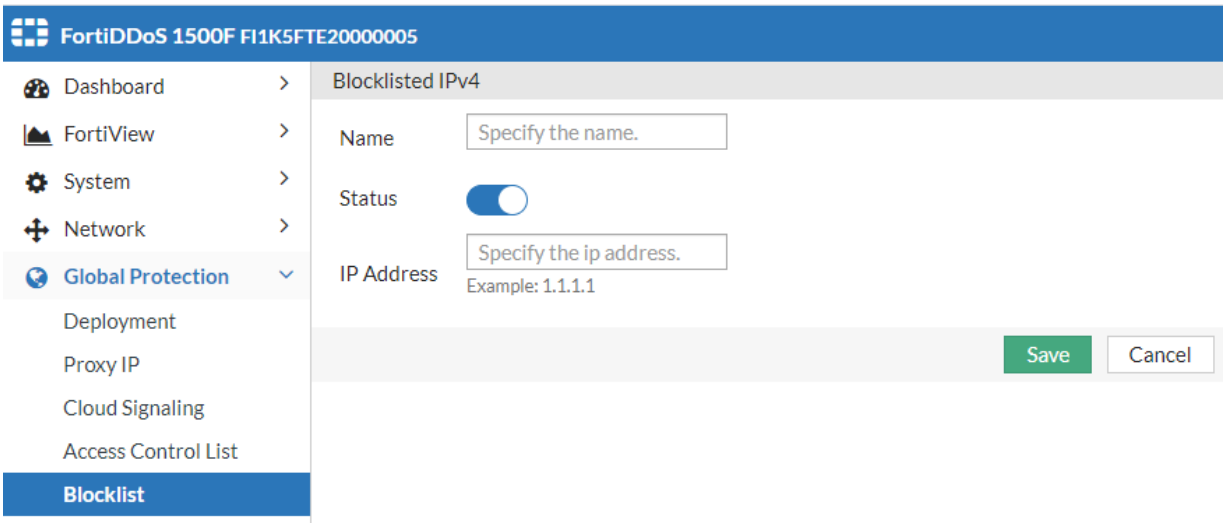
Use Blocklisted IPv4 Address option to deny ACL large sets of blocklisted IPv4 addresses.

Note: FortiDDoS does not support large IPv6 blockslists. Use Global ACLs instead.

To configure:

1. Go to *Global Protection* > *Blocklist* > *Blocklisted IPv4*.
2. Select the option based on the requirement:
   - **Upload**: Choose and upload the file with the list of blocklisted addresses. The supported file formats are Text, MS-DOS, CSV MS-DOS and CSV (comma delimited).
     Note:
     - List entries must be individual IP address with no netmask of any type. Order is not important.
     - If you upload a new file, the new file replaces the older database but does not affect the individually added address from *Create New* below. There is no “append” function for uploaded files.
     - FortiDDoS supports a maximum of 1 million IPv4 addresses in the upload file.
     - Uploads can take several minutes and there is no progress meter. Failure and success messages are displayed as appropriate.
   - **Download**: Save the blocklisted address list to your system. This file includes uploaded and individually added addresses.
   - **Clear**: Clear the current address list AND any individually added addresses from the GUI page list.
   - **Create New**: Add a new single address and click Save to include in the existing list. Added individual addresses are listed on the Blocklist page. FortiDDoS supports a maximum of 1024 manually added IP

Addresses.



- **Delete**: Delete added individual selected addresses from the list on the Blocklist page.

Configuring blocklisted domains

Use *Blocklisted Domains* option to deny ACL large sets of DNS domains.

To configure:

1. Go to *Global Protection* > *Blocklist* > *Blocklisted Domains*.
2. Select the option based on the requirement:
   - **Upload**: Choose and upload the file with the list of blocklisted domains. The supported file formats are Text, MS-DOS, CSV MS-DOS and CSV (comma delimited).
     Note:
     - List entries must be individual Fully Qualified Domain Names (FQDNs), including the TLD (e.g. mail.fortinet.com). Wildcard Domain Names are not supported.
     - If you upload a new file, the new file replaces the older database but does not affect the individually added address from *Create New* below. There is no “append” function for uploaded files.
     - FortiDDoS supports a maximum of 1 million FQDNs in the uploaded list.
     - Uploads can take several minutes and there is no progress meter. Failure and success messages are displayed as appropriate.
   - **Download**: Save the file with the list of blocklisted domains to your system. This file includes uploaded and individually added FQDNs.
   - **Clear**: Clear the current FQDN list AND any individually added FQDNs from the GUI page list.
   - **Create New**: Add a new single blocklisted domain and click *Save* to include it in the existing list. FortiDDoS allows a maximum of 1024 added Domains.
   - **Delete**: Enter the specific domain address to remove from the existing list and click *Delete*.

Note:

- Since a Domain name is present in both the Query and Response, Domain Blocklist will drop any Responses it sees containing blocklisted domains, even if FortiDDoS does not see the Query. This is useful in two circumstances:
  a. Asymmetric traffic where FortiDDoS is seeing the inbound traffic link only (does not see outbound Queries). Thus Domain Blocklist is effective on ISP peering and transit links to block malicious and botnet C&C Domains.
  b. Reflected Response Floods may use malicious FQDNs, in which case Domain Blocklist may see the flood before DQRM sees it.

Configuring Do Not Track / Track and Allow policies

Use to specify IP addresses that FortiDDoS *Do Not Track* or *Track and Allow*.

- *Do Not Track*—Does not monitor or track traffic to or from the configured IP addresses in any way
- *Track and Allow*—Monitors and reports but does not restrict traffic to/from the configured IP addresses

Use these allow-list policies with extreme care. No mitigation is performed when either of these policies is applied. Avoid using these polices for your protected IP addresses.

Do Not Track traffic is completely invisible to FortiDDoS with no monitoring nor mitigation

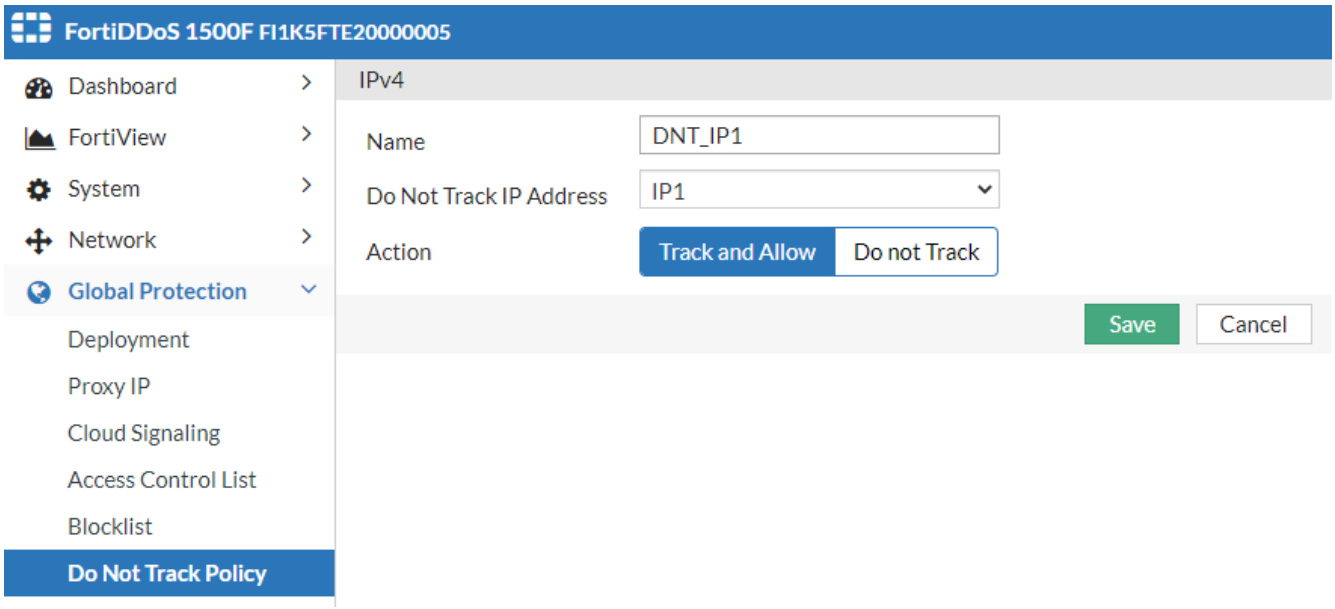
Track and Allow traffic is visible, displaying on graphs and logs with virtual drops (like a mini-Detection Mode) but it may not be obvious from the displayed information that the traffic is not being blocked.

Before you begin:

- You must have configured address objects that you want to match in policy rules. See Define system ACL objects on page 37.

To configure a Do Not Track / Track and Allow policy:

1. Go to *Global Protection* > *Do Not Track Policy* > *IPv4* or *IPv6*
2. Click *Create New*.
3. Complete the configuration as described in the table below.
4. Save the configuration.



Settings	Guidelines
Name	Configuration name. a-Z,0-9, - , _ only (no spaces)
Do Not Track IP Address	Dropdown menu of IP Addresses, Subnets or IP Ranges previously configured in *System* > *Address and Service*. **Note:** Do Not Track does not support Geolocation, Groups or Services
Action	• Track and Allow—Traffic is not dropped for any reason. Traffic is monitored and virtual drops are displayed in graphs and logs. Traffic is included in Traffic Statistics for Threshold settings. • Do not track—Traffic is invisible – no monitoring, no graphs, logs or drops of any kind.

Configured policies are shown on the *Do Not Track Policy* page. You can Edit, Delete, and Clone policies from the GUI using the icons on the right.

Configuring GRE tunnel endpoint addresses

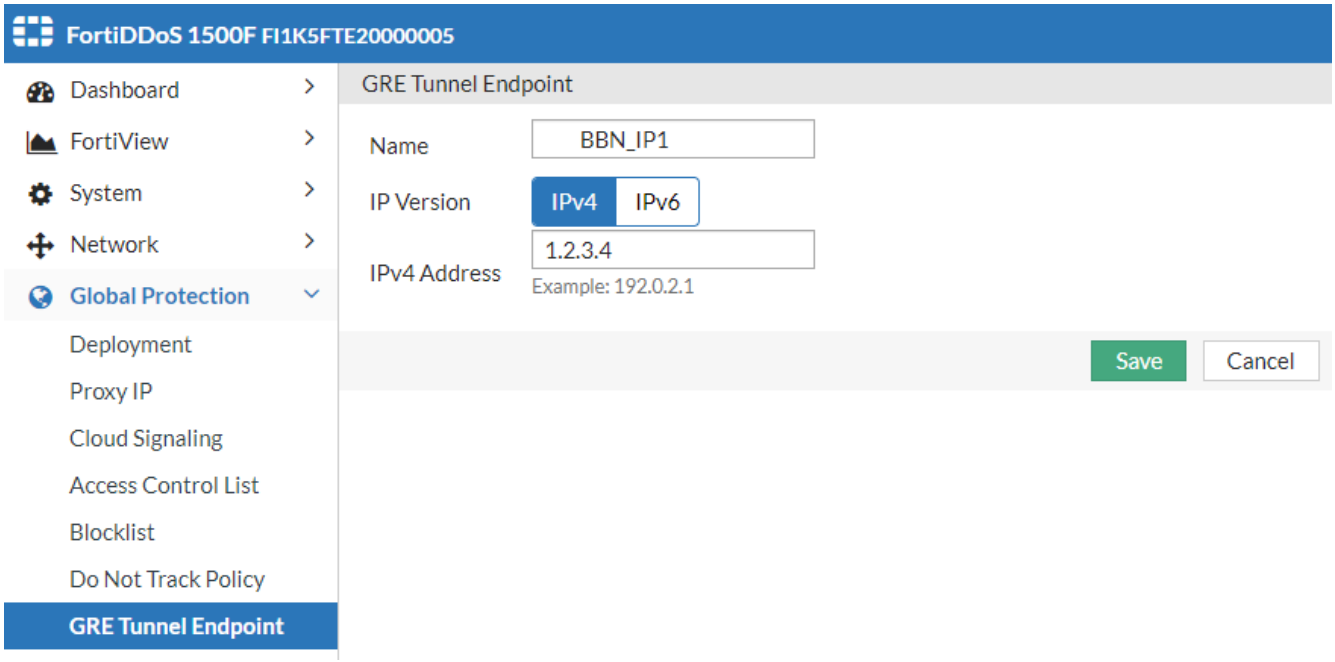
Overview

If you are using always-on or on-demand cloud DDoS mitigation, in most cases the Service Provider will return clean traffic to you via a GRE tunnel. Since the GRE tunnel encapsulates all other traffic, it can mask anomalies and other attack traffic missed by the cloud provider. Using the GRE tunnel endpoint feature, FortiDDoS can process this traffic to give you an identical graphical view and complete mitigation for the original packets.

This feature can also be used to monitor other Point-to-Point GRE tunnels you may use.

To monitor GRE tunnels

1. Go to *Global Protection* > *GRE Tunnel Endpoint*.
2. Click *Create New*.
3. Enter the settings according to the table below for both the service provider IPs and your terminating IPs. Click *Save*.
4. The entries will be displayed on the GRE Tunnel Endpoint list page.



Setting	Description
Name	a-Z, 0-9, _, - only (no spaces)
IP Version	IPv4 or IPv6
IP Address	IPv4 or IPv6 address of: • Source IP (outside) public IP address(es) of the Service Provider's GRE tunnel(s). • Destination (your protected) public IP address(es) of the device (usually your firewall) terminating the GRE tunnel(s). **Note:** • These addresses must not be part of the /24 subnet that is diverted to the Cloud DDoS service provider • IP address with no netmask (assumed /32)

Since any IP addresses terminating the GRE tunnel on your firewall are public IP addresses, there is some risk they could be attacked if the attacker can discover the addresses.

We recommend that you create a separate SPP for your GRE terminating IPs.

1. Create a new *Service Protection* > *Service Protection Policy*.
2. Save, Edit and Add Protection Subnets for your terminating IP address(es). Do not include the Service Provider's IP addresses. Your GRE IPs should be the only IPs or subnets in this SPP.
   a. Configure this SPP to system minimum Thresholds. This can be done by running Traffic Statistic for a 1-hour period and setting System Recommendations. Since there is normally no traffic on this SPP, the Thresholds will be set to the default Minimums.
   b. Set Protocol 47 (GRE) Thresholds to system maximums in both directions. You may want to adjust this threshold to 3x actual traffic but you will only be able to see GRE traffic when the Cloud DDoS Mitigation service is sending GRE traffic.
3. Consider ACLing all Protocols except 1 for ICMP and 6 for BGP signaling via TCP. Consider ACLing all TCP ports except 179 (BGP) and set the ICMP Protocol rate threshold under 100pps.
   None of the GRE-encapsulated "inner" traffic will be seen on this SPP, since it will be assigned to SPPs based on the inner IP address headers.
4. You will see the "outer" GRE traffic for this SPP in *Monitor* > *Layer 3/4/7* > *Layer 3* > *Protocols*. Enter *Protocol 47*.

Non-FortiDDoS Requirements:

- It is important to ensure that your network MTU/MSS is set correctly to prevent significant fragmentation of arriving traffic with the added GRE overhead. Normally, both MTU and MSS must be lowered to prevent fragmentation of TCP and UDP packets, but please discuss with your Cloud DDoS Mitigation Service Provider.
- Check that Path MTU is working end-to-end through the GRE tunnel.
- Determine if your cloud mitigation service provider will use Direct Server Response (normal) where outbound traffic will be sent via your local ISP or routing mode (Inbound and outbound traffic in GRE).
  Ensure that your firewall is capable of decapsulating the full inbound normal data rate of your clean traffic (Direct Server Return) or total traffic (Routing Mode).

Operation

When the system sees GRE traffic destined to one of the defined GRE Endpoint IP addresses in the list and the Source also matches an IP address in the list, it does the following:

- Always allows the GRE packet.
- Inspects the "inner" L3/L4/L7 headers of the GRE packet, which is the original packet, and assigns the traffic to the Protection Subnet and SPP as it normally would for non-GRE traffic. All settings and thresholds as configured for the SPP, are used for these SPPs. Monitor graphs, logs, reports and so on will all operate on this 'clean' traffic as if it was the only traffic present. If the Cloud Mitigation Service Provider has missed any mitigations, they will be performed on this traffic, determined by the SPP Detection or Prevention Mode, with appropriate graphs and logs.
- Displays the ingress/egress GRE traffic in the *Monitor* > *Layer 3/4/7* > *Layer 3* > *Protocol 47* graph.
- If the system sees GRE traffic destined to an IP that is not matched by another address in the Endpoint list, it will treat it as normal traffic and assign it to the appropriate SPP as GRE protocol 47 traffic without further inner header inspection.

Service Protection

This section includes the following topics:

Service Protection Policy Overview

Service Protection Policy is a critical feature and foundation behind FortiDDoS technology.

It allows users to:

- Associate DDoS mitigation policies to subnets to be protected.
- Configure thresholds manually and automatically, using FortiDDoS Traffic learning mechanism to prevent volumetric DDoS attacks.
- Configure subnets with Cloud Signaling thresholds
- Configure ACLs on different services
- Link Protection profiles for DNS, TCP, IP, ICMP, etc. with SPP Rule

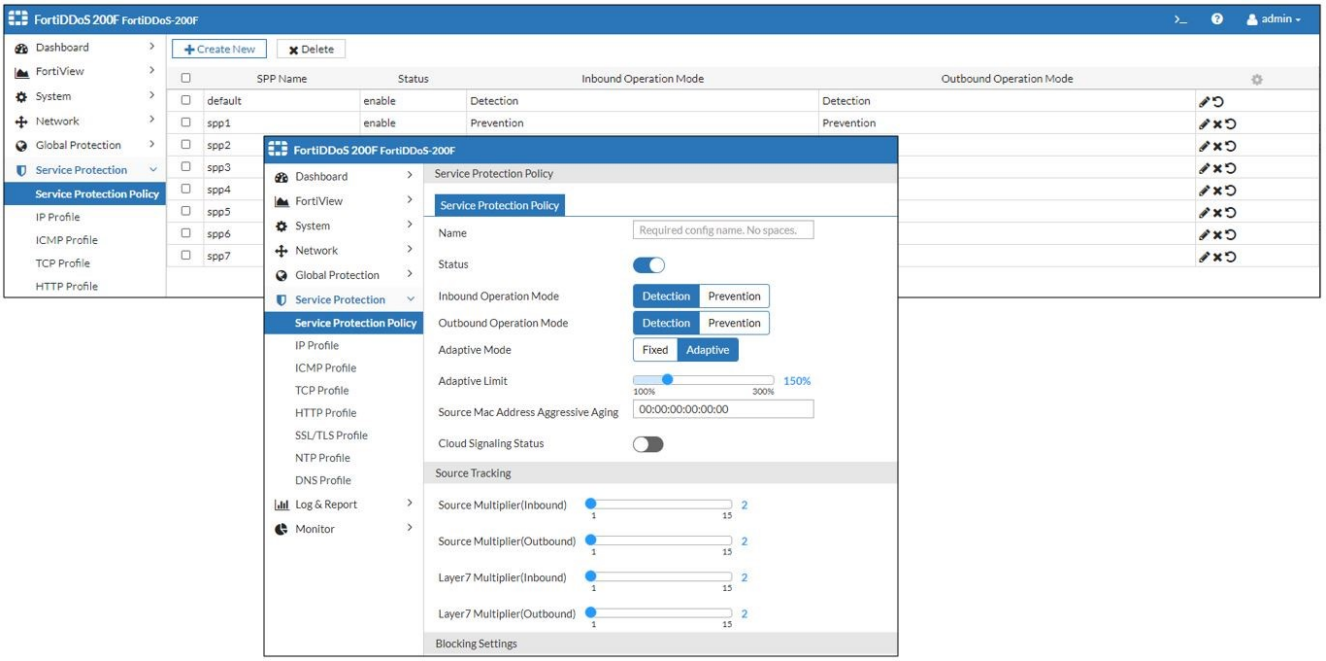
Before you begin:

- You must have a good understanding of the features you want to enable. Refer to Key Concepts for more information.
- You must have Read-Write permission for Protection Profile settings.

Configuring Service Protection Policies

Every Service Protection Policy(SPP) Rule has its own Round Robin Database (Graph), generates its own mysql events, and protects a separate set of subnets.

Every FortiDDoS System is built with Default SPP by default.



To create SPP rule:

On the *Service Protection Policy* tab, click *Create New* and follow the prompts.

Note:

- Initially, the SPP Status is set to *Disabled* and you cannot enable the SPP until at least one Protection Subnet is configured.

Do not forget to enable the SPP Status after entering the Protection Subnets. If you do not enable, all traffic for that SPP is forwarded to the default SPP and no learning or mitigation will be done by the SPP.

- Creating a new SPP rule may be disallowed if the system reaches the maximum limit of SPP rules per platform (as defined in the FortiDDoS datasheets).
- Creating an SPP Rule triggers a Round Robin Database(RRD) creation for that SPP, which takes approximately 3-7 minutes depending upon the platform.

To configure using the CLI:

```
config ddos spp rule
   edit <spp_name>
   next
end
```

To edit SPP rule:

Double click the SPP Rule entry and modify the existing configuration.

This action may not be allowed if the SPP Rule Reset Action is in progress

To configure using the CLI:

```
config ddos spp rule
   edit <spp_name>
   next
end
```

To reset SPP rule:

Click the Reset button for each SPP rule entry.

This action is used to reset all Configuration and Traffic data associated with the SPP Rule.

SPP RRD Reset operation from CLI is not allowed while SPP Reset operation is in progress.

To configure using the CLI:

```
execute spp-factory-reset spp <spp_name>
```

To delete SPP rule:

Check the boxes next to the SPP rules you want to delete and then click the *Delete* button.

This action is not applicable to the default SPP Rule.

To configure using the CLI:

```
config ddos spp rule
   delete <spp_name>
   next
end
```

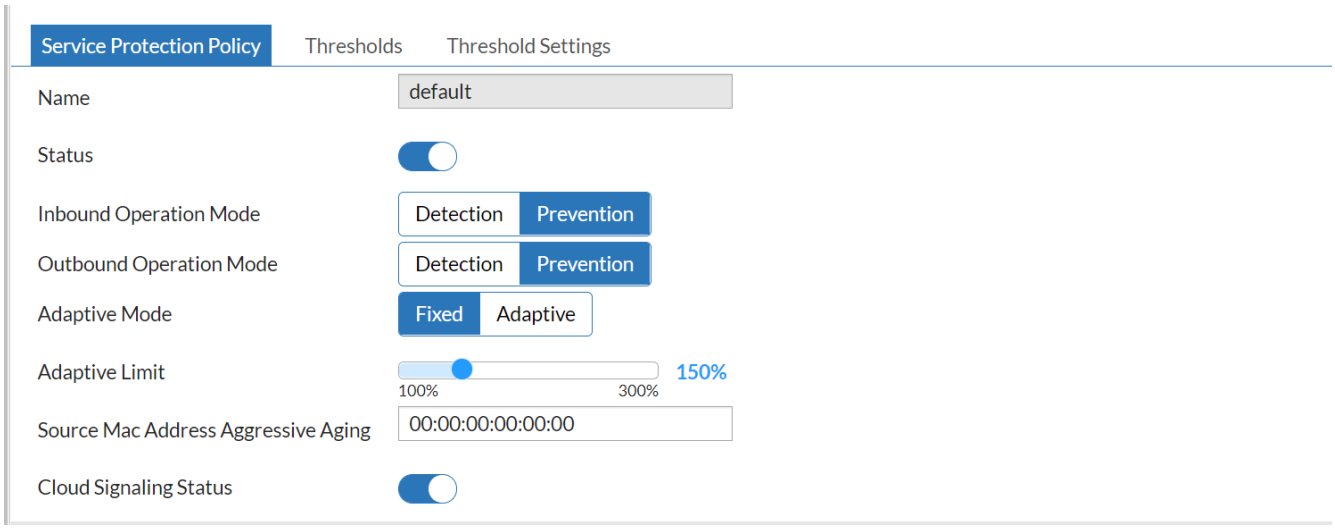
Service Protection Policy Feature Settings

Settings	Guidelines
Name	Name of SPP rule. This field accepts alphanumeric characters and doesn't allow special characters. It should match regular expression `/^[A-Z a-z0-9_.-]*@?[A-Za-z0-9_.-]*$/`.
Status	This feature control allows the user to disable the SPP Rule. This action will divert traffic to Default SPP Rule or any other SPP which will have next longest prefix match.
Inbound Operation Mode	Set the mode for traffic received from WAN-side interfaces: • Detection—Logs events and builds traffic statistics for the profile but does

Settings	Guidelines
	not limit or block traffic. • Prevention—Limits and blocks traffic that exceeds thresholds.
Outbound Operation Mode	Set the mode for traffic received from LAN-side interfaces: • Detection—Logs events and builds traffic statistics for the profile but does not limit or block traffic. • Prevention—Limits and blocks traffic that exceeds thresholds.
Adaptive Mode	• Fixed—Does not use the adaptive limit. The configured minimum thresholds are the maximum limits. • Adaptive—Uses the adaptive limit. The configured minimum thresholds multiplied by the adaptive limit are the maximum limits.
Adaptive Limit	A percentage of the configured minimum threshold that establishes the upper limit of the estimated threshold. The adaptive limit is an upper rate limit beyond which the system blocks all traffic. The valid range is 100% to 300%. For example, the default is 150%. The system uses the dynamic threshold estimation algorithm to raise the calculated threshold up to 150% of the value of the configured minimum threshold. Thus, if the inbound threshold for Protocol 17 (UDP) is 10,000, the threshold never falls below 10,000 and never exceeds 15,000. When the adaptive limit is 100, the system does not use dynamic threshold estimation to adjust thresholds.
Source MAC Address Aggressive Aging	MAC address used to send TCP resets to the protected server when aggressive aging is triggered. Please note, any packets generate by FortiDDoS will use MAC address specified here. By default, the system uses the MAC address of the management interface (mgmt1), but the MAC address displayed in the web UI is `00:00:00:00:00:00`. If you change this setting, the system uses the MAC address you specify.
Cloud Signaling Status	This setting allows to enable/disable Cloud signaling feature for this specific SPP Rule.

To configure using the CLI:

```
config ddos spp rule
   edit <spp_name>
      set status { enable | disable }
      set inbound-operating-mode { detection | prevention }
      set outbound-operating-mode { detection | prevention }
      set adaptive-mode { fixed | adaptive }
      set adaptive-limit <integer>
      set source-mac-address-aggressive-aging <string>
      set cloud-signaling-status { enable | disable }
   next
end
```



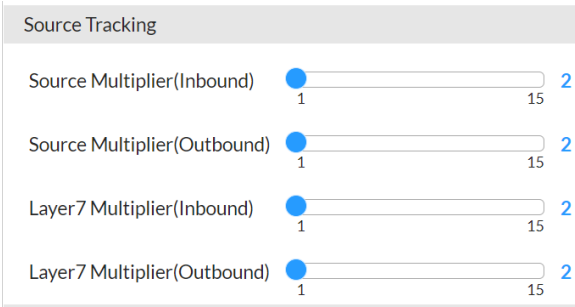
Source tracking

This feature allows users to penalize source creating non-source attacks i.e. Protocol Flood, so that 1 high volume source shouldn't affect other legitimate sources.

Settings	Guidelines
Source Multiplier Inbound/Outbound	Applies the specified multiplier to the packet count for traffic with a source IP address that the system has identified as the source of a flood. In effect, the multiplier makes traffic from the source violate thresholds sooner. The default is 2. For example, if the most active source threshold is 100 packets per second, and the source multiplier is 4, an identified source attacker will violate the threshold if it sends 26 packets per second. Because incoming traffic is more likely to be the source of a threat, you can configure different multipliers for incoming and outgoing traffic.
Layer 7 Multiplier Inbound/Outbound	Applies the specified multiplier to the packet count for traffic that the system has detected is related to a Layer 7 HTTP flood. The system tracks HTTP headers (URL or Host, Referer, Cookie or User-Agent header) and associates traffic with matching headers with the attack. The default is 2. **Note:** When both Source flood and Layer 7 flood conditions are met, the packet count multipliers are compounded. For example, when there is a User Agent flood attack, a source is sending a User-Agent that is overloaded. If the Source multiplier is 4 and the Layer 7 multiplier is 64, the total multiplier that is applied to such traffic is 4 x 64 = 256. In effect, each time the source sends a Layer 7 packet with that particular User-Agent header, FortiDDoS considers each packet the equivalent of 256 packets.

To configure using the CLI:

```
config ddos spp rule
   edit <spp_name>
      set source-multiplier-inbound <integer>
      set source-multiplier-outbound <integer>
      set layer-7-multiplier-inbound <integer>
      set layer-7-multiplier-outbound <integer>
   next
end
```



Blocking settings

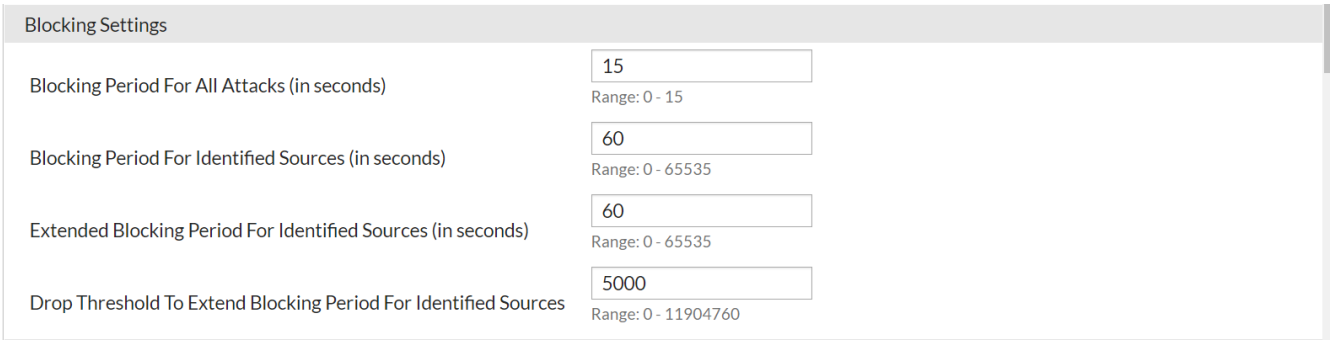
Settings	Guidelines
Blocking Period for All Attacks	When an attack threshold is triggered, traffic from any Source IPs sending this type of traffic is blocked for this period of time. This provides the system an opportunity to Source Track all Sources associated with this attack. If a Source does not exceed Source Tracking thresholds during this time, it is unblocked immediately. The default is 15 seconds. The valid range is 1 to 15 s. During the blocking period above, Sources identified by Source Tracking will be further blocked for the duration of the Blocking Period for Identified Sources, described below.
Blocking Period for Identified Sources	How long to block all traffic from a source IP address identified by Source Tracking during the initial Blacking Period above. The default is 60 seconds. The valid range is 1 to 255 s. When an attack threshold is triggered, while in the initial blocking period above, the system multiplies the packet rate from any blocked source by the value of the source multiplier. If the calculated rate exceeds the value of the most-active-source threshold, the system identifies the IP address of the source as a source attacker and blocks that Source for the period entered here (extending the initial blocking period). At the end of this Blocking Period, the Source IP traffic is evaluated again by the criteria below.
Extended Blocking Period for Identified Sources	If a blocked Source IP continues to send attack traffic and exceeds the number of dropped packets described below, during the Blocking Period above, the blocking period is again extended by this Extended Blocking Period.

Settings	Guidelines
	The default is 60 seconds. The valid range is 1 to 255 s. At the end of this Extended Blocking Period, the Source IP is evaluated again by the same drops-per-Extended Blocking Period criteria and continues to be blocked for the Extended Blocking Period until the drop rate falls below the Threshold.
Drop Threshold to Extend Blocking Period for Identified Sources	Number of dropped packets that trigger the extended blocking period. The default is 5,000 dropped packets.

The multiple Blocking Periods described above minimizes false positives. For example, if the system sees a Fragment Threshold crossed, it blocks all the Source IPs sending fragments for the initial Blocking Period, while evaluating all the Sources. If a Source is sending at a lower fragment rate than the Source Tracking rate, it will be released after no longer than 15 seconds (default) and usually much faster than that. Sources Identified by Source Tracking as over-threshold will immediately be blocked for the duration of the Blocking Period for Identified Sources (60 s default). At the end of that period, if those Sources have fallen below the Drop Threshold count, they will be unblocked. If they exceed the Drop Threshold count, they will be blocked for the duration of the Extended Blocking Period (60 s default) and evaluated again, remaining blocked until their drop rate declines below the Drop Threshold count.

To configure using the CLI:

```
config ddos spp rule
   edit <spp_name>
      set blocking-period <int>
      set source-blocking-period <int>
      set extended-blocking-period <int>
      set drop-threshold-within-blocking-period <int>
   next
end
```



Service port settings

By default, the FortiDDoS system listens for HTTP traffic on service port 80 and SSL traffic on service port 43. If the servers in your network use nonstandard ports for HTTP or SSL traffic, you can configure the system to listen for HTTP & SSL on nonstandard service ports. You can configure up to 128 HTTP or SSL service ports or port ranges.

Note: If you have configured or removed a Service Port AFTER you have created System Recommended Thresholds, you must run them again for every SPP.

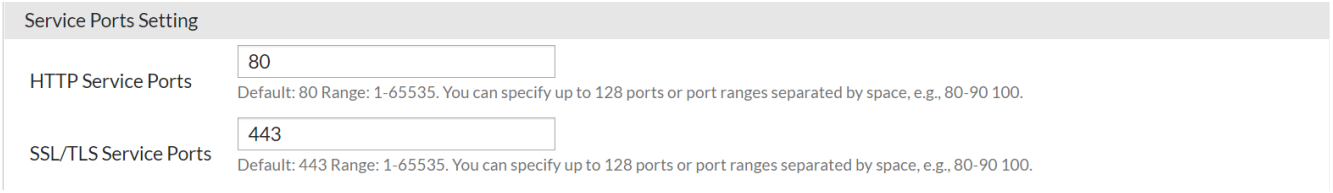
The system recommended threshold procedure excludes HTTP & SSL service ports from the port configuration ranges that it generates. When user-configured HTTP and SSL service ports are enabled, the packet rate thresholds for the user-configured ports are set to a high rate. If HTTP or SSL service port configuration is subsequently removed, the threshold remains at the high rate until you change it manually or perform the System Recommended Threshold procedure.

Before you begin:

- You must have Read-Write permission for Global Settings.

To configure HTTP Service Port settings:

1. Go to *Service Protection* > *Service Protection Policy* > *{SPP Rule}* > *Service Protection Policy* > *Service Port Settings*
2. Enter list of ports or port ranges, each separated by a space
3. Click *Save*.



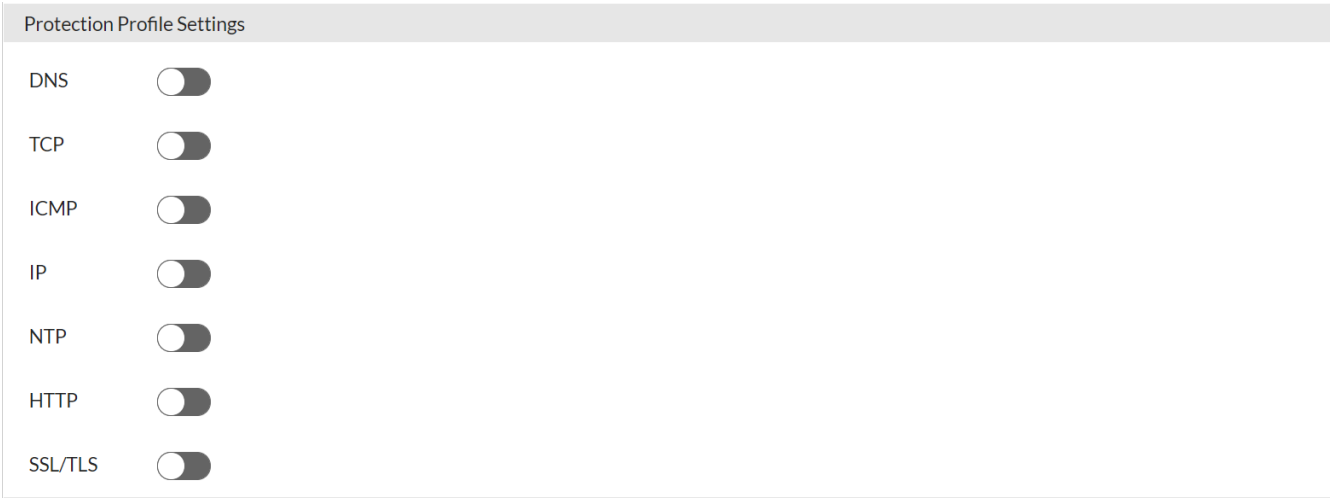
To configure using the CLI:

```
config ddos spp rule
   edit <spp_name>
      set http-service-port <value>
      set ssl-service-port <value>
   next
end
```

Protection profile settings

This section of Service Protection Policy allows the user to associate different protocol mitigations to SPP Rule. Every service protection policy can link profiles for mitigations of TCP, DNS, IP, ICMP, HTTP, SSL/TLS, NTP.

Note: Each SPP Rule can only be associated with one profile of each type at a time.



To configure using the CLI:

```
config ddos spp rule
   edit <spp_name>
      set http-profile <http_profile_name>
      set ntp-profile <ntp_profile_name>
      set dns-profile <dns_profile_name>
      set tcp-profile <tcp_profile_name>
      set ssltls-profile <ssltls_profile_name>
      set ip-profile <ip_profile_name>
      set icmp-profile <icmp_profile_name>
   next
end
```

Protection subnets

These are IPv4/IPv6 subnets configured with SPP Rule for which SPP settings are applicable to. These subnets are inside networks that FortiDDoS should to protect. Every subnet also has parameters for Signaling as Signaling threshold KPPS (i.e. unit of thousand packet per seconds) and Mbps.

Note: Default SPP is built on the system with 2 default Subnets Any-IPv4 and Any-IPv6. Traffic that is not classified by any IPv4 or IPv6 subnet on system will be classified under these 2 default subnets.

To add a new subnet:

Click Create New under Protection Subnets.

Note: Every SPP Rule has a maximum limit of subnets as specified in the FortiDDoS-F Data sheet.

To edit a subnet:

Double click an entry or click the edit icon next to the entry.

Note: This action is not applicable for Default subnets Any-IPv4 and Any-IPv6.

To clone a subnet:

Click the clone icon next to the entry.

Note: This action is only available in the GUI

To delete a subnet:

Check the boxes next to the entries you want to delete and then click the *Delete* button.

This action is not applicable to default subnets Any-IPv4 and Any-IPv6.

To configure using the CLI:

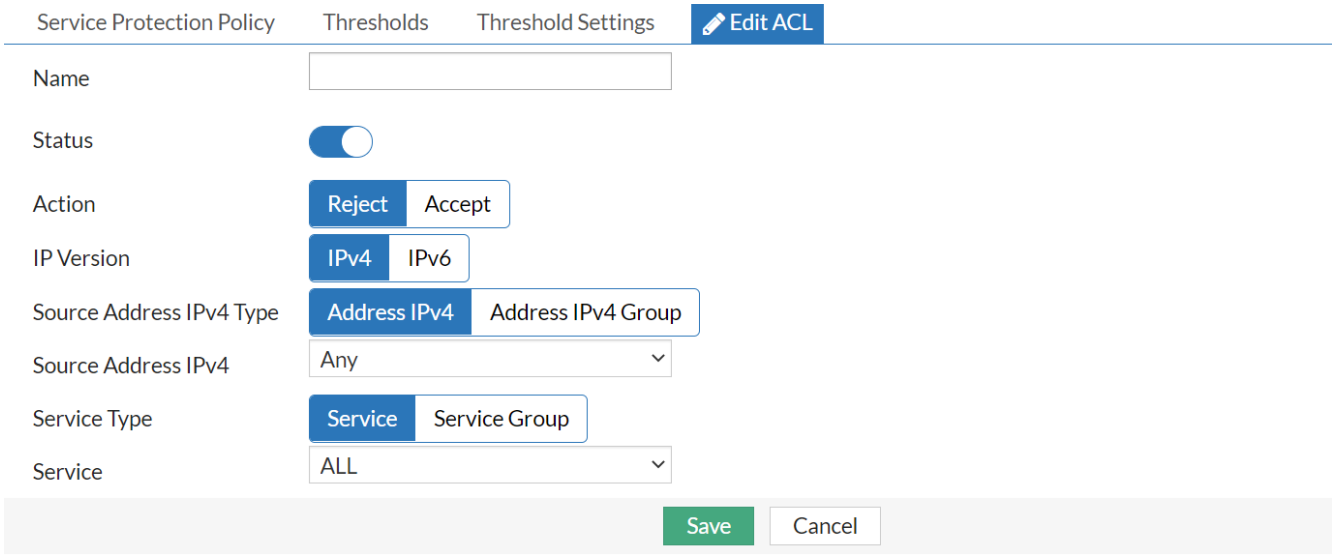
```
config ddos spp rule
   edit <spp_name>
      config address
         edit <subnet_name>
            set type { ipv4-netmask | ipv6-prefix}
            set ip-netmask <ipv4-netmask>
            set ipv6-prefix <ipv6-prefix>
            set signaling-threshold-kpps <integer>
            set set signaling-threshold-mbps <integer>
         next
      end
   next
end
```

Settings	Guidelines
Type	Choose between IPv4 Netmask and IPv6 Prefix
IPv6/IPv6 Adress	Configure subnet with prefix based upon Type selected
Signaling Threshold Kpps	These thresholds are used for Attack Signaling to Cloud DDoS service Providers by sending REST API information when traffic crosses this value for a particular subnet Make sure following configuration is created successfully for these settings to take into effect • Configure a valid Third Party Cloud Signaling device at *Global Protection* > *Cloud Signaling* > *Devices* • Enable Cloud Signaling Status for SPP rule
Signaling Threshold Mbps	

ACLs

This feature provides the option for the user to have more restricted access to traffic going to specific SPP Rule. It allows the user to reject/accept traffic from IPv4/IPv6 Address/Address Group sending traffic which match certain Service/Service group traffic. This can offload a lot of burden from DDoS Mitigation by eliminating unwanted traffic.

Note: Any traffic that matches SPP Rule with action Accept will be tracked and allowed and no DDoS Mitigation mechanisms will be applied.



Settings	Guidelines
Name	Name of ACL
Status	Control to enable or disable ACL
Action	Reject or Accept traffic
IP Version	IPv4 or IPv6
Source Address IPv4 Type	Address IPv4 or Address IPv4 Group
Source Address IPv4	• Address IPv4 : Entry configured under *System* > *Address and Service* > *Address IPv4* • Address IPv4 Group: Entry configured under *System* > *Address and Service* > *Address IPv4 Group*
Source Address IPv6 Type	Address IPv6 or Address IPv6 Group
Source Address IPv6	• Address IPv6 : Entry configured under *System* > *Address and Service* > *Address IPv6* • Address IPv6 Group: Entry configured under *System* > *Address and Service* > *Address IPv6 Group*
Service Type	Service or Service Group
Service	• Service: Entry configured under *System* > *Address and Service* > *Service* • Service Group: Entry configured under *System* > *Address and Service* > *Service Group*

To configure using the CLI:

```
config ddos spp rule
   edit <spp_name>
      config acl
         edit <acl_name>
            set status { enable | disable }
            set action { reject | accept }
            set ip-version { IPv4 | IPv6 }
            set source-address4-type { addr4 | addr-grp4 }
            set source-address-v4 <IPv4 Address>
            set source-address-v4-group <IPv4 Address Group>
            set source-address6-type { addr6 | addr-grp6 }
            set source-address-v6 <IPv6 Address>
            set source-address-v6-group <IPv6 Address Group>
            set service-type { service | service-grp}
            set service-id <Service>
            set service-grp-id <Service Group>
         next
      end
   next
end
```

Thresholds

Thresholds Overview

You can use the *Service Protection* > *Service Protection Policy* > *Thresholds* page to review system recommended thresholds and to make manual adjustments as you fine tune the configuration.

One of the key features of the FortiDDoS solution is the availability of system recommended thresholds that are adapted automatically according to statistical trends and tested heuristics. We recommend that in most cases, you should rely on the system intelligence. In some cases, such as demonstration, test, and troubleshooting situations, you might want to specify user-defined values for one or more thresholds. The threshold configuration is open, and can be updated manually.

Thresholds View

Before you begin:

- You must have an expert understanding of packet rates and other Layer 3, Layer 4, and Layer 7 parameters that you want to set manually. Refer to Understanding FortiDDoS rate limiting thresholds on page 24.
- You must have Read-Write permission for Protection Profile settings.

To configure threshold settings:

1. Go to *Service Protection* > *Service Protection Policy* > *{SPP Rule}* > *Thresholds*.
2. Select the type of Threshold from the drop-down list.
3. Double-click the row for the threshold you want to edit or click *Create New*.

4. Set thresholds for inbound and outbound traffic for the settings described in the table below.
5. Save the configuration.

Threshold Settings Configuration

Threshold	Guidelines	Graph
	Scalars	
syn	Packet/second rate of SYN packets received. Threshold for a SYN Flood event. When total SYNs to the SPP exceeds the threshold, the SYN flood mitigation mode tests are applied to all new connection requests from IP addresses that are not already in the legitimate IP address table. **Prerequisite:** A TCP Profile with following settings should be linked: SYN Flood Mitigation => Enabled TCP Session Feature Control : SYN Validation => Enabled	**Drop Monitor:** Flood Drops > Layer 4 **Traffic Monitor:** Layer 3/4/7 > Layer 4 > SYN
new-connections	Connection/second rate of new connections. Threshold for zombie floods (when attackers hijack legitimate IP addresses to launch DDoS attacks). When it detects a zombie flood, FortiDDoS blocks all new connection requests for the configured blocking period. In order to be effective, the new-connections threshold should always be higher than the syn threshold. We recommend that you use the FortiDDoS generated threshold unless you have a specific reason to change it. **Prerequisite:** A TCP Profile with following settings should be linked to generate SYN Flood scenario: SYN Flood Mitigation => Enabled TCP Session Feature Control : SYN Validation => Enabled	**Drop Monitor:** Flood Drops > Layer 4 **Traffic Monitor:** Layer 3/4/7 > Layer 4 > Other
syn-per-src	Packet/second rate of SYN packets from any one source. No single source in an SPP is allowed to exceed this threshold. Threshold for a SYN Flood from Source event. The system applies the blocking period for identified sources. Only SYNs from identified source will be blocked	**Drop Monitor:** Flood Drops > Layer 4 **Traffic Monitor:** Layer 3/4/7 > Layer 4 > SYN

Threshold	Guidelines	Graph
	Scalars	
most-active-source	Packet/second rate for the most active source. A source that sends packets at a rate that surpasses this threshold is considered a threat. Threshold for a source flood. No single source in an SPP is allowed to exceed this threshold, and the system applies the blocking period for identified sources. All traffic from identified source will be blocked	**Drop Monitor:** Flood Drops > Layer 3 **Traffic Monitor:** Layer 3/4/7 > Layer 3 > Sources
concurrent-connections-per-source	Count of TCP connections from a single source. The TCP connection counter is incremented when a connection moves to the established state and decremented when a session is timed out or closes. This threshold is used to identify suspicious source IP behavior. An inordinate number of connections is a symptom of both slow and fast TCP connection attacks. The system applies the blocking period for identified sources for SYN (session initiation). If the aggressive aging *high-concurrent-connection-per-source* option is enabled, the system also sends a TCP RST to the server to reset the connection.	**Drop Monitor:** Flood Drops > Layer 4 **Traffic Monitor:** Layer 3/4/7 > Layer 4 > Other
syn-per-dst	Packet/second rate for SYN packets to a single destination. When the per-destination limits are exceeded for a particular destination, the SYN flood mitigation mode tests are applied to all new connection requests to that particular destination. Traffic to other destinations is not subject to the tests. The system applies the blocking period for identified sources. **Prerequisite:** A TCP Profile with following settings should be linked to generate SYN Flood scenario: SYN Flood Mitigation => Enabled TCP Session Feature Control : SYN Validation => Enabled	**Drop Monitor:** Flood Drops > Layer 4 **Traffic Monitor:** Layer 3/4/7 > Layer 4 > SYN

Threshold	Guidelines	Graph
	Scalars	
method-per-source	Packet/second rate for Method packets (GET, HEAD, OPTION, POST, etc) from a single Source. When the per-source limits are exceeded for a particular source, the system applies the blocking period for identified sources sending HTTP traffic. The connection to the server may also be RST if *Protection Profiles* > *SPP Settings* > *TCP* Tab: *Aggressive Aging TCP Connections Feature Control: Layer 7 Flood* is enabled.	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > HTTP
most-active-destination	Packet/second rate for the most active destination. A destination that is sent packets at this rate is considered under attack. Threshold for a destination flood.	**Drop Monitor:** Flood Drops > Layer 3 **Traffic Monitor:** Layer 3/4/7 > Layer 3 > Destinations
oth-fragment	Packet/second rate of fragmented packets received for Protocols Except TCP and UDP. Although the IP specification allows IP fragmentation, excessive fragmented packets can cause some systems to hang or crash.	**Drop Monitor:** Flood Drops > Layer 3 **Traffic Monitor:** Layer 3/4/7 > Layer 3 > Other
udp-fragment	Packet/second rate of UDP fragmented packets received. Although the IP specification allows IP fragmentation, excessive fragmented packets can cause some systems to hang or crash.	**Drop Monitor:** Flood Drops > Layer 3 **Traffic Monitor:** Layer 3/4/7 > Layer 3 > Other
tcp-fragment	Packet/second rate of TCP fragmented packets received. Although the IP specification allows IP fragmentation, excessive fragmented packets can cause some systems to hang or crash.	**Drop Monitor:** Flood Drops > Layer 3 **Traffic Monitor:** Layer 3/4/7 > Layer 3 > Other
dns-query-udp	Queries/second. Threshold for a DNS Query Flood event for traffic over UDP. **Prerequisite:** A DNS Profile should be linked to SPP rule	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > DNS
dns-query-tcp	Queries/second. Threshold for a DNS Query Flood event for traffic over TCP. **Prerequisite:** A DNS Profile should be linked to SPP rule	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > DNS
dns-question-count-udp	Question count/second. Threshold for a DNS Question Flood over UDP event.	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:**

Threshold	Guidelines	Graph
	Scalars	
	Prerequisite: A DNS Profile should be linked to SPP rule	Layer 3/4/7 > Layer 7 > DNS
dns-question-count-tcp	Question count/second. Threshold for a DNS Question Flood over TCP event. **Prerequisite:** A DNS Profile should be linked to SPP rule	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > DNS
dns-mx-count-udp	Packet/second rate of DNS queries for MX records (QTYPE=15). Threshold for a DNS MX Flood over UDP event. **Prerequisite:** A DNS Profile should be linked to SPP rule	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > DNS
dns-mx-count-tcp	Packet/second rate of DNS queries for MX records (QTYPE=15). Threshold for a DNS MX Flood over TCP event. **Prerequisite:** A DNS Profile should be linked to SPP rule	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > DNS
dns-all-udp	Packet/second rate of DNS queries for all DNS records (QTYPE=255). Threshold for a DNS ALL Flood over UDP event. **Prerequisite:** A DNS Profile should be linked to SPP rule	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > DNS
dns-all-tcp	Packet/second rate of DNS queries for all DNS records (QTYPE=255). Threshold for a DNS ALL Flood over TCP event. **Prerequisite:** A DNS Profile should be linked to SPP rule	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > DNS
dns-zone-xfer-tcp	Packet/second rate of DNS zone transfer (AXFR) queries (QTYPE=252). Threshold for a DNS Zone Transfer Flood event. **Prerequisite:** A DNS Profile should be linked to SPP rule	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > DNS
dns-fragment-udp	Packet/second rate of fragmented packets received. Threshold for a DNS Fragment Flood over UDP event. **Prerequisite:** A DNS Profile should be linked to SPP rule	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > DNS
dns-fragment-tcp	Packet/second rate of fragmented packets received. Threshold for a DNS Fragment Flood over TCP event.	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:**

Threshold	Guidelines	Graph
	Scalars	
	Prerequisite: A DNS Profile should be linked to SPP rule	Layer 3/4/7 > Layer 7 > DNS
dns-query-per-src	Packet/second rate of normal DNS queries from any one source. No single source in an SPP is allowed to exceed this threshold. Threshold for a DNS Query Per Source flood event. The system applies the blocking period for identified sources. **Prerequisite:** A DNS Profile should be linked to SPP rule with DNS Source blocking feature set to Enable	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > DNS
dns-packet-track-per-src	Packet/second rate of a source that demonstrates suspicious activity, a score based on heuristics that • count fragmented packets • response not found in DQRM • queries that generate responses with RCODE other than 0. Threshold for a DNS Suspicious Sources flood event. The system applies the blocking period for identified sources. **Prerequisite:** A DNS Profile should be linked to SPP rule with DNS Source blocking feature set to Enable	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > DNS
ntp-req	Rate Limit of NTP Requests to or from the SPP	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > NTP
ntp-resp	Rate Limit of NTP Responses to or from the SPP. Usage: This Threshold can be set for any environment but if FortiDDoS sees both Requests and Responses (symmetric traffic or both asymmetric links pass through FortiDDoS) the Unsolicited Response Anomaly feature above will respond to NTP Response Floods faster than this Thresholds. These is no harm in using both. If FortiDDoS is in Asymmetric Mode, use this Threshold and DISABLE the NTP Unsolicited Response Anomaly.	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > NTP

Threshold	Guidelines	Graph
	Scalars	
	Note: NTP Response attacks are common. Always set a Response Threshold or use NTP Unsolicited Response (NRM) Anomaly.	
ntp-bcast	Rate Limit of NTP Broadcast packets to or from the SPP. Usage:.You should never see NTP Broadcast packets on public networks. If, during Learning/Detection Mode, you see these in either direction, examine the protected IPs involved to see if they are originating, terminating or spoofed. Unless you know you are broadcasting for some reason, this Thresholds can be set to zero.	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > NTP
ntp-resp-per-dst	Rate Limit of NTP Responses per individual Destination. Usage: This Threshold can be set for any environment. This threshold will normally be less than or equal to the “Response Threshold” above. If FortiDDoS sees both Requests and Responses (symmetric traffic or both asymmetric links pass through FortiDDoS) the Unsolicited Response Anomaly feature above will respond to NTP Response per Destination Floods faster than this Thresholds. These is no harm in using both. If FortiDDoS is in Asymmetric Mode, use this Threshold and DISABLE the NTP Unsolicited Response anomaly.	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > NTP
	HTTP Methods	
HTTP/1.1 uses the following set of common methods: • GET • HEAD • OPTIONS • TRACE • POST • PUT • DELETE • CONNECT	Packet/second rate for the specified HTTP method. Threshold for an HTTP method flood attack. When the maximum rate is reached, the system drops packets matching the parameter. If the aggressive aging *layer7-flood* option is enabled, the system also sends a TCP RST to the server to reset the connection.	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > HTTP
	Protocols	

Threshold	Guidelines	Graph
	Scalars	
Protocol Start / End	Packet/second rate for the specified protocol (0-255). Threshold for a Protocol Flood event. When you specify a threshold for protocols, enter a range, even if you are specifying a threshold for a single protocol. For example, to set a threshold for protocol 6, enter 6 for both Protocol Start and Protocol End.	**Drop Monitor:** Flood Drops > Layer 3 **Traffic Monitor:** Layer 3/4/7 > Layer 3 > Protocols
	TCP Ports	
Port Start / End	Packet/second rate for the specified TCP port (0-65535). Threshold for a Port Flood event. Monitoring the packet rate for ports is helpful to prevent floods against a specific application such as HTML, FTP, SMTP or SQL. TCP accommodates 64K (65,536) ports, most of which may never be used by a particular server. Conversely, a server might see most or all of its traffic on a small group of TCP ports. For this reason, globally assigning a single threshold to all ports generally does not provide useful protection. However, you can globally set a (usually low) TCP Port Threshold for all TCP ports and then manually configure a higher threshold for the ports your protected network is using. When you specify a threshold for ports, you enter a range, even if you are specifying a threshold for a single port. For example, to set a threshold for port 8080, enter 8080 for both Port Start and Port End.	**Drop Monitor:** Flood Drops > Layer 4 **Traffic Monitor:** Layer 3/4/7 > Layer 4 > TCP Ports
	UDP Ports	
Port Start / End	Packet/second rate for the specified UDP port (0-65535). Threshold for a Port Flood event. When you specify a threshold for ports, you enter a range, even if you are specifying a threshold for a single port. For example, to set a threshold for port 53, enter 53 for both Port Start and Port End.	**Drop Monitor:** Flood Drops > Layer 4 **Traffic Monitor:** Layer 3/4/7 > Layer 4 > UDP Ports
	ICMP Types/Codes	
ICMP Type/Code Start/End	Packet/second rate for the specified ICMP type/code range (0:0-255:255). The ICMP header includes an 8-bit type field, followed by an 8-bit code field. Threshold for an ICMP Type/Code Flood event.	**Drop Monitor:** Flood Drops > Layer 4 **Traffic Monitor:** Layer 3/4/7 > Layer 4 > Other

Threshold	Guidelines	Graph
	Scalars	
	A popular use for ICMP is the “Echo groping” message (type 8) and its corresponding reply (type 0), which are often useful tools to test connectivity and response time. In some cases, this message and reply can also be used as an attack weapon to effectively disable a target system’s network software. Take care when you set the ICMP type 0 and type 8 thresholds to ensure the desired functionality is preserved.	
	HTTP Headers	
URL	Packet/second rate for packets with the specified URL match. When the maximum rate is reached, the system drops packets matching the parameter. If the aggressive aging *layer7-flood* option is enabled, the system also sends a TCP RST to the server to reset the connection. Specify the URL for a specific website. Botnets make it easy to launch attacks on specific URLs. When such an attack happens, FortiDDoS can isolate the URL and limit just the traffic that is associated with it, while all other traffic is unaffected. The URL is found in the website’s HTTP GET or POST operations. For example, the URL for http://www.website.com/index.html is */index.html*. When you specify a threshold for a URL, the system generates a corresponding hash index value. FortiDDoS displays the hash index value in the list of URL thresholds. Make note of it. You can use the hash value to select this URL elsewhere in the web UI. To view statistics associated with the threshold, go to *Monitor* > *Specific Graphs* > *URLs*, and then for *Please enter URL/Hash index*, enter either the original URL you specified or the hash index value. The valid range of hash index values for URLs is 0-64k per SPP.	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > HTTP

Threshold	Guidelines	Graph
	Scalars	
	You can use the special prefix *sys_reco_v* to create hash index ranges that aggregate URLs that you are interested in only as an aggregate. For example, assume your team wants to pay close attention to a five websites, and all others can be treated essentially the same. With the first five, your configuration is specific, so you know the website URL and the corresponding hash index, and you can use FortiDDoS to track it specifically. The system does not track the others with specificity, but you can track, as an aggregate, whether those sites experience rising and falling rates, including attacks. Create entries for the five priority websites and note their hash index numbers. Let's assume the hash index numbers are 1, 20, 21, 39, 40. **1.** Create ranges to aggregate the gaps: **a.** The first gap is from 2-19, so you create a configuration named sys_reco_v2_19. This includes hash numbers 2 through 19. **b.** The second gap is from 22-38, so you create a configuration named sys_reco_v22_38. **c.** The next gap is from 41 to the end of the range, so you create a configuration named sys_reco_v41_8192. **Note:** You cannot carve out a small block out of a large block. If you want to use hash index values that are already in use, you must delete the existing range and then create two ranges.	
Host, Referer, Cookie, User-Agent headers	Packet/second rate for packets with the specified header matches. When the maximum rate is reached, the system drops packets matching the parameter. If the aggressive aging layer7-flood option is enabled, the system also sends a TCP RST to the server to reset idle connections. A connection is deemed idle if it has not sent traffic in the last 2 minutes.	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > HTTP

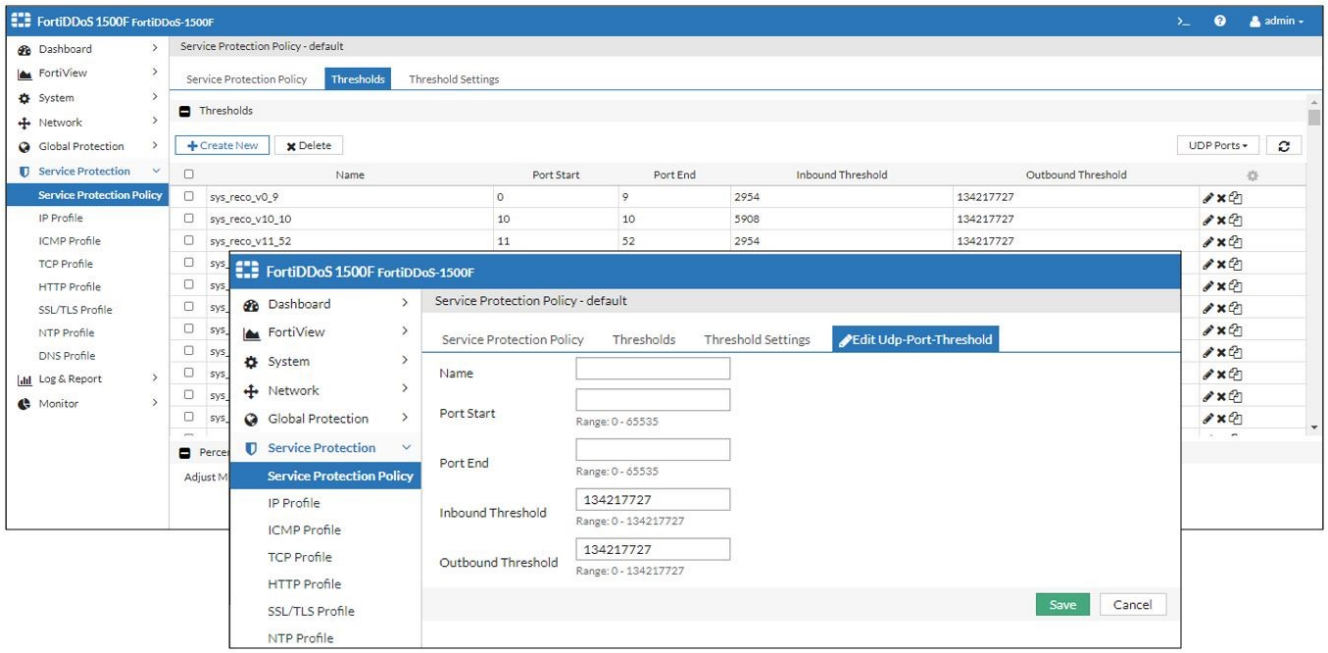
Threshold	Guidelines	Graph
	Scalars	
	Specify HTTP header values. With the advent of botnets, it is easy to launch attacks using scripts. Most of the scripts use the same code. The chances that they all use the same Host, Referer, Cookie, or User-Agent header fields is very high. When such an attack happens, FortiDDoS can easily isolate the four headers among many and limit traffic associated with that specific header, while all other traffic is unaffected. As with URL hash indexes, you can use the sys_reco_v prefix to define hash index ranges that aggregate header values you are not specifically interested in. The valid range of hash index values is 0-511 for each setting for each SPP: Host, Referer, Cookie, User-Agent	
	DNS Response Codes	
Rcode start-Rcode end	Packet/second rate for the specified DNS Response code (0-15). Threshold for DNS Response code Flood event.	**Drop Monitor:** Flood Drops > Layer 7 **Traffic Monitor:** Layer 3/4/7 > Layer 7 > DNS

To configure using the CLI:

```
config ddos spp rule
   edit <spp_name>
      config scalar-threshold
         edit <threshold_name>
            set scalar-type {syn |syn-per-src | most-active-source | concurrent-connections-
                 per-source | most-active-destination | method-per-source | oth-fragment | udp-
                 fragment | tcp-fragment | new-connections | syn-per-dst | dns-query-udp | dns-
                 query-tcp | dns-question-count-udp | dns-question-count-tcp | dns-mx-count-udp
                 | dns-mx-count-tcp | dns-all-udp | dns-all-tcp | dns-zone-xfer-tcp | dns-
                 fragment-udp | dns-fragment-tcp | dns-query-per-src | dns-packet-track-per-src
                 | ntp-req | ntp-resp | ntp-bcast | ntp-resp-per-dst}
            set inbound-threshold <integer>
            set outbound-threshold <integer>
         next
      end
      config protocol-threshold
         edit <threshold_name>
            set protocol-start <protocol_int>
            set protocol-end <protocol_int>
            set inbound-threshold <integer>
            set outbound-threshold <integer>
         next
      end
```

```
config http-method-threshold
   edit <threshold_name>
      set method { get |head| options | trace | post | put | delete | connect }
      set inbound-threshold <integer>
      set outbound-threshold <integer>
   next
end
config tcp-port-threshold
   edit <threshold_name>
      set port-start <port_int>
      set port-end <port_int>
      set inbound-threshold <integer>
      set outbound-threshold <integer>
   next
end
config udp-port-threshold
   edit <threshold_name>
      set port-start <port_int>
      set port-end <port_int>
      set inbound-threshold <integer>
      set outbound-threshold <integer>
   next
end
config icmp-type-code-threshold
   edit <threshold_name>
      set icmp-type-start <type_int>
      set icmp-code-start <code_int>
      set icmp-type-end <type_int>
      set icmp-code-end <code_int>
      set inbound-threshold <integer>
      set outbound-threshold <integer>
   next
end
config http-url-threshold
   edit <threshold_name>
      set url <url_string>
      set inbound-threshold <integer>
      set outbound-threshold <integer>
   next
end
config http-host-threshold
   edit <threshold_name>
      set host <host_string>
      set inbound-threshold <integer>
      set outbound-threshold <integer>
   next
end
config http-referer-threshold
   edit <threshold_name>
      set referer <referer_string>
      set inbound-threshold <integer>
      set outbound-threshold <integer>
   next
end
config http-cookie-threshold
   edit <threshold_name>
      set cookie <cookie_string>
```

```
            set inbound-threshold <integer>
            set outbound-threshold <integer>
         next
      end
      config http-user-agent-threshold
         edit <threshold_name>
            set user-agent <user-agent_string>
            set inbound-threshold <integer>
            set outbound-threshold <integer>
         next
      end
      config dns-rcode-threshold
         edit <threshold_name>
            set rcode-start <rcode_int>
            set rcode-end <rcode_int>
            set inbound-threshold <integer>
            set outbound-threshold <integer>
         next
      end
   next
end
```



Threshold Settings

This section of Service Protection Policy gives lot of techniques to smartly use Thresholds using FortiDDoS traffic learning mechanism. Here are few areas to look upon:

- **Traffic Statistics Generation:** This allows user to get traffic data about all L3, L4, L7 parameters for duration Last 1 hour, 8 hours, 24 hours, 1 week, 1 month and 1 year. This features gives an overview to user that what kind of traffic, system is seeing for a specific duration. This data serves as an input for System Recommendation feature.
- **System Recommendation:** This feature allows user to apply thresholds based upon Traffic statistics data, which in turn let user have mitigation levels based upon traffic volume. This feature can help set almost 264,000 thresholds per SPP per direction

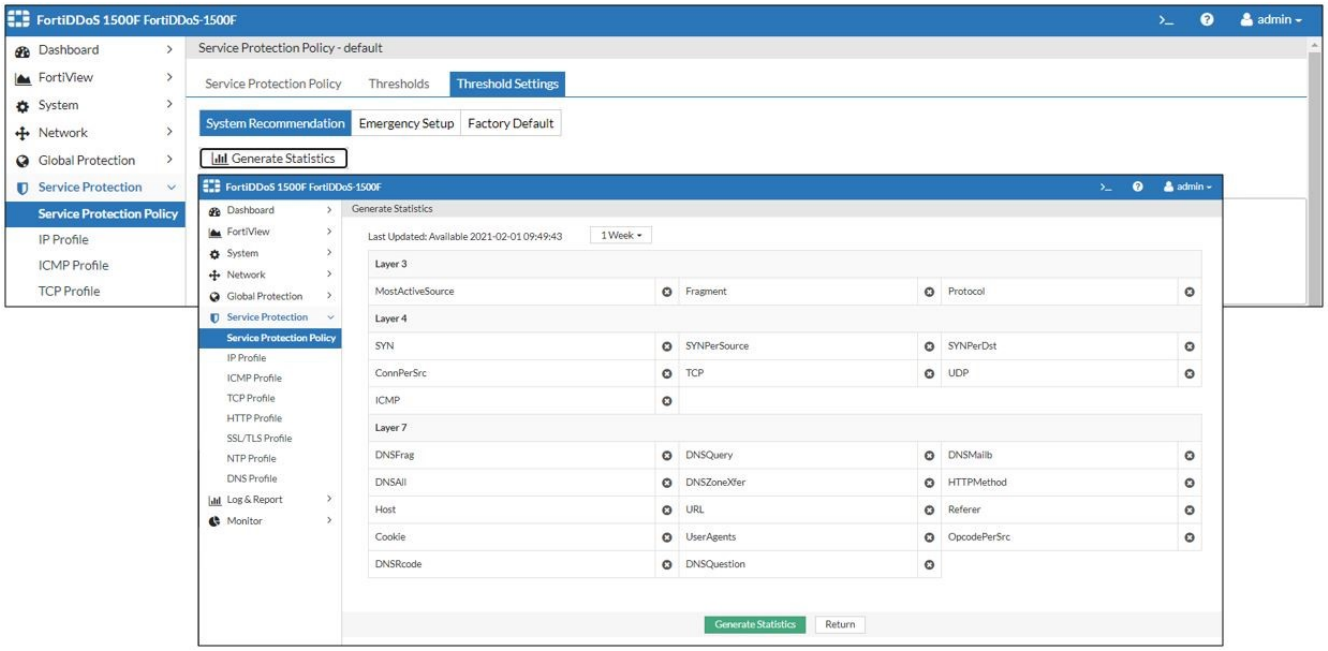
- **Emergency Setup:** This feature allows user to set thresholds in panic situation, when attack happens in initial learning period.
- **Factory Defaults:** This feature allows user to remove configured thresholds either all or by Layer 3/4/7

Generate Traffic Statistics

Baseline traffic statistics overview

The baseline traffic statistics are the maximum value (rate or count) measured by the counter for each parameter, in each direction in each Service Protection Policy during the observation period. The system saves data points every five minutes. During a 1-hour period, for example, there are 12, 5-minute observation periods. FortiDDoS saves a data point for each 5-minute interval. If you choose a 1-hour period, the system generates the maximum value across these 12 periods of 5-minute intervals.

The baseline statistics are used to establish the configured minimum threshold and ultimately the absolute maximum rate limit.



Generating baseline traffic statistics

You can generate baseline traffic statistics based on the following observation periods:

- Past 1 hour
- Past 8 hours
- Past 1 day
- Past 1 week – recommended for enterprise customers
- Past 1 month – recommended for ISP/Hosting customers
- Past 1 year
- Past 10 minutes – CLI only, normally used for PoC or training

Use a time period that is representative of typical traffic volume and has had no attacks.

Before you begin:

• You must have Read-Write permission for Protection Profile settings.

• Note that the FortiDDoS is accessed when you generate traffic statistics or set system recommended thresholds. Do not perform multiple operations simultaneously.

To generate baseline traffic statistics:

1. Go to *Service Protection* > *Service Protection Policy* > *{SPP Rule}* > *Threshold Settings* > *System Recommendation*, and click Generate Statistics
2. Select the time period from the drop-down list.
3. Select *Generate Statistics*.
4. It takes several minutes for the process to complete. Click *Refresh* to track the status. The process is complete when the status shows "*Available*" and a timestamp.

Note: VM platform maintains a single resource to store traffic data for each of TCP Ports (1024-65535), URL(1024-65535), UDP ports (10240-65535) & ICMP type Code (40:0-255:255). So, it is possible to see one single entry in Traffic statistics data for these ports in VM platforms only.

To configure using the CLI:

```
execute generate-traffic-stats spp <rule_name> <report_period>
      1h|8h|1d|1w|1m|1y|600s
```

Displaying baseline traffic statistics

You can review the statistics that are the basis of the system recommended thresholds.

Before you begin:

• You must have generated traffic statistics as described above.

• You must have Read-Write permission for Protection Profile settings.

To display baseline traffic statistics

1. Go to *Service Protection* > *Service Protection Policy* > *{SPP Rule}* > *Threshold Settings* > *System Recommendation*.
2. Select the type of statistics from the drop-down list.
3. Select the time period from the drop-down list.

Note: By default, the system does not display parameters with counts lower than default Low threshold value i.e. 500

Clear *Do not show values below low threshold option* if you want to see these low counts

System Recommendations

System Recommendation thresholds are the heart of FortiDDoS operation. For long-term successful mitigation of all kinds of DDoS attacks, you must use the following process to create effective mitigation:

1. Create Service Protection Profile Rules (SPPs) and Configure Protection Subnets
2. Allow the system to learn traffic patterns for at least 1 week

3. Create Traffic Statistics reports for each SPP rule
4. Create System Recommendation Thresholds (below)

Failing to follow these steps may require a remediation process, which will take significantly longer than the original setup. If you have not done so, please complete steps 1-3 before attempting System Recommendation.

System Recommendation uses the Traffic Statistics previously generated to create about 264,000 thresholds per Service Protection Profile in each direction. Some key points:

- It is impossible to set 264,000 parameters manually. Hence the automation of System Recommendation thresholds. As a comparison, Emergency Setup sets only 3 thresholds that are relevant to inbound DDoS attacks.
- It would be extremely difficult to manage changes on 264,000 parameters after the thresholds are set. For this reason, FortiDDoS groups similar, contiguous parameters such as groups of TCP Ports, UDP Ports, Protocols and ICMP Types and Codes into ranges. For example, TCP Ports between 7000 and 8000 are not used often and may show no traffic during the Learning Period. If so, a single threshold value is created for the entire range of ports between 7000 and 8000. Each port has a threshold but they are all the same after System Recommendation is complete. Thresholds and ranges may be changed manually at any time but the System Recommended ranges and thresholds have been developed over many years of DDoS mitigation, usually making need for manual threshold changes unnecessary.
- FortiDDoS also associates traffic in both directions to the “Service Ports” under 10,000. Ephemeral Ports above 10,000 should show little traffic.
- If needed, FortiDDoS will create up to 512 ranges for each of the parameters above. These number of ranges are not often created, but if you see more than 40 to 50 ranges for a particular parameter, you may want to modify the default Low Traffic Thresholds described below. See below or contact FortiCare for support with these changes.

We strongly recommend you use the System Recommendation feature to set thresholds. The system recommendation procedure sets the configured minimum threshold to:

- A multiple (entered as a percentage and normally the default seen above) of the learned rates generated from the Traffic Statistics algorithm. OR
- A minimum Low Traffic threshold, whichever is higher

Note: If Traffic Statistics have not been completed for an SPP and a matching time-period, the System Recommendation operation is not allowed for the same. Be sure the period selector dropdown for System Recommendation matches the period you used to create Traffic Statistics.

You can use the *Service Protection* > *Service Protection Policy* > *{SPP Rule}* > *Threshold Settings* > *System Recommendation* tab to set change the multiplier and the minimum Low Traffic threshold for OSI Layers 3-7 and various parameter groups within Layer 4. These are typically not changed from the defaults, but if they are changed, Changes to these settings are persistent and saved to config. You can change these settings at any time and re-Save System Recommendations for the selected Traffic Statistics. Changed System Recommendations take effect immediately which might impact mitigation. Change the SPP operating Mode to Detection before changing System Recommendations. Then return the SPP to Prevention Mode if there are no unexpected drops in the logs.

Also note that if you have manually changed any Thresholds and then recreate System Recommendation Thresholds, the manual Thresholds will be overwritten.

The resulting configured minimum thresholds are populated on the *Service Protection* > *Service Protection Policy* > *{SPP Rule}* > *Thresholds* tab. As you become a FortiDDoS expert, you can further tune the thresholds on that page.

Note: In the explanations below, System Recommendations sets some Thresholds to system maximums or does not set them at all, which has the same effect. These Thresholds are either rarely used for special circumstances or are covered by other mitigations. For example, you do not normally want to block Layer 3 Protocol 6 (TCP) or Protocol 17 (UDP) just because that protocol traffic is high, so it is not included in Thresholds. There are many other parameters above Layer 3 that will detect and mitigate attacks. However, if you are protecting web servers that never see UDP

traffic you can manually set a very low UDP Protocol 17 threshold, which provides better protection from UDP-based attacks.

How the System Recommendation feature sets thresholds for different L3, L4 and L7 parameters

Thresholds are set to either the Traffic Statistics' maximum rate seen for that parameter over the period of the report, multiplied by the Layer 3, Layer 4 or Layer 7 Percentage shown on the page, or to the Low Traffic threshold, whichever is higher.

For example, if the Traffic Statistics for a TCP port (a Layer 4 parameter) are 100pps, the System Recommendations first multiplies that by the amount displayed in Layer 4: TCP > TCP Port Percentage (default 200% or 2x). 100 pps x 2 = 200 pps.

It then compares this 200 pps rate with the TCP Port Low Traffic rate, lower in the table (default 500 pps). Since the multiplied traffic statistics rate of 200 pps is lower than 500 pps, that port gets a System Recommended Threshold of 500 pps. If another TCP Port has a Traffic Statistics rate of 1000 pps, that is multiplied by 2, to 2000 pps which is higher than the Low Traffic threshold of 500 pps so that port threshold is set to 2000 pps.

When all port calculations are complete, the system then groups contiguous ports with similar packet rates into single ranges. For example, TCP ports between 6000 and 7000 are seldom used and may all have 500 pps thresholds. The system will create and display a single range for TCP Ports 6000-7000 with a threshold of 500 pps.

The system continues with Traffic Statistics multipliers or Low Traffic threshold and ranges through all parameters for the SPP. This process takes a few seconds.

Note, TCP and UDP Port calculations and ranges purposely omit some ports such as UDP 53 and TCP 80 and 443 (among others). FortiDDoS does not want to rate limit traffic to these ports solely on the port data rate when other parameters like SYNs, DNS Queries, SSL Renegotiation will provide more granular mitigation. You can manually add Thresholds for missing ports, but this is usually not required.

Once complete, Thresholds can be found on *Service Protection* > *Service Protection Policy* > *{SPP Rule}* > *Thresholds* with various sets of parameters shown on their own pages. Thresholds can be manually changed, added or deleted from those pages.

Note: DDoS attacks are not subtle and typically will be 100's of thousands of pps. Setting a default low threshold to 1000 or even 10,000 will have little impact on mitigation. If in doubt contact Fortinet for advice.

Threshold Group	Notes
Scalars	Some Thresholds are not set by System Recommendation (equivalent to system maximums), because they are used in specific applications only. They may be set manually if needed. • Layer 3/4 Scalar Thresholds: Most Active Destination, New Connections • Layer 7 Scalar Thresholds: DNS Query per Source, DNS Packet Track per Source (Suspicious Sources on Monitor Graphs) **Note:** All Outbound thresholds are set to Max if Traffic Stats generated Empty data
DNS R-Code	Layer 7 Scalar DNS R-code Thresholds: These thresholds are manually created and intended for use only in systems where the DNS mitigation feature *Match Response With Queries (DQRM)* will not work: • FortiDDoS sees only part of the traffic in an asymmetric network • FortiDDos sees Encrypted DNS packets from Firewalls, Web Proxies, Email

Threshold Group	Notes
	servers or other devices doing web/domain filtering via vendor services. DNS Response Code thresholds can be determined by viewing and recording the peak rate of RCode(0-15) over a period of time, usually 1 week or 1 month. (*Traffic Monitor > Layer 3/4/7 > Layer 7 > DNS > DNS Response Code*).
Fragment	Fragments from all protocols will be learned by Traffic Statistics as above. The learned traffic will be multiplied by the Layer 3 percentage in System Recommendations (our use the default low threshold) but the resulting Threshold will be applied to three different scalar parameters: • Fragment –monitoring the rate of fragmented packets from Protocols other than TCP and UDP. • TCP Fragment – monitoring the rate for TCP fragmented packets. • UDP Fragment – monitoring the rate for UDP fragmented packets. Fragmented packets are a very common attack type but be careful with these Thresholds. Working from home has increased the level of Protocol 50 and UDP fragments because: • Home routers that work with IPSEC (Protocol 50 / ESP) often do not support Path MTU and do not reduce the packet size before IPSEC headers are added, resulting in higher fragmented packet rates • Home routers that don't support IPSEC are forced to encapsulate the TCP or UDP packets in IPSEC and then encapsulate them again in UDP over Port 4500 (IPSEC NAT traversal), adding more bytes to the packet and again causing significant fragmentation.
Protocol	The system recommendation sets Thresholds and ranges for all 256 Protocols except for Protocol 6 (TCP) and Protocol 17 (UDP). **Special case to consider:** In the context of new Mirai floods which target all 65,535 UDP ports, it is useful to set a *UDP Protocol* "backup" threshold: **1.** Go to *Traffic Monitor > Layer 3/4/7 > Layer 3 > Protocols* and set the Protocol field to 17. Observe the peak rate over the last week or month. Multiply that rate by 5 and record it. if you see very large, infrequent spikes (50kpps or more), ignore these and look for the peak traffic without those spikes. **2.** Next, go to *Service Protection Policy > {SPP Rule} > Thresholds > Protocols*. Add a new range as "Proto_17" or similar. Set Protocol Start and End to ""17"". Set the Inbound Threshold to the number you recorded above. Leave the Outbound Threshold at default. Save the Range Policy. It will appear at the bottom of the list - list order is not important to the system.
ICMP Type/Code	There are 65,536 allowable ICMP Types and Codes. However, less than 150 are valid for IPv4 and IPv6 traffic. You may create *ICMP Profile with ICMP Type Code Anomaly enabled* and link to SPP rule to remove any unused ICMP Types and Codes as anomalies. Whether all 65k types/codes or the reduced valid set is used, FortiDDoS will set thresholds for all 65,536 Types and Codes. Contiguous ICMP type/codes that have the similar inbound and/or outbound traffic rates are grouped into ranges.

Threshold Group	Notes
	A maximum of 512 ranges will be created to reduce management complexity. Normally only a few ranges are needed. Very few ICMP Types and Codes should show packet rates above default. If you see more than 4 or 5 ranges, contact Fortinet Support for advice. Please note that on all platforms, a single threshold entry is created for ICMP Type Code range 40:0-255:255 with threshold determined by recording the peak rate in that range.
TCP Port	Ports 0-10239 will be grouped into a series of ranges for ports with similar traffic. A single threshold is set for all ports above 10240. The System Recommendation procedure does not set the threshold for widely used TCP service ports 20-23, 25, 80, 110, 143 and 443 because there are more granular TCP L4-L7 parameters to detect floods. The thresholds for these ports are not shown – you will see gaps in the Port Threshold ranges. These ports are internally set to high values. If these ports are not in use for a specific SPP, you can add thresholds or ACL the ports. You can identify if these ports are in use by examining the Traffic Statistics in the GUI. The system does not set the threshold for user-configured *HTTP & SSL service ports (Service Protection > Service Protection Policy > {SPP Rule} > Service Port Settings)*. The thresholds for these are set to high values and will also be missing from the Port ranges as above. The system recommendation procedure does not set an Inbound or Outbound threshold for TCP port 53 because there are more granular DNS TCP parameters to detect floods. In reports and logs all traffic to or from 'service ports' 0-10239 or user-defined HTTP & SSL ports are associated with that port. Ephemeral high ports are not included in this traffic as they are generally irrelevant to protection of the service ports. If traffic is seen where both the Source Port and Destination Port are > 10240, the Destination Port will be shown on graphs and logs. A maximum of 512 different port ranges will be defined by the System Recommendation Algorithm. **Notes:** • Because of the way the Algorithm operates, the Low Traffic Thresholds (default 500) may be changed slightly when System Recommendations are created. This is normal and does not affect mitigation. • Managing 512 TCP Port ranges (52 pages on the GUI) can be difficult. Please see the instructions below to reduce Port ranges if needed.
UDP Port	The system recommendation procedure does not set an Inbound or Outbound threshold for UDP port 53 and UDP port 123 because there are more granular DNS UDP and NTP parameters to detect floods. The system sets system maximum Outbound Thresholds for UDP ports < 10240.A single Threshold is set for all ports >10239.

Threshold Group	Notes
	In reports and logs, all traffic to or from UDP 'service ports' 0-10239. Ephemeral high ports are not included in this traffic as they are generally irrelevant to protection of the service ports. If traffic is seen where both the Source Port and Destination Port are >10239, the Destination Port will be shown on graphs and logs. **Notes:** • UDP Port 53 is not assigned to a range. The expectation is that other parameters like Query thresholds will protect this port. You can manually create a threshold if you wish. A maximum of 512 different port ranges will be defined by the System Recommendation algorithm. • Managing 512 UDP Port ranges (52 pages on the GUI) can be difficult. Please see the instruction below to reduce the number of ranges if needed.
HTTP Method per Source	The aggregate of all 8 Methods sent per Source is tracked for up to 4 million sources depending on model. FortiDDoS does not decrypt HTTPS so HTTP Methods per Source may not be seen.
HTTP Methods	Thresholds are set to either the observed maximum multiplied by the Layer 7 percentage, or to the Low Traffic threshold, whichever is higher, for all 8 HTTP Methods. FortiDDoS does not decrypt HTTPS so Methods may not be seen.
HTTP URL, Host, Cookie, Referer, User-Agent	The rate meters for URLs and HTTP headers are based on indexes. For each SPP in the HTTP Header, FortiDDoS indexes on the first 2047 characters of up to 64,000 URLs, 512 Hosts, 512 Cookies, 512 Referers and 512 User Agents. • Packet rates vary across these indexes, SPPs, and traffic direction, depending on the time the baseline is taken. • The “observed maximum” used by the system recommendation procedure is the peak packet rate for all indexes (excluding indexes with zero traffic). Thresholds are set to either the observed maximum multiplied by the Layer 7 percentage, or to the low traffic threshold, whichever is higher. FortiDDoS does not decrypt HTTPS so URL, Host, Cookie, Referer and User-Agent traffic may not be seen.

Before you begin:

• You must have generated traffic statistics for a learning period – *Service Protection* > *Service Protection Policy* > *{SPP Rule}* > *Threshold Settings* > *System Recommendation* > *Generate Statistics*. Ensure that the traffic statistics report that you generate for use with System Recommendation is for a period that is long enough to be a representative period of activity. A rule of thumb is 1 week for enterprise deployments and 1 month for ISP deployments – longer is always better. Shorter periods will usually require additional tuning. If necessary, reset statistics for the SPP before initiating the learning period.

• You must have Read-Write permission for Protection Profile settings.

To generate the system recommended thresholds:

1. Go to *Service Protection* > *Service Protection Policy* > *{SPP Rule}* > *Threshold Settings* > *System Recommendation*

2. Select the time period you wish to use for Traffic Statistics. If Apply to Thresholds button is disabled, there are no Traffic Statistics generated for the period you have selected. You will see system default System Recommendation settings for L3, L4 and L7 percentage multipliers used to increase the Thresholds above the accrual Traffic Statistics. You will also see default low traffic Thresholds for low traffic parameters. If you are an expert, you can adjust the System Recommendation settings as described in the table below. The adjusted settings will be persistent. They will not return to default after use.
3. Complete the configuration as described in the table.

Settings	Guidelines
Layer 3/4/7 Percentage	Multiply the generated Traffic Statistics by the specified percentage to compute the recommended thresholds. For example, if the value is 300%, the threshold is three times the Traffic Statistics learned rate. The default adjustment for the various layers is: • Layer 3 = 300(%) • Layer 4 = 200(%) • Layer 7 = 200(%) • Valid range is 100 (% - no change) to 500 (% - 5x the Traffic Statistics rate) Most users should not change these settings from default. Expert users may change these carefully.
Layer 3/4/7 Low Traffic Threshold	Specify a minimum threshold to use instead of the recommended rate when the recommended rate is lower than this value. This setting is helpful when you think that the generated maximum rates are too low to be useful. The default is 500 with the following exceptions: • All Scalars and all UDP ports <10239 have their Outbound Thresholds automatically set to system maximum rates, to avoid outbound false-positive drops. These thresholds can be modified after creation if necessary by expert users. • Changing the low traffic threshold from default 500 is may be required for high traffic users with a lot of TCP and UDP Port traffic, in order to decrease the number of ranges. See the instructions below, if needed. • Changes to the low traffic threshold are persistent and will not revert to defaults after use. For example, if the generated maximum packet rate for inbound Layer 4 TCP packets is 2,000 and the outgoing rate is 3,000. The value of Layer 4 percentage is 300 (percent) and the value of Layer 4 low traffic threshold is 8,000. In this example: • The recommended threshold for inbound packets is 6,000 (2,000 * 300% = 6,000). However, because 6,000 is less than the low traffic threshold of 8,000, the system sets the threshold to 8,000. • The recommended threshold for outbound packets is 9,000 (3,000 * 300% = 9,000). Since 9,000 is greater than the low traffic threshold of 8,000, the system sets the threshold to 9,000.

4. Click *Apply To Thresholds* to generate the system recommended thresholds. Changes take effect immediately.
5. Go to *Service Protection* > *Service Protection Policy* > *{SPP Rule}* > *Thresholds* and review the thresholds.

Adjusting the system recommended thresholds

From step 5 above, Look specifically at TCP and UDP Port thresholds on *Service Protection* > *Service Protection Policy* > *{SPP Rule}* > *Thresholds*. If number of Port Threshold Ranges is more than 40, it is advisable to change the Low Traffic Threshold for this parameter to reduce the number of ranges.

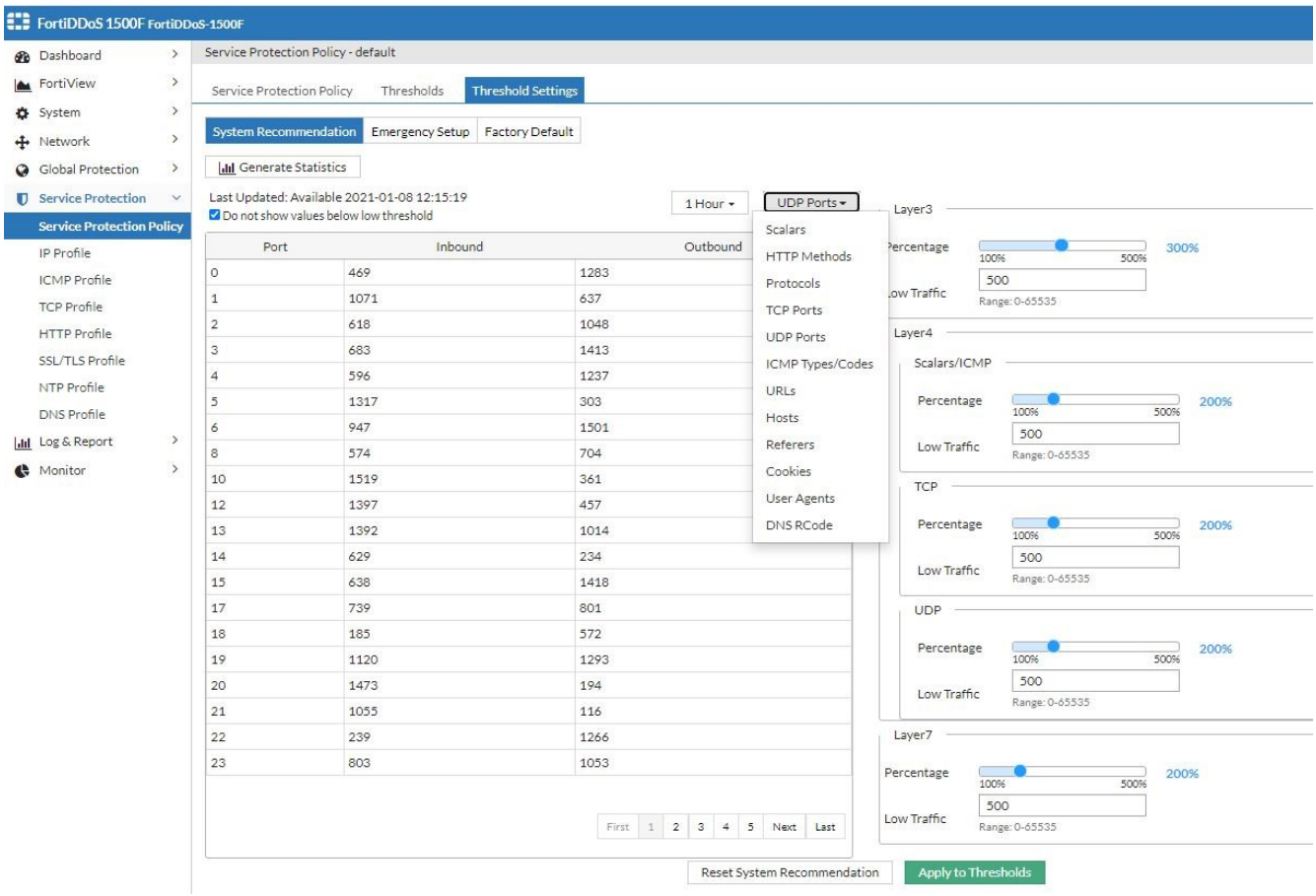
You will notice in *Service Protection* > *Service Protection Policy* > *{SPP Rule}* > *Threshold Settings* > *System Recommendation*, there are separate Low Traffic Thresholds for:

- Layer 4 Scalars and ICMP
- TCP Ports
- UDP Ports

If, for example, the UDP Port page shows 100 ranges, then return to *System Recommendations* and double the *UDP Ports Low Traffic Threshold* without changing any other settings. Save this and check the *UDP Port Thresholds* page again to see if ranges are now under 40. If not, double the *UDP Ports Low Traffic Threshold* again and check again until ranges are under 40. Do the same with TCP ports. Other parameters should not create large numbers of ranges.

To configure using the CLI:

```
config ddos spp rule
   edit <spp_name>
      set system-recommendation enable
      set threshold-system-recommended-report-period
      {1-hour | 8-hours | 1-day | 1-week | 1-month | 1-year | 10-
           min}
      set threshold-system-recommended-layer-3-low-traffic
           <integer> set threshold-system-recommended-layer-3-
           percentage <integer>
      set threshold-system-recommended-layer-4-low-traffic
           <integer> set threshold-system-recommended-layer-4-
           percentage <integer> set threshold-system-recommended-
           layer-4-tcp-port-low-traffic <integer>
      set threshold-system-recommended-layer-4-tcp-port-percentage
           <integer>
      set threshold-system-recommended-layer-4-udp-port-low-traffic
            <integer>
      set threshold-system-recommended-layer-4-udp-port-percentage
           <integer>
      set threshold-system-recommended-layer-7-low-traffic
           <integer>
      set threshold-system-recommended-layer-7-percentage <integer>
   next
end
```



Manual Threshold Setting

Any Threshold can be manually adjusted using the edit button for the Threshold or range from the GUI and adjusting the Inbound and/or Outbound Thresholds. For most applications where outbound traffic is not relevant to DDoS mitigation, outbound thresholds should be set very high to avoid 'false-positives' on graphing. Some outbound drops can impact Inbound traffic even if the outbound direction is set in Detection Mode.

For example, outbound TCP 'floods' can result in the TCP session being removed from the session tables, resulting in inbound traffic for that session being dropped as 'Foreign Packets'. Outbound Thresholds should be tuned to ensure no drops are seen.

Threshold	Label	Order
Scalar	Any meaningful label. Follow the field entry guidelines. Generally, non-unicode characters with no spaces are allowed.	Not Important

Threshold	Label	Order
Protocols	Any meaningful label. Follow the field entry guidelines. Generally, non-unicode characters with no spaces are allowed.	The order is not important but Protocol number ranges cannot overlap. For example, if there is a range of Protocol 18-255 set and you want to add a specific Threshold for Protocol 47 (GRE), you need to delete the 18-155 range and create 3 new ranges: 18-46, 47-47, and 48-255. These can be created in any order but numerical order makes it easier for future users to understand.
HTTP Methods	N/A	Each HTTP Method should have system-generated Thresholds. These can be modified but no Method can be added and none should be removed.
TCP and UDP Ports	Must NOT match the System recommended label (sys_reco_vX_Y). Otherwise, any meaningful label. Follow field entry guidelines. Generally non-unicode characters with no spaces are allowed.	Order is not important but port number ranges cannot overlap. For example, if there is a range of Ports 10000-65535 set and you want to add a specific Threshold for Port 11211, you need to delete the 10000-65535 range and create 3 new ranges: 10000-11210, 11211-11211, 11212-65535. These can be created in any order but numerical order makes it easier for future users to understand.
ICMP Types Codes	Must NOT match the System recommended label (sys_reco_vX_Y). Otherwise, any meaningful label. Follow field entry guidelines. Generally non-unicode characters with no spaces are allowed.	Order not important but Type/Code ranges cannot overlap. There are 65535 possible ICMP Types and Codes, so modifying this manually should not be done by non-experts. Please contact Fortinet TAC for help with this, if needed.
URLs, Hosts, Referers, Cookies, User Agents	If you wish to add an individual entry for any of these parameters, the label must NOT match the System Recommended label (sys_reco_vX_Y). Otherwise, any meaningful label. Follow field entry guidelines. Generally non-unicode characters with no spaces allowed.	Entries for these parameters are hashed by the system and cannot be 'un-hashed' so are difficult to interpret. For this reason, is it not recommended that you attempt to change any HTTP parameter ranges. If these parameters are causing issues, either manually change the thresholds only or re-run Traffic Statistics and System Recommendations to create new ranges and Thresholds.

Adding TCP or UDP Port Ranges

After the System Recommendations are created, there will only be one range for TCP and UDP “high” (>9999) ports labeled as “sys_reco_v10000_65535”.

If you use specific and/or want to exclude specific high ports, you must enter these manually. You cannot have overlapping port ranges. To add a port or range, first delete the existing range.

For example, if you want to allow Port 4500 for high traffic and leave all others as default:

1. Delete the port range “sys_reco_v10000_65535”.
2. Add port '4500':
   Name: IPSEC
   Port Start: 4500
   Port End: 4500
   Inbound Threshold: as required to system max of 16,777,215
   Outbound Threshold: as required to system max of 16,777,215
3. Replace deleted range with two ranges:
   Add Range
   Name: Default10000_4499
   Port Start: 10000
   Port End: 4499
   Inbound Threshold: 500
   Outbound Threshold: 500

   Add Range
   Name: DefaultAbove4500
   Port Start: 4501
   Port End: 65535
   Inbound Threshold: 500
   Outbound Threshold: 500

Note the following:

- Name labels can be alphanumeric plus “-“ and “_” only, 35 characters maximum.
- It is not necessary to follow the system label syntax of “sys_reco_vXXX_YYYYY” for ports or protocols. You must follow this for all other thresholds.
- Sorting is not supported for values under 'Threshold' column. If you expect to enter many manual ranges, plan ahead to add them in Start Port order. The entry order of Thresholds has no impact on the system but it is easier to read in numerical order.

Adjusting minimum thresholds by percentage

You can arbitrarily adjust SPP thresholds by percentage. This is useful when you expect a spike in legitimate traffic (for example, because of a news story or an advertising campaign). You can adjust the thresholds by as much as 300%.

Before you begin:

- Go to *Protection Profiles* > *Thresholds* > *Thresholds* and note the settings so that you can later verify the adjustment procedure or subsequently reset the thresholds to the values before the adjustment procedure.
- You must have Read-Write permission for Protection Profile settings

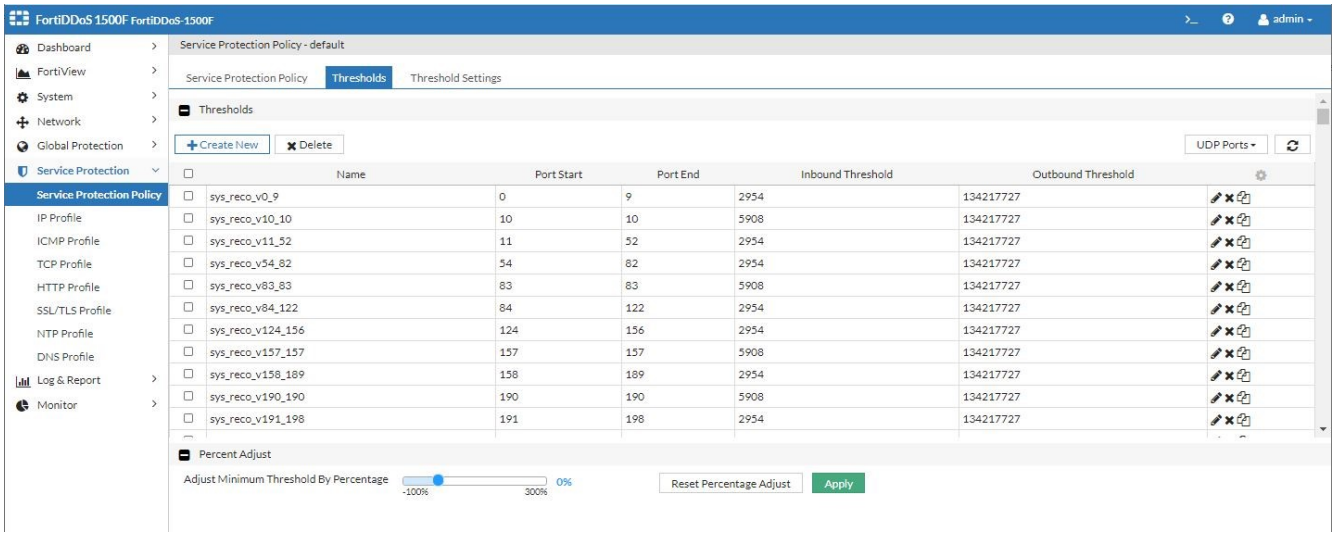
To adjust minimum thresholds by percentage:

1. Go to *Service Protection* > *Service Protection Policy* > *{SPP Rule}* > *Thresholds* > *Percent Adjust*.
2. Specify a percentage in the text box. The range of adjustment is from -100% to (+)300%
   For example:
   - 100 pps Threshold + 20% adjustment = 120 pps
   - 100 pps Threshold - 17% adjustment = -83 pps (Be careful while raising and lowering thresholds this way.)
   - 100 pps Threshold + 120% adjustment = 220 pps
   - 100 pps Threshold - 20% adjustment = 80 pps
   - 100 pps Threshold - 100% adjustment = 0 pps
3. Save the configuration.
4. Go to *Protection Profiles* > *Thresholds* > *Thresholds* and verify that the adjustment has been applied.

To configure using the CLI:

```
config ddos spp rule
   edit <spp_name>
      set threshold-percent-adjust <integer>
   next
end
```

Note: <integer> value can be in range -100 to 300



Emergency Setup

You can use the emergency setup option to set adjust only certain key thresholds based on empirical knowledge. You can expect these adjustments to protect against common attacks. For example, if you are already under attack, you can use emergency setup to deploy the unit without an initial learning period.

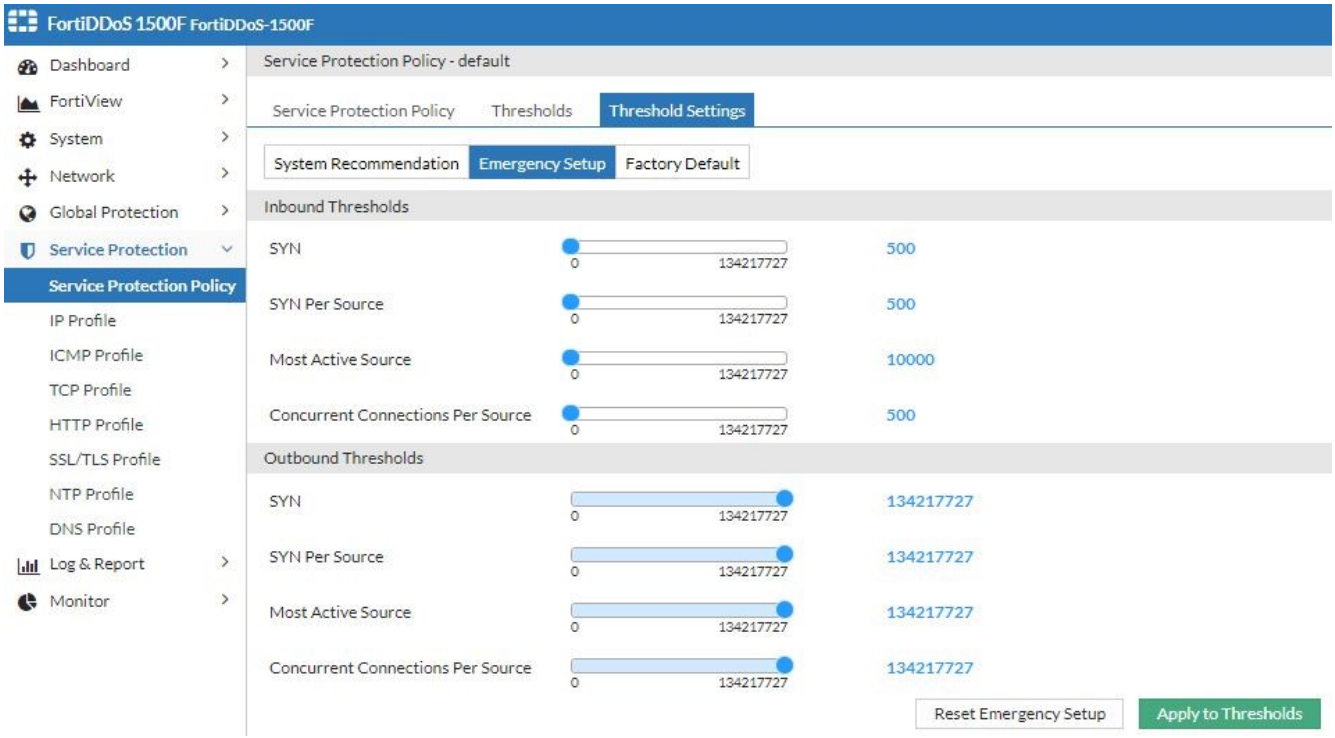
Warning: The thresholds set by Emergency Setup are a fraction of the full configuration and they are designed for use with smaller networks (less than 1Gbps). Always leave the Service Protection Profile in Detection Mode when using Emergency Setup until you can see if these thresholds impact legitimate traffic.

Before you begin:

You must have Read-Write permission for Protection Profile settings.

To apply SPP threshold settings:

1. Go to *Service Protection* > *Service Protection Policy*.
2. Select the {SPP Rule} you want to configure from table.
3. Select tab *Threshold Settings*
4. Select tab *Emergency Setup*
5. Make changes to all threshold settings as per requirement
6. Click *Apply to Thresholds*.
7. Click *Reset Emergency Setup* to all default threshold values.



To configure using the CLI:

```
config ddos spp emergency-setup-profile
   edit emergency
      set threshold-inbound-concurrent-connections-per-source-
           threshold <Inbound Concurrent Connections per Source
           Threshold>
      set threshold-inbound-most-active-source-threshold <Inbound
           Most Active Source Threshold>
      set threshold-inbound-syn-per-source-threshold <Inbound
           SYN/source Threshold>
      set threshold-inbound-syn-threshold <Inbound SYN Threshold>
      set threshold-outbound-concurrent-connections-per-source-
           threshold <Outbound Concurrent Connections per Source
           Threshold>
      set threshold-outbound-most-active-source-threshold <Outbound
           Most Active Source Threshold>
      set threshold-outbound-syn-per-source-threshold <Outbound
           SYN/source Threshold>
      set threshold-outbound-syn-threshold <Outbound SYN Threshold>
      next
   end
execute thresholds-emergency-setup spp <rule_name> profile
      <emergency_prof_name>
```

To Reset SPP Emergency Setup threshold settings to factory default:

1. Go to *Service Protection* > *Service Protection Policy*.
2. Select the SPP you want to configure from table.
3. Select tab *Threshold Settings*
4. Select tab *Emergency Setup*
5. Make changes to all threshold settings as per requirement
6. Click *Reset Emergency Setup* to all default threshold values.

Factory Default

In some situations, you might want to reset thresholds for an SPP. For example:

• You want to ensure that the application does not drop any packets due to rate thresholds. (The factory default values are high so that the appliance can be placed Inline and not immediately drop traffic.)

• You are conducting a demonstration or test, or you are troubleshooting an issue.

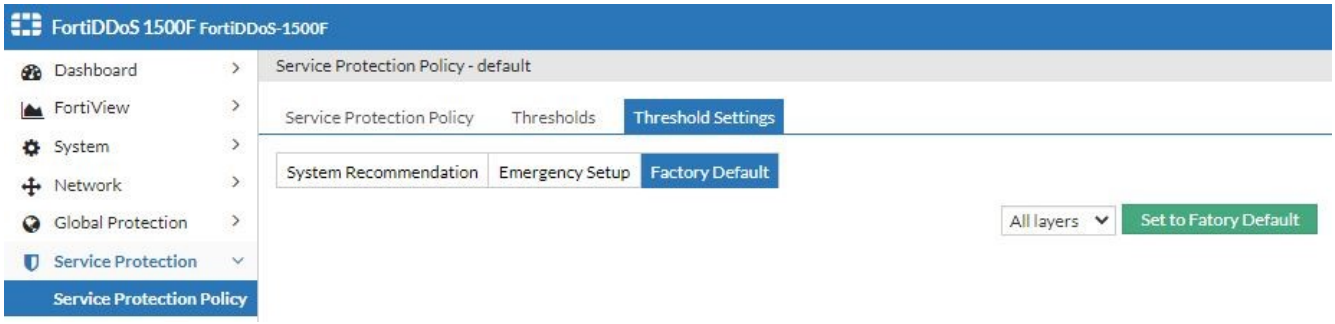
Before you begin:

You must have Read-Write permission for Protection Profile settings.

To reset SPP threshold settings:

1. Go to *Service Protection* > *Service Protection Policy*.
2. Select the SPP you want to configure from table.
3. Select tab *Threshold Settings*
4. Select tab *Factory Default*

5. Select *Threshold type* from the drop down menu.
6. Click *Set to Factory Default*.



To configure using the CLI:

```
execute thresholds-factory-defaults spp <rule_name> <L3|L4|L7|All>
```

SPP Profiles Overview

The Service Protection Policy Profile configurations for IP, ICMP, TCP, HTTP, SSL/TLS, NTP and DNS includes key feature settings that might vary among SPPs. It is IMPORTANT to configure these and assign each type of SPP Profile to the SPPs. SPPs without SPP Profiles assigned to them will not mitigate fully.

A single Profile may be used for many SPPs and/or a Single SPP may use multiple Profiles for the same parameters (e.g. a TCP Profile for Detection Mode and one for Prevention Mode). Only one SPP Profile of each type can be assigned to an SPP at one time (there is no switching of SPP Profiles between Detection and Prevention, for example - they must be changed manually).

You can edit SPP Profiles when they are assigned to an SPP but keep in mind that if that SPP Profile is assigned to multiple SPPs, the changes will affect them all.

A maximum of 64 SPP Profiles can be created for each of the SPP Profile Types above.

Before you begin:

- You must have a good understanding of the features You want to enable. Refer to Key Concepts.
- You must have Read-Write permission for Protection Profile settings.

To configure SPP Profiles

1. Go To Service Protection and select a Profile you want to configure (IP | ICMP | TCP | HTTP | SSL/TLS | NTP | DNS)
2. Select:
   a. **+ Create New** to create a new Profile
   b. **Edit** (pencil icon) at the right of any row from an existing list of Profiles to edit that Profile
   c. **Clone** (two pages icon) at the right of any row to duplicate an existing Profile for further editing
3. Edit and Save the Profile

To Assign Service Protection Policy Profiles to Service Protection Policies (SPPs):

1. Go to Service Protection > Service Protection Policy
2. Select:
   a. **+ Create New** - Create a new SPP Policy or
   b. **Edit** (pencil icon) at the right of any row from an existing list of SPP Policies to edit that SPP or
   c. **Clone** (two pages icon) at the right of any row to duplicate an existing SPP for further editing
3. Scroll down to Protection Profile Settings
4. Enable the Profile Type by toggling the button to the right
5. From the pull-down menu, select the Profile you want to assign to the SPP. All available Profiles of that type will show in the menu.

IP Profile

Use the IP Profile to configure various IP parameters and ACLs. Always assign an IP profile to every SPP.

Use a single IP Rpofile for all SPPs unless you need specialized ACLs for Fragments, IP Reputation or Domain Reputation.

All IP Profile parameters can be used with symmetric or asymmtric traffic.

You can create a maximum of 64 IP Profiles.

IP Reputation

The FortiGuard IP Reputation service is a licensed subscription that maintains a database of malicious IP addresses that pose a threat to your network and clients. After you purchase IP Reputation, you register the service contract to the FortiDDoS appliance serial number. Then, you can schedule updates to the IP

Reputation list.

IP Reputation is not required for DDoS mitigation. It is not a Threat Signature subscription which is not required with FortiDDoS. IP Reputation is a subset of FortiGuard's full web/domain/IP filtering service, containing IPs with known affiliations to DDoS attacks and known Anonymous Proxies (like Tor). Either or both subsets can be enabled.

If you are using existing Firewall/Proxy/Web/Domain/IP filtering products or services, FortiGuard IP Reputation services subscription is not required.

IP Reputation is enabled/disabled within this IP Profile. If this IP Profile is assigned to an SPP, then all traffic in that SPP will be checked for IP Reputation. If, for some reason, you want an SPP to ignore IP Reputation anomalies, create a different DNS Profile with IP Reputation disabled.

First set up FortiGuard access in **System > FortiGuard**. To use over-the-network updates, the management port must be able to access the Internet and DNS. If the system is behind a web proxy, set up Tunneling (proxy).

After you have set up FortiGuard and enabled the feature, the FortiDDoS system downloads the most recent definitions file and then maintains updates for it according to the schedule you configure.

The **Dashboard > Status: License Information** portlet and **System > FortiGuard: License Information** both display the status of the most recent update (IP Reputation Service Definition). If the download is successful and new definitions are available, the lists are replaced; otherwise, the previous list remains in use. The License Information portlet will also display the status of your IP Reputation license IP Reputation Service Contract Date). If your license

expires, the IP Reputation database is removed from the appliance. This is to prevent stale entries from affecting your traffic. You can configure how the FortiDDoS system receives scheduled updates.

Note: Since an IP Address is seen in both the inbound and outbound traffic, IP Reputation will drop any packet it sees containing the IP Reputation address, even if FortiDDoS does not see one direction of the traffic in asymmetric environments.

Field/Selection	Description	Recommendations (For Web Servers, Firewalls, DNS Servers)
Name	1-35 characters (a-Z, 0-9, "-", "_" only)	
IP Strict Anomalies	Drops packets where: • IP version other than 4 or 6 • Header length less than 5 words • End of packet (EOP) before 20 bytes of IPv4 Data • Total length less than 20 bytes • EOP comes before the length specified by Total length • End of Header before the data offset (while parsing options) • Length field in LSRR/SSRR option is other than (3+(n*4)) where n takes value greater than or equal to 1 • Pointer in LSRR/SSRR is other than (n*4) where n takes value greater than or equal to 1 • For IP Options length less than 3	Recommended enabled for all SPPs. If traffic appears to be affected, disable to troubleshoot. This parameter has been default-enabled on FortiDDoS for many years and has never been seen to cause failure of legitimate traffic.
IP Private Check	Drops packets where the Source IP is from the Internet Private address space such as 10.0.0.0/8.	
IP Multicast Check	Drops packets where the Source IP is from the Internet Multicast address space such as 224.0.0.0/24.	
IP Fragment Check		
Other Protocol Fragment	Drops fragmented packets from Protocols other than TCP or UDP	Expert use. Normally not recommended. Use Fragment Thresholds. Use only for specific applications - e.g. Drop UDP fragments ONLY for servers that NEVER see UDP traffic.
TCP Fragment	Drops fragmented TCP packets.	
UDP Fragment	Drops fragmented TCP packets.	
IP Reputation Categories		
DDoS	Downloads IP Reputation files to ACL only known DDoS and C&C Ips.	Requires FortiGuard IP Reputation Subscription. Use as desired.
Anonymous Proxies	Downloads IP Reputation files to ACL only known Anoymous Proxies such as Tor.	

ICMP Profile

Use the ICMP Profile to configure various ICMP parameters.

Use a single ICMP Profile for all SPPs unless you need specialized ACLs.

All ICMP Profile parameters can be used with symmetric or asymmetric traffic

You can create a maximum of 64 ICMP Profiles.

Field/Selection	Description	Recommendations (For Web Servers, Firewalls, DNS Servers)
Name	1-35 characters (a-Z, 0-9, "-", "_" only)	
ICMP Strict Anomalies	Drops ICMP Checksum Error, missing payload and other ICMP header anomalies.	Recommended enabled for all SPPs.
ICMP Type Code Anomaly	Drops ICMP Type/Code packets where the Type/Code is not ratified by IETF/IANA. Note, less than 200 of the possible 65,536 Type/Code possibilities are ratified. FortiDDoS sets Thresholds for all 65,536 Type/Codes and will mitigate without the ACL but this will drop even single non-ratified packets.	Recommended enabled for all SPPs unless substantial IPv6 traffic. New IPv6 Types/Codes are being added frequently. If you are using substantial IPv6, use the existing ICMP Type/Code Thresholds.
ICMP Type Code ACL	Enable to create ICMP Type Code ACLs.	Expert use
• Name	1-35 characters (a-Z, 0-9, "-", "_" only)	
• ICMP Type Start	0-255	
• ICMP Type End	0-255	
• ICMP Code Start	0-255	
• ICMP Code End	0-255	
• ICMP Version	Select either or both ICMP (v4 - Protocol 1) or ICMPv6 (Protocol 58)	

TCP Profile

Use the TCP Profile to configure various TCP parameters. A TCP Profile should be used for ALL SPPs, even ones that host primarily UDP service.

Some TCP Profile parameters CANNOT be used with asymmetric traffic. Be aware of your routing environment and **Global Protection > Deployment > Asymmetric Mode setting**.

You can create a maximum of 64 TCP Profiles.

Note 1: It is IMPORTANT that SYN Validation is enabled when this profile is used for any SPP in Prevention Mode. If SYN Validation is NOT enabled, the SYN Thresholds are ignored and there is is no protection from SYN floods.

Note 2: SYN Flood Mitigation requires interaction with the sending Client which will not happen if the SPP is in DETECTION Mode. You should create a TCP-Detection mode Profile with SYN Validation disabled and TCP-Prevention mode Profile with SYN Validation enabled and change this profile when you change Detection/Prevention Modes for the SPP.

Field/Selection	Description	Recommendations		
		Detection Mode	Prevention Mode	
			Symmetric Traffic	Asymmetric Traffic
Name	1-35 characters (a-Z, 0-9, "-", "_" only)			
SYN Flood Protection				
SYN Flood Mitigation Mode	• SYN cookie (Recommended)—Sends a SYN/ACK with a cookie value in the TCP sequence field. If it receives an ACK back with the right cookie, a SYN/RST packet is sent and the IP address is added to the legitimate IP address table. When the client then automatically retries, it succeeds in making a TCP connection. Fortinet recommends this option. • ACK cookie—Sends the client two ACK packets: one with a correct ACK number and another with a wrong number. The system determines whether the source is spoofed based on the client's response. If the client's response indicates that the source is not spoofed, FortiDDoS allows the connection and adds the source to the legitimate IP address table. Fortinet recommends this option if you have enough bandwidth in the reverse direction of the attack. • SYN retransmission—Drops the initial SYNs to force the client to send a SYN again. If the expected number of retransmitted SYNs arrive within the predetermined time period, the system considers the source to be legitimate.	SYN Cookie		

Field/Selection	Description	Recommendations		
		Detection Mode	Prevention Mode	
			Symmetric Traffic	Asymmetric Traffic
	FortiDDoS then allows the connection to go through and adds the source to the legitimate IP address table. Fortinet no longer recommends this option			
SYN Flood Mitigation Direction	Inbound Recommended Outbound not normally required - Expert use	Inbound		
SYN With Payload	SYN with Payload blocks SYN packets that are tno header-only packets - they have additional, usually-malicious payload. Attackers use SYN with Payload to increase the size of their attacks. However, a draft IETF standard (Fast Open) allows payload with SYNs and some Hosting companies are experimenting with it. If you see SYNwithPayload drops, investigate the Protected IPs. Inbound Recommended Outbound not normally required - Expert use	Inbound		
TCP Slow Connection Protection	Use this section to specify: • Slow connection detection settings (Type, Threshold and ObservationPeriod). These settings are only used if Slow TCP Connections is enabled below in TCP Session Settings. • Slow Connection Source Blocking option Note the following: • Do not use Slow Connection settings with asymmetric traffic. FortiDDoS counts Bytes for the connection in both directions since a single command may result in a large file download with occasional ACKs from the client. If FortiDDoS does not see the outbound packets (for example), it may trigger a false positive Slow Connection. • Do not use Slow Connections settings with any authenticating servers such as SSL-VPN, FTP or any server that allows	Expert - Many servers allow logins or allow long idle times. These will trigger TCP Slow Connections and unexpectedly drop legitimate connections. Use FortiWeb of FortiADC to manage slow connections on these types of servers.	No	

Field/Selection	Description	Recommendations		
		Detection Mode	Prevention Mode	
			Symmetric Traffic	Asymmetric Traffic
	a user to login and stay idle for any period of time (e-commerce, for example). Idle sessions will trigger Slow Connection mitigation and may drop the user's session unexpectedly. • Slow Connection settings are best tuned while the system is in Prevention Mode. If attempting in Detection Mode, enable Block Sources with Slow TCP Connections. This will provide additional logging information, BUT it may also result in a large number of 'Foreign Packet' drops which can be ignored.			
• Slow Connection Type	Select one of the following options from the drop-down: • Moderate: Uses predefined thresholds to detect slow connection attacks. • Aggressive: Uses more aggressive (lower) thresholds to detect slow connection attacks. • User Defined: Enables advanced users to specify custom thresholds to detect slow connection attacks. • None (Default): Do not monitor for slow connection attacks. If this setting is chosen, disable **TCP Sessions Settings > Aggressive Aging Feature Control: Slow TCP Connections** below as well. **Note:** To reduce false positives, Fortinet recommends you to initially set the option to moderate and switch to aggressive only if required. When the 'User Defined' option is selected, the defaults are set to 1 Byte per 15 seconds which allows lower rates than the default 'moderate' setting. We recommend to use the predefined moderate and Aggressive values as guidelines to help you specify your own settings.	Expert	No	

Field/Selection	Description	Recommendations		
		Detection Mode	Prevention Mode	
			Symmetric Traffic	Asymmetric Traffic
	Thresholds are triggered when a session sends or receives data at a SLOWER rate than the number of Bytes over the Observation Threshold.			
• Block Sources With Slow TCP Connections	Normally enabled if above Slow Connection Type is not None. This results in an attack log called 'Slow Connection: Source flood'. this log includes the Source IP of the Slow Connection, which is useful for analysis and potentially ACLing the Source. Use this option with care. Using Block Sources will block all traffic from those Sources. For example, if one client behind a firewall is creating a Slow Connection, all traffic from the firewall will be blocked. Disabling this option results in an attack event called Foreign Packets (Aggressive Aging and Slow Connections) which is shared with other Aggressive Aging events (see Aggressive aging.)	Expert	No	
• Slow Connection Byte Threshold	The number of Bytes that must be seen within the Observation Period below to prevent triggering Slow Connection Mitigation. Note, this number is pre-filled for Types: Moderate or Aggressive and can be customized for Type: User Defined. If Type: None is selected, numbers are shown in the Byte Threshold but are ignored.	Expert	No	
• Slow Connection Observation Period	The time period (in seconds) during which Bytes are counted. Once the Byte threshold above is crossed, the Observation Period is reset and the Byte count starts again. Note, this number is pre-filled for Types: Moderate or Aggressive and can be customized for Type: User Defined. If Type: None is selected, numbers are shownin the Observation Period but are ignored.	Expert	No	

Field/Selection	Description	Recommendations		
		Detection Mode	Prevention Mode	
			Symmetric Traffic	Asymmetric Traffic
TCP Packets Validation				
TCP Session Feature Control:				
• Sequence Validation	Drops packets with invalid TCP sequence numbers. Note: Some vendors intentionally use non-standard sequence numbers for end-to-end signaling between WANop devices. If you see large numbers of OUTBOUND Sequence Validation Drops, disable the feature.	Enable	Enable	Disable
• SYN Validation	Enables SYN Flood validation using the method selected above. If this is NOT enabled, SYN Thresholds are ignored and SYN Floods are not mitigated. If this feature is enabled in DETECTION Mode and there is a SYN Flood, the system is unable to send validation packets, resulting in unusual logging. This feature should be disabled while in DETECTION Mode.	Disable	Enable	
• State Transition Anomalies Validation	Drops packets with TCP state transitions that are invalid. For example, if an ACK packet is received when FortiDDoS has not observed a SYN/ACK packet, it is a state transition anomaly. FortiDDoS features can be used in Asyymetric Mode, provided Allow Inbound SYN-ACK is also enabled. See Global Protection features.	Enable	Enable	
• Foreign Packet Validation	Drops TCP packets without an existing TCP connection and reports them as a foreign packet. In most cases, the foreign packets validation is useful for filtering out junk. **Note:** Inbound Foreign Packets will be passed in DETECTION Mode and may result in matching outbound Foeign Packets. If in doubt, disable Foreign Packet Validation when the SPP is in DETECTION mode.	Disable	Enable	

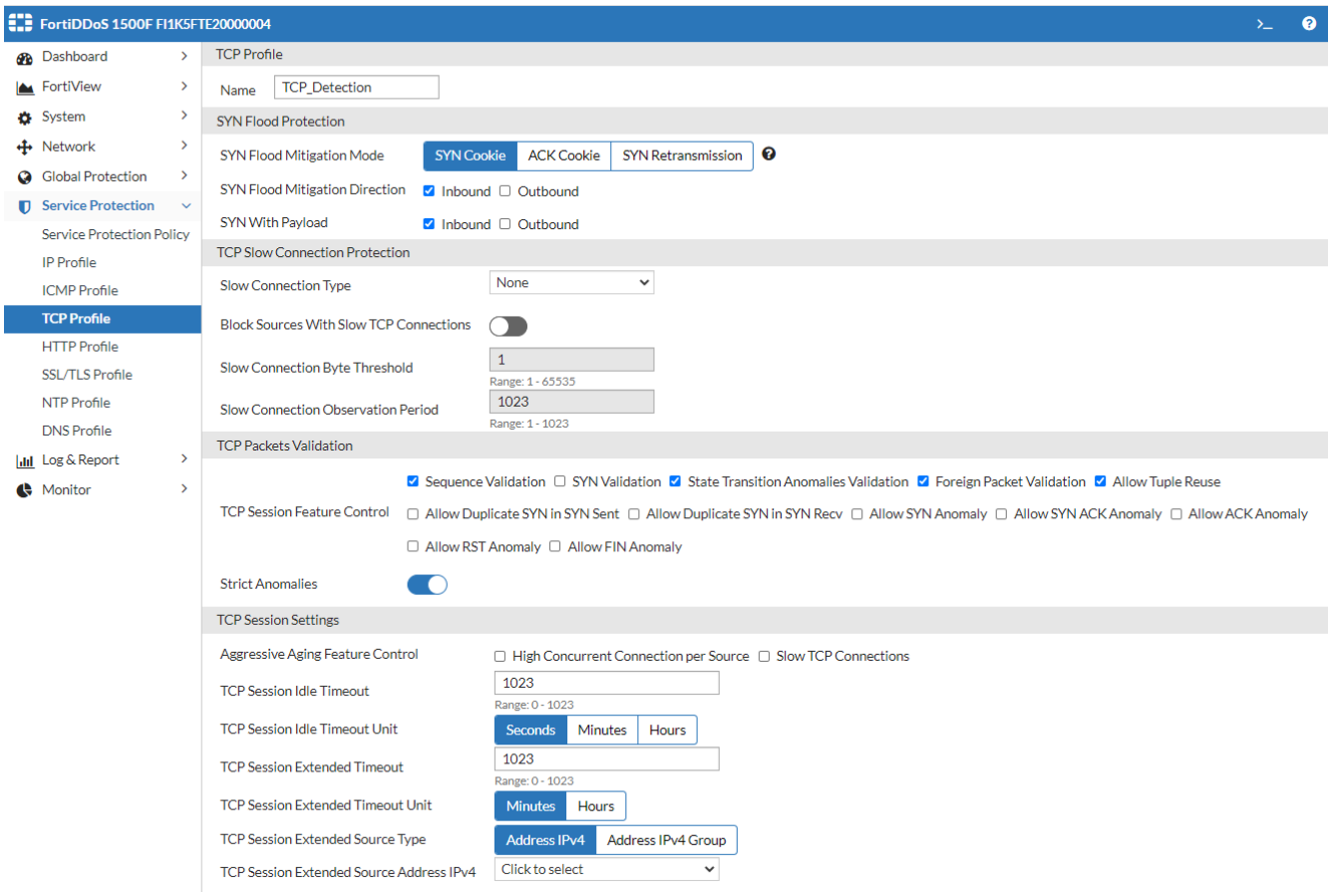
Field/Selection	Description	Recommendations		
		Detection Mode	Prevention Mode	
			Symmetric Traffic	Asymmetric Traffic
• Allow Tuple Reuse	Allows a new connection with the same 5-tuple (Sooure IP:port, Protocol, Destination IP:Port) while the existing connection is in the closed or close-wait, fin-wait, time-wait states.	Enable		
• Allow Duplicate SYN in SYN Sent	Allows duplicate TCP SYN packets during the SYN-SENT state. It allows this type of packet even if the sequence numbers are different.	Enable	Optional but not necessary	
• Allow Duplicate SYN in SYN Recv	Allows duplicate TCP SYN packets during the SYNRECV state. It allows this type of packet even if the sequence numbers are different.	Disable		
• Allow SYN Anomaly • Allow SYN ACK Anomaly • Allow ACK Anomaly • Allow RST Anomaly • Allow FIN Anomaly	Allows duplicate TCP packets during any other state even if the sequence numbers are different from the existing connection entry. This is equivalent to allowing the packet without updating an existing connection entry with the new information from the allowed packet.	Use on Fortinet recommendation only		
• Strict Anomalies	Drops various TCP Header Anomalies including: • TCP Checksum Error • TCP Invalid Flag Combination • Other header anomalies, such as incomplete packet • SYN or FIN or RST is set for fragmented packets • Data offset is less than 5 for a TCP packet • End of packet is detected before the 20 bytes of TCP header • Length field in Window scale option other than 3 in a TCP packet	Enable		

Field/Selection	Description	Recommendations		
		Detection Mode	Prevention Mode	
			Symmetric Traffic	Asymmetric Traffic
TCP Session Settings				
Aggressive Aging Feature Control	Controls sending RSTs to servers			
High Concurrent Connection per Source	Sends TCP RSTs to the protected destination server(s) to reset connections from the identified Source IP when the Concurrent Connection per Source threshold is crossed.	Optional. System cannot send RSTs in Detection mode which may result in unusualy logging.	Enable	
Slow TCP Connections	Sends TCP RSTs to the protected destination server(s) to reset connections from the identified source depending on the Slow Connection settings above.	Optional. System cannot send RSTs in Detection mode which may result in unusually logging.	Expert	No
TCP Session Idle Timeout	Idle timeout period for any TCP session. The default value is 528 seconds. Use this timer to age idle TCP sessions (sessions with no traffic for long periods), for all connections and ports. This timer should match other idle timers in your infrastructure such as firewalls.	Always monitored		This setting is ignored in Asymmetric Mode
TCP Session Idle Timeout Unit	Seconds, Minutes, Hours.			

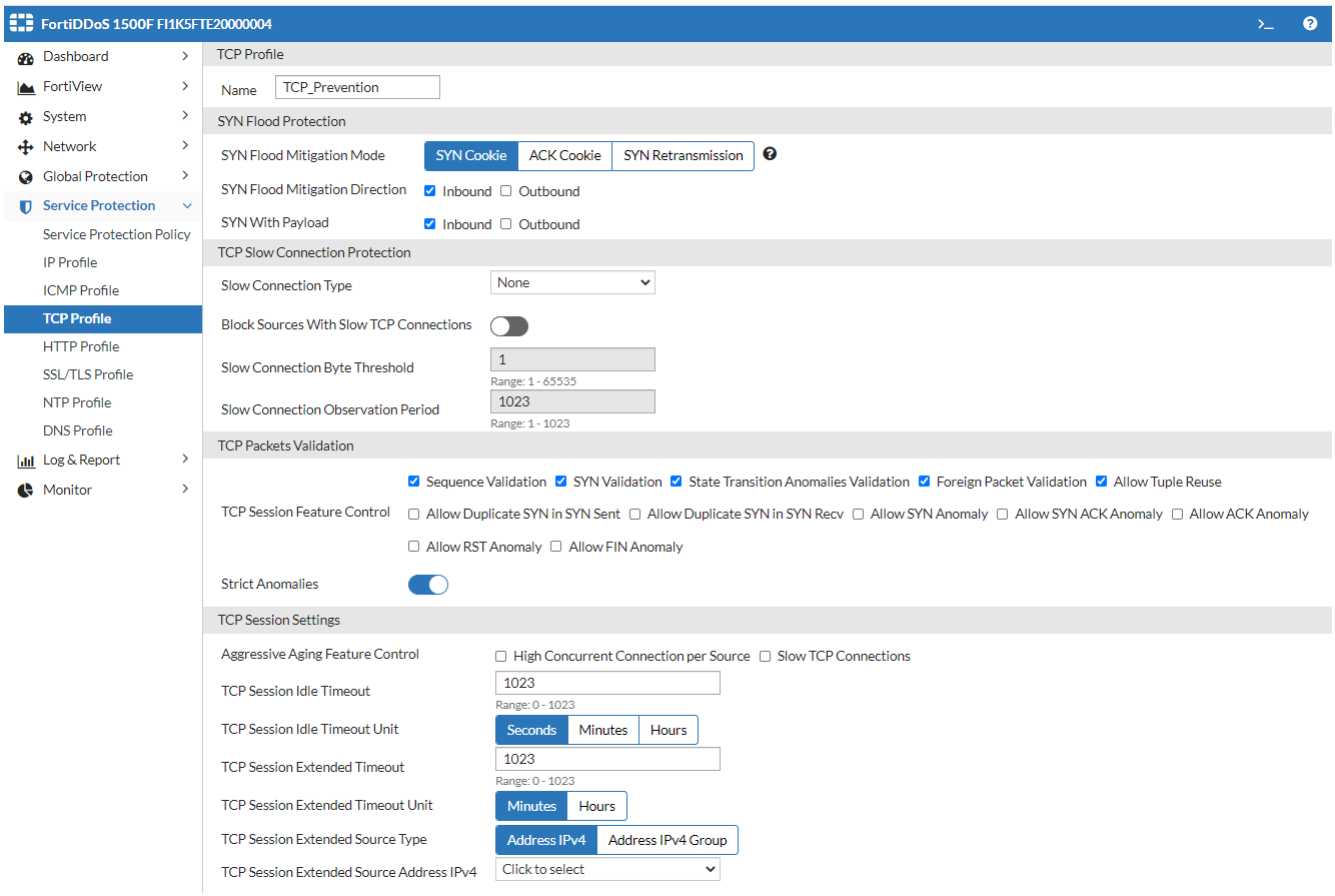
Field/Selection	Description	Recommendations		
		Detection Mode	Prevention Mode	
			Symmetric Traffic	Asymmetric Traffic
TCP Session Extended Timeout	Extended timeout value for specific IP addresses (IPv4 only) where the timeout should be longer than the idle timeout period. For example, this setting can be configured for specific IP addresses in environments where persistent SSH/TELNET/HTTP connections are used. This timer should be longer than the TCP Session Idle Timeout. See also, Session timeout precedence and application, below.	Always monitored		This setting is ignored in Asymmetric Mode
TCP Session Extended Timeout Unit	Seconds, Minutes, Hours.			
TCP Session Extended Source Type	IPv4 Address or IPv4 Address Group	Always monitored		This setting is ignored in Asymmetric Mode
TCP Session Extended Source Address IPv4	Select from the Global IP address / IP Address Group definitions			

Example Settings:

TCP Detection Mode



TCP Prevention Mode



HTTP Profile

Note: HTTP Profile is not valid for HTTPS services. See SSL/TLS. However many HTTPS servers support HTTP if only to redirect to HTTPS. Use the HTTP Profile for any SPP where TCP connections can be made to TCP 80 or other TCP ports defined for HTTP.

As detailed below, some settings are recommended for expert use only.

HTTP Profile parameters can be used with symmetric or asymmetric traffic.

The same SSL/TLS profile can be used by multiple SPPs but any SPP can only use one SSL/TLS profile at a time.

All HTTP parameters can be used with symmetric or asymmetric traffic. You can create a maximum of 64 TCP Profiles.

Field/Selection	Description	Recommendation		
		Web Servers (If HTTP is used)	Firewalls (Optional)	DNS ServersIf (If HTTP is used)
Name	1-35 characters (a-Z, 0-9, "-", "_" only)			
Known Method Anomaly	Drops any HTTP packet with the selected Method(s).	Expert use. All HTTP Methods have Thresholds		

Field/Selection	Description	Recommendation		
		Web Servers (If HTTP is used)	Firewalls (Optional)	DNS ServersIf (If HTTP is used)
• GET • HEAD • OPTIONS • TRACE • POST • PUT • DELETE • CONNECT	Dropped packets will be shown in the Monitor Graphs as well as in the Attack Log.	set. Additionally, there is a Methods-per-Source Threshold. If you are unsure which Methods are used, allow the system to manage the Thresholds and do not use this feature.		
Unknown Method Anomaly	While 8 Methods are defined above the HTTP Method field allows 16 entries (0-15). Drops undefined Methods. Dropped packets will be shown in the Monitor Graphs as well as in the Attack Log.	Expert use		
Version Anomaly	Drops HTTP traffic with an HTTP version other than one of the following: 0.9, 1.0, 1.1 or 1.2. Dropped packets will be shown in the Monitor Graphs as well as in the Attack Log. Dropped packets will be shown in the Monitor Graphs as well as in the Attack Log.	Expert use. You can enable this feature while in DETECTION Mode. If you see many Version Anomalies OUTBOUND, disable this features before entering Prevention Mode.		
Do Not Parse HTTP Version 0.9	Drops HTTP traffic with HTTP version 0.9. This version has been deprecated for security and should not be supported by web servers.	Expert use		
Drop Range Header	Drops sessions when the HTTP request includes the HTTP Range header. The Range header can be abused by attackers to exhaust HTTP server resources. However some services expect to see Rannge Headers. Dropped packets will be shown in the Monitor Graphs as well as in the Attack Log.	Expert use		

Field/Selection	Description	Recommendation		
		Web Servers (If HTTP is used)	Firewalls (Optional)	DNS ServersIf (If HTTP is used)
Persistent Transaction	A simple HTTP transaction is one where the client makes a single request for HTTP content within a TCP session. Persistent connections allow the browser / HTTP client to utilize the same connection for different object requests to the same host name. If Persistent HTTP Transactions feature is enabled, FortiDDoS checks for application-level conformity in every packet of a TCP connection. If this feature is disabled (default), checks are limited to the first transaction of a TCP connection. It is recommended to use the disabled state to avoid HTTP anomalies, especially due to IP fragmentation and TCP segmentation.	Expert use		
Incomplete Request Action	An incomplete HTTP message does not end with "/r/n/r/n"	Expert use. Many clients now have very large Cookies which result in segmentation of the HTTP GET message. This results in the "/r/n/r/n" characters being missing in one or more segmented packets and these packets will be dropped, preventing successful sessions.		
• None	No Action if incomplete message seen. (Default)			
• Drop	Drops packetswhere the HTTP message does not end with "/r/n/r/n".			
• Block Source With Incomplete Request	Blocks Source IP that sent the incomplete request. Shown only when "Drop" Incomplete Request action is selected			
• Aggressive Aging	If an incomplete request is detected, sends a RST to the server to remove the session from the server connection table.			
Aggressive Aging Flood	If an HTTP Method Flood is detected, sends a RST to the server to remove the session from the server connection table.	Recommended		
GET Flood Mitigation (Validation) Direction	Uses redirect messaging to test that the sending Client is legitimate			
• Inbound	Enables Get Flood Validation inbound	Recommended		
• Outbound	Enables Get Flood Validation inbound	Expert use		

Field/Selection	Description	Recommendation		
		Web Servers (If HTTP is used)	Firewalls (Optional)	DNS ServersIf (If HTTP is used)
POST Flood Mitigation Direction	Uses redirect messaging to test that the sending Client is legitimate			
• Inbound	Enables POST Flood Validation inbound	Recommended		
• Outbound	Enables POST Flood Validation inbound	Expert use		
HTTP Parameter ACL	Used to create an ACL for any of the following HTTP Parameters. (Methods can be ACLed above)	Expert use		
• Name	1-35 characters (a-Z, 0-9, "-", "_" only)			
• Type	Select URL/Host/Referer/Cookie/User Agent			
• Regex	Enter Regex expression to describe the parameter selected above	Expert use		

SSL/TLS Profile

Use the SSL/TLS Profile for any SPP where TCP connections can be made to TCP 433 or other TCP ports defined for SSL/TLS. SSL/TLS Pprofile parameters can be used with symmetric or asymmetric traffic.

As detailed below, some settings are recommended for expert use only. The same SSL/TLS profile can be used by multiple SPPs but any SPP can only use one SSL/TLS profile at a time. You can create a maximum of 64 SSL/TLS Profiles.

Field/Selection	Description	Recommendations		
		Web servers (recommended)	Firewalls (No)	DNS servers (Only if 443 is open)
Name	1-35 characters (a-Z, 0-9, "-", "_" only)			
Protocol Anomaly	Drops packets where SSL Protocol is not 20-23			
Version Anomaly	Drops packets where version is not SSL 3.0 or TLS 1.0, 1.1 or 1.2			
Cipher Anomaly	Drops packets that don't conform to existing Cipher suites (~400 valid).			

Field/Selection	Description	Recommendations		
		Web servers (recommended)	Firewalls (No)	DNS servers (Only if 443 is open)
Block Incomplete Request	Enable/Disable Block Incomplete TLS Request Slow-connection. When the actual data length of TLS record is less than its length field value or the data length of handshake protocol is less than its length field value, the request is considered as Incomplete Request which will be dropped and logged.			
Aggressive Aging Incomplete Request	If an incomplete request is detected, sends a RST to the server to remove the session from the server connection table.			
Block Source With Incomplete Request	Blocks Source IP that sent the incomplete request			
Renegotiation Check	Establishes a threshold of number of SSL renegotiations allowed (default 5) over a time period (default 1s). Most ADCs and WAFs do not allow any renegotiations. This should be used only if a WAF or ADC are not between FortiDDoS and Servers.	Expert use. SSL renegotiations are monitored in both directions and thus not recommended for SPPs containing outbound services like Firewalls, Proxies or WiFi gateways.		
• Renegotiation Aging Time	Default 1s. Range 1-65535			
• Renegotiation Threshold	Default 5 renegotiations. Range 1-65535			

NTP Profile

Use the NTP Profile to configure various NTP Anomaly and ACL parameters. An NTP Profile should be used for ALL SPPs. NTP Reflection Floods are used against all types of targets, whether you host NTP, are using NTP or not.

Note: Some NTP Parameters as detailed below, cannot be used in asymmetric traffic environments. Use NTP Thresholds when you cannot use these NTP parameters.

The same NTP Profile can be used by multiple SPPs but any SPP can only use one NTP profile at a time.

You can create a maximum of 64 NTP Profiles.

Field/Selection	Description	Recommendations		
		Detection Mode	Prevention Mode	
			Symmetric Traffic	Asymmetric Traffic
Name	1-35 characters (a-Z, 0-9, "-", "_" only)			
Data Length Anomaly Check	Each NTP version has a specified maximum data length in the Query or Response. FortiDDoS will match the actual data length to the defined data length for the identified Version and drop any packet that does match correctly.	Enable		
Stratum Anomaly Check	NTP includes Stratum information to describe the accuracy of the server clock. The RFC supports 0-15 “stratum” but the Stratum field allows 256. Any number above 15 is an anomaly and will be dropped. In addition, if the Stratum is 2 or greater a Reference ID must be included in the request and response. If it is not included, it will be dropped.	Enable		
Version Anomaly Check	NTP Version must be between 1 and 4. If the Version is 1, then the Mode must be 0.	Enable		
Control Header Anomalies Check	FortiDDoS monitors 9 different Control header anomalies • Request LEAP INDICATOR as zero • Request with ERROR or MORE bits set • Request with non-zero OFFSET • Request with reserved OPCODE (>7). • Response with COUNT value as 0 • Fragmented error response (E=1 and M=1) • First response with M=1 with non-zero OFFSET • Response with reserved STATUS values(>7)	Normally, this anomaly can be enabled for all conditions. However if you are hosting an NTP server, you many need to disable this option. Enable and monitor during Learning/ Detection and evaluate the number of events and drops in both directions. If unsure contact Fortinet Support.		

Field/Selection	Description	Recommendations		
		Detection Mode	Prevention Mode	
			Symmetric Traffic	Asymmetric Traffic
Retransmission Check	If multiple identical Requests are seen before a Response is seen subsequent identical Requests are dropped. **Note:** This feature will not work where there is asymmetric traffic and FortiDDoS may not see all Responses. Disable this feature if FortiDDoS is in Asymmetric Mode.	Disable if asymmetric traffic. Use NTP Query and Response Thresholds.		
Sequence Mismatch Check	Detects header Sequence number errors in Queries and Responses. **Note:** This feature will not work where there is asymmetric traffic and FortiDDoS may not see all Responses.			
Unsolicited Response Check	FortiDDoS records all passing NTP Requests. When a matching NTP Response is seen the record is cleared. If an NTP Response has seen that was not Requested, it is “unsolicited” and dropped immediately. **Note:** This feature mitigates NTP Reflected Response Floods from the first packet, without the requirement for a Response Threshold. However, this feature will not work where there is asymmetric traffic and FortiDDoS may not see all Requests or Responses. If the system is in Asymmetric Mode, disable this feature and use Response Threshold below.			
Mode Mismatch Check	Some Modes must be different in the Client Query and Server Response while some Modes are the same for both. FortiDDoS monitors valid combinations and if any are invalid, that packet will be dropped. The only valid Mode pairs for Requests/Responses are 1/2, 3/4, 6/6 or 7/7.			

Field/Selection	Description	Recommendations		
		Detection Mode	Prevention Mode	
			Symmetric Traffic	Asymmetric Traffic
	Note: Mode Mismatch (MM) is like Unsolicited Response, working only with symmetric traffic. If FortiDDoS is in Asymmetric Mode, disable this feature.			
Reflection Deny	No parameters. If you enable Reflection Deny, you are creating a rule to deny NTP Mode 7 and NTP Mode 6 packets in Queries and Responses. These packets are not needed and are frequently abused to create reflected, amplified NTP DDoS attacks.	Enable		

DNS Profile

Use the DNS Profile to configure various DNS parameters and ACLs. Always assign an DNS profile to SPP.

All DNS Profile parameters can be used with symmetric or asymmtric traffic.

You can create a maximum of 64 DNS Profiles.

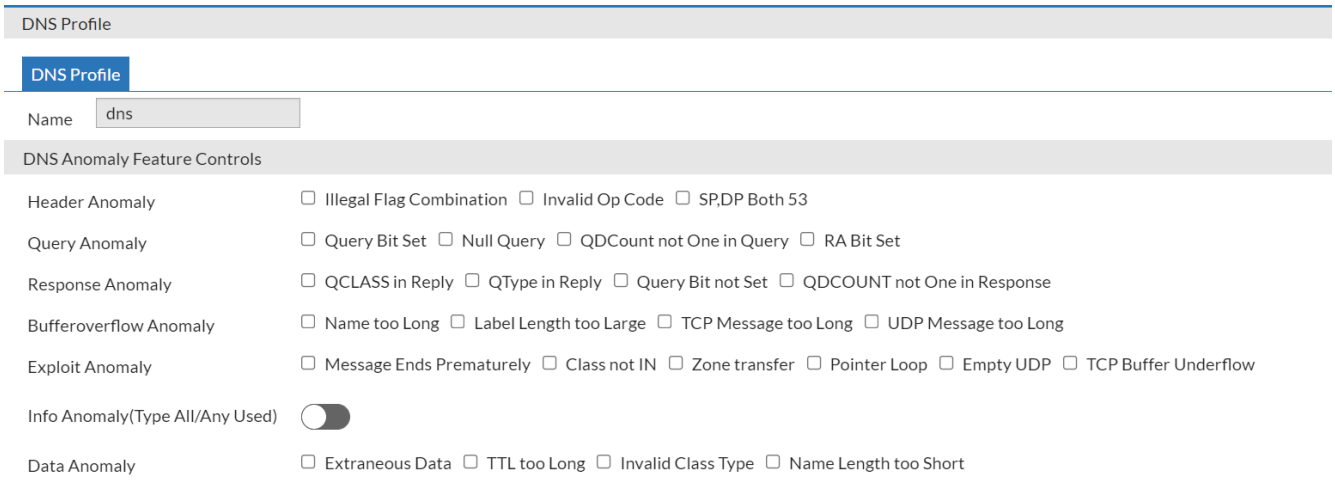
DNS Anomalies Feature Control

Use the DNS Anomalies Feature Control section to configure DNS traffic anomaly detection. DNS Anomalies (and DNS Feature Controls) cannot be used in SPPs that contain devices such as Firewalls, Proxies, Gateways, mail servers that produce encrypted DNS packets destined for port 53 on their cloud services. For example, FortiGate firewalls by default send encrypted DNS packets to FortiGuard UDP Port 53. The FortiGuard DNS port can be modified to UDP port 8888 which is recommended but other products maynot be modifiable.

FortiDDoS interprets these encrypted DNS packets as anomalies and drops them. This can result in no Internet access for any LAN-based client.

Devices sending encrypted packets should be isolated in a separate SPP with DNS Anomaly and Feature Controls disabled.

In order to discover if these devices exist in the SPP and identify the IP addresses of the devices, in *Detection Mode*, enable all DNS anomalies. In *Log & Report > Log Access > DDoS Attack Log*: Top Attacks widget, with the direction set to *Outbound*, look for DNS Anomaly drops across a wide range of anomalies. If you are seeing Outbound DNS Anomaly drops, drill down (using page icon to the right of Attack description) to see the detailed attack logs. Drill down further to see the Protected IPs. These will be the devices sending encrypted DNS. Move these IP addresses to a separate SPP and disable all DNS Anomalies and Features for that SPP.

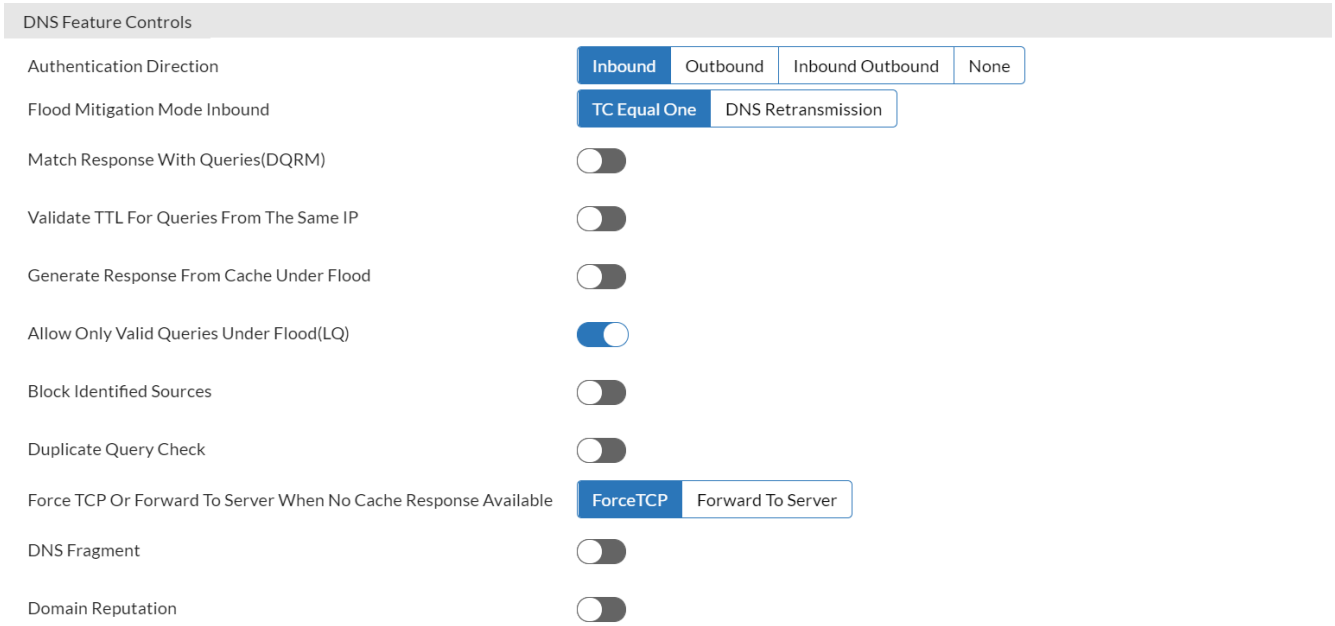


DNS Feature Controls

Use this section to configure DNS feature controls. For an overview of DNS features, see Understanding FortiDDoS DNS attack mitigation on page 72.

There are two network conditions where most DNS Feature controls must be disabled:

- If the FortiDDoS appliance is operating in Asymmetric traffic mode and cannot see both directions of the DNS traffic. See Understanding FortiDDoS Asymmetric Mode for TCP on page 68 for more information.
- In SPPs that contain Firewalls, Proxies, Gateways, mail servers or other equipment that generates encrypted DNS packets.



The DNS Resource Record Type

The DNS Resource Record Type ACL allows blocking of any number of DNS Resource Record Types by QTYPE number. The DNS QTYPE field allows 65,536 TYPES of which fewer than 100 are defined and less are in common use.

The following Qtypes can be blocked:

- Known Qtypes which are not needed (for example: ALL/ANY=255)
- Deprecated Qtypes (for example: NULL=10)
- Undefined Qtypes (for example: 32770-65279)

DNS Resource Record Type ACLs are defined in numeric ranges. A single ACL entry has DNS Resource

Record Type Start = DNS Resource Record Type End.

Settings	Guidelines for use with SPPs that contain Fire-walls, Proxies, Gateways, Email servers and other outbound generators of DNS Queries.	Guidelines for Symmetric traffic (or Asymmetric where FortiDDoS sees all traffic)	Guidelines for Asymmetric Mode, where FortiDDoS does not see all traffic.
Match responses with queries (DQRM)	Many Firewalls, including FortiGates, send encrypted SSL-over-UDP DNS Queries to destination UDP port 53. FortiDDoS sees these as DNS anomalies and drops them, preventing Internet access for users behind the firewall or other proxy devices. SSL-over-UDP DNS Queries do not meet any RFC but our experience is that they are standard industry practice for many firewalls, proxies, gateways, mail servers and other equipment that uses cloud services to detect malicious domains. FortiGate specifically can move the FortiGuard DNS Query port from 53 to 8888 and this is recommended if possible. However, in many cases, the equipment is unknown or is not capable of changing the Queries from UDP port 53. In this case, the Firewall or other equipment sending these encrypted DNS Queries should be isolated in a separate SPP with all DNS anomalies and DNS Feature controls disabled.	Enable/disable the DNS query response match (DQRM) table. Enable on all SPPs that do not carry encrypted DNS Queries.	Disable. DQRM depends on seeing both Queries and Responses. If these are not seen, DQRM will have unexpected results and may block users from the Internet.
Allow only valid queries under flood (LQ)		Enable/disable the legitimate query (LQ) table. LQ should normally be enabled ONLY on SPPs containing public Recursive or Authoritative DNS servers. It has little value for SPPs sending outbound Queries like firewalls and proxies.	Disable. The LQ table is populated based on seeing an r-code=0, 'good' DNS Response. This may not be available with asymmetric traffic.
Validate TTL for queries from the same IP under flood		Enable/disable the time-to-live (TTL) table. TTL validation should normally be enabled ONLY on SPPs containing public Recursive or Authoritative DNS servers. It has little value for SPPs sending outbound Queries like firewalls and proxies.	Disable. The TTL table is populated based on seeing an r-code=0, "good" DNS Response. This may not be available with asymmetric traffic.
DNS UDP Anti-spoofing Method inbound/outbound		Enable/disable anti-spoofing checks for inbound and outbound UDP DNS traffic. This can be used for all types of services. See firewall notes in second column.	Enable inbound if this leg of the traffic might see inbound DNS Queries
DNS flood mitigation mode inbound/outbound		Specify the antispoofing method if the source IP address is not already in the legitimate IP table (LIP):	Enable as for normal traffic suggestions.

Settings	Guidelines for use with SPPs that contain Fire-walls, Proxies, Gateways, Email servers and other outbound generators of DNS Queries.	Guidelines for Symmetric traffic (or Asymmetric where FortiDDoS sees all traffic)	Guidelines for Asymmetric Mode, where FortiDDoS does not see all traffic.
		• Force TCP (TC=1)—Return a DNS response to the client that has the DNS Truncate bit set and no response record data. A properly implemented DNS client will respond to the spoofed response by retrying the original DNS query using TCP port 53. TC=1 reduces the amount of inbound traffic, particularly for Authoritative DNS servers. If you are protecting authoritative servers, use this. This is recommended for protecting Recursive servers. • DNS Query Retransmission—Drop packets and test for valid retransmission. A valid client is expected to retransmit the Queries within preset time windows. DNS Query Retransmission reduces the amount of outbound traffic generated by FortiDDoS. If your outbound traffic is limited, use this.	
Generate response from cache under flood		Enable/disable DNS caching. Generally, more valuable for DNS Authoritative servers and may assist Recursive	Disable. Cache is created from outbound Responses which may not be seen.

Settings	Guidelines for use with SPPs that contain Fire-walls, Proxies, Gateways, Email servers and other outbound generators of DNS Queries.	Guidelines for Symmetric traffic (or Asymmetric where FortiDDoS sees all traffic)	Guidelines for Asymmetric Mode, where FortiDDoS does not see all traffic.
		servers under attack. No valid for outbound gateways, firewalls, etc.	
Force TCP or forward to server when no cache response available		If DNS caching is enabled ('Generate Response From Cache Under Flood' setting above), one of the following behaviors must be configured: • Force TCP (TC=1)—Return a DNS response to the client that has the DNS Truncate bit set and no response record data. A properly implemented DNS client will respond to the spoofed response by retrying the original DNS query using TCP port 53. Use with Authoritative DNS Servers. • Forward to Server—Forward the DNS query to the DNS server. Use with Recursive Servers If DNS caching is disabled, this setting is hidden and by default it will forward the DNS query to the DNS server.	Enable TC=1 if seeing inbound traffic.
Duplicate query check before response		Enable/disable checks for repeated queries from the same source. If enabled, under non-flood conditions, the system checks and drops repeated UDP/TCP queries from the same source if it sends them at a rate greater than 3 per	Enable if seeing inbound traffic.

Settings	Guidelines for use with SPPs that contain Fire-walls, Proxies, Gateways, Email servers and other outbound generators of DNS Queries.	Guidelines for Symmetric traffic (or Asymmetric where FortiDDoS sees all traffic)	Guidelines for Asymmetric Mode, where FortiDDoS does not see all traffic.
		second. Under flood conditions, the duplicate query check is done for TCP and not for UDP.	
Block identified sources		Enable/disable source IP address blocking periods for violators of any DNS-protection feature (ACL, anomalies, or flood meters). Disabled by default. DNS floods are often spoofed, so we do not recommend blocking an identified source to avoid punishing legitimate clients. Instead, we recommend you rely on the other DNS protection methods. They make packet-by-packet determinations and are not prone to false positives The configuration is open, allowing you to enable source blocking if you want to experiment with it in your network. If enabled, when a threshold is reached, packets are dropped and the identified sources are subject to the Blocking Period for Identified Sources configured on the Global Settings > Settings page. • Layer 7 > DNS > Query Per Source > DNS Query Per Source Egress Max Packet Rate/Sec • Layer 7 > DNS > Suspicious Sources > Packet Track Per	Disable

Settings	Guidelines for use with SPPs that contain Fire-walls, Proxies, Gateways, Email servers and other outbound generators of DNS Queries.	Guidelines for Symmetric traffic (or Asymmetric where FortiDDoS sees all traffic)	Guidelines for Asymmetric Mode, where FortiDDoS does not see all traffic.
		Source Egress Max Packet Rate/Sec	
Restrict DNS Queries to Specific Subnets		Enable/disable restriction to DNS queries from unwanted sources from the Internet. This feature allows service providers to protect their recursive or open DNS resolvers. In a typical deployment, the service provider will keep their open resolvers on the 'LAN' or the protected side of FortiDDoS and their own customers will be on the Internet side. On the Internet side, there will also be rogue DNS clients who send unwanted DNS query floods. To ensure that the DNS queries are only allowed from the service provider's customers, the service provider must add those subnets into the Restricted Subnets list. By restricting the DNS queries to specific subnets, the service provider can avoid responding to unwanted queries and thus protecting DNS infrastructure from getting overloaded.	Optional. But disable on outbound leg if installed there. For this reason, this feature is not recommended for HA pairs where one system is on primary inbound and one is on primary outbound. See Fortinet support for more details
DNS Fragment		Enable/disable checks for DNS packets.	Enable if seeing inbound traffic.

Settings	Guidelines for use with SPPs that contain Fire-walls, Proxies, Gateways, Email servers and other outbound generators of DNS Queries.	Guidelines for Symmetric traffic (or Asymmetric where FortiDDoS sees all traffic)	Guidelines for Asymmetric Mode, where FortiDDoS does not see all traffic.
Domain Reputation		Enable/disable domain reputation. If enabled, domain names in DNS query and response will used to match items in the Domain reputation database file. Domain Reputation updated through FortiGuard.	Enable if seeing inbound traffic.
DNS Resource Record Type ACL		Config range number of Resource Record Type.	Enable if seeing inbound traffic.

To configure with CLI:

```
config ddos spp dns profile
edit <dns profile name>
set dns-headeranomaly-feature-control {illegal-flag-combination invalid-op-code sp-equals-dp}
set dns-queryanomaly-feature-control {qr-bit-set null-query qdcount-not-one-in-query ra-bit-
     set}
set dns-responseanomaly-feature-control {qclass-in-reply qtype-in-reply qr-bit-not-set qd-
     count-not-one-in-response}
set dns-bufferoverflow-anomaly-feature-control {long-name-length long-label-length tcp-
     message-long udp-message-long}
set dns-exploitanomaly-feature-control {premature-end-of-packet class-not-in zone-transfer
     pointer-loop empty-udp tcp-buffer-underflow}
set dns-infoanomaly-feature-control {enable/disable}
set dns-dataanomaly-feature-control {extraneous-data long-ttl invalid-class-type short-name-
     length}
set dns-authentication-direction {none inbound outbound inbound-outbound}
set dns-flood-mitigation-mode-inbound {TC-equal-one dns-retransmission}
set dns-flood-mitigation-mode-outbound {TC-equal-one dns-retransmission}
set match-response-with-queries {enable/disable}
set validate-ttl-for-queries-from-the-same-ip {enable/disable}
set generate-response-from-cache-under-flood {enable/disable}
set allow-only-valid-queries-under-flood {enable/disable}
set source-blocking-in-dns {enable/disable}
set duplicate-query-check {enable/disable}
set force-tcp-or-forward-to-server {forcetcp/forward-to-server}
set aggressive-aging-incomplete-request {enable/disable}
set dns-fragment {enable/disable}
set domain-reputation {enable/disable}
config dns-resource-record-type-acl
edit <rule name>
set dns-resource-record-type-start <1-65535>
set dns-resource-record-type-end <1-65535>
next
end
next
```

```
    end
```

Monitor Graphs

This section includes the following topics:

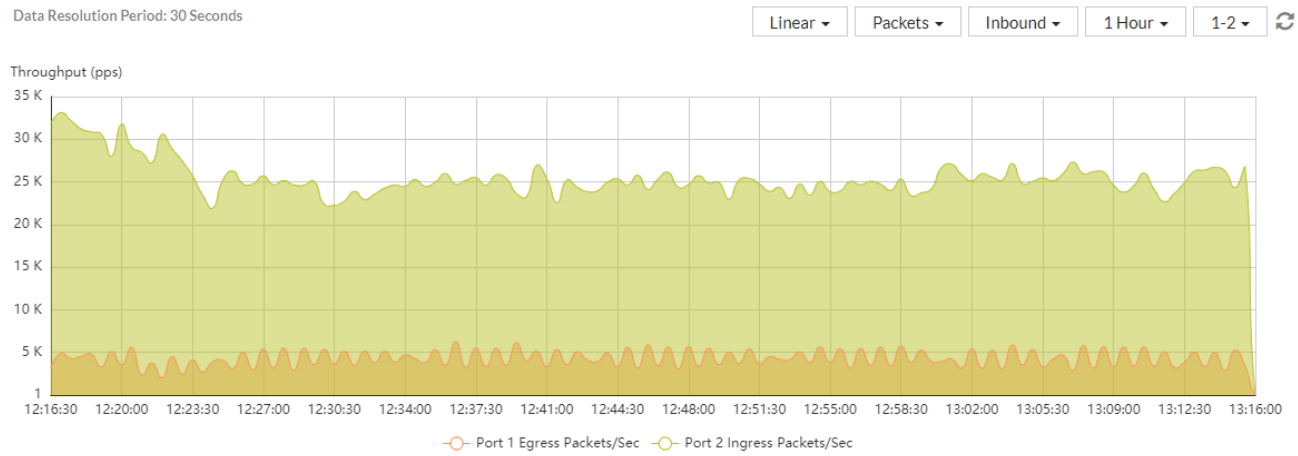
Monitor graphs overview

You can use the Monitor graphs to track trends in throughput rates, source and destination traffic, connections, and drops related to FortiDDoS detection and prevention settings.

Note: FortiDDoS Ingress/Egress traffic reporting is different from most network products. In order to immediately show attack drops, the graphs structure shows the differential in traffic arriving from the internet to FortiDDoS and traffic from FortiDDoS towards your infrastructure, the ingress/egress is structured like this.

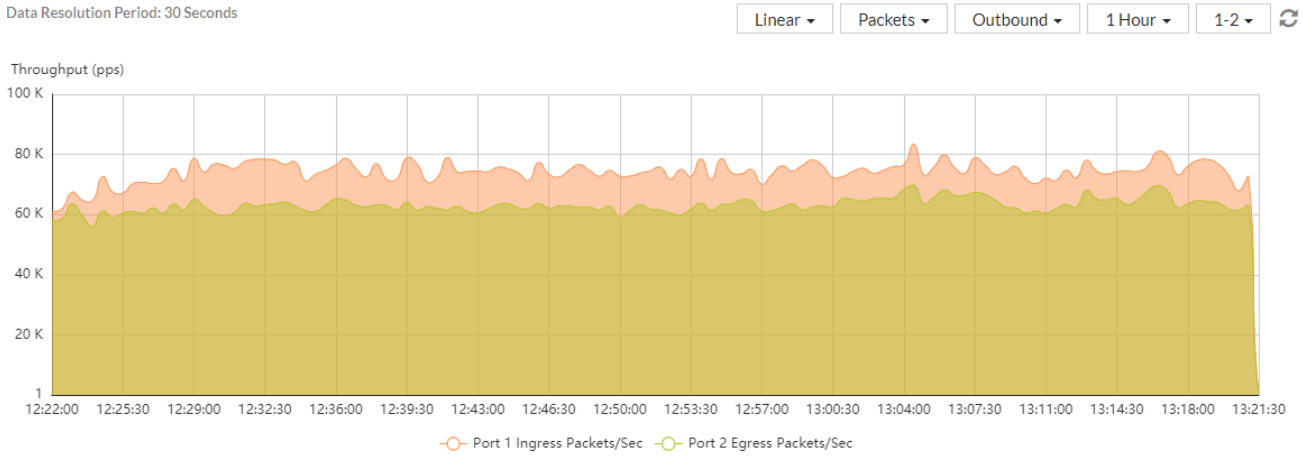
		From	To
Inbound	Ingress	Internet	FortiDDoS
	Egress	FortiDDoS	Internal network
Outbound	Ingress	Internal network	FortiDDoS
	Egress	FortiDDoS	Internet

The graph below shoes that the green Ingress traffic is significantly higher than the orange Egress traffic. This indicates that FortiDDoS is dropping traffic as it passes through the system and you are under attack.



The labels show that Ingress is from Port 2 (Internet facing port) and Egress is from Port 1 (internal network facing port), unlike a firewall where ingress and egress is shown for the same port.

Ingress/Egress is reversed for the outbound direction. Again, you will see immediately if FortiDDoS is dropping packets as they traverse the system.



Other graph features:

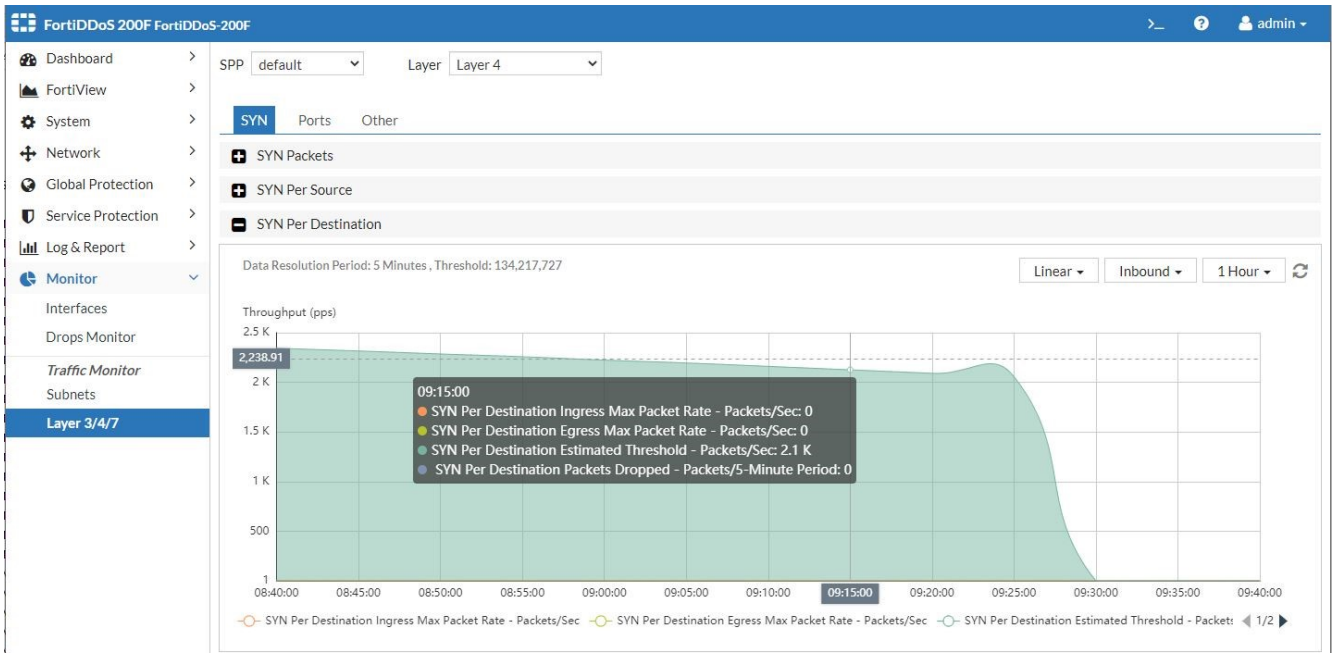
- All graphs support both Inbound and Outbound views.
- Most graphs are in packets-per-second but some graphs also show bits-per-second and some will show counts like Connections per Second or Drops.
- Many graphs are SPP-related and will show a drop-down menu to select the SPP to view
- All graphs can switch the Y-Axis view between Linear and Logarithmic. Logarithmic is useful when there is a combination of very high and very low sub-graphs within the same graph.
- All graphs can display traffic and/or drops for 1-hour, 8-hours, 1-day, 1-week, 1-month or 1-year.
- Most graphs do not refresh automatically so there is a refresh icon a the top-right of the graph.
- Subgraph views such as the Port 1 Ingress Packets/Sec above can be hidden by clicking anywhere on the label. Click again to unhide. Hidden sub-graphs will be unhidden if you leave the graph page.
- If there are a very large number of sub-graphs on the page, you will see pagination arrows to the left of the labels to see other labels.

The Monitor graphs menu includes the following categories:

- **Dashboard**
  - Aggregate physical *Interfaces* traffic
  - Aggregate all-*SPP* traffic
  - Aggregate all-SPP *Drops*
- ***FortiView > SPP > View*** **provides a per-SPP view of**:
  - Traffic rates
  - Source *Countries* traffic rates
  - SPP *Attacks* aggregate drops
  - SPP *Protocols* aggregate traffic rate
- **Monitor**
  - Interfaces
    - Per interface-port-pair graph showing:
      - Inbound Ingress traffic (from the internet to FortiDDoS)
  - Drops Monitor
    - Per-SPP Layer 3 to Layer 7 attack graphs for:
      - Aggregate Drops
      - Flood Drops
      - ACL Drops
      - Anomaly Drops
      - Memory Drops
  - Traffic Monitor
    - Per-SPP Protection *Subnets* traffic rates
    - Per-SPP *Layer 3/4/7* traffic rates and attack drops

The multiple views and granular filters are useful for comparing and contrasting trends broadly, and for drilling into details. For example, you can use the Aggregate drops graph to get an overall picture on security events and see whether to review ACL graphs, flood graphs, or anomalies graphs next.

The following graph is an example of a monitor graph.



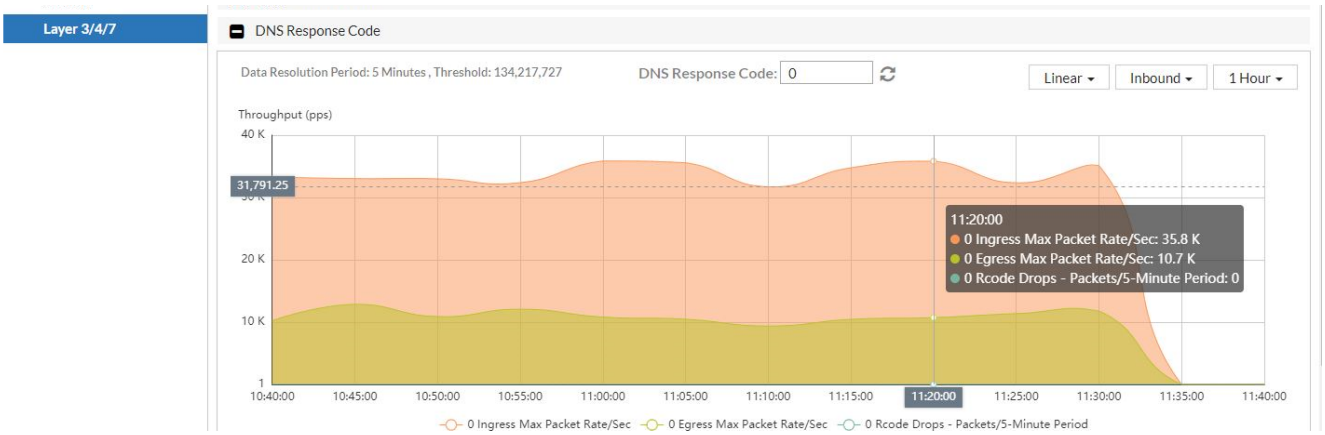
It shows the following information:

- Data resolution Period - Whether data points for the graph are rolled up in 30 second, 5 minute, 1 hour, 3 hour, or 45 hour windows.
- Threshold - The configured minimum threshold (matches the setting on the *Service Protection* > *Service Protection Policy* > *{SPP Rule}* >*Thresholds*).
- Y-Axis Linear or Logarithmic selection which allows easier viewing of both low-rate and high-rate parameters at the same time
- Inbound or Outbound traffic direction
- Duration of the graph from 1 hour to 1 year
- Throughput - A graph of the throughput rate for the selected protocol during the time period. Depending on context, some graphs will:
  - Allow selection of pps or bps (Interface and SPP Traffic graphs, for example)
  - Display counts (Connections per Second graph, for example)
- Packets dropped - A graph of packets dropped because the threshold was exceeded, validation was undertaken or other reasons depending on the parameter.
- Parameter sub-graphs may be hidden by clicking on the matching legend label along the bottom of the graph. When graphs support many parameters, the right side of the legend will show additional “pages” of labels with directional arrows (< 1 / 2 >)

Tool-tip Data point details

The following figure shows tool-tip information displayed when the mouse pointer hovers over a point in the graph. The tool-tip has details about that data point.

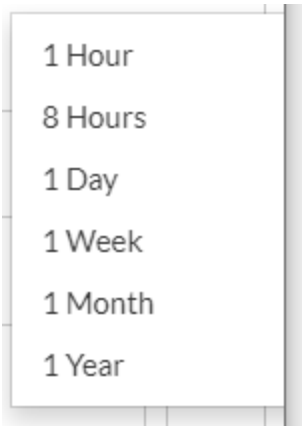
Tool-tip information for point on graph line



Reading Monitor graphs

Definitions

- **Graph Period** - The links at the top-right of every graph page select the full period (width) of the graph.



- **Data Resolution Period** - When a Graph Period is selected, the *Data Resolution Period* (scale) of the graph is automatically changed. This shows the measurement interval within the Graph Period. The Data Resolution Period is always displayed at the top-left of the graph page. This Period is the time between each graph point on the x-axis of the graph.

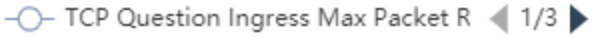
Sub-graph labels

Many graphs include several sub-graphs and two types of sub-graphs – data rates and drops – for specific parameters. If not obvious from the graph types, labels below the graph will include one of two labels:

- **Packets/Sec** for data rate sub-graphs.
- **Packets/5-Minute Period** for drop graphs. See the Graphs showing drops below for details on how these are displayed.

Sub-graph labels are color-matched to the sub-graphs long the bottom edge of the graph. You may hide specific sub-graph displays from the graph by clicking the label. All sub-graphs and labels will default-on if you leave that page.

Graphs that contain many subgraph labels will display “pagination” information to the right of all labels.



Monitor Graph Data Resolution

All Monitor graphs calculate the MAXIMUM data rate (pps, bps, connections, etc.) over a 5-minute period and depending on the graph Period (upper-right 1-hour, 8-hour, 1-day, etc.) selection, display:

- For 1-hour, 8-hour and 1-day selections, the MAXIMUM data rate per 5-minute period.
- For all other Period selections, the graph shows the MAXIMUM of the 5-minute MAXIMUM rates across the Period Selected. For example, for the:
  - 1-week Period, the graph shows the MAXIMUM rate from the highest of the 12 x 5-minute MAXIMUM rates across a 1-hour period.
  - 1-month Period, the graph shows the MAXIMUM from the highest of the 36 x 5-minute MAXIMUM rates across a 3-hour period.

Special Traffic Graphs

One-hour Graph Periods for:

- *Dashboard* > *Interfaces* (aggregate Interface traffic)
- *FortiView* > *SPP* > *View* > *SPP Traffic Chart*
- *Monitor* > *Interfaces*

Use a 30-second Data Resolution Period to provide better granularity. All other Graph Periods follow the information above.

Graphs showing drops

Drop graphs display the highest number of dropped packets for any 5-minute interval within the Data Resolution Period displayed at the top-left of the graph.

For 1-hour, 8-hour and 1-day Periods, the Data Resolution Period is 5-minutes and the drop graph shows the maximum drops per-5-minute interval.

For Periods longer than 1-day, drops are not aggregated - only the maximum 5-minute drop count for any interval over each Data Resolution Period is displayed. For example, for a 1-week Graph Period (top-right of the page), the Data Resolution Period (top-left) is 1-hour and the drop graphs will show the maximum number of drops seen for any of the 12 x 5-minute intervals in that hour. The drops are not accumulated for the entire hour. The same is true for longer Periods.

Graphs Y-Axis

To display both large flood drops and smaller anomaly drops, on the same graph, set the Y-axis view to 'Logarithmic' at the top-right of the page.

Graph Refresh

Graphs on the *Dashboard* > *Status* page auto-refresh every 30 seconds.

All other graphs do not auto-refresh. There is a circular arrow icon at the top-right of every page to manually refresh.

Using Interface graphs

Use the *Monitor* > *Interfaces* graphs to monitor network interface throughput. FortiDDoS ports are configured as network interface pairs. You configure odd-numbered ports for the LAN-side connection and even-numbered ports for the WAN-side connection.

The *Interfaces* graph includes the following information:

• *Direction* – View Inbound or Outbound traffic

• *Graph Period* - View the graph for 1 hour to 1 year

• *Interface Pair* – Varies from 1-2 through 7-8 to 1-2 through 15-16 depending on the model

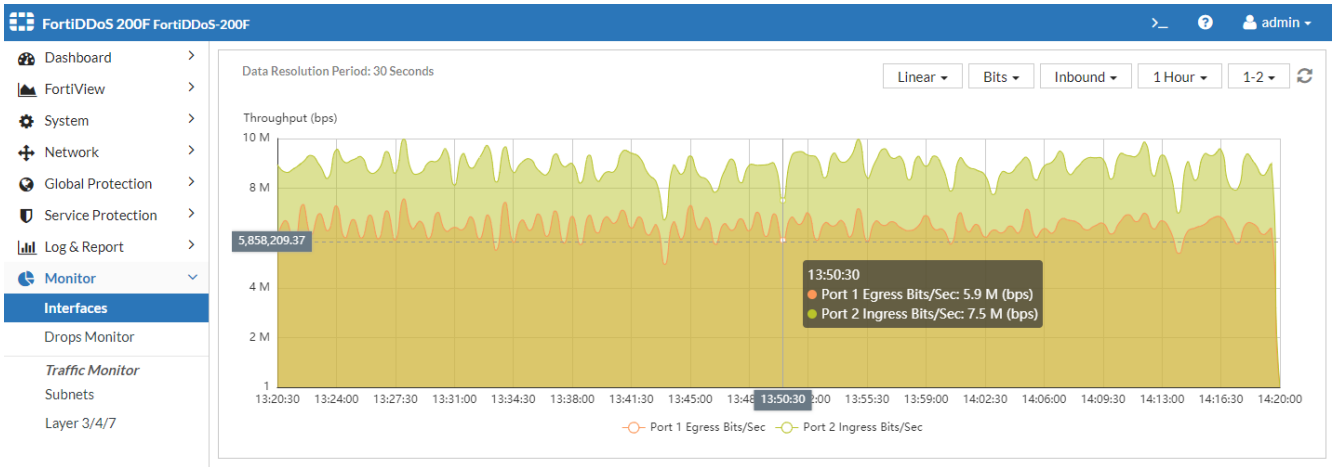
• *Y-Axis scale* – Linear or Logarithmic

• *Throughput* – Ingress/Egress traffic rates selectable in packets per second (Packets) or bits per second (Bits)

FortiDDoS displays Ingress/Egress traffic differently from other networking products. In order to show the affect FortiDDoS may be having on traffic in either direction FortiDDoS shows:

- Inbound Ingress traffic from the Internet to FortiDDoS
- Inbound Egress traffic from FortiDDoS to your protected network

This way, you will immediately see if FortiDDoS is dropping packets as they pass through the system. In the screenshot below, it is obvious that the Port 2 Ingress (from the Internet) is higher than the Port 2 Egress (to your protected network).



Conversely:

- Outbound Ingress shows traffic from your protected network to FortiDDoS
- Outbound Egress shows traffic from FortiDDoS to the Internet

Again, this will immediately show if FortiDDoS is influencing the traffic as it passes through the system.

At the shortest 1-hour Graph Period, the Interfaces graph displays the average data rate of Ingress and Egress packets for each 30-second Data Resolution Period. As the Graph Period lengthens, the Data Resolution Period also increases and displays the maximum average data rate seen during each Data Resolution Period within the Graph Period.

For example, when looking at the 1-hour Graph Period you see only 1 x 30-second Data Resolution Period displaying 1Gbps at 14:31:30, with no other periods showing any traffic. If you change to the 1-hour Graph Period, 1 x 5-minute Data Resolution Period (at 14:35:00) will show 1Gbps.

Note: Interfaces statistics are not maintained per SPP. You cannot view by SPP, and Interfaces statistics are not reset when you reset SPP statistics. Interfaces statistics are global data that gets reset only when you perform a complete factory reset and/or reformat the log disk.

Before you begin:

- You must have Read permission for the Monitor menu.
- Refer to Reading Monitor graphs to understand the graphs in detail.

To display the graphs:

1. Go to *Monitor* > *Interfaces* > *{Port-Pair selection}*.

Using the SPP Traffic graphs

Use the *FortiView* > *SPP* > *View SPP* Traffic Chart graph to monitor overall throughput for a selected SPP.

The SPP Traffic Chart includes the following view options:

- Direction – View Inbound or Outbound traffic
- Graph Period - View the graph for 1 hour to 1 year
- Y-Axis scale – Linear or Logarithmic
- Throughput – Ingress/Egress traffic rates selectable in packets per second (Packets) or bits per second (Bits) FortiDDoS displays Ingress/Egress traffic differently from other networking products. In order to show the affect the FortiDDoS SPP may be having on traffic in either direction FortiDDoS shows:
  - Inbound Ingress traffic from the Internet to FortiDDoS SPP
  - Inbound Egress traffic from FortiDDoS SPP to your protected network

You can customize the following query terms: SPP, period, and direction.

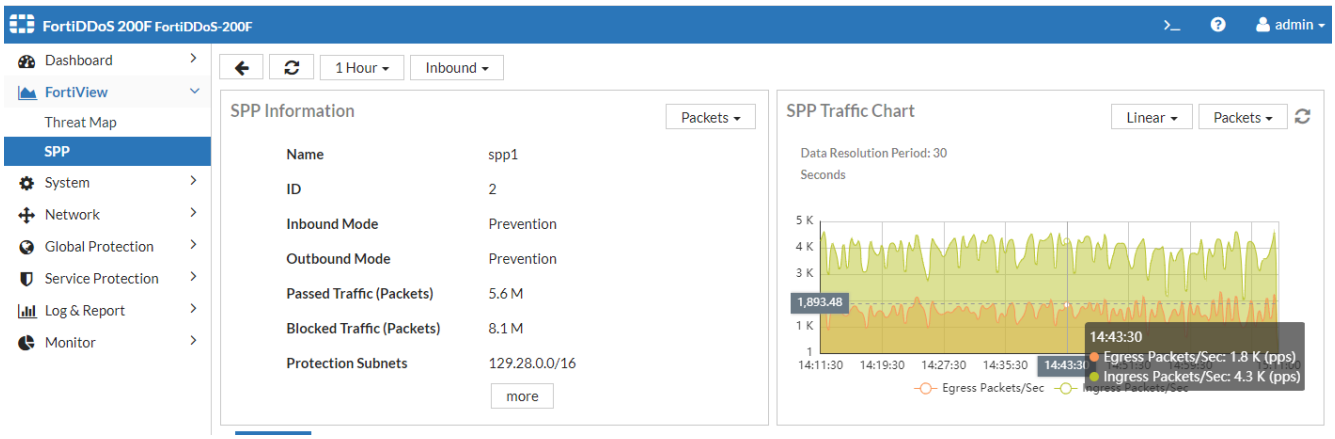
Before you begin:

- You must have Read permission for the Monitor menu.
- Refer to Reading Monitor graphs to understand the graphs in detail.

To display the graphs:

1. Go to *FortiView* > *SPP*
2. From the list, select *View* for the appropriate SPP

Below is the SPP Traffic Chart for “spp1”



Using Subnets graphs

Subnets graphs show the inbound and outbound ingress and egress traffic for individual SPP Protection Subnets. Use these graphs to observe specific traffic to a Protection Subnet. Since Protection Subnets can be configured from a single IP to a large subnet, considerable flexibility is offered to see traffic patterns and attacks to protected devices. No drops are shown on these graphs, but divergence of the green and blue graph lines will clearly show attack events.

The Subnets graph includes the following graphs:

- Inbound or Outbound Ingress and Egress traffic in:
  - Packets - Throughput in packets per second.
  - Bits - Throughput in bits per second.

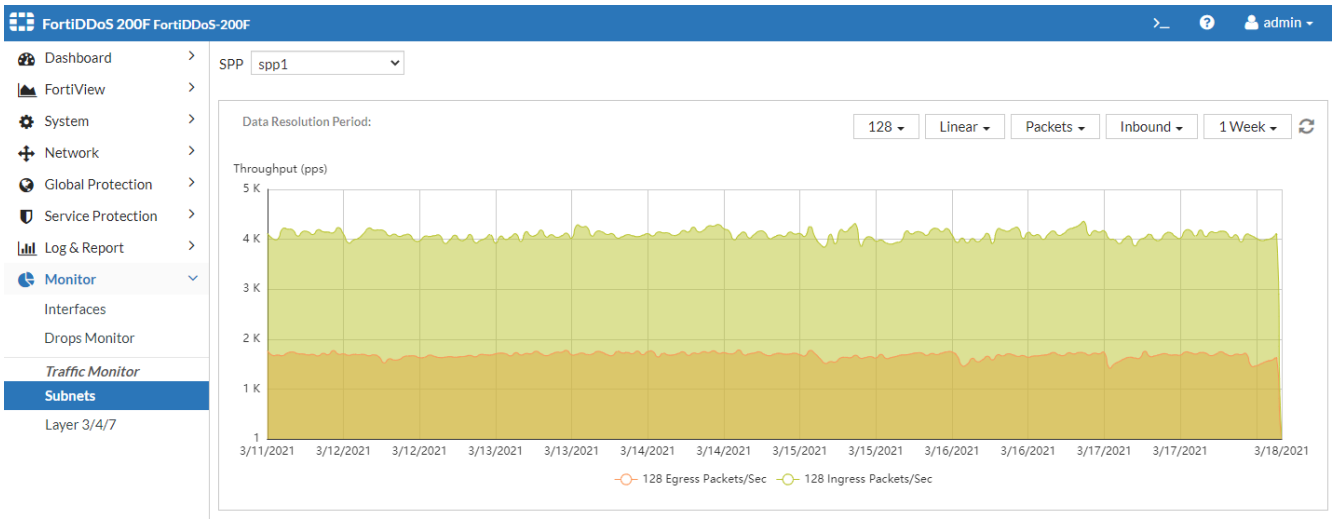
You can further customize the graph view by: SPP, Protection Subnet within the SPP, Reporting Period and Linear or Logarithmic Y-Axis.

Before you begin:

- You must have Read permission for the Monitor menu.
- Refer to Reading Monitor graphs on page 294 to understand the graphs in detail.

To display the graphs:

1. Go to *Monitor* > *Subnets*
2. Select the SPP from the drop-down menu.
3. Select the Protection Subnet from the drop-down menu.
4. Select other parameters as desired.



Using Drops Monitor graphs

Use the *Monitor* > *Drops Monitor* graphs to monitor trends in drops over time. The Drops Monitor graphs plots the following data per SPP:

- Aggregate Graph of all drops from Floods, ACLs, Anomalies and Memory issue at all Layers 3/4/7
- Flood / ACL / Anomaly / Memory category tabs showing:
  - Aggregate of all Layer 3/4/7drop
  - Layer 3 drops with additional subgraph details
  - Layer 4 drops with additional subgraph details
  - Layer 7 drops with additional subgraph details

At each category and Layer, customize these additional graph parameters:

- SPP
- Reporting Period (1-hr to 1-yr),
- Linear or Logarithmic Y-Axis

Placing the cursor on the Monitor graph will display a tool-tip with additional information.

FortiDDoS displays graph drops every 5 minutes (Attack Logs may report faster). The graphs do not auto-refresh. There is a refresh icon at the top-right of every graph.

Using the Aggregate Drops graph

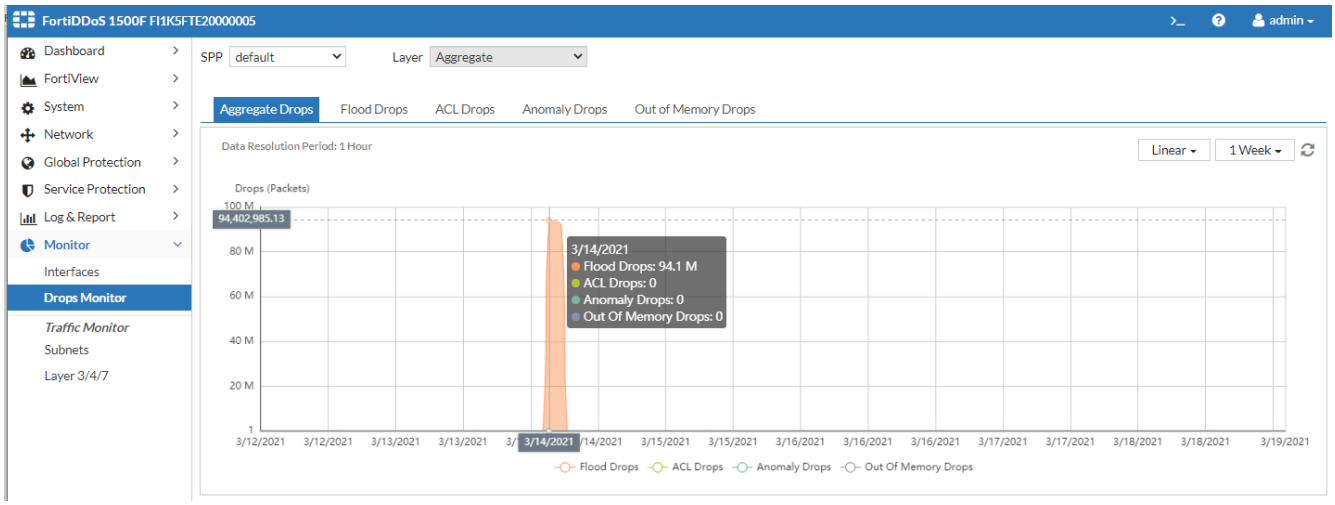
You use the Aggregate drops graph to monitor trends in drops over time. The Aggregate drops graph plots the following data for all Layer 3/4/7 per SPP:

- Flood Drops - Aggregate of drops due to packet rate thresholds.
- ACL Drops - Aggregate of drops due to ACL rules.
- Anomaly Drops - Aggregate of drops due to anomaly detection methods.

- Out of Memory Drops - Aggregate of drops due to built-in rules that detect memory attacks on the FortiDDoS system itself.

You can customize the following viewing parameters: SPP, Reporting Period (1-hr to 1-yr), Linear/Logarithmic Y-Axis

Placing the cursor on the Monitor graph will display a tool-tip with additional information.



Before you begin:

- You must have Read permission for the Monitor menu.
- Refer to Reading Monitor graphs on page 294 to understand the graphs in detail.

To display the graph:

1. Go to *Monitor* > *Drops Monitor* > *Aggregate Drops* > [SPP] [Y-Axis View] [Reporting Period].

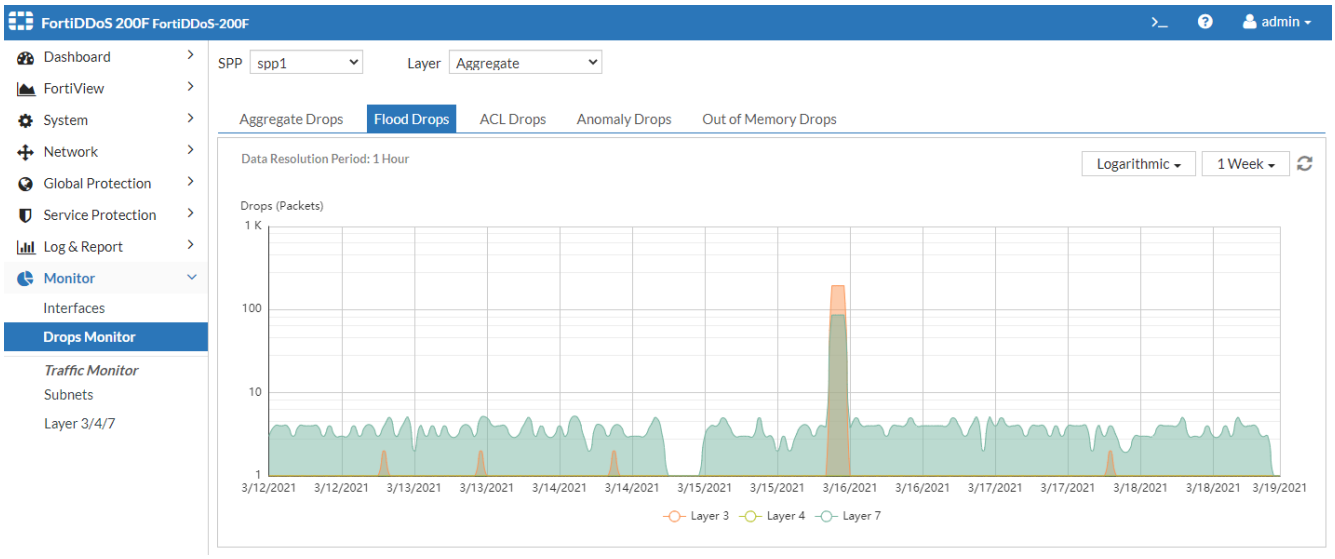
Using the Flood Drops graphs

Use the Flood Drops graphs to monitor drops due to SPP packet rate thresholds that detect flood attacks.

Customize the graph with the following viewing parameters: SPP, Reporting Period (1-hr to 1-yr), Linear/Logarithmic Y-Axis.

Placing the cursor on the Monitor graph will display a tool-tip with additional information.

For many parameters additional information will be see in the Traffic Monitor Graphs.



Before you begin:

- You must have Read permission for the Monitor menu.
- Refer to Reading Monitor graphs on page 294 to understand the graphs in detail.

To display the graph:

1. Go to *Monitor* > *Drops Monitor* > *Flood Drops* > [SPP] [Aggregate/Layer 3/4/7] [Y-Axis View] [Reporting Period].

The following summarizes the statistics displayed in the graphs.

Statistic	Description
Aggregate	
Layer 3	Aggregation of drops due to SPP Layer 3 thresholds.
Layer 4	Aggregation of drops due to SPP Layer 4 thresholds.
Layer 7	Aggregation of drops due to SPP Layer 7 thresholds.
Layer 3	
Protocols	Aggregation of drops due to protocols thresholds. These counters track the packet rate for each protocol.
Fragmented Packets	Drops due to the SPP Fragment thresholds (TCP/UDP/Other Protocols).
Source Flood	Drops due to the SPP Most Active Source (MAS) threshold. This counter tracks dropped packets from source IP addresses.
Destination Flood	Drops due to the SPP Most Active Destination (MAD) threshold. This counter tracks dropped packets to protected IP addresses. **Note**: The Most Active Destination Threshold is set to system maximum by System Recommendations.

Statistic	Description
Layer 4	
SYN	Drops due to the SPP SYN threshold. This counter shows drops due to SYN (Source IP) Validation for the aggregate rate of all SYNs into the SPP. Further SYN detail is available in the *Traffic Monitor > Layer 4* graphs
TCP Ports	Aggregation of drops due to the SPP rate-limiting thresholds for TCP ports.
UDP Ports	Aggregation of drops due to the SPP rate-limiting thresholds for UDP ports.
ICMP Types/Codes	Aggregation of drops due to the SPP rate-limiting thresholds for ICMP types/codes.
Zombie Flood	Drops due to the SPP New Connections threshold, which sets a limit for legitimate IPs. FortiDDoS assumes a zombie flood is underway when the number of allowed legitimate IP addresses during a SYN flood exceeds a set threshold. These packets indicate that non-spoofed IP addresses are creating a DDoS attack by generating a large number SYN packets. Note: The New Connections Threshold is set to system maximum by System Recommendations.
SYN Per Source Flood	Drops due to the SPP SYN per Source threshold. This counter shows drops due to SYN per Source IP rate limiting within the SPP. No SYN Validation is done for SYN per Source. Further SYN per Source detail is available in the Traffic Monitor > Layer 4 graphs.
Connections Per Source	Drops due to the SPP Concurrent Connections per Source rate-limiting threshold.
SYN Per Destination	Drops due to the SPP SYN per Destination threshold. This counter shows drops due to SYN Validation for over-threshold Protected IPs (Destinations) within the SPP. Further SYN per Destination detail is available in the *Traffic Monitor > Layer 4* graphs
Slow Connection	Drops due to SPP slow connection detection and blocking of identified sources of slow connection attacks.
Layer 7	
Aggregate	Display of aggregate Flood drops for: • HTTP • SSL/TLS • DNS • NTP
HTTP	Display of Flood drops due to HTTP thresholds for: • Methods (GET, HEAD, OPTIONS, TRACE, POST, PUT, DELETE, CONNECT) • Method per Source (aggregation of any Methods per Source IP) • URL • Host • Referer • Cookie • User Agent
SSL/TLS	Display of drops from SSL/TLS Incomplete Request Source Flood.
DNS	Display of drops due to DNS thresholds:

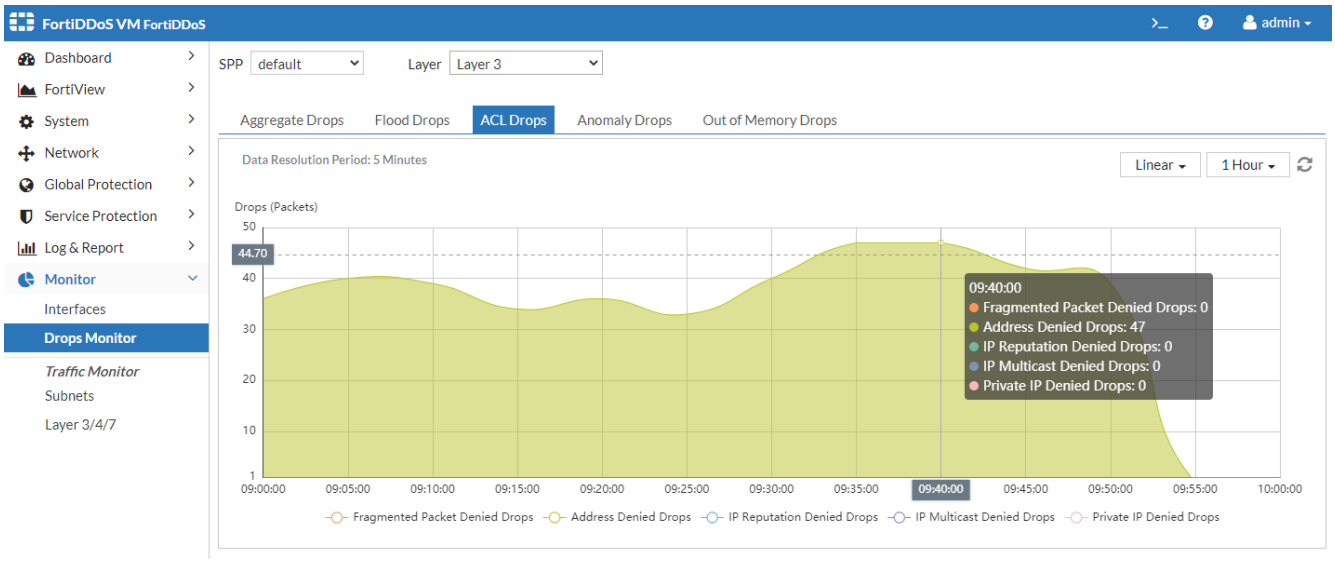
Statistic	Description
	• Unsolicited DNS Response Drop - Drops when a DNS Response is received but there is no DNS Query entry in the DNS Query Response Matching (DQRM) table. • LQ Drops - Drops during any type of UDP Query Flood when the Query is not in the Legitimate Query (LQ) table. • TTL Drop - Drops during any type of UDP Query Flood when a source IP address sends a repeated DNS UDP Query for the same destination before the TTL has expired. It is expected that the query should not be repeated until the TTL expires. • Cache Drop - Drops during any type of UDP Query Flood when a response was served from the Cache or because a response was not found in the cache and the system is configured to drop such queries. • Spoofed IP Drop - Drops due UDP DNS anti-spoofing checks (Retransmission or TC=1/Force TCP) • Unexpected Query Drop - Drops due to Duplicate Query checks. • Query Per Source Drop - Drops due to the DNS UDP Query per Source threshold. This rate-limiting threshold tracks DNS UDP Query rates from source IP addresses and does not attempt Source or Query validation. . • Suspicious Sources Drop - Drops due to the UDP DNS Packet Track per Source threshold. This rate-limiting threshold tracks sources that demonstrate suspicious activity (a score based on heuristics that count fragmented packets, response not found in DQRM, or queries that generate responses with RCODE other than 0). • Fragment Drop - Drops due to rate-limiting DNS Fragment threshold for UDP traffic. • TCP Query Drop - Drops due to the rate-limiting DNS Query TCP threshold for TCP traffic • TCP Question Drop Drops due to the rate-limiting DNS Question Count TCP threshold for TCP traffic. • TCP MX Drop Drops due to the rate-limiting DNS MX Count TCP threshold for TCP traffic. • TCP All Drop Drops due to the rate-limiting DNS All TCP threshold for TCP traffic. • TCP Zone Transfer Drop - Drops due to the rate-limiting DNS Zone Transfer TCP threshold for TCP traffic.
NTP	Display of drops due to NTP thresholds: • Request Flood Drops - Drops due to rate-limiting NTP Request threshold • Response Flood Drops - Drops due to rate-limiting NTP Response threshold • Broadcast Packet Flood Drops - Drops due to rate-limiting NTP Broadcast threshold • Response per Destination Flood Drops - Drops due to rate-limiting NTP Response per Destination threshold

Using the ACL Drops graphs

Use the ACL Drops graphs to monitor drops due to SPP ACL rules. Note, some drops due to Global ACL rules may appear in SPPs including the default SPP.

Customize the graph with the following viewing parameters: SPP, Reporting Period (1-hr to 1-yr), Linear/Logarithmic Y-Axis.

Placing the cursor on the Monitor graph will display a tool-tip with additional information.



Before you begin:

- You must have Read permission for the Monitor menu.
- Refer to Reading Monitor graphs on page 294 to understand the graphs in detail.

To display the graph:

1. Go to *Monitor* > *Drops Monitor* > *ACL Drops* > [SPP] [Aggregate/Layer 3/4/7] [Y-Axis View] [Reporting Period].

Statistic	Description
Aggregate	
Layer 3	An aggregation of drops due to ACL rules based on Layer 3 parameters.
Layer 4	An aggregation of drops due to ACL rules based on Layer 4 parameters.
Layer 7	An aggregation of drops due to ACL rules based on Layer 7 parameters.
Layer 3	
Fragmented Packet Denied Drops	Drops due to Service ACL for UDP, TCP and/or Other Protocols Fragment.
Address Denied	Drops due to ACL rules based on IP address, geolocation, or Blocklisted IPv4
IP Reputation Denied	Drops due to ACL rules based on IP Reputation active Subscription settings in IP Profile
IP Multicast	Drops due to ACL rules based on IP Multicast Check setting in IP Profile assigned to the SPP.
IP Private Denied	Drops due to ACL rules based on IP Private Check setting in IP Profile assigned to the SPP.
Layer 4	
Aggregate	Aggregate Layer 4 drops due to SPP ICMP Type/Code and other ACL

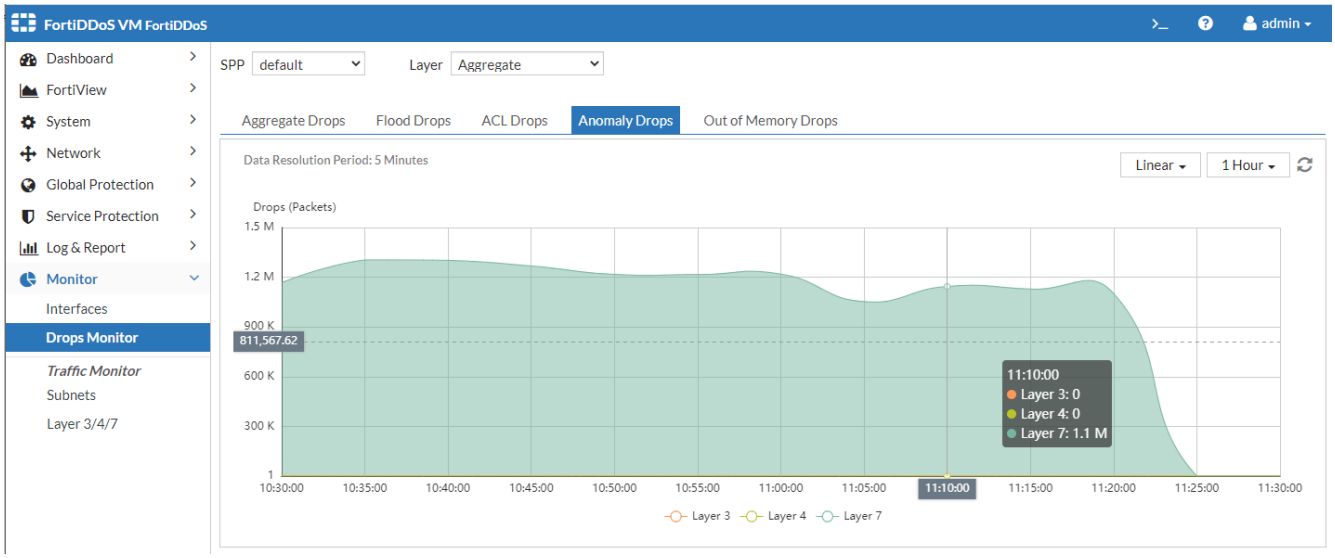
Statistic	Description
ACL Rule Drops	Drops due to SPP ACL rules
Layer 7	
Aggregate	Aggregate drops due to rules for • HTTP • DNS • NTP
HTTP	Drops due to HTTP ACL rules for: • URL Denied • Host Denied • Referer Denied • Cookie Denied • User Agent Denied
DNS	Drops due to DNS ACL rules for: • DNS Fragments • Blocklisted Domains • DNS Resource Record Type
NTP	Drops due to NTP ACL rules for: • NTP Reflection Deny

Using the Anomaly Drops graphs

Use the Anomaly Drops graphs to monitor drops due to Layer 3, Layer 4, and Layer 7 anomalies.

Customize the graph with the following viewing parameters: SPP, Reporting Period (1-hr to 1-yr), Linear/Logarithmic Y-Axis.

Placing the cursor on the Monitor graph will display a tool-tip with additional information.



Before you begin:

- You must have Read permission for the Monitor menu.
- Refer to Reading Monitor graphs on page 294 to understand the graphs in detail.

To display the graph:

1. Go to *Monitor* > *Drops Monitor* > *Anomaly Drops* > [SPP] [Aggregate/Layer 3/4/7] [Y-Axis View] [Reporting Period].

Statistic	Description
Aggregate	Aggregation of all anomaly drops for: • Layer 3 • Layer 4 • Layer 7

Layer 3	Drops due to (IP Profile Strict Anomalies option):
	• IP Header Checksum Error
	• (Other) Layer 3 anomalies, including:
	• Drops due to the Layer 3 anomalies, including:
	  • IP version other than 4 or 6
	  • Header length less than 5 words
	  • End of packet (EOP) before 20 bytes of IPV4 Data
	  • Total length less than 20 bytes
	  • EOP comes before the length specified by Total length
	  • End of Header before the data offset (while parsing options)
	  • Length field in LSRR/SSRR option is other than (3+(n*4)) where n takes value greater than or equal to 1
	  • Pointer in LSRR/SSRR is other than (n*4) where n takes value greater than or equal to 1
	  • For IP Options length less than 3
	  • Reserved flag set
	  • More fragments and Don't Fragment Flags both set
	• Source and Destination Address Match - Source and Destination addresses are the same (LAND attack).
	• Source/Destination as LocalHost - Source or Destination address is the same as the localhost (loopback address spoofing).

Layer 4	
Aggregate	Aggregate graphs showing all anomaly drops due to Layer 4: • Header • State
Header	Anomaly drops due to (IP and TCP Profile Strict Anomalies options): • TCP checksum errors • UDP checksum errors • ICMP Checksum errors • TCP Invalid Flag Combination –Invalid TCP flag combinations such as SYN-PSH-RST

Statistic	Description

	• (other) Anomaly Detected, including:
	  • Other header anomalies, such as incomplete packet
	  • Urgent flag is set then the urgent pointer must be non-zero
	  • SYN or FIN or RST is set for fragmented packets
	  • Data offset is less than 5 for a TCP packet
	  • End of packet is detected before the 20 bytes of TCP header
	  • EOP before the data offset indicated data offset
	  • Length field in Window scale option other than 3 in a TCP packet
	  • Missing UDP payload
	  • Missing ICMP payload
	  • SYN with payload (TCP Profile option)
	• Invalid ICMPv4 Type/Code via Protocol 1 (ICMP Profile option) – Invalidates (makes anomalies) the >64,000 available ICMP Types/Codes that are not IETF/IANA ratified and in-use.
	• Invalid ICMPv6 Type/Code via Protocol 58 (ICMP Profile option) – Invalidates (makes anomalies) the >64,000 available ICMP Types/Codes that are not IETF/IANA ratified and in-use.

State	Anomaly drops due to (TCP Profile options): • Foreign Packets – Out-of-State TCP packets • Forward Transmission Not Within Window - Packets outside the receiver's windows (TCP Profile Sequence Validation option) • Reverse Transmission Not Within Window - Packets outside the receiver's windows (TCP Profile Sequence Validation option) • TCP State Transition - Packets that violate the TCP Protocol state transition rules or sequence numbers (TCP Profile State Transition Validation option) • Foreign Packets (Aggressive aging and Slow Connections) – Packets no longer in active sessions due to aggressive aging or slow connection blocking (TCP Profile option)
Layer 7	
Aggregate	Aggregate of drops due to anomalies for: • HTTP • SSL/TLS • DNS • NTP
HTTP Header	HTTP Anomaly Drops (HTTP Profile options) for: • Known Method - Drops packets if the METHOD matches with any of the eight known OpCodes selected as not allowed in the HTTP Profile (GET, HEAD, OPTIONS, TRACE, POST, PUT, DELETE, CONNECT) • Unknown Method – Drops packets whose METHOD is outside the 8 known Methods (any Method that is not: GET, HEAD, OPTIONS, TRACE, POST, PUT, DELETE, CONNECT) • Invalid HTTP Version - packets with an invalid HTTP version • Range Present - packets with a header range request • Incomplete HTTP Request - HTTP requests that do not end in the correct end-of-packet information.

Statistic	Description
SSL	SSL/TLS Anomaly Drops (SSL/TLS Profile options) for: • SSL Renegotiation – packets dropped due to excessive numbers of renegotiation requests over time as configured in the SSL/TLS Profile • SSL Protocol errors • SSL Version errors • SSL Cipher suite errors • SSL Incomplete Request errors
DNS	DNS Anomaly Drops (DNS Profile Options) for: • Header • Query • Response • Buffer Overflow • Exploit • Info • Data
NTP	NTP Anomaly Drops (NTP Profile Options) for: • Header • Data Length • Stratum • Version • Control Header • State • Duplicate Queries before Response • Sequence Mismatch • Unsolicited Response • Mode Mismatch

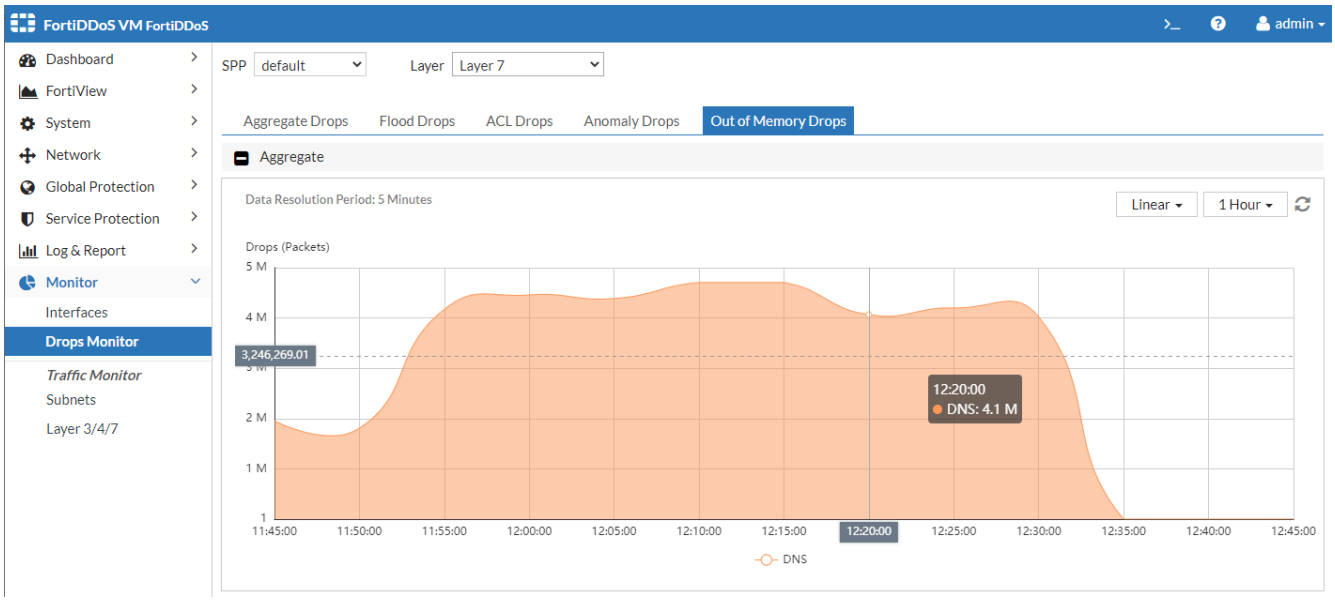
Using the Out of Memory Drops graphs

Use the Out of Memory Drops graphs to monitor drops due to memory attacks on the FortiDDoS system.

If Layer 3 or Layer 4 graphs report any dropped traffic, contact Fortinet for assistance. DNS Out of Memory drops are not uncommon during DNS Response Floods are not harmful to the system nor to legitimate traffic.

Customize the graph with the following viewing parameters: SPP, Reporting Period (1-hr to 1-yr), Linear/Logarithmic Y-Axis.

Placing the cursor on the Monitor graph will display a tool-tip with additional information.



Before you begin:

- You must have Read permission for the Monitor menu.
- Refer to Reading Monitor graphs on page 294 to understand the graphs in detail.

To display the graphs:

1. Go to *Monitor* > *Drops Monitor* > *Out of Memory Drops* > [SPP] [Aggregate/Layer 3/4/7] [Y-Axis View] [Reporting Period].

Statistic	Description
Aggregate	Aggregation of all Out of Memory drops for: • Layer 3 • Layer 4 • Layer 7
Layer 3	Drops due to Out of Memory for: • Source Table • Destination Table
Layer 4	Drops due to TCP Out of Memory (Connection Table)
Layer 7	
Aggregate	Drops due to TCP Out of Memory
DNS	Drops due to TCP Out of Memory

Using Traffic Monitor Layer 3/4/7 graphs

Use the Layer 3 graphs to monitor trends in Layer 3 traffic parameter rates and drops.

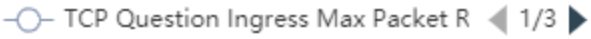
Customize the graph with the following viewing parameters: SPP, Linear/Logarithmic Y-Axis, Direction, Reporting Period (1-hr to 1-yr).

Most graphs in this group will show Inbound/Outbound and Ingress/Egress. Remember Inbound Ingress is from the Internet to FortiDDoS and Inbound Egress is from FortiDDoS to your network. Any divergence of Ingress and Egress traffic on the graph indicated that the system is dropping packets (real, in Prevention mode or virtually in Detection Mode).

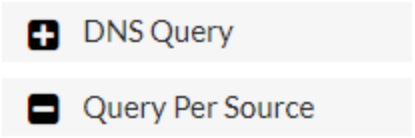
If Ingress and Egress traffic diverges, you will also see Drop Counts on this graph if the drop reason is directly related to this graph. You may see Ingress/Egress divergence on a graph but no drops. This indicates that the traffic on this graph was affected by drops on another graph. For example, a high rate of Layer 3 Anomalies may affect a Layer 3 Protocol graph but the drops will be shown on the Anomalies graphs.

If you are uncertain about what is causing the drops, use the *Dashboard* > *Top Attacks* page to find the actual attack vector and then choose the appropriate graph.

Placing the cursor on the Monitor graph will display a tool-tip with additional information.

On graphs with many subgraphs all graph labels may not show at once. If so, the right side of the label section will show navigation arrows to display further graph labels: 

On pages with multiple graphs, you can scroll to see all graphs or you can use the +/- icon at the top-left of each graph name to hide that graph. The pages always open with all graphs showing.



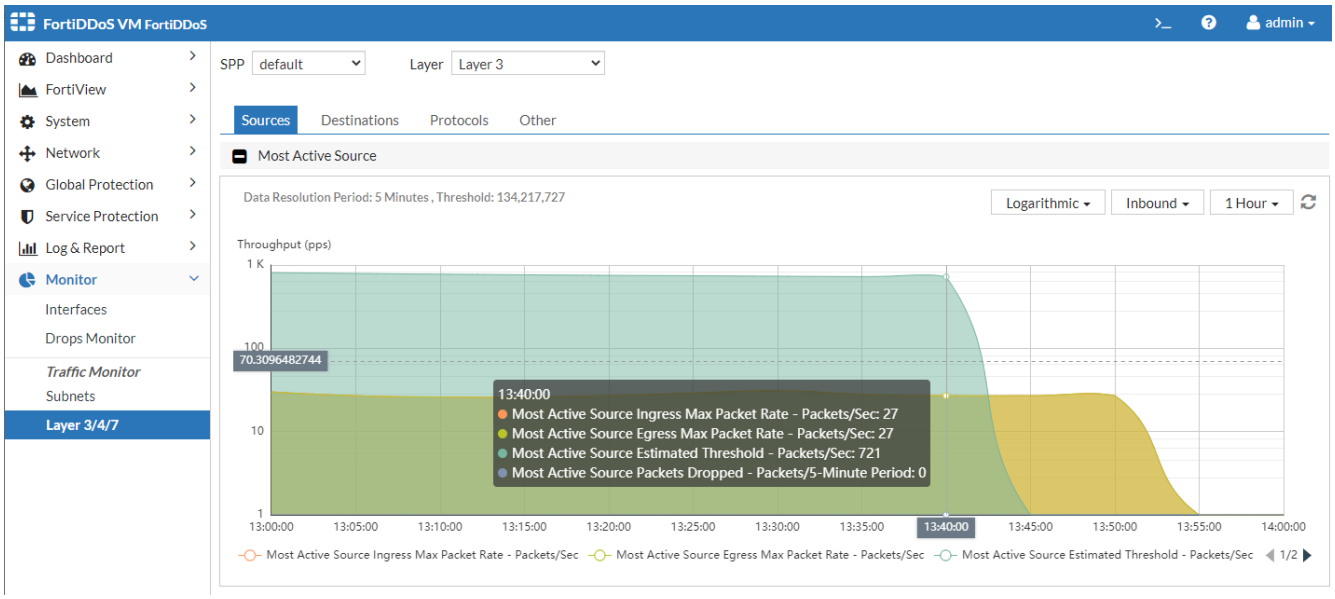
Estimated Thresholds

FortiDDoS sets Thresholds by learning traffic, creating Traffic Statistics Reports and from them creating System Recommended Thresholds (also called configured minimum thresholds in some text) shown on the top left of the graph (Threshold: 500, for example).

For selected “Scalar” parameters, the system then creates a continuously adaptive, machine-learned Estimated Threshold which automatically adjusts the System Recommended Threshold, based on historical traffic, traffic trend and “seasonality”. Action is taken by the system only when traffic exceeds the higher of the System Recommended Threshold or the adaptive Estimated Threshold. Estimated Thresholds are by default limited to 150% of the System Recommended Threshold to prevent excess traffic. The 150% limit is user-modifiable in System Recommendations.

Using the Layer 3 graphs

Example Layer 3 Graph



Before you begin:

• You must have Read permission for the *Monitor* menu.

• Refer to Reading Monitor graphs on page 294 to understand the graphs in detail.

To display the graphs:

- Go to *Monitor / Traffic Monitor /* > *Layer 3/4/7* > *Layer 3* > [SPP] [Sources / Destinations / Protocols / Other] [Y-Axis view] [Direction] [Reporting Period].

The follow table summarizes the statistics displayed in each graph.

Layer 3 graphs

Statistic	Description
Sources Tab	Displays pps Traffic, Threshold, Estimated Threshold and per-5-minute Drop information for: • Most Active Source Ingress Traffic (pps) - Trend in observed ingress packet rate of the most active source address. Note that this is not necessarily a graph of the same source over time, but rather a trend of the rate for the most active source during each sampling period. • Most Active Source Egress (pps) - Trend in observed egress packet rate of the most active source address. Note that this is not necessarily a graph of the same source over time, but rather a trend of the rate for the most active source during each sampling period. • Most Active Source Estimated Threshold (pps) - Trend in the Estimated Threshold described above. • Most Active Source Packets Dropped (Packets/5-Minute Period) – Displays drops caused by the rate-limiting most-active-source threshold
Destinations Tab	Displays pps Traffic, Threshold, Estimated Threshold and per-5-minute Drop information for:

Statistic	Description
	• Most Active Destination Ingress Traffic (pps) - Trend in observed ingress packet rate of the most active destination address. Note that this is not necessarily a graph of the same destination over time, but rather a trend of the rate for the most active destinations during each sampling period. • Most Active Destination Egress Traffic (pps) - Trend in observed egress packet rate of the most active destination address. Note that this is not necessarily a graph of the same destination over time, but rather a trend of the rate for the most active destinations during each sampling period. • Most Active Destination Estimated Threshold - Trend in the estimated threshold described above. • Most Active Source Packets Dropped (Packets/5-Minute Period) – Displays drops caused by the rate-limiting most-active-destination threshold **Note**: FortiDDoS System Recommendations does not set a Most Active Destination Threshold (i.e. sets the Threshold to system maximum). You can add a manual Threshold if desired.

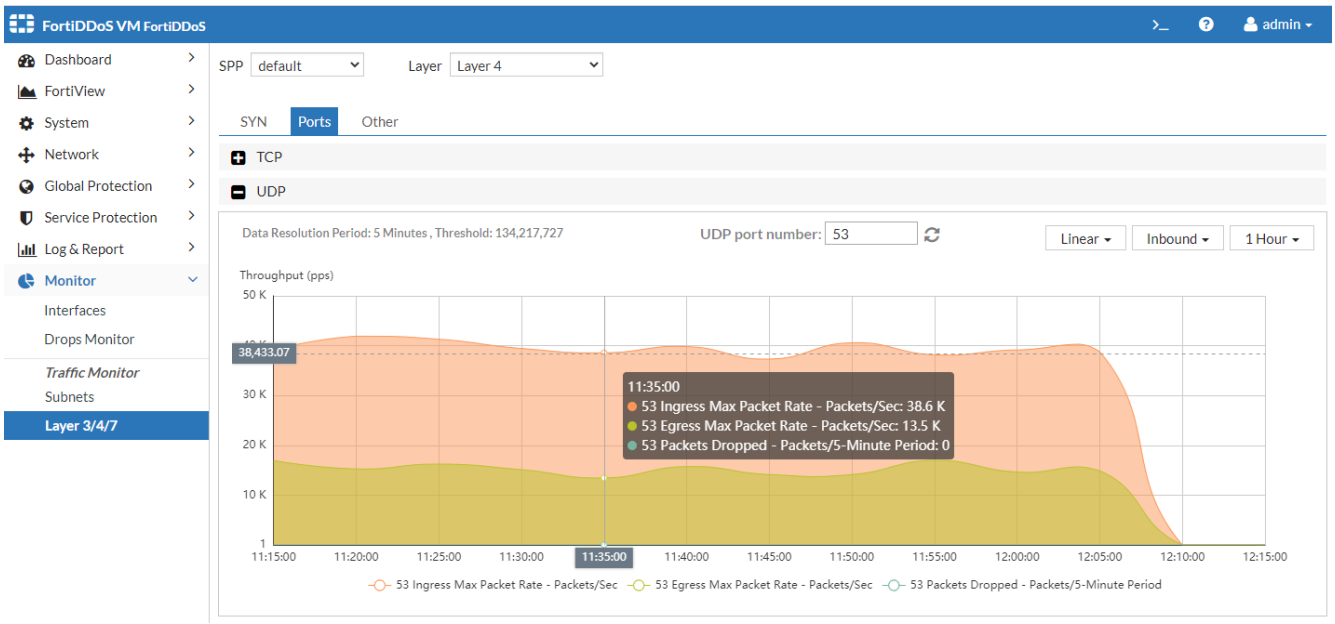
Protocols Tab	Displays pps Traffic, Threshold and per-5-minute Drop information for:
	• Selected Layer 3 Protocols from 0-255
	  • [Protocol] Ingress Traffic (pps) - Trend in observed ingress packet rate of this Protocol
	  • [Protocol] Egress Traffic (pps) - Trend in observed egress packet rate of this Protocol
	Note:
	• When the Protocol number is selected, the current System Recommended Threshold for that Protocol is shown at the top-left of the graph.
	• FortiDDoS System Recommendations does not set Thresholds (i.e. uses system maximums) for:
	  • TCP (Protocol 6)
	  • UDP (Protocol 17)
	Other mitigations normally protect from attacks using these Protocols. You can add Thresholds for these Protocols if desired.

Other Tab	
Count of Unique Sources	Displays the total count of unique source IP addresses in the session table.
Fragmented Packets	Displays pps Traffic, Threshold, Estimated Threshold and per-5-minute Drop and ACL information for: • Other Fragments Ingress Traffic (pps) – Fragments for Protocols other than TCP or UDP • Other Fragments Egress Traffic (pps) • Other Fragments Estimated Threshold (pps) – See Estimated Thresholds above • Other Fragments Packets Dropped (Packets/5-Minute Period) – Displays drops caused by the rate-limiting Other Fragments threshold • Other Fragments Packets Blocked (Packets/5-Minute Period) – Displays drops caused by Other Fragment Check ACL in the IP Profile assigned to

Statistic	Description
	this SPP. **Note**: Other Fragment Check ACL is not recommended. Misconfigured clients can create significant GRE (Protocol 47) and IPSEC (Protocol 5) fragmentation. Use System Recommended Thresholds. • TCP Fragments Ingress Traffic (pps) – Fragments for Protocols other than TCP or UDP • TCP Fragments Egress Traffic (pps) • TCP Fragments Estimated Threshold (pps) – See Estimated Thresholds above • TCP Fragments Packets Dropped (Packets/5-Minute Period) – Displays drops caused by the rate-limiting Other Fragments threshold • TCP Fragments Packets Blocked (Packets/5-Minute Period) – Displays drops caused by the TCP Fragment Check in the IP Profile assigned to this SPP. **Note**: TCP Fragment Check ACL is not recommended. Misconfigured clients can create significant TCP fragmentation. Use System Recommended Thresholds. • UDP Fragments Ingress Traffic (pps) – Fragments for Protocols other than TCP or UDP • UDP Fragments Egress Traffic (pps) • UDP Fragments Estimated Threshold (pps) – See Estimated Thresholds above • UDP Fragments Packets Dropped (Packets/5-Minute Period) – Displays drops caused by the rate-limiting Other Fragments threshold • UDP Fragments Packets Blocked (Packets/5-Minute Period) – Displays drops caused by UDP Fragment Check in the IP Profile assigned to this SPP. **Note**: TCP Fragment Check ACL is not recommended. Misconfigured clients can create significant TCP fragmentation. Use System Recommended Thresholds.

Using the Layer 4 graphs

Example Layer 4 graph



Before you begin:

• You must have Read permission for the *Monitor* menu.

• Refer to Reading Monitor graphs on page 294 to understand the graphs in detail.

To display the graphs:

- Go to *Monitor / Traffic Monitor /* > *Layer 3/4/7* > *Layer 4* > [SPP] [Sources / Destinations / Protocols / Other] [Y-Axis view] [Direction] [Reporting Period].

The follow table summarizes the statistics displayed in each graph.

Layer 4 graphs

Statistic	Description
SYN Tab	
SYN	Displays SYN Traffic, Threshold, Estimated Threshold and per-5-minute Drop information for: • SYN Ingress Max Packet Rate (SYNs/sec) - Trend in observed ingress SYN rate for all SYNs into the SPP. • SYN Egress Max Packet Rate (SYNs/sec) - Trend in observed egress SYN rate for all SYNs into the SPP. • SYN packet rate Estimated Threshold (SYNs/sec) - Trend in the SYN Estimated Threshold rate as described above. • SYN packets dropped (Packets/5-Minute Period) - Trend in drops due to the SYN Validation triggered by the SYN Threshold /Estimated Threshold. **Note**: SYN Validation option in the TCP Profile assigned to this SPP must be enabled for any SYN mitigation. If source IPs are successfully validated, SYNs may be allowed to exceed the threshold.

Statistic	Description
SYN Per Source	Displays SYN per Source Traffic, Threshold, Estimated Threshold and per-5-minute Drop information for: • Ingress SYN per Source Max Packet Rate (SYNs/sec) - Trend in observed ingress maximum rate of SYN packets from a single source IP. • Egress SYN per Source Max Packet Rate (SYNs/sec) - Trend in observed egress maximum rate of SYN packets from a single source IP. • SYN per Source packet rate Estimated Threshold (SYNs/sec) - Trend in the SYN per Source Estimated Threshold rate as described above. • SYN per Source packets dropped (Packets/5-Minute Period) - Trend in drops due to the SYN per Source rate-limiting Threshold. **Note**: SYN Validation is not performed on identified Sources that exceed the SYN per Source rate – Sources are rate-limited to the SYN per Source threshold.
SYN Per Destination	Displays SYN per Destination Traffic, Threshold, Estimated Threshold and per-5-minute Drop information for: • SYN per Destination Ingress Max Packet Rate (SYNs/sec) - Trend in observed ingress SYN rate for SYNs to protected Destination IPs. • SYN per Destination Egress Max Packet Rate (SYNs/sec) - Trend in observed egress SYN rate for all SYNs into the SPP. • SYN per Destination packet rate Estimated Threshold (SYNs/sec) - Trend in the SYN per Destination Estimated Threshold rate as described above. • SYN per Destination packets dropped (Packets/5-Minute Period) - Trend in drops due to the SYN Validation triggered by the SYN Threshold /Estimated Threshold. **Note**: SYN Validation option in the TCP Profile assigned to this SPP must be enabled for any SYN per Destination mitigation. If source IPs are successfully validated, SYN per Destination may be allowed to exceed the threshold.
Ports Tab	
TCP	Displays TCP Port Traffic, Threshold, Estimated Threshold and per-5-minute Drop information for: • TCP <Port> Ingress Max Packet Rate (packets/sec) - Trend in observed ingress maximum packet rate to the specified port. A spike in this graph shows a possible port flood. • TCP <Port> Egress Max Packet Rate - Packets/sec - Trend in observed egress maximum packet rate to the specified port. • TCP <Port> Packets Dropped - Packets/ Packets/5-Minute Period - Trend in packets dropped due to the rate-limiting Threshold. **Note:** • FortiDDoS is primarily interested in protecting TCP “service” ports. Traditionally “service” ports have been the well-known ports below port 1024. As applications expanded, many ports over 1024 are used for well-known services such as MSSQL (1433) or RDP (3389). FortiDDoS treats all TCP ports under 10,000 as “service” ports. When a client connects to a service port all the inbound traffic to that port and outbound traffic from that port is associated with the port and the ephemeral client port is ignored. If you see

Statistic	Description
	high ports (>10239) in logs, that means high ports are “talking” to other high ports. This may happen with gaming and FTP, for example. The FTP control port is 21 but the server opens a high port and the client uses a new high port to connect to the server “data” port while the control session stays open. You can also define 128 HTTP Service Ports and 128 SSL Service Ports for any port from 1-65535. More information is available in the Service Protection section. • FortiDDoS F-series appliances set ranges and thresholds for ports 0-10239 and a single range and threshold for all ports above 10240. Logs will report on all ports from 0-65535. FortiDDoS F-Series VMs set ranges and thresholds for ports 0-1023 and a single range and threshold for all ports over 1024. Logs will report on all ports from 0-1023 but only report port 1024 for higher ports.
UDP	Displays UDP Port Traffic, Threshold, Estimated Threshold and per-5-minute Drop information for: • UDP <Port> Ingress Max Packet Rate (packets/sec) - Trend in observed ingress maximum packet rate to the specified port. • UDP <Port> Egress Max Packet Rate - Packets/sec - Trend in observed egress maximum packet rate to the specified port. • UDP <Port> Packets Dropped - Packets/ Packets/5-Minute Period - Trend in packets dropped due to the rate-limiting Threshold. **Note**: FortiDDoS is primarily interested in protecting TCP “service” ports. Traditionally “service” ports have been the well-known ports below port 1024. As applications expanded, many ports over 1024 are used for well-known services such as MSSQL (1433) or RDP (3389). FortiDDoS treats all TCP ports under 10,000 as “service” ports. When a client connects to a service port all the inbound traffic to that port and outbound traffic from that port is associated with the port and the ephemeral client port is ignored.
Other Tab	
Concurrent Connections per Source	Displays Concurrent Connections per Source count, Threshold, Estimated Threshold and per-5-minute Drop information for: • Maximum Concurrent Connections per Source (count) - Trend in observed count of concurrent connections for the busiest source each second. • Estimated Threshold for Concurrent Connections per Source (count) - Trend in the Concurrent Connections per Source Estimated Threshold rate as described above. • Concurrent Connections per Source dropped (count per 5-minutes) - Trend in Connections dropped due to the rate-limiting Threshold.
New Connections	Displays New Connections count, Threshold, Estimated Threshold and per-5-minute Drop information for: • Max New Connections Establishment (Connections/sec) – Trend in new connection rate. • Estimated Threshold for New Connections Establishment (Connections/sec) - Trend in the New Connections Estimated Threshold rate as described

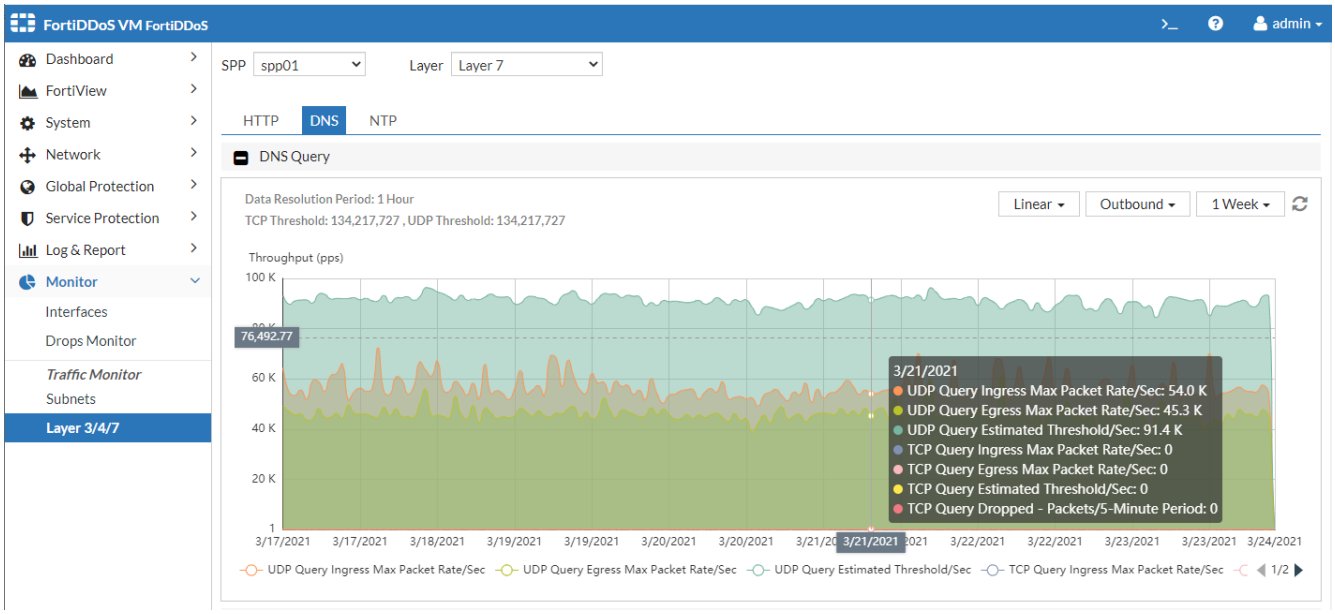
Statistic	Description
	above. • New Connections dropped (count per 5-minutes) - Trend in Connections dropped due to the rate-limiting Threshold.
Non-Spoofed IPs	Displays the number of entries in the global Legitimate IP (LIP) Table. The Legitimate IP table displays the count of Source IP addresses that have been successfully validated by one of the 2 SYN Validation parameters (SYN or SYN per Destination). This table will only be populated during SYN Floods and thus if the graph is showing non-zero numbers there has been a SYN or SYN per Destination Flood in one or more of the SPPs. The legitimate IP address table is maintained and reported as a global count. The graph is identical for all SPPs, when a SYN flood occurs in any SPP.
TCP Sessions	TCP Sessions is an information-only graph that displays counts of the following parameters: • Established Connections (count) - Trend in count of entries in the TCP state table that are in the established state (completed three-way handshake). • Number of Entries in TCP State Table (count) - rend in count of all entries in the TCP state table, including half-open connections. If the values for the number of entries in the TCP state table are significantly higher than those for Established Connections, it shows a possible SYN flood attack. **Note**: The TCP Sessions graph is a global count. It will show identical counts for all SPPs. If this graph looks abnormal, check the three SYN graphs for each SPP.

ICMP	Displays traffic and drops information for ICMP Types and Codes. Because there are 255 x 255 (65,536) possible Types and Codes there are 2 additional fields on this graph for Type (0-255) and Code (0-255). When a Type/Code is entered, the system converts this to an index number, which appears in the label of each subgraph. For example Type 8 / Code 0 (ping) is index 2048.
	Look in *Dashboard* > *Top Attacks*: Top Attacked ICMP Type/Codes to see if any Types/Codes are displayed. Enter those in this graph to see the activity.
	• Ingress Max Packet Rate (pps) – Trend in ingress traffic for this Type/Code
	• Egress Max Packet Rate (pps) – Trend in egress traffic for this Type/Code
	• Packets Dropped (drops per 5-minutes) - Packets dropped due to the Type/Code rate-limiting Threshold.
	• Packets Blocked (drops per 5-minutes) – Packets blocked due to an ICMP Type/Code ACL contained in the ICMP Profile assigned to this SPP.
	Note:
	• ICMP Type/Code graphs are displayed differently for different FortiDDoS F-Series Models
	  • Thresholds and Ranges – Appliance and VM Thresholds are set for every Type/Code and ranges are set for:
	  • Types/Code indexes from 0-10239
	  • A single range is set for index 10240-65536
	  • Graphs:
	  • Appliances display traffic/drops/blocked for all Type Codes to index

Statistic	Description
	65536 • VMs display traffic/drops/blocked for Type Codes to index 10239. The peak data rate and drops for any indexes from 10240-65535 are all displayed on the 10240 index graph. The actual Type/Code (133/0, for example, not the index) is displayed in any Attack Log. • You may need to review the ICMP Profile, Dashboard > Top Attacks > Top ACL Attacks and/or the Attack Logs to identify which Type/Code graph to show the ACL drops. • ICMPv4 uses Layer 3 Protocol 1 while ICMPv6 used Layer 3 Protocol 58. Some ICMP Types/Codes are used on both Protocols and some are unique to one Protocol. The Traffic and Drops graphs show all Type/Codes for any Protocol. The ICMP Profile ACL can select ICMPv4, ICMPv6 or both. • As of 2021/03 there are only 113 ICMP Types/Code pairs ratified by IETF and IANA out total the total 65,536 available pairs. Attackers may randomize Types/Codes in an attempt to avoid detection. The ICMP Type Code Anomaly option is available in any ICMP Profile, which automatically drops any Type/Code outside the ratified Types/Codes, without using the rate-limiting Threshold.

Using the Layer 7 graphs

Example Layer 7 graph



Before you begin:

• You must have Read permission for the *Monitor* menu.

• Refer to Reading Monitor graphs on page 294 to understand the graphs in detail.

To display the graphs:

• Go to *Monitor / Traffic Monitor /* > *Layer 3/4/7* > *Layer 7* > [SPP] [HTTP / DNS / NTP] [Y-Axis view] [Direction] [Reporting Period]. Some Graphs may have additional parameter selection such as [Method].

Layer 7 graphs

Statistic	Description
HTTP Tab	
Methods	Displays HTTP Method Traffic, Threshold, Estimated Threshold and per-5-minute Drop information. The following Methods are monitored: [GET | HEAD | OPTIONS | TRACE | POST | PUT | DELETE | CONNECT] Subgraphs for: • [Method] Ingress Max Packet Rate (pps) - Trend in observed ingress maximum rate for the selected HTTP method. • [Method] Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for the selected HTTP method. • [Method] Estimated Threshold (pps) - Trend in the HTTP Method Estimated Threshold rate as described above. • [Method] Packets Dropped (drops per 5-minutes) - Trend in [Method] packets dropped due to the rate-limiting Threshold and/or GET/Post Flood Mitigation settings in the HTTP Profile assigned to an SPP. **Note:** • Selected Methods can be ACLed per SPP via the HTTP Profile assigned to that SPP. • Source IP Validation for GET and POST Floods is available by setting GET and/or POST Flood Mitigation features in the HTTP Profile assigned to this SPP.
Method per Source	Displays HTTP Method per Source Traffic, Threshold, Estimated Threshold and per-5-minute Drop information: • Method per Source Ingress Max Packet Rate (pps) - Trend in observed ingress maximum rate for any single Source IP. • Method per Source Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for any single Source IP. • Method per Source Estimated Threshold (pps) - Trend in the HTTP Method Estimated Threshold rate as described above. • Method per Source Packets Dropped (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting Methods per Source Threshold
URLs	Displays HTTP URL Traffic, Threshold, Estimated Threshold and per-5-minute Drop information. URL can be over 4000 characters long, resulting in almost unlimited numbers of URLs. FortiDDoS tracks the top 32,000 URLs but uses a single Threshold learned from Traffic Statistics to rate-limit any URL. URLs are one-way hashed and the hash index is shown on the graph. In order to use this graph, observe URL Drops in the Attack Logs to obtain the hash index under attack. • URL <Index> Ingress Max Packet Rate (pps) - Trend in observed URL <Index> ingress maximum rate.

Statistic	Description
	• URL <Index> Egress Max Packet Rate (pps) - Trend in observed URL <Index> egress maximum rate. • URL <Index> Packets Dropped (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting URL Threshold. • URL <Index> Packets Blocked (drops per 5-minutes) - Trend in packets dropped due to any URL ACLs created in an HTTP Profile assigned to an SPP. **Note**: Specific URLs may be ACLed via the HTTP Profile assigned to an SPP.
Hosts	Displays HTTP Host Traffic, Threshold, Estimated Threshold and per-5-minute Drop information. FortiDDoS tracks the top 512 Hosts but uses a single Threshold learned from Traffic Statistics to rate-limit any Host. Hosts are one-way hashed and the hash index is shown on the graph. In order to use this graph, observe Host Drops in the Attack Logs to obtain the hash index under attack. • Host <Index> Ingress Max Packet Rate (pps) - Trend in observed Host <Index> ingress maximum rate. • Host <Index> Egress Max Packet Rate (pps) - Trend in observed Host <Index> egress maximum rate. • Host <Index> Packets Dropped (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting Host Threshold. • Host <Index> Packets Blocked (drops per 5-minutes) - Trend in packets dropped due to any Host ACLs created in an HTTP Profile assigned to an SPP. **Note**: Specific Hosts may be ACLed via the HTTP Profile assigned to an SPP.
Referers	Displays HTTP Referer Traffic, Threshold, Estimated Threshold and per-5-minute Drop information. FortiDDoS tracks the top 512 Referers but uses a single Threshold learned from Traffic Statistics to rate-limit any Referer. Hosts are one-way hashed and the hash index is shown on the graph. In order to use this graph, observe Referer Drops in the Attack Logs to obtain the hash index under attack. • Referer <Index> Ingress Max Packet Rate (pps) - Trend in observed Referer <Index> ingress maximum rate. • Referer <Index> Egress Max Packet Rate (pps) - Trend in observed Referer <Index> egress maximum rate. • Referer <Index> Packets Dropped (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting Referer Threshold. • Referer <Index> Packets Blocked (drops per 5-minutes) - Trend in packets dropped due to any Referer ACLs created in an HTTP Profile assigned to an SPP. **Note**: Specific Referer may be ACLed via the HTTP Profile assigned to an SPP.
Cookies	Displays HTTP Cookie Traffic, Threshold, Estimated Threshold and per-5-minute Drop information. FortiDDoS tracks the top 512 Cookies but uses a single Threshold learned from Traffic Statistics to rate-limit any Cookie. Cookies are one-way hashed and the hash index is shown on the graph. In order to use this graph, observe Cookie Drops in the Attack Logs to obtain the hash index under attack.

Statistic	Description
	• Cookie <Index> Ingress Max Packet Rate (pps) - Trend in observed Cookie <Index> ingress maximum rate. • Cookie <Index> Egress Max Packet Rate (pps) - Trend in observed Cookie <Index> egress maximum rate. • Cookie <Index> Packets Dropped (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting Cookie Threshold. • Cookie <Index> Packets Blocked (drops per 5-minutes) - Trend in packets dropped due to any Cookie ACLs created in an HTTP Profile assigned to an SPP **Note**: Specific Cookies may be ACLed via the HTTP Profile assigned to an SPP.
User Agents	Displays HTTP User Agent Traffic, Threshold, Estimated Threshold and per-5-minute Drop information. FortiDDoS tracks the top 512 User Agents but uses a single Threshold learned from Traffic Statistics to rate-limit any Cookie. Cookies are one-way hashed and the hash index is shown on the graph. In order to use this graph, observe User Agent Drops in the Attack Logs to obtain the hash index under attack. • User Agent <Index> Ingress Max Packet Rate (pps) - Trend in observed User Agent <Index> ingress maximum rate. • User Agent <Index> Egress Max Packet Rate (pps) - Trend in observed User Agent <Index> egress maximum rate. • User Agent <Index> Packets Dropped (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting User Agent Threshold. • User Agent <Index> Packets Blocked (drops per 5-minutes) - Trend in packets dropped due to any User Agent ACLs created in an HTTP Profile assigned to an SPP **Note**: Specific User Agents may be ACLed via the HTTP Profile assigned to an SPP.
DNS Tab	
DNS Query	Displays DNS Query Traffic, Threshold, Estimated Threshold and per-5-minute Drop information. Subgraphs for: • UDP Query Ingress Max Packet Rate (pps) - Trend in observed ingress maximum rate for UDP Queries • UDP Query Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for UDP Queries. • UDP Query Estimated Threshold (pps) - Trend in the UDP Query Method Estimated Threshold rate as described above. • TCP Query Ingress Max Packet Rate (pps) - Trend in observed ingress maximum rate for TCP Queries • TCP Query Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for TCP Queries. • TCP Query Estimated Threshold (pps) - Trend in the TCP Query Method Estimated Threshold rate as described above. • TCP Query Dropped (drops per 5-minutes) - Trend in packets dropped due to

Statistic	Description
	the rate-limiting TCP Query Threshold **Note:** • When the DNS Query Threshold is crossed, the system begins DNS Source and Query (payload) validation. If DNS Anti-spoofing and Validations options are not enabled in a DNS Profile assigned to an SPP, no DNS Query mitigation will be done. • If over-threshold DNS Queries pass both Source and Query validation, they will be allowed and you may see Query rates on the graph higher than the Threshold. • Drops caused by UDP Query Validations are displayed in *Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS graph* • TCP Queries will be Source validated with Layer 4 SYN validations and will then be rate-limited (no Query validation) by the independent TCP Query Threshold.
Query Per Source	Displays DNS UDP/TCP Query per Source Traffic, Threshold, Estimated Threshold and per-5-minute Drop information. • Query per Source Ingress Max Packet Rate (pps) - Trend in observed ingress maximum DNS Query rate for any single Source IP. • Query per Source Egress Max Packet Rate (pps) - Trend in observed egress maximum DNS Query rate for any single Source IP. • Query per Source Estimated Threshold (pps) - Trend in the DNS Query Estimated Threshold rate as described above. • Query per Source Packets Dropped - Trend in packets dropped due to the rate-limiting DNS Query per Source Threshold **Note**: If Block Identified Source is disabled in a DNS Profile assigned to an SPP, the Query per Source Threshold will not be tracked nor displayed on the graph.
Suspicious Sources	Displays DNS Packet-Track per Source (Suspicious Sources) Traffic, Threshold, Estimated Threshold and per-5-minute Drop information. Packet-Track per Source (Suspicious Sources) is based on a machine-learned, heuristics-based score that counts fragmented packets, Response not found in DQRM and/or queries that generate responses with RCODE other than 0, for any Source. • Packet-Track per Source Ingress Max Packet Rate (pps) - Trend in observed ingress maximum rate for any single Source IP. • Packet-Track per Source Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for any single Source IP. • Packet-Track per Source Estimated Threshold (pps) - Trend in the Estimated Threshold rate as described above. • Packet-Track per Source Packets Dropped - Trend in packets dropped due to the rate-limiting Packet-Track per Source Threshold **Note**: If Block Identified Source in a DNS Profile assigned to an SPP is disabled, the DNS Packet-Track per Source (Suspicious Sources) Threshold will not be tracked nor displayed on the graph.

Statistic	Description
Question Count	Displays the sum of all Question Count fields in all DNS UDP/TCP Query Packets, Threshold, Estimated Threshold and per-5-minute Drop information. • UDP Question Ingress Max Packet Rate (Sum of Question Count per second) - Trend in observed ingress maximum count for UDP Questions • UDP Question Egress Max Packet Rate (Sum of Question Count per second) - Trend in observed egress maximum rate for UDP Questions. • UDP Question Estimated Threshold (Sum of Question Count per second) - Trend in the UDP Query Method Estimated Threshold rate as described above. • TCP Question Ingress Max Packet Rate (Sum of Question Count per second) - Trend in observed ingress maximum rate for TCP Questions • TCP Question Egress Max Packet Rate (Sum of Question Count per second) - Trend in observed egress maximum rate for TCP Questions. • TCP Question Estimated Threshold (Sum of Question Count per second) - Trend in the TCP Query Method Estimated Threshold rate as described above. • TCP Question Dropped (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting TCP Query Threshold **Note:** • The Qcount field in a DNS Queries allows a maximum entry of 255. This implies that the Client is asking for A-Records from 255 FQDN Names, for example. However, the DNS Response only allows a single Response, so any Qcount number over 1 is invalid and suspicious. The Question Count graphs should match the DNS Query graphs. • When the DNS Question Count Threshold is crossed, the system begins DNS Source and Query (payload) validation. If DNS Anti-spoofing and Validations options are not enabled in a DNS Profile assigned to an SPP, no DNS Question Count mitigation will be done. • If over-threshold DNS Question Count pass both Source and Query validation, they will be allowed and you may see Question Counts on the graph higher than the Threshold. • Drops caused by UDP Question Count Validations are displayed in *Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS graph* • TCP Question Counts will be Source validated with Layer 4 SYN validations and will then be rate-limited (no Query validation) by the independent TCP Question Count Threshold.
Fragment	Displays the DNS UDP/TCP Query Fragment Traffic, Threshold, Estimated Threshold and per-5-minute Drop information. **Note**: Only the first fragment in a series of fragments provides Layer 4 information to identify the packet as a DNS Fragment. These fragments will be displayed on this graph. Subsequent fragments have only Layer 3 information and will be displayed on *Monitor > / Traffic Monitor / > Layer 3 /4/7 > Layer 3 > Other > Fragmented Packet graph* • UDP Fragment Ingress Max Packet Rate (pps) - Trend in observed ingress maximum count for UDP Fragments

Statistic	Description
	• UDP Fragment Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for UDP Fragments. • UDP Fragment Estimated Threshold (pps) - Trend in the Fragment Estimated Threshold rate as described above. • TCP Fragment Ingress Max Packet Rate (pps) - Trend in observed ingress maximum rate for TCP Fragments. • TCP Fragment Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for TCP Fragments. • TCP Fragment Estimated Threshold (pps) - Trend in the TCP Fragment Estimated Threshold rate as described above. • TCP Fragment Dropped (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting TCP Fragment Threshold
QType MX	Displays the DNS UDP/TCP Query Type MX (email) Traffic, Threshold, Estimated Threshold and per-5-minute Drop information. • UDP Query Type MX Ingress Max Packet Rate (pps) - Trend in observed ingress maximum count for UDP Query Type MX • UDP Query Type MX Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for UDP Query Type MX. • UDP Query Type MX Estimated Threshold (pps) - Trend in the UDP Query Type MX Estimated Threshold rate as described above. • TCP Query Type MX Ingress Max Packet Rate (pps) - Trend in observed ingress maximum rate for TCP Query Type MX. • TCP Query Type MX Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for TCP Query Type MX. • TCP Query Type MX Estimated Threshold (pps) - Trend in the TCP Query Type MX Estimated Threshold rate as described above. • TCP Query Type MX Dropped (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting Query Type MX Threshold **Note:** • When the DNS Query Type MX Threshold is crossed, the system begins DNS Source and Query (payload) validation. If DNS Anti-spoofing and Validations options are not enabled in a DNS Profile assigned to an SPP, no DNS Query mitigation will be done. • If over-threshold DNS Queries pass both Source and Query validation, they will be allowed and you may see Query Type MX rates on the graph higher than the Threshold. • Drops caused by UDP Query Validations are displayed in Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS graph • TCP Type MX Queries will be Source validated with Layer 4 SYN validations and will then be rate-limited (no Query validation) by the independent TCP Query Type MX Threshold.
QType All	Displays the DNS UDP/TCP Query Type ALL (ANY/*) Traffic, Threshold, Estimated Threshold and per-5-minute Drop information. • UDP Query Type ALL Ingress Max Packet Rate (pps) - Trend in observed ingress maximum count for UDP Query Type ALL

Statistic	Description
	• UDP Query Type ALL Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for UDP Query Type ALL. • UDP Query Type ALL Estimated Threshold (pps) - Trend in the UDP Query Type ALL Estimated Threshold rate as described above. • TCP Query Type ALL Ingress Max Packet Rate (pps) - Trend in observed ingress maximum rate for TCP Query Type ALL. • TCP Query Type ALL Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for TCP Query Type ALL. • TCP Query Type ALL Estimated Threshold (pps) - Trend in the TCP Query Type ALL Estimated Threshold rate as described above. • TCP Query Type ALL Dropped (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting Query Type ALL Threshold **Note:** • When the DNS Query Type ALL Threshold is crossed, the system begins DNS Source and Query (payload) validation. If DNS Anti-spoofing and Validations options are not enabled in a DNS Profile assigned to an SPP, no DNS Query mitigation will be done. • If over-threshold DNS Queries pass both Source and Query validation, they will be allowed and you may see Query Type ALL rates on the graph higher than the Threshold. • Drops caused by UDP Query Validations are displayed in Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS graph • TCP Type ALL Queries will be Source validated with Layer 4 SYN validations and will then be rate-limited (no Query validation) by the independent TCP Query Type ALL Threshold.
QType Zone Transfer	Displays the DNS TCP Query Type Zone Transfer Traffic, Threshold, Estimated Threshold and per-5-minute Drop information. • TCP Query Type Zone Transfer Ingress Max Packet Rate (pps) - Trend in observed ingress maximum rate for TCP Query Type Zone Transfer. • TCP Query Zone Transfer Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for TCP Query Type Zone Transfer. • TCP Query Zone Transfer Estimated Threshold (pps) - Trend in the TCP Query Type ALL Estimated Threshold rate as described above. • TCP Query Zone Transfer Dropped (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting Query Type Zone Transfer Threshold **Note**: Zone Transfer requests must be TCP. If attackers use UDP, the UDP Query Thresholds and mitigations will apply.
DNS Response Code	Displays the DNS Response Code Traffic, Threshold, Estimated Threshold and per-5-minute Drop information. DNS Responses contain a Response Code indicating information about the Response. The field allows 15 different Response Codes but many are unassigned, not implemented or rarely used. The most-used Response Codes are 0=Good Response | 1=Query Format Error | 2=Server Failure | 3=NxDomain | 5=Refused | The DNS Response Code graph contains an additional selection field to enter the Response Code of interest from 0-15.

Statistic	Description
	• DNS Rcode [0-15] Ingress Max Packet Rate (pps) - Trend in observed ingress maximum rate for DNS Rcode [0-15] • DNS Rcode [0-15] Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for DNS Rcode [0-15] • DNS Rcode [0-15] Ingress Drops (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting DNS Rcode [0-15] Threshold
NTP Tab	
Request	Displays NTP Traffic, Threshold, Estimated Threshold and per-5-minute Drop information for: • NTP Request Ingress Max Packet Rate (pps) - Trend in observed ingress maximum rate for NTP Requests • NTP Request Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for NTP Requests. • NTP Requests Dropped (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting NTP Request Threshold
Response	Displays NTP Response Traffic, Threshold, Estimated Threshold and per-5-minute Drop information for: • NTP Response Ingress Max Packet Rate (pps) - Trend in observed ingress maximum rate for NTP Responses. • NTP Response Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for NTP Responses. • NTP Responses Dropped (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting NTP Response Threshold.
Broadcast	Displays NTP Broadcast Traffic, Threshold, Estimated Threshold and per-5-minute Drop information for: • NTP Broadcast packet Ingress Max Packet Rate (pps) - Trend in observed ingress maximum rate for NTP Broadcast packets. • NTP Broadcast packet Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for NTP Broadcast packets. • NTP Broadcast packets Dropped (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting NTP Broadcast packet Threshold
Response Per Destination	Displays NTP Response per Destination Traffic, Threshold, Estimated Threshold and per-5-minute Drop information for: • NTP Response per Destination Ingress Max Packet Rate (pps) - Trend in observed ingress maximum rate for NTP Response per Destination packets to any single protected Destination IP address. • NTP Response per Destination Egress Max Packet Rate (pps) - Trend in observed egress maximum rate for NTP Response per Destination packets to any single protected Destination IP address. • NTP Response per Destination packets Dropped (drops per 5-minutes) - Trend in packets dropped due to the rate-limiting NTP Response per Destination Threshold.

Logs and Reports

This section includes the following topics:

Log Configuration

Logs and reports overview

The FortiDDoS system supports the logging and reporting features you expect in a security appliance:

- Local logging
- Remote logging (syslog and SNMP traps)
- FortiAnalyzer and FortiSIEM support (syslog only)
- SNMP (MIB Queires, Alarm and Attack Log Traps)
- Email Alerts (SMTP alerts for selected admin Events)
- SQL Query support (expert only with support of development team)
- Real-time system status and traffic monitoring
- Configurable system event and security event logging
- Filtering of log tables
- Customizable, scheduled and Threshold-based reports, with multiple formats and delivery options

The table below details the remote logging and services available in the system as well as where they are configured:

Event	Remote Logging	Settings
CPU, Memory, Disk Capacity Alarms	SNMP Traps	*System > SNMP > System Information / Config*
Event Logs	Syslog messages	*Log & Report > Log Configuration > Event Log Remote*
	Alert Email Messages (Selected Events)	*Log & Report > Log Configuration > Alert Email Settings*
Attack Logs	SNMP Traps	*Log & Report > Log Configuration > SNMP Trap Receivers*

Event	Remote Logging	Settings
	Syslog messages	*Log & Report > Log Configuration > DDoS Attack Log Remote*

System Data	Remote Queries	Settings
Traffic Data and other info	SNMP MIB Queries	*System > SNMP > System Information / Config*

Configuring local log settings

The local log is a data-store hosted on the FortiDDoS system. The local log disk configuration applies to the system event log.

Typically, you use the local log to capture information about system health and system administration activities, to verify that your configuration and tunings behave as expected, and to understand threats in recent traffic periods. It is both standard practice and best practice to send security log data to secure remote servers where it can be stored long term and analyzed using preferred analytic tools.

Local log disk settings are configurable. You can select a subset of system events. The DDoS attack log events are not configurable.

Before you begin:

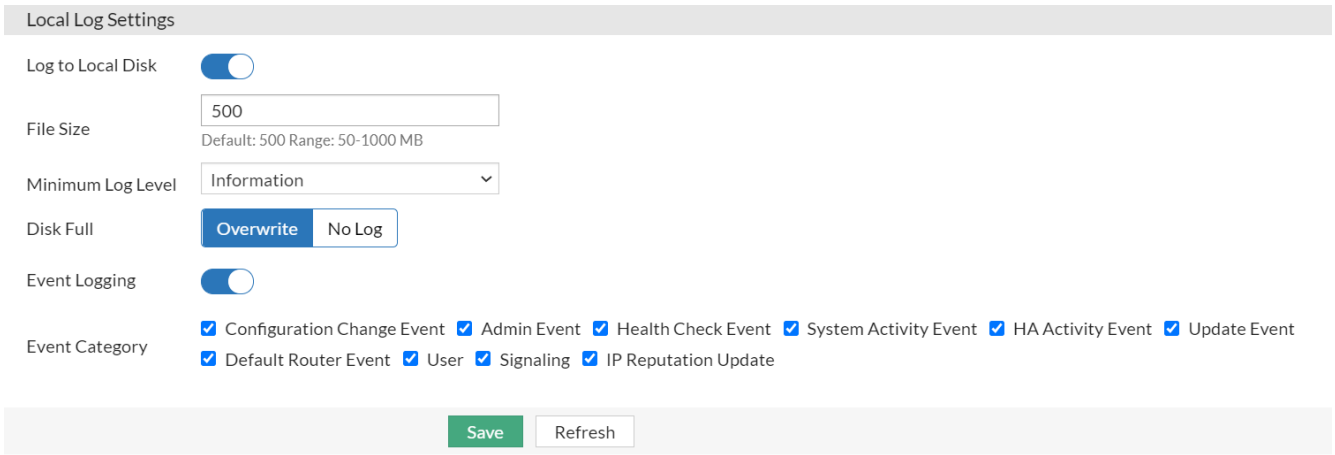
- You must have Read-Write permission for Log & Report settings.

See also: Using the event log table, Using the DDoS attack log table.

To configure local log settings:

1. Go to *Log & Report > Log Configuration > Local Log Settings*.
2. Complete the configuration as described in the table below.
3. Save the configuration.

Local log configuration page



Local logging configuration guidelines

Settings	Guidelines
Logging and Archiving	
Log to Local Disk	Select to display settings to manage the disk used for logging.
Minimum Log Level	Select the lowest severity to log from the following choices: • Emergency—The system has become unstable. • Alert—Immediate action is required. • Critical—Functionality is affected. • Error—An error condition exists and functionality could be affected. • Warning—Functionality might be affected. • Notification—Information about normal events. • Information—General information about system operations. • Debug—Detailed information about the system that can be used to troubleshoot unexpected behavior. For example, if you select **Error**, the system collects logs with level Error, Critical, Alert, and Emergency. If you select **Alert**, the system collects logs with level Alert and Emergency. The log level setting applies to both system events and DDoS security events. **Tip**: To prolong disk life, do not collect notification, information, and debug level logs for long periods of time.
File Size	Maximum disk space for local logs. The default is 500 MB.
Disk full	Select log behavior when the maximum disk space for local logs is reached: • Overwrite—Continue logging. Overwrite the earliest logs. • No Log—Stop logging.
Event Logging	
Event Logging	Select to enable event logging and then select the types of event category that you want included in the event log.

CLI commands:

```
config log setting local
   set loglevel notification
   set event-log-category configuration admin health_check system
        ha update default_gateway user spp_switching ir_update
end
```

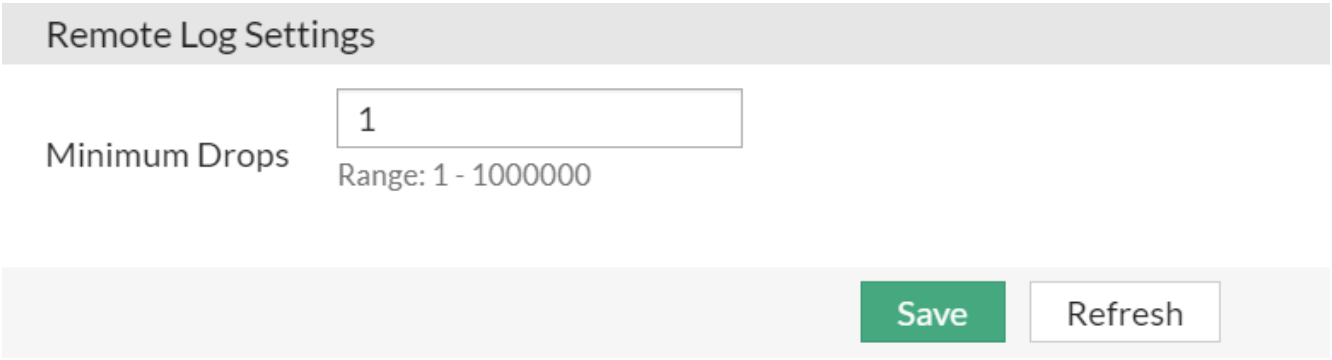
Configuring remote log settings

Remote log settings can be configured to suppress low-drop logs by defining a minimum threshold value. At this threshold or higher, the drops will be sent to syslog and SNMP trap receivers. All the log information can still be viewed under Attack Log, Reports and Executive Summary.

To configure remote log settings:

1. Go to *Log & Report* > *Log Configuration* > *Remote Log Settings*.
2. Enter the *Minimum Drops* count. The default value is '1'.
3. Save the configuration.

Remote log settings



To configure with CLI:

```
config log setting remote-log-settings
   set minimum-drops 100
end
```

Configuring remote log server settings for event logs

A remote log server is a system provisioned specifically to collect logs for long term storage and analysis with preferred analytic tools. We recommend FortiAnalyzer.

The system has two configurations to support sending logs to remote log servers: remote log server settings for system event logs, and remote log server settings for DDoS logs.

The system event log configuration applies to system-wide data, such as system health indicators and system administrator activities. The DDoS log configuration applies to security data.

You can configure up to three Log Remote or Remote Event Log Servers.

Before you begin:

- You must have Read-Write permission for Log & Report settings.

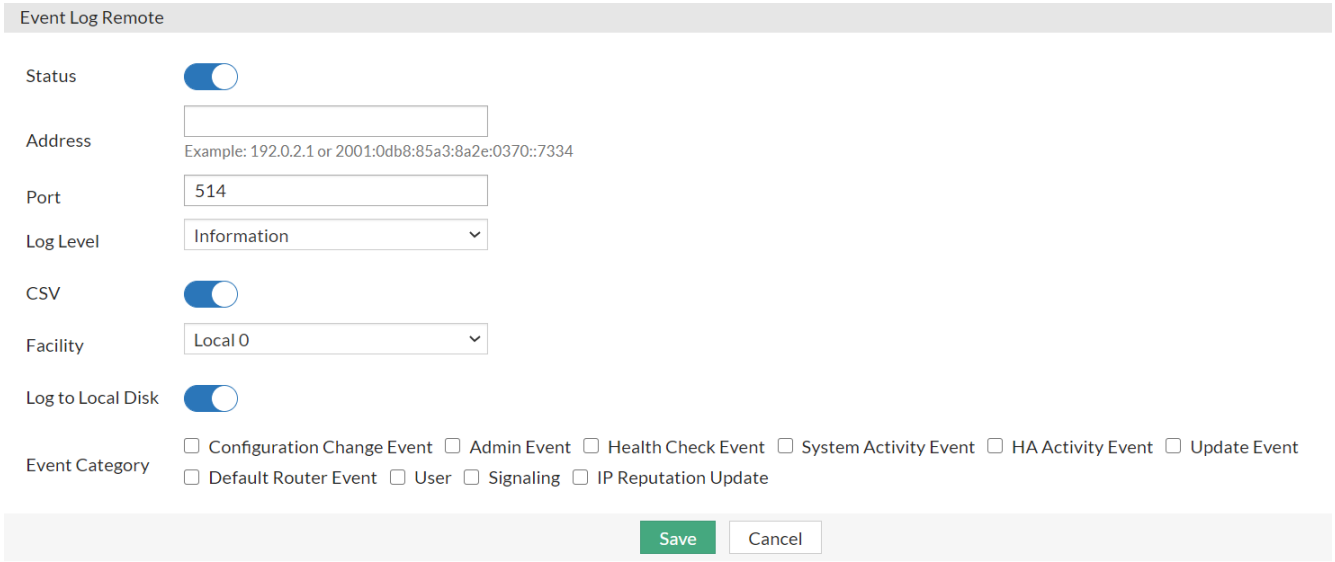
See also: Configuring remote log server settings for DDoS attack log.

To configure remote event log settings:

1. Go to *Log & Report* > *Log Configuration* > *Event Log Remote*.
2. Click *Add*.

3. Complete the configuration as described in the table below.
4. Save the configuration.

Remote log server settings



Remote log configuration guidelines

Settings	Guidelines
Status	Select to display settings to manage the disk used for logging.
Address	IP address of the FortiAnalyzer or syslog server.
Port	Listening port number of the FortiAnalyzer/syslog server. Usually this is UDP port 514.
Log Level	Select the severity to log from the following choices: • Emergency—The system has become unstable. • Alert—Immediate action is required. • Critical—Functionality is affected. • Error—An error condition exists and functionality could be affected. • Warning—Functionality might be affected. • Notification—Information about normal events. • Information—General information about system operations. • Debug—Detailed information about the system that can be used to troubleshoot unexpected behavior
CSV Format	Send logs in CSV format. Do not use with FortiAnalyzer.
Minimum Log Level	Select the lowest severity to log from the following choices: • Emergency—The system has become unstable. • Alert—Immediate action is required. • Critical—Functionality is affected. • Error—An error condition exists and functionality could be affected.

Settings	Guidelines
	• Warning—Functionality might be affected. • Notification—Information about normal events. • Information—General information about system operations. • Debug—Detailed information about the system that can be used to troubleshoot unexpected behavior. For example, if you select **Error**, the system sends the syslog server logs with level Error, Critical, Alert, and Emergency. If you select **Alert**, the system collects logs with level Alert and Emergency.
Facility	Identifier that is not used by any other device on your network when sending logs to FortiAnalyzer/syslog.
Event Logging	Select to enable event logging and then select the types of events that you want included in the event log.
RFC 5424 Compliance	Enable to comply with RFC 5424 guidelines
Encrypt Syslog to FortiAnalyzer	Enable to send encrypted Syslog to FortiAnalyzer. Please do not combine with RFC 5424 settings if you choose this option.

The following is an example of an event syslog message:

```
device_id=SYSLOG-AC1E997F type=generic pri=information itime=1431633173 msg="date=2015-05-
13,time=13:25:13,tz=PDT,devid=FI800B3913000032,log_
id=0000002168,type=event,subtype=config,level=information,msg_id=426204,user=admin,ui=ssh
(172.30.153.9),action=none,status=none,reason=none,msg='changed settings for 'ddos spp
      setting'
on domain 'SPP-1'"
```

Event syslog fields

Field	Example
Syslog device ID	device_id=SYSLOG-AC1E997F
Syslog type	type=generic
Syslog log level	pri=information
Syslog time	itime=1431633173
Log datestamp	date=2015-05-13
Log timestamp	13:25:13
Log time zone	tz=PDT
Device ID	devid=FI800B3913000032
Log ID	log_id=0000002168
Log type	type=event

Field	Example
Log subtype	subtype=config
Log level	level=information
Message ID	msg_id=426204
Admin user	user=admin
Admin UI	ui=ssh(172.30.153.9)
Action	action=none
Status	status=none
Reason string	reason=none
Log message	msg='changed settings for 'ddos spp setting' on domain 'SPP-1'"'

CLI commands:

```
config log setting remote
   edit 1
      set status enable
      set server 172.30.153.105
      set comma-separated-value enable
      set event-log-status enable
      set event-log-category configuration spp_switching ir_update
   next
end
```

Configuring remote log server settings for DDoS attack log

The DDoS attack log remote server configuration applies to security event data. You configure individual remote log server configurations for each SPP.

You can set up two remote DDoS Attack Log Remote syslog servers per SPP.

Before you begin:

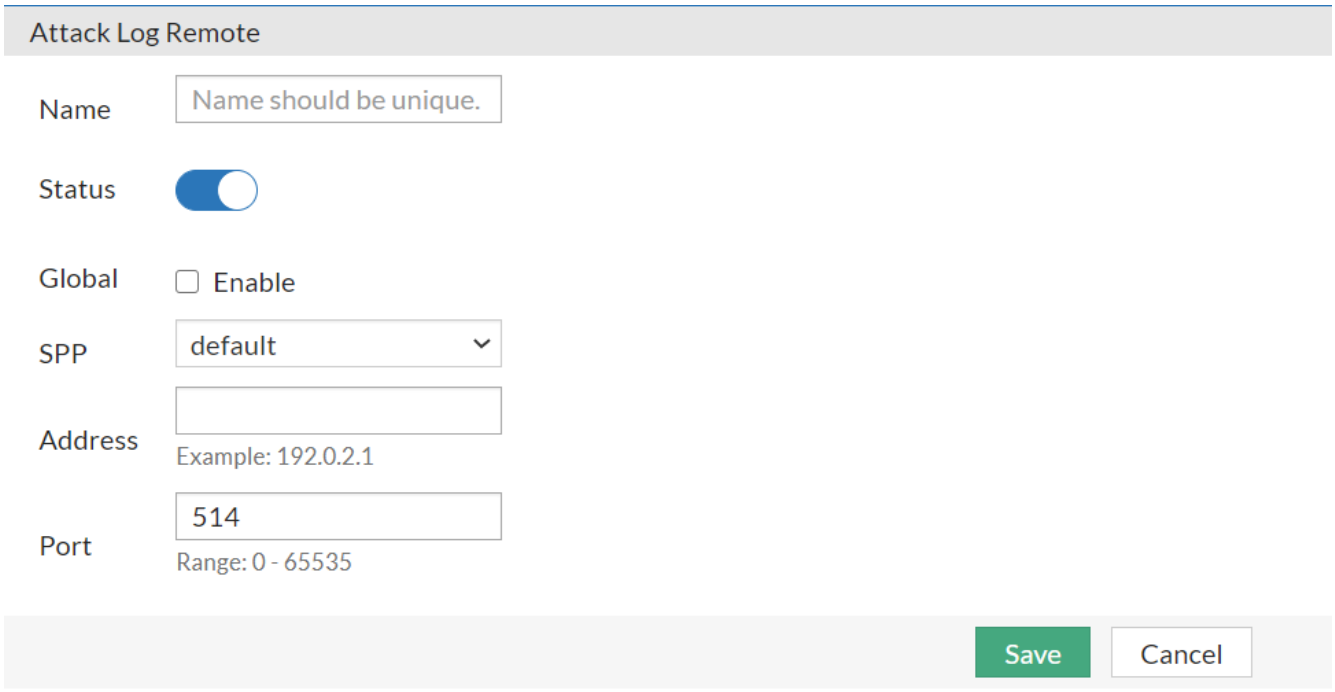
- You must have Read-Write permission for Log & Report settings.

See also: Configuring remote log server settings for event logs.

To configure remote log settings for the Attack Log Remote:

1. Go to *Log & Report* > *Log Configuration* > *Attack Log Remote*.
2. Click *Add*.
3. Complete the configuration as described in the table below.
4. Save the configuration.

Attack Log remote logging configuration page



Attack Log remote logging configuration guidelines

Settings	Guidelines
Name	Configuration name.
Status	Select to enable sending DDoS attack logs to a remote server.
SPP	Select the SPP whose logs are stored in the remote location. You can specify only one remote log server for each SPP.
Address	IP address of the FortiAnalyzer/syslog server.
Port	Listening port number of the FortiAnalyzer/syslog server. Usually this is UDP port 514.

The following example shows a DDoS attack syslog message:

```
Oct 10 10:56:00 170.30.100.162 devid=FI-1KB3913000012 date=2018-10-10 time=10:56:00
tz=PDT type=attack spp=2 evecode=2 evesubcode=87 description="HTTP Method flood
from source" dir=1 protocol=6 sip=41.1.61.9 dip=41.20.0.20 dport=80 dropcount=72
subnet_id=7 facility=Local0 level=Notice direction=inbound spp_name="2Two" subnet_
name="Seven"
```

DDoS attack syslog fields

Field	Example (from the sample message above)	Details
Syslog send timestamp	`Oct 10 10:56:00`	Local FortiDDoS time
Syslog client IP address	`170.30.100.162`	FortiDDoS Source Management Port
FortiDDoS device ID	`devid=FI-1KB3913000012`	Serial Number of the FortiDDoS
Log datestamp	`date=2018-10-10`	FortiDDoS local date
Log timestamp	`time=10:56:00`	FortiDDoS local time
Log time zone	`tz=PDT`	FortiDDoS local time zone
Log type	`type=attack`	Attack or Event Log
SPP ID	`spp=2`	Name of the FortiDDoS Service Protection Profile
Event code	`evecode=2`	See the Appendix – DDoS Attack Log Reference
Event subcode	`evesubcode=87`	See the Appendix – DDoS Attack Log Reference
Event type	`description="HTTP Method flood from source"`	Event name - see the Appendix – DDoS Attack Log Reference
Direction ID (1=inbound, 0=outbound)	`dir=1`	Direction of attack traffic - see 'Direction' below for textual direction.
Protocol	`protocol=6`	Layer 3 Protocol
Source IP address	`sip=41.1.61.9`	Only included if non-spoofed Source IP address
Protected IP address	`dip=41.20.0.20`	Protected IP address included in the FortiDDoS SPP Policies
Associated port	`dport=80`	TCP or UDP Port under attack if applicable
Drop count	`dropcount=72`	Number of dropped packets over 1-minute (Interrupt) or 5-minutes (Periodic) - see the Appendix – DDoS Attack Log Reference.
Subnet ID	`subnet_id=7`	Index number of the SPP Policy where the Protected IP is contained - see 'Subnet name' below.
Facility	`facility=Local0`	Defined by the customer in SNMP configuration
Level	`level=Notice`	Default severity level
Direction	`direction=inbound`	Textual direction of the attack traffic
SPP name	`spp_name="2Two"`	Service Protection Profile name that contains the SPP Policy/subnet that further contains the Protected IP address under attack

Field	Example (from the sample message above)	Details
Subnet name	`subnet_name="Seven"`	Configured name of the SPP Policy/subnet

To configure with the CLI:

```
config log setting ddos-attack-log-remote
   edit Attack_log_Syslog
      set status enable
      set spp default
      set ip-address 172.30.153.105
   next
end
```

Using FortiAnalyzer to collect DDoS attack logs

FortiAnalyzer platforms integrate network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout your network.

FortiAnalyzer now supports the FortiDDoS attack log. FortiAnalyzer includes the following predefined reports for FortiDDoS:

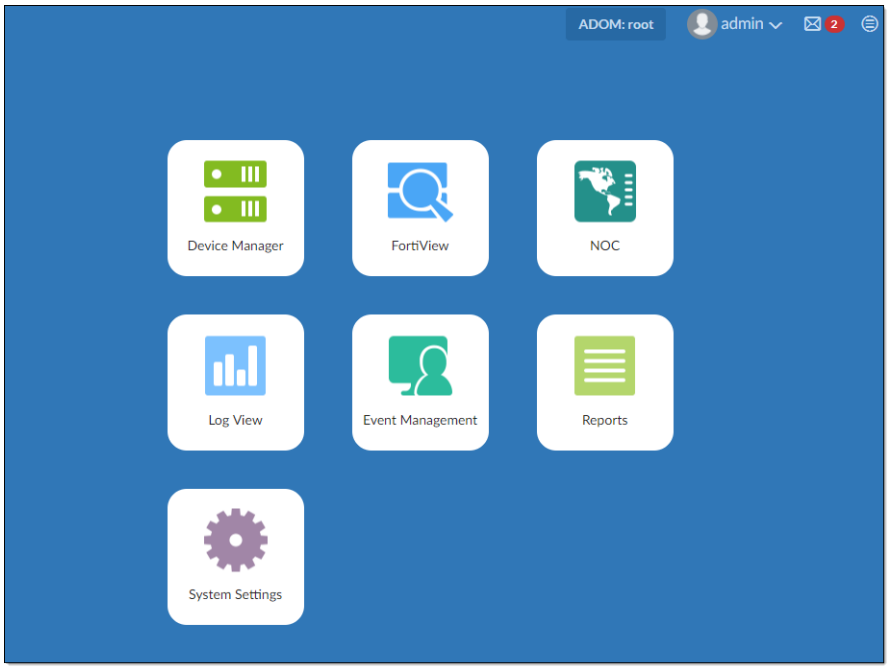
- Attacks by time period
- Attackers by time period
- Top 20 Attacks
- To 20 Attack Types

FortiAnalyzer reports can also be fully customized by the user.

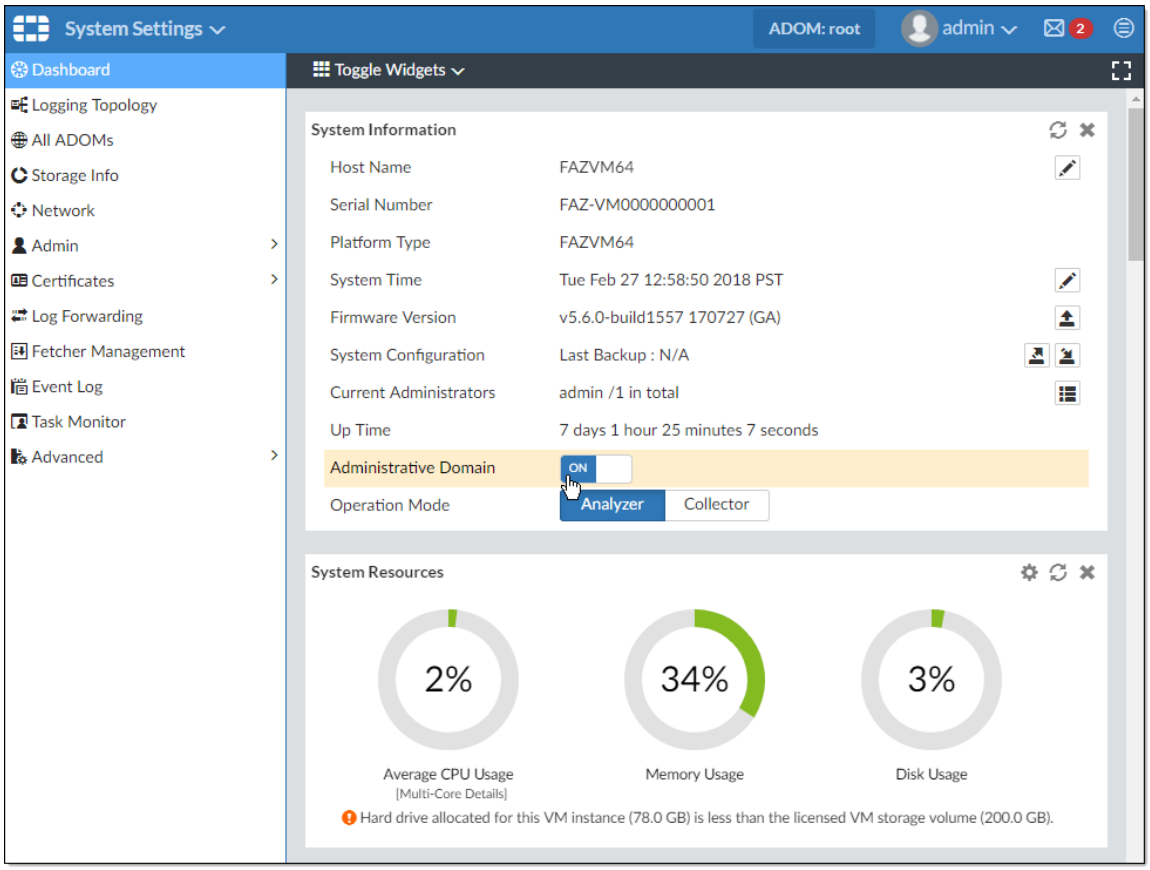
Refer to FortiAnalyzer documentation for version support details and detailed procedures on how to use FortiAnalyzer. This section describes the workflow for collecting DDoS attack logs.

To set up log collection:

1. Log in to FortiAnalyzer as root. The following screen is displayed.

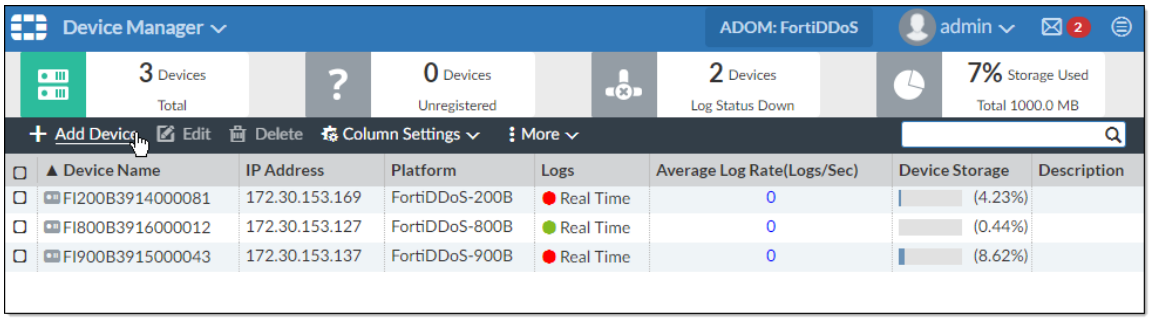


2. Click **System Settings** widget and enable **Administrative Domain**.

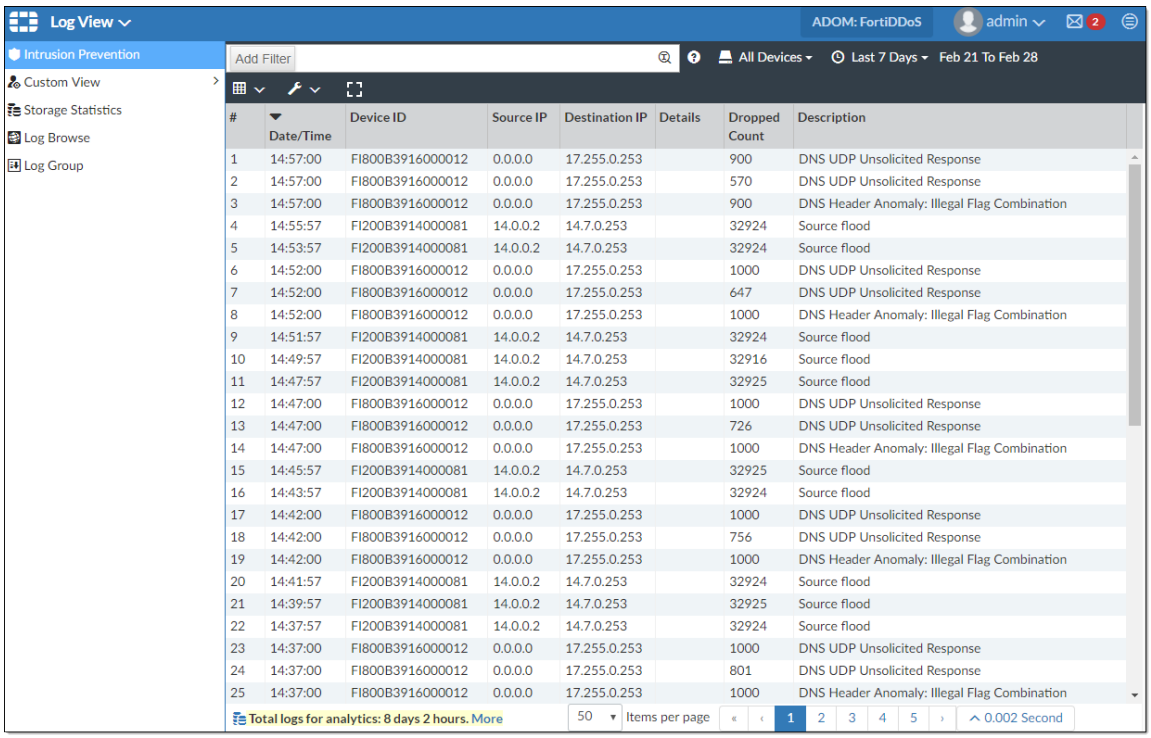


3. On FortiDDoS, use the DDoS Attack Log Remote configuration to send logs to the FortiAnalyzer IP address. FortiDDoS starts sending logs to FortiAnalyzer. Once FortiAnalyzer begins receiving logs from FortiDDoS, **FortiDDoS** appears in the Administrative Domains (ADOM).
4. On FortiAnalyzer, select **Device Manager**from the top-left drop-down.
   The **Devices Unregistered** count will change to 1.

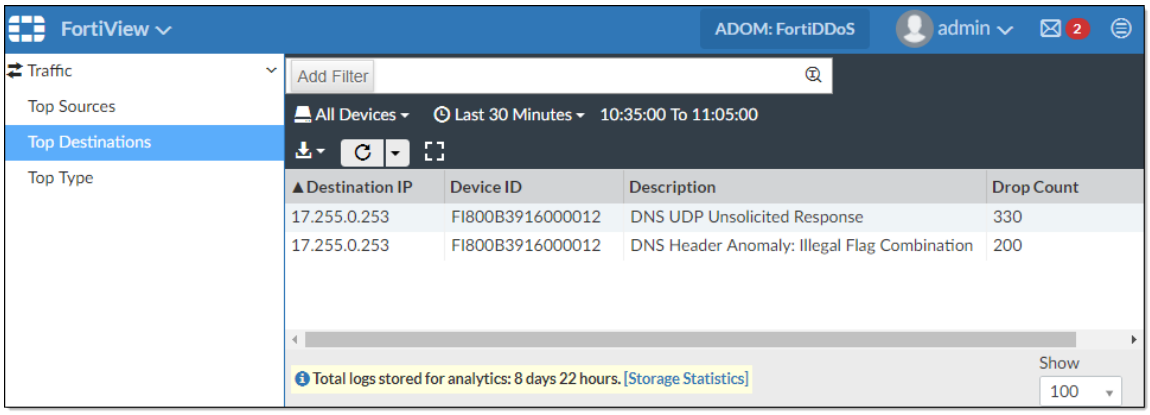
   If you need to add a device manually:
   a) Click **ADOM: root** on the top menu and switch to 'FDDoS'.
   b) Select the **Device Manager** widget.
   c) Click **Add Device** to enter the device details in the Add Device wizard.



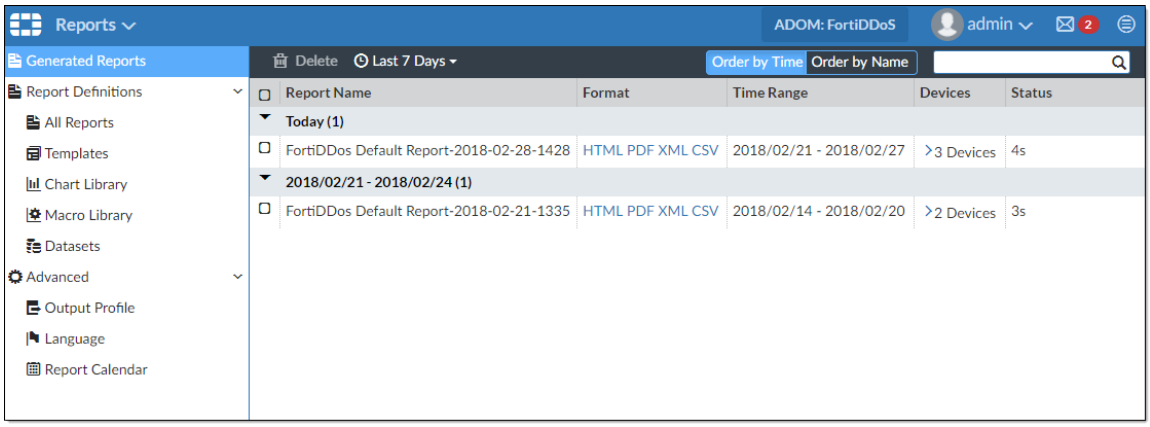
5. Click **ADOM: root** on the top menu to switch from 'root' to 'FortiDDoS'.
6. Go to the **Device Manager** and verify that the FortiDDoS device has been added.
7. Click **Log View** from the top-left drop-down to see the log information under various tabs on the left panel.



8. Click **FortiView** from the top-left drop-down to see the attack logs. Navigate to the **Top Sources**, **Top Destinations** and **Top Type** on the left panel to view more details.



9. Go to the **Reports** from the top-left drop-down. You can generate the reports in HTML, PDF, XML or CSV format.

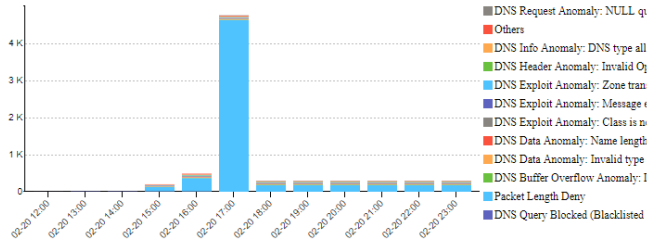


See the sample report below.

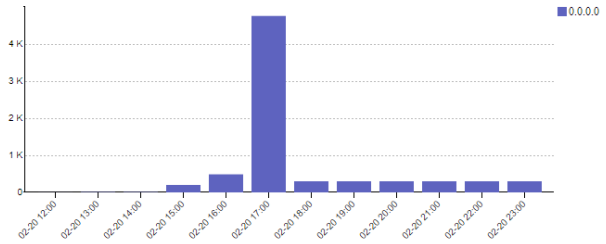
FortiDDos Default Report

Report Date: February 21, 2018 13:35
Data Range: 2018-02-14 00:00 2018-02-20 23:59 PST (FAZ local)

Attacks by Time Period



Attackers by Time Period



Top 20 Attacks

#	Attack Source	Description	Total	% of Subtotal
1	0.0.0.0	Packet Length Deny	6,180	84.97%
		DNS Buffer Overflow Anomaly: Label length too large	103	1.42%
		DNS Data Anomaly: Invalid type class	103	1.42%
		Others	**887**	**12.20%**
		Subtotal	**7,273**	**100.00%**
	Total		**7,273**	**100.00%**

Top 20 Attack Types

#	Type	Description	Total	% of Subtotal
1	attack	Packet Length Deny	6,180	84.97%
		DNS Buffer Overflow Anomaly: Label length too large	103	1.42%
		DNS Data Anomaly: Invalid type class	103	1.42%
		Others	**887**	**12.20%**
		Subtotal	**7,273**	**100.00%**
	Total		**7,273**	**100.00%**

Top 20 Destinations

#	Destination	Description	Total	% of Subtotal
1	67.255.0.253	Packet Length Deny	6110	100.00%
		Subtotal	**6110**	**84.01%**
2	17.255.0.253	DNS Buffer Overflow Anomaly: Label length too large	103	9.42%
		DNS Data Anomaly: Invalid type class	103	9.42%
		DNS Data Anomaly: Name length too short	103	9.42%
		Others	**784**	**71.73%**
		Subtotal	**1093**	**15.03%**
3	10.255.0.253	Packet Length Deny	12	100.00%
		Subtotal	**12**	**0.16%**
4	62.255.0.253	Packet Length Deny	12	100.00%
		Subtotal	**12**	**0.16%**
5	65.255.0.253	Packet Length Deny	11	100.00%
		Subtotal	**11**	**0.15%**
6	64.255.0.253	Packet Length Deny	10	100.00%
		Subtotal	**10**	**0.14%**
7	66.255.0.253	Packet Length Deny	10	100.00%
		Subtotal	**10**	**0.14%**
8	63.255.0.253	Packet Length Deny	8	100.00%
		Subtotal	**8**	**0.11%**
9	61.255.0.253	Packet Length Deny	7	100.00%
		Subtotal	**7**	**0.10%**
	Total		**7273**	**100.00%**

Top 20 Destinations by Type

#	Type	Destination	Total	% of Subtotal
1	attack	67.255.0.253	6,110	84.01%
		17.255.0.253	1,093	15.03%
		10.255.0.253	12	0.16%
		Others	**58**	**0.80%**
		Subtotal	**7,273**	**100.00%**
	Total		**7,273**	**100.00%**

Appendix A

Devices

FI200B3914000081
FI800B3916000012

Using FortiSIEM to collect DDoS attack and event logs

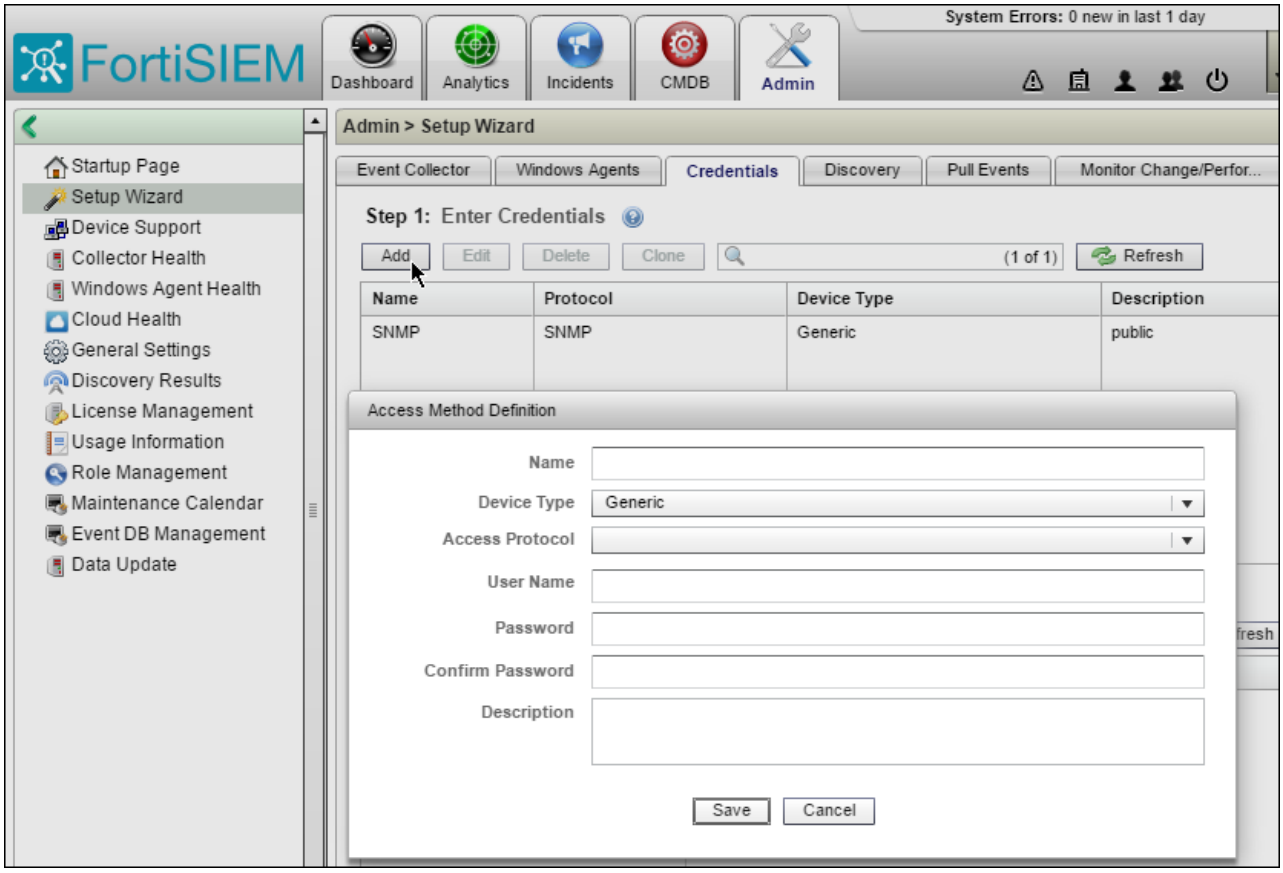
FortiSIEM provides an all-in-one, seamlessly integrated and service-oriented IT infrastructure monitoring solution that covers performance, availability, change, and security monitoring aspects of network devices, servers, and applications.

FortiSIEM now supports FortiDDoS attack and event logs. FortiSIEM processes FortiDDoS events via syslog. You can configure FortiDDoS to send syslog to FortiSIEM.

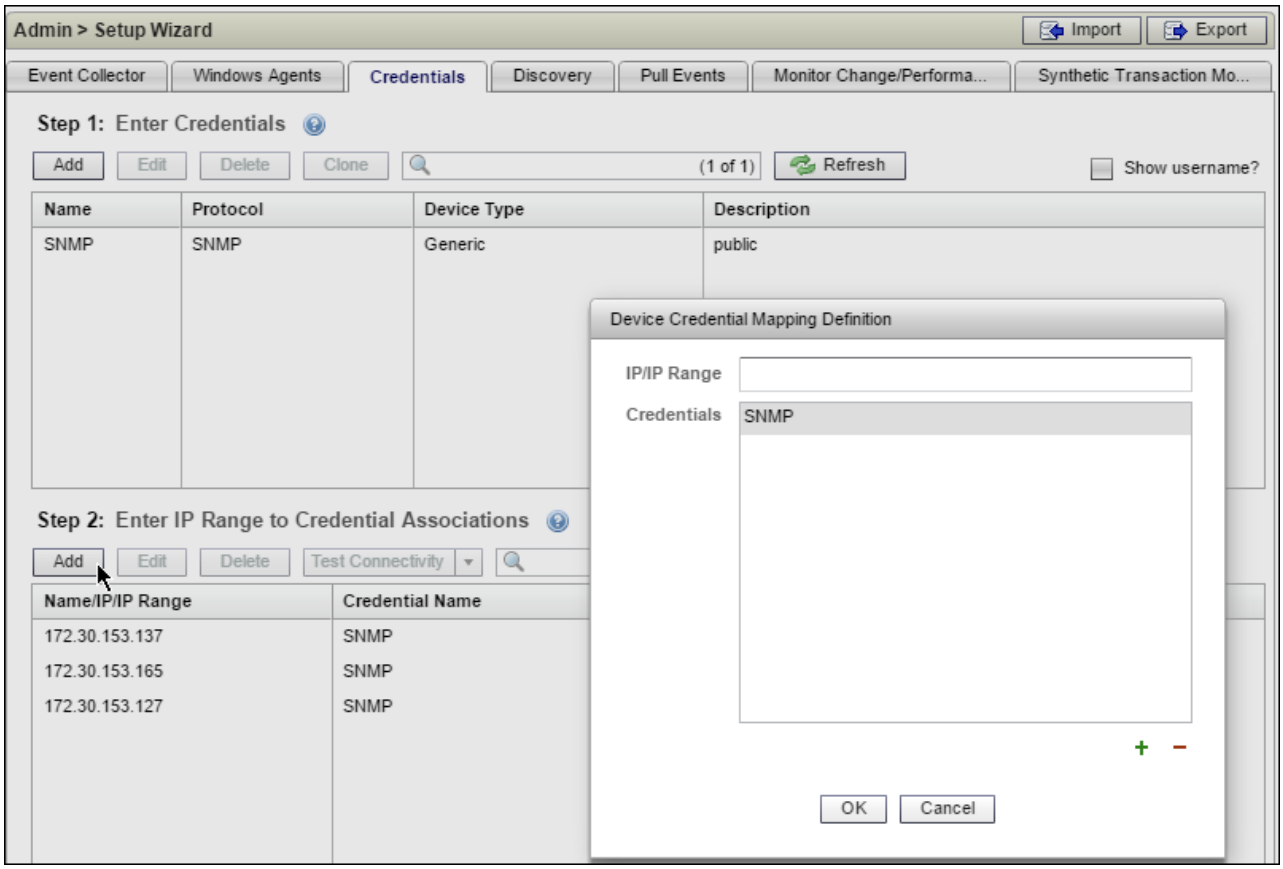
Refer to FortiSIEM User Guide for version support details and detailed procedures on how to use FortiSIEM. This section describes the workflow for collecting DDoS attack logs.

To set up log collection:

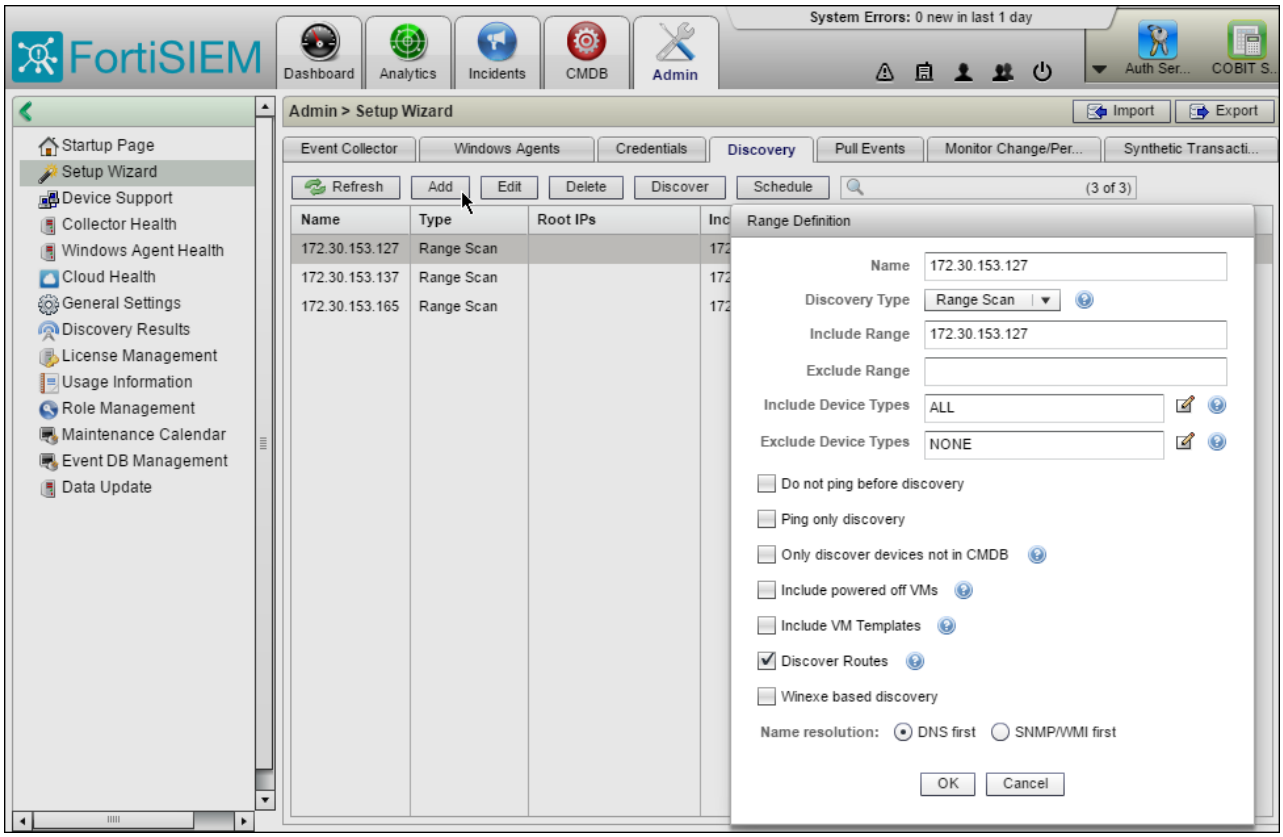
1. On FortiDDoS, use **DDoS Attack Log Remote** configuration to send logs to the FortiSIEM IP address. Refer to section Configuring remote log server settings for DDoS attack logs and follow the procedure for configuration. Once the configuration is saved, FortiDDoS begins sending logs to FortiSIEM.
2. Use **Event Log Remote** configuration to send logs to the FortiSIEM IP address. Refer to section Configuring remote log server settings for event logs and follow the procedure for configuration. Once the configuration is saved, FortiDDoS begins sending event logs to FortiSIEM.
3. Go to **System** > **SNMP** and follow the steps under Configuring SNMP for system event reporting.
4. Log in to FortiSIEM and go to **Admin** > **Setup Wizard** > **Credentials** tab.
5. Click **Add** under **Step 1: Enter Credentials** and enter the details of the device in the **Access Method Definition** dialog box.



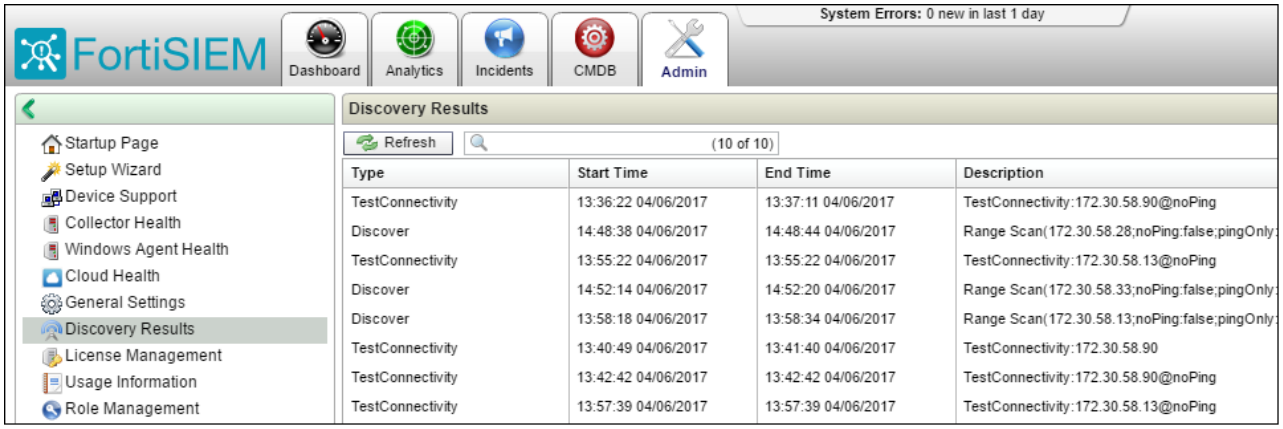
6. Click **Add** under **Step 2: Enter IP Range to Credential Association** and enter the **IP/IP Range** and **Credentials** of the device in the **Device Credential Mapping Definition** dialog box.



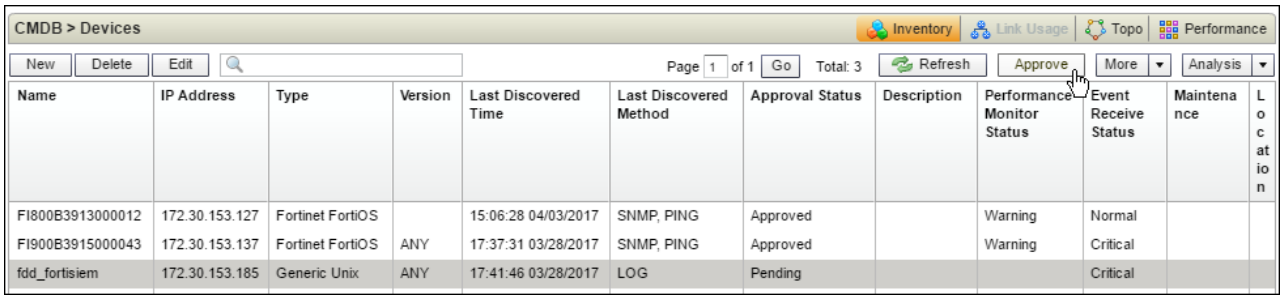
7. Go to **Admin**> **Setup Wizard** > **Discovery** tab and add the **Range Definition** details.



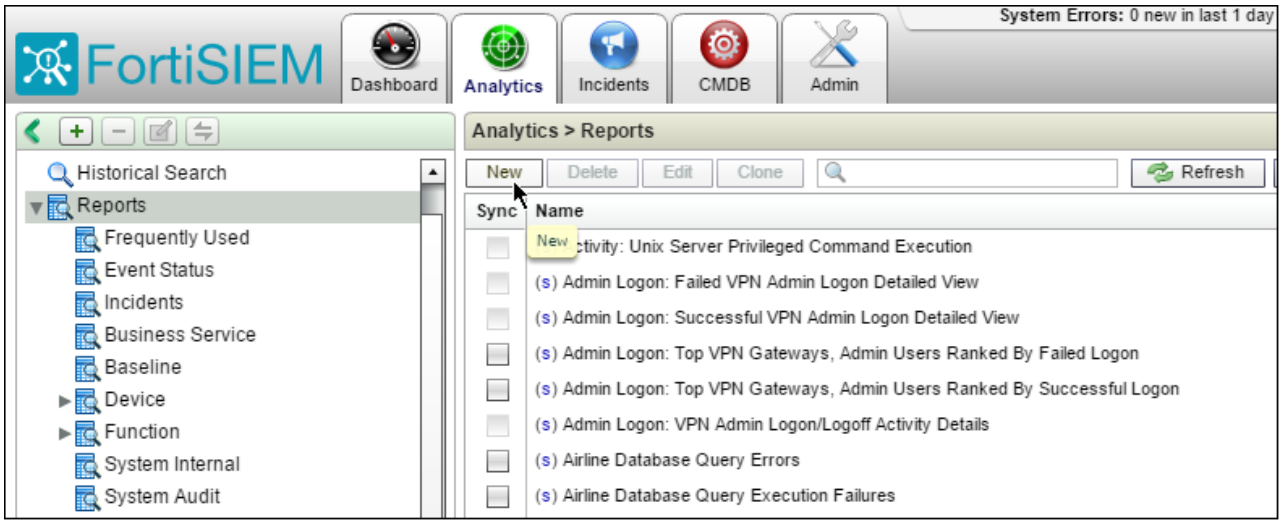
8. Select the added range and run discovery by clicking **Discover**.
9. Go to **Admin** > **Discovery Results** and verify the discovered FortiDDoS devices from the list.



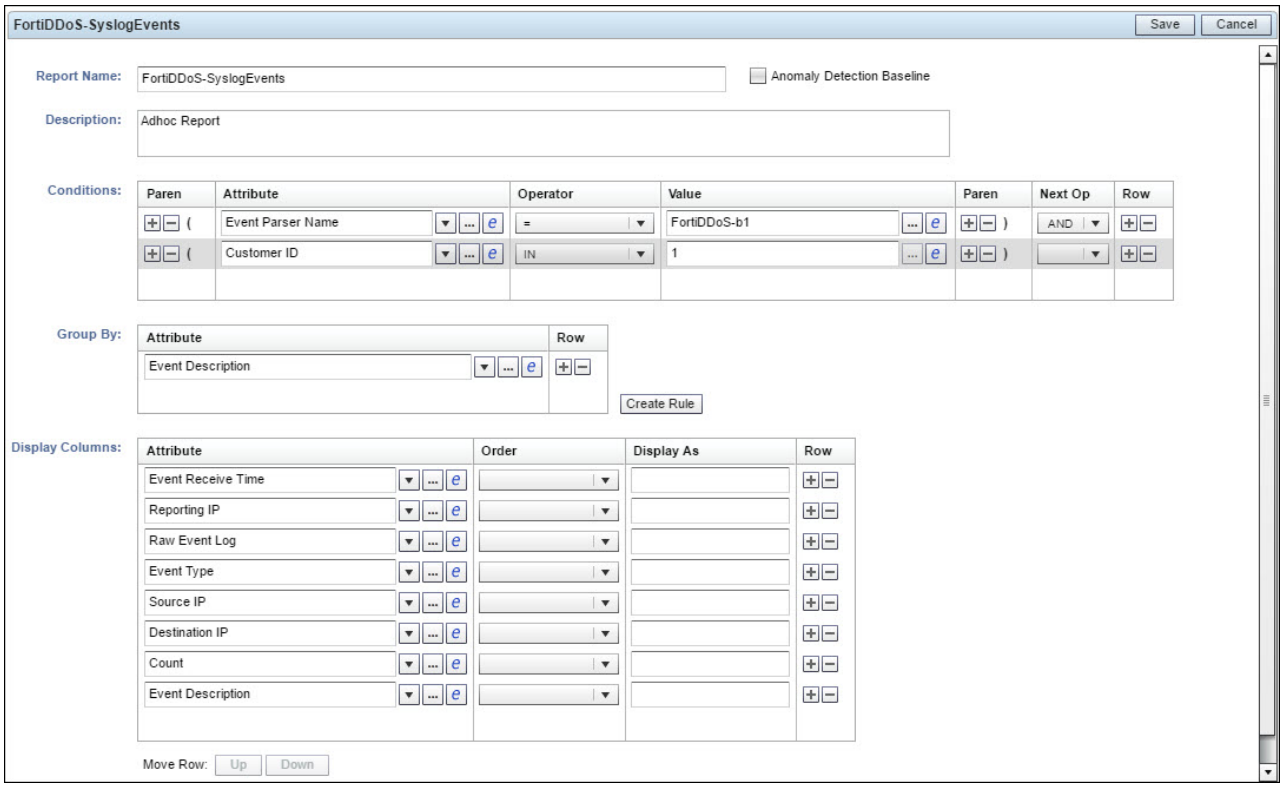
10. Go to **CMDB** > **Devices.** Select the added device from the list and click **Approve**.



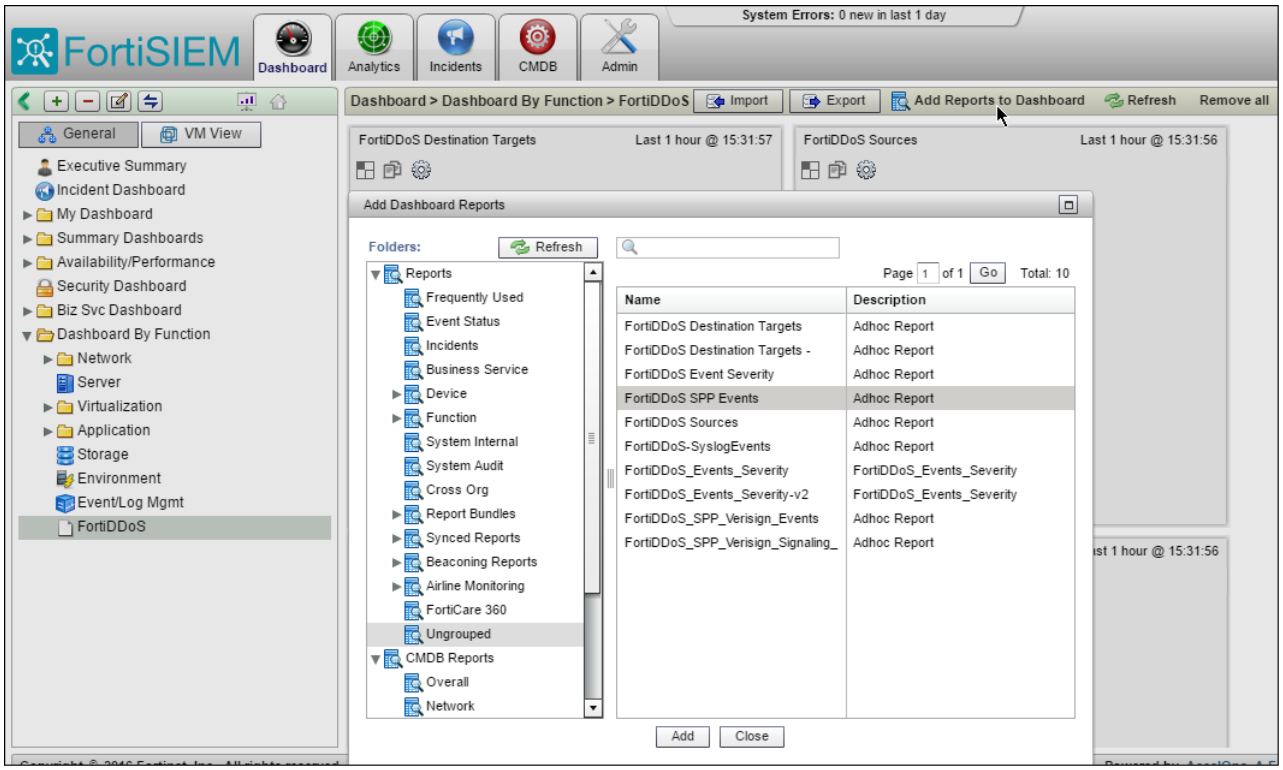
11. Go to **Analytics** > **Reports** and click **New** to configure a new report.



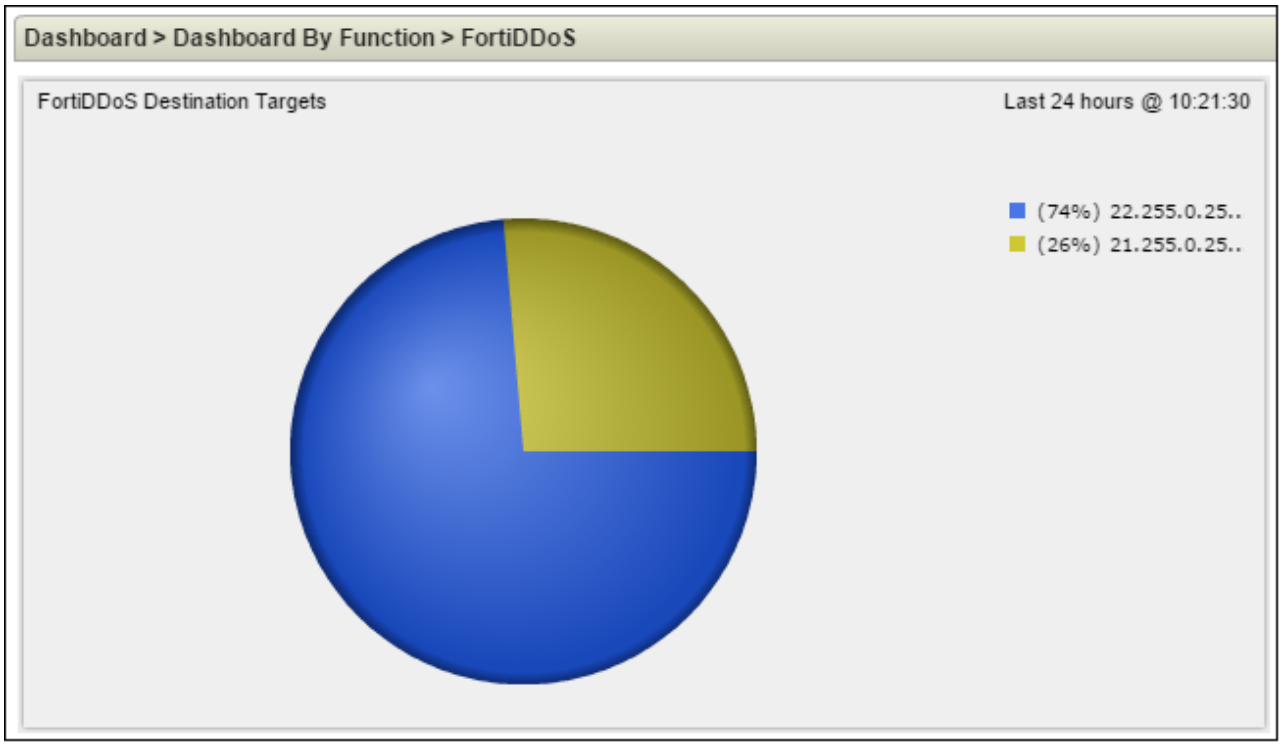
12. Enter the new report details in the **Add New Report** window and click **Save**.

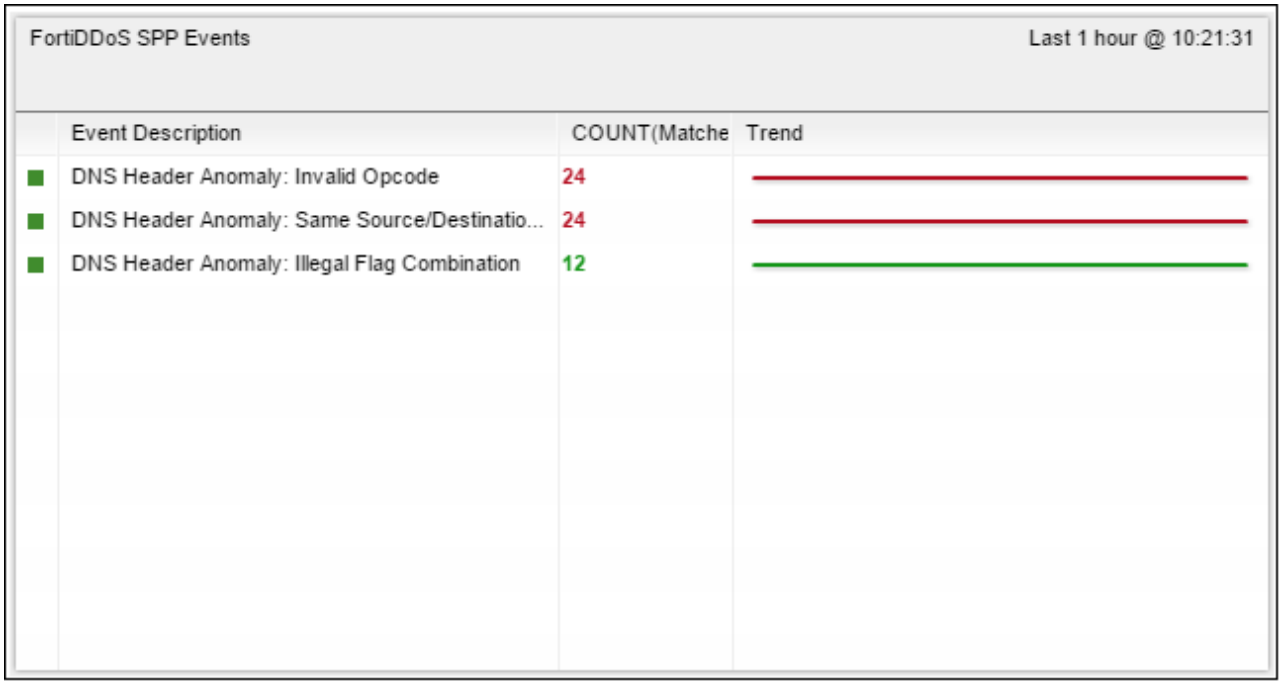


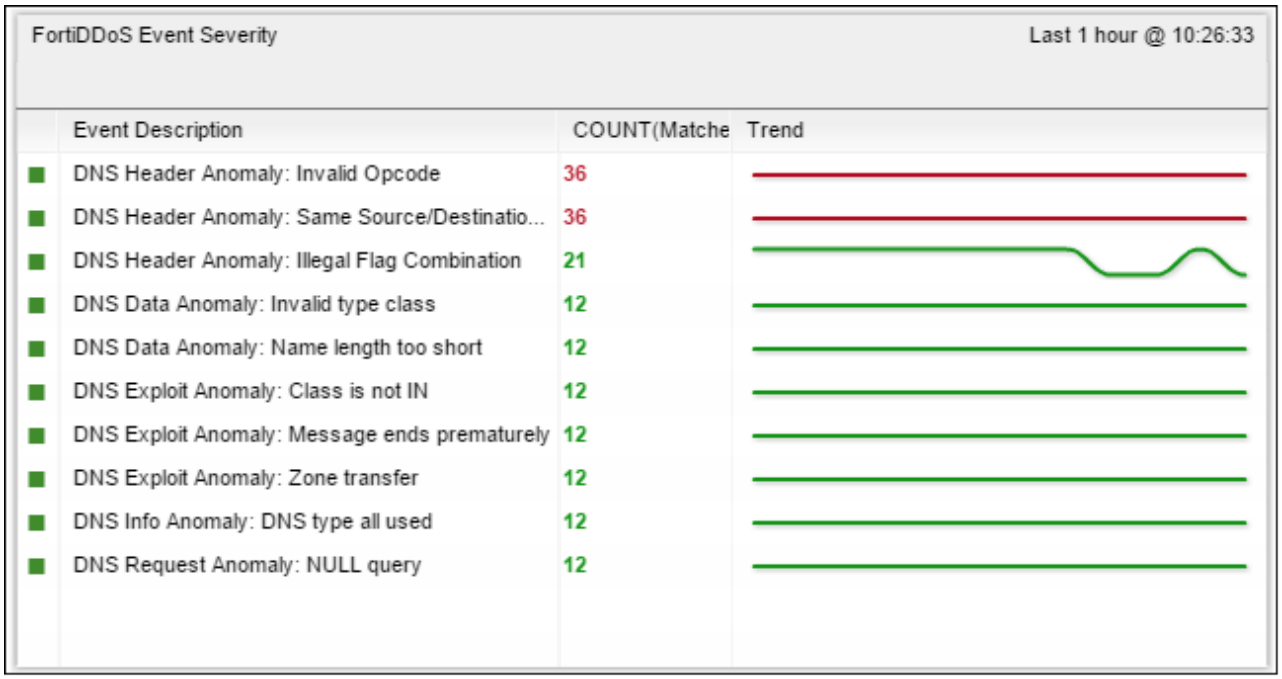
13. Go to **Dashboard** > **Dashboard by Function**. Select the group and click **Add Reports to Dashboard**.

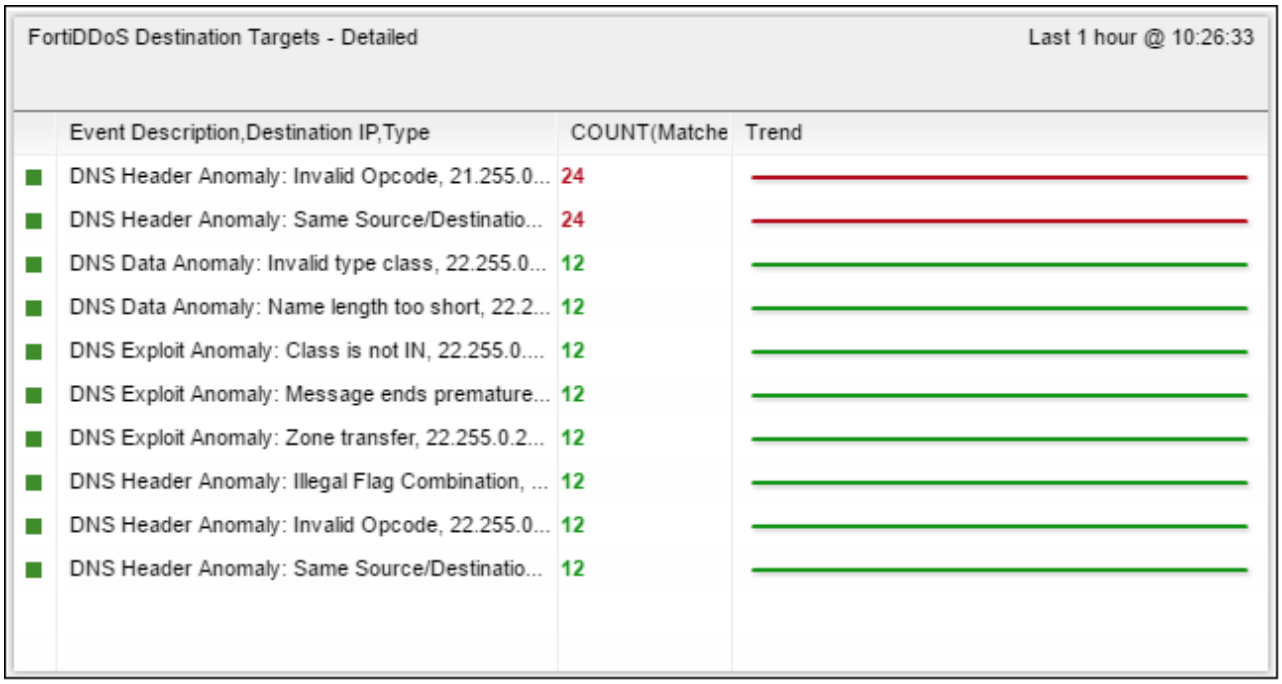


14. Select the required reports from the list and click **Add**.
15. Go to **Dashboard** > **Executive Summary** to see the selected reports. The following figures show the sample dashboard reports.









Configuring alert email settings

Alerts are emails sent to specified recipients when specified events are triggered.

The *Alert Mail Settings* > *Mail Server* tab sets up server settings for sending two types of Alert Mails:

- Event logs (found in the *Alert Mail Settings* > *Setting* tab), with recipients in the *Alert Mail Settings* > *Recipient* tab. You can specify event categories that will result in an Alert Mail via the *Setting* tab.

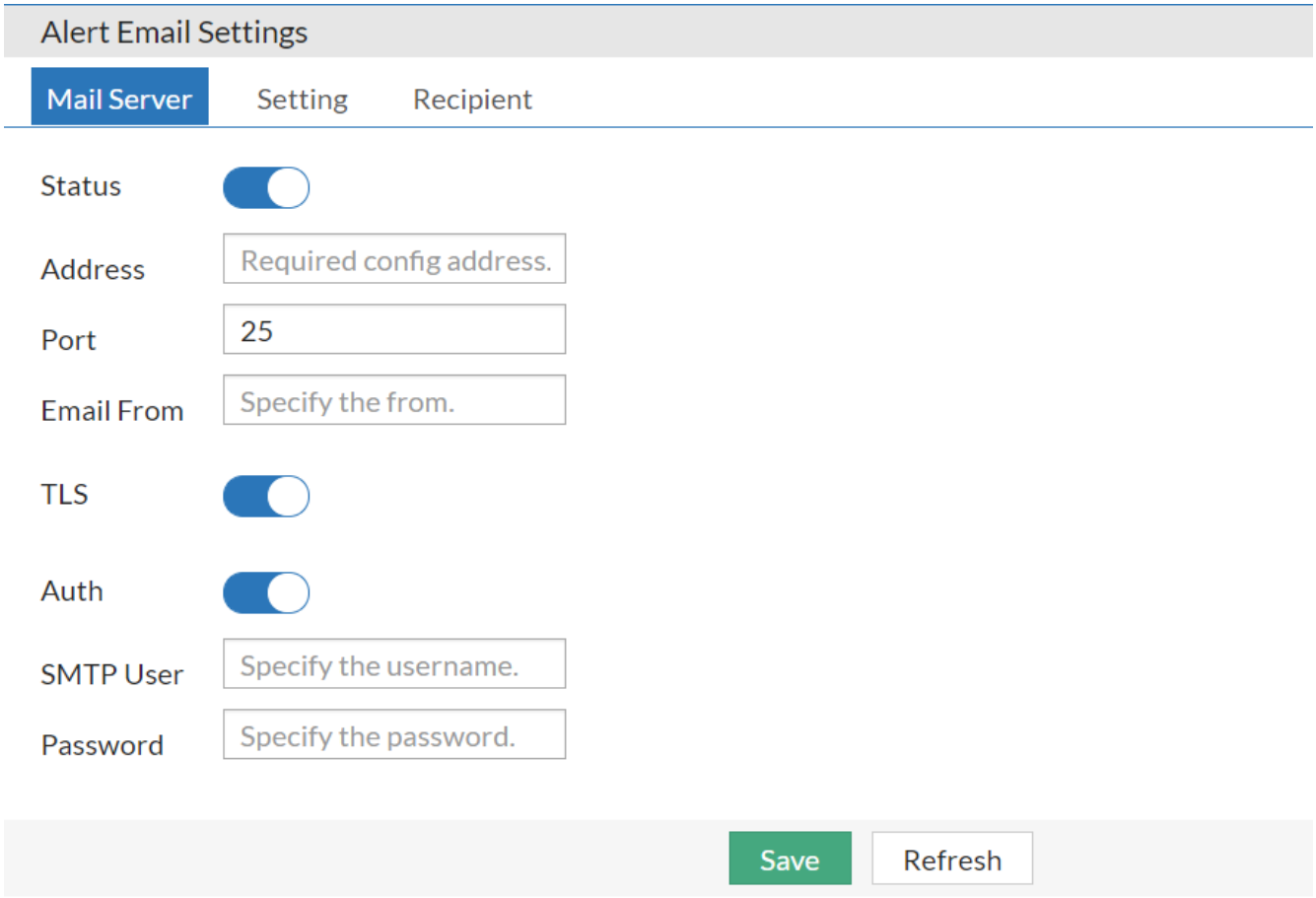
- Emailed Reports, defined in *Log & Report > Report Configuration*. Recipients and other email information is configurable in each Report.

Before you begin:

- You must have Read-Write permission for Log & Report settings.

To configure alert email settings:

1. Go to *Log & Report > Log Configuration > Alert Email Settings*.
2. Complete the configuration under the tabs: Mail Server, Settings and Recipients as described in the table below.
3. Save the configuration.



Alert mail configuration guidelines

Settings	Guidelines
Mail Server	
SMTP Server	IP address or FQDN of an SMTP server (such as FortiMail) or email server that the appliance can connect to in order to send alerts and/or generated reports.

Settings	Guidelines
Port	Listening port number of the server. Usually, SMTP is 25.
Email From	Sender email address used in alert email.
Authentication	Enable or disable authentication. **Note**: FortiDDoS cannot use RADIUS, LDAP or TACACS+ as a client to authenticate to email servers. It can only do basic user/password authentication.
TLS	Enable or disable TLS encryption for SMTPS. Normally, you will also change the Port setting above to Port 465.
SMTP Username	Username for authentication to the SMTP server.
SMTP Password	Password for authentication to the SMTP server.
Settings	
By Category	If Disabled, all Alert Events categories are sent based on the minimum severity selected (from 'Debug' to 'Emergency'). If Enabled, all events logs, no matter the severity, will be sent for the categories of events selected in the check-boxes.
Log Level (if Category is Disabled)	Select the minimum log level severity to send Alert Emails for all events.
Category (if Category is Enabled)	Select the categories to receive alerts for.
Interval time (min)	If identical alerts are occurring continuously, select the interval between each email that will be sent while the event continues.
Recipient	
Name	Name of the recipient for Event Log (from Settings above) Alert Mails. Report recipients are independent and are entered in the Report configuration.
Mail To	Up to three recipient email addresses, one per field. **Tip**: To temporarily disable alert emails, delete all recipients. This allows you to preserve the other SMTP settings in case you want to enable alert emails in the future.

To configure with the CLI:

```
config system mailserver
   set address mail.fortinet.com
   set username fddadmin
   set password ENC
        EEntXbrVJmOnZq/xFo2nzhCBU+vonWAPzsKyXO6Qjn/ZUI3l5OrdmoW8TtZVxNDKQ5YRhJawR1e
        wflirKvCg2E31/puFUJ+OwQZpWQz5QzcZp+Bp
   set from fortiddos@fortinet.com
end
config log alertemail setting
   set categories ha admin diskfull healthcheck update default_gateway
   set deferq-interval 50
end
config log alertemail recipient
   edit admin
      set address admin@fortiddos.com
   next
end
```

Configuring Attack Log purge settings

Attack Log purging is the deleting of logs to preserve log space and maintain log system performance.

By default, DDoS Attack Logs are purged on a first-in, first-out basis when the log reaches 1,000,000 entries. Attack Log purge settings are configurable. You can specify a different threshold, and you can purge logs manually.

Before you begin:

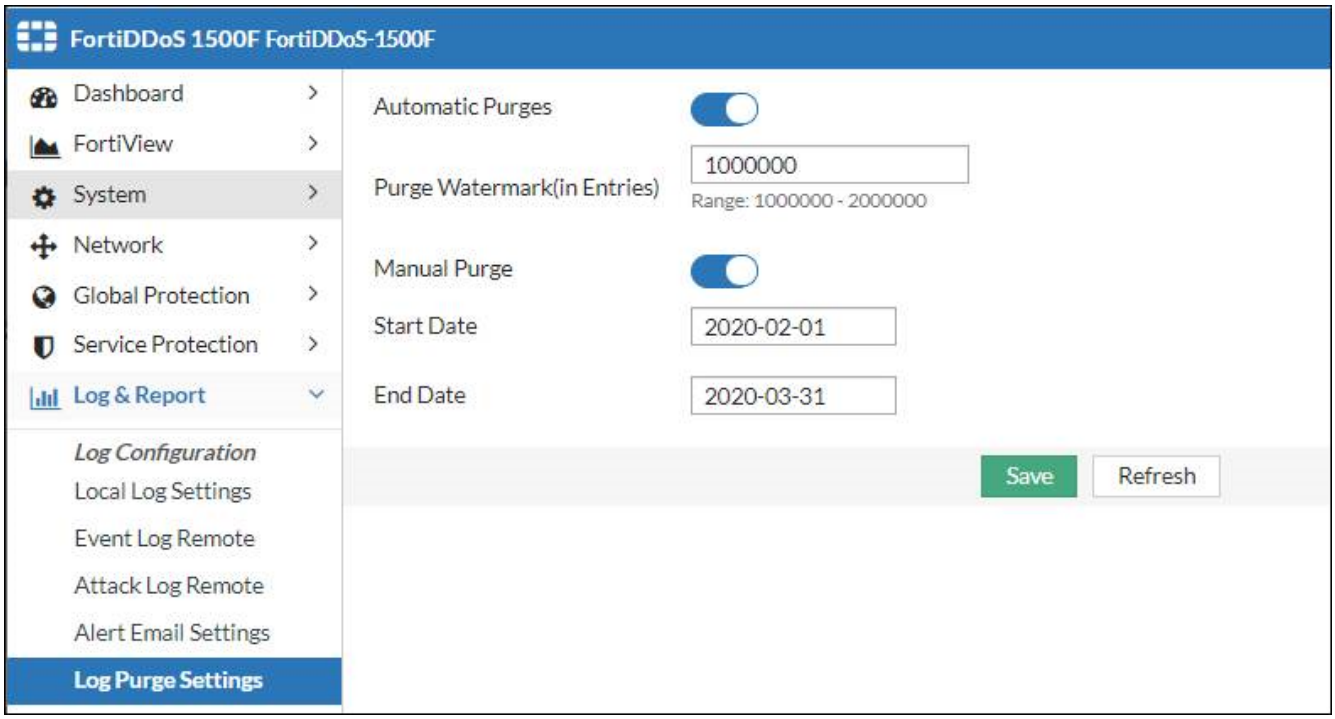
- You must have Read-Write permission for Log & Report settings.

To configure purge settings:

1. Go to **Log & Report** > **Log Configuration** > **Log Purge Settings**.
2. Complete the configuration as described in the table below.
3. Save the configuration.

Attack Log purge settings configuration guidelines

Settings	Guidelines
Automatic Purge	Select to automatically purge Attack Logs after the max number of entries is reached.
Purge older events when the number of events is over	Purge the earliest Attack Logs when this threshold is reached. The default is 1,000,000 entries.
Manual Purge	Select to purge entries logged during the specified period.
Start Date / End Date	Specify a period when purging logs manually. The period begins at 0:00 on the start date and ends at 23:59 on the end date.



To configure with CLI:

```
config ddos global attack-event-purge
   set purge-watermark 2000000
end
```

Configuring SNMP trap receivers for remote DDoS attack reporting

You must configure SNMP trap receivers for FortiDDoS attack events separately from the system event trap receivers.

Attack Event Trap Receivers allow you to have separate configurations for each SPP, if necessary. You can configure up-to two SNMP trap receivers per SPP. The same trap receiver can be used by multiple SPPs but it must be configured for each SPP.

Before you begin:

- You must have Read-Write permission for Log & Report settings.

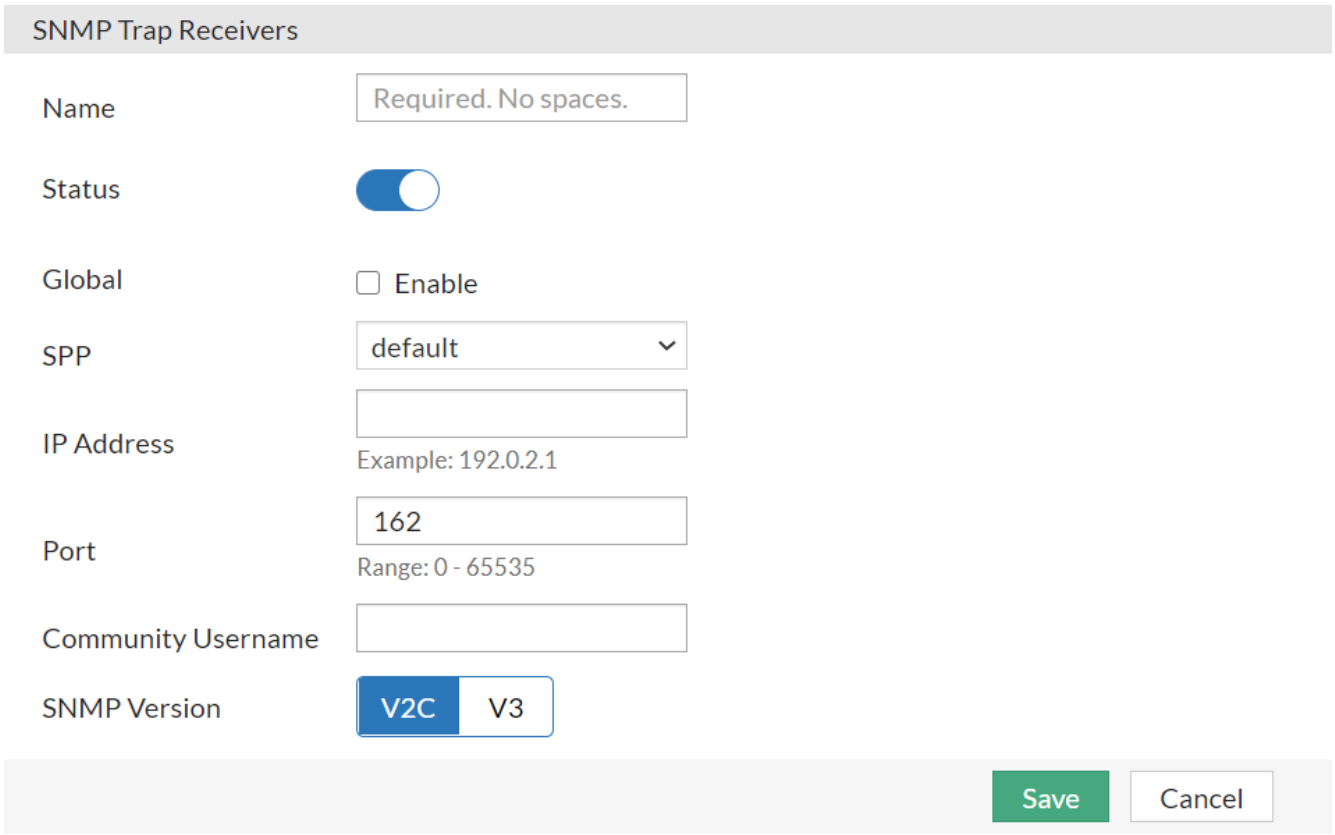
To configure SNMP trap receivers:

1. Go to *Log & Report* > *Log Configuration* > *SNMP Trap Receivers*.
2. Click *Add* to display the configuration editor.
3. Complete the configuration as described in the table below.
4. Save the configuration.

SNMP Trap Receivers configuration guidelines

Settings	Guidelines
Name	Identifies this SNMP trap receiver in the list of receivers.
Enable	Enable the configuration.
SPP	Select the SPP for the configuration.
IP Address	IP address of the SNMP manager that receives attack log traps.
Port	Listening port of the SNMP manager. The default value is 162.
Community Username	String that specifies the SNMP community to which the FortiDDoS system and the SNMP manager at the specified address belong.
SNMP Version	• v2c • v3
SNMPv3	
Engine ID	ID that uniquely identifies the SNMP agent. If the Engine ID is not entered by the user, the MAC address of the management port is used to generate the Engine ID. For example, if the MAC address is: 08:5b:0e:9f:05:f0, the Engine ID will be: 8000304404085b0e9f05f0 which is the concatenation of the MAC address and Fortinet's IANA-registered Private Enterprise Number: 8000304404. To see the default or user-entered Engine ID, use the CLI command `get snmp engine-id`. The MAC address can be obtained using the CLI command `get system interface mgmt1` which displays information about the management port.
v3 Access Type	Three SNMPv3 security modes are available: • No Authentication • Authentication - enter Authentication Passphrase as required by the SNMP Manager. • Privacy - enter BOTH Authentication and Privacy Passphrases required by the SNMP Manager. The security protocols for SNMPv3 Attack Log Traps are fixed as: • Authentication Protocol is SHA1 (MD5 is not available) • Privacy Protocol is AES (DES is not available)
Authentication Passphrase	If Authentication is required, enter the authentication passphrase required by the SNMP manager.
Privacy Passphrase	If Privacy is required, enter the privacy passphrase required by the SNMP manager. Privacy Mode also requires an Authentication Passphrase.

SNMP trap receiver page



To configure with the CLI:

```
config log setting ddos-attack-snmp-trap-receivers
   edit Attack_trap_receiver
      set status enable
      set spp default
      set ip-address 172.30.153.155
      set community-username public
   next
end
```

Log Access

Using the DDoS attack log table

The DDoS Attack Log table displays the attack event records for the selected SPP or All SPPs. The DDoS Attack Log table is updated every few seconds. It contains a maximum of 1 million events. If the number of events exceeds 1 million, the system deletes the 200,000 oldest events.

Before you begin:

- You must have an administrator account with the System Admin option enabled.

To view and filter the log:

1. Go to *Log & Report* > *Log Access* > *Logs*> *DDoS Attack Log* tab
2. Use the check boxes to select the types of attack events to view.
3. Click *Filter Settings* to display additional filter tools for Date (and Time), Direction, Source IP, Protected IP, Associated Port, Protocol, ICMP Type Code and SPP Policy.
4. Click *OK* to apply the filter.
   You can apply multiple filters. They will each display in the filter area. You can clear any filter by clicking "X" in the filter description or all filters using the *Clear All Filters* button.
   Note: These filters are not persistent. If you leave the DDoS Attack Log page, they will be cleared.

Sample DDoS Attack Log table
[placholder screenshot]

DDoS Attack Log Fields

Column	Example	Description
Event ID	462380959	Log ID
Timestamp	2015-05-05 16:31:00	Log timestamp
SPP ID	0	SPP ID
Source IP	28.0.0.40	Source IP address. Reported only for drops where a single source can be identified as non-spoofed (see Source tracking table).
Protected IP	74.255.0.253	Protected IP address. • For outbound traffic, Protected IP is the Source IP. • For inbound traffic, Protected IP is the Destination IP.
Direction	Inbound	Direction: Inbound, Outbound. • For TCP, this is the direction of the session/connection. • For UDP, this is the direction of the packet.
Protocol	6/tcp	Protocol number/name if assigned. The Protocol field may display a blank value if there is traffic from multiple protocols since FPGA does not report a specific protocol in this scenario.
ICMP type/code	0/8	ICMP type/code number
Event Type	SYN flood	Event type
Associated port	69	Associated port number. • For TCP, this is the Associated Port of the session or connection (not the traffic direction). If the session originates or terminates on a 'service port' (<10000), all the traffic in any direction will be associated with that Port.

Column	Example	Description
		• For UDP, this is the destination port in the direction of the traffic UNLESS the traffic originates or terminates on a 'service port' (<10000 or a defined UDP Service Port in *Global Settings* > *Settings* > *UDP Service Ports*). In this case, 'Associated Port' will show the service port, regardless of the traffic direction.
Drop Count	14	Packets dropped per this event.
Operating Mode	Prevention	Prevention or Detection Mode depending on the SPP Setting when the log was generated. Note: Since this indicator was not available prior to 5.2.0, any logs from dates prior to 5.2.0 installation will display “Prevention” no matter what the actual Mode was at that time.
Event Detail	'500'	Reason string. This will be the hash index for HTTP.
Subnet ID	0	Subnet ID

Note: In the DDoS attack log, a table cell displays ”-” (hyphen or a blank) if data is not collected or invalid or multiple values for the same field occur in the same event.

The table displays most recent records first and the columns Event ID, Timestamp, SPP ID, Direction, Event Type and Drop Count. By default, the DDoS Attack Log table displays 10 years of events or the maximum allowed under Log Purge Settings (Default 1M, max 2M). To view the details of an Event, click the Preview icon at the right end of any line.

See Appendix A: DDoS Attack Log Reference for details on log categories and event types.

Using the event log table

The Event log table under *Log & Report* > *Log Access* > *Logs* and *FortiView* > *Logs* > *Event Log* tab displays logs related to system-wide status and administrator activity.

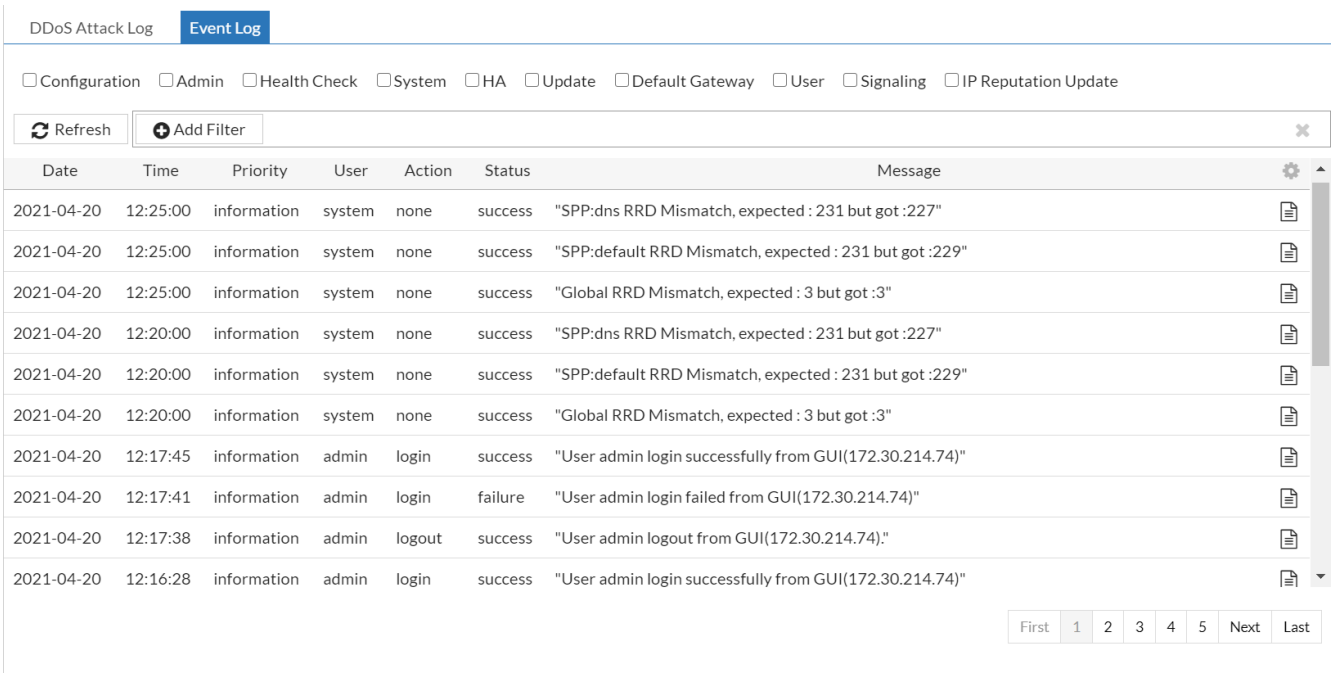
Before you begin:

- You must have enabled local logging. See Configuring local log settings.
- You must have Read-Write permission for Log & Report settings.

To view and filter the log:

1. Go to *Log & Report* > *Log Access* > *Logs* > *Event Log*
2. Click **Filter Settings** to display the filter tools.
3. Use the tools to create filter logic.
4. Click **Apply** to apply the filter and redisplay the log.

Event log table



Event log fields

Column	Example	Description
Date	2015-05-04	Log date
Time	15:50:37	Log time
Log ID	1005081	Log ID
Type	event	Log type: event
Sub Type	config	Log subtype: config, admin, system, ha, update, healthcheck, vserver, router, user, antidos.
Priority	information	Log level
Msg ID	36609	Message ID
User	admin	User that performed the operation
UI	GUI(172.30.153.4)	User interface from which the operation was performed
Action	none	Administrator action
Status	success	Status of the event
Message	"changed settings for 'ddos spp threshold-adjust' on domain 'SPP-0'"	Log message

Note: By default, this table displays the most recent records first and all columns. If no filters or check boxes are selected, the table displays data from the last 10 years. This the default filter applied internally.

- You can click a column heading to display controls to sort the rows or show/hide columns.
- You click a row to select a record. Log details for the selected event are displayed below the table.

- You can use the Filter Settings controls to filter the rows displayed in the table based on event type, severity, action, status, and other values.

Attack Log Backup

You can download the DDoS Attack Log collection, which you may want to do if you are following manual procedures for storing log data or a manual process for purging the local log.

The download file is a MySQL export. You can import it into a MySQL database server to rebuild the flg database, including the dlog table.

Before you begin:

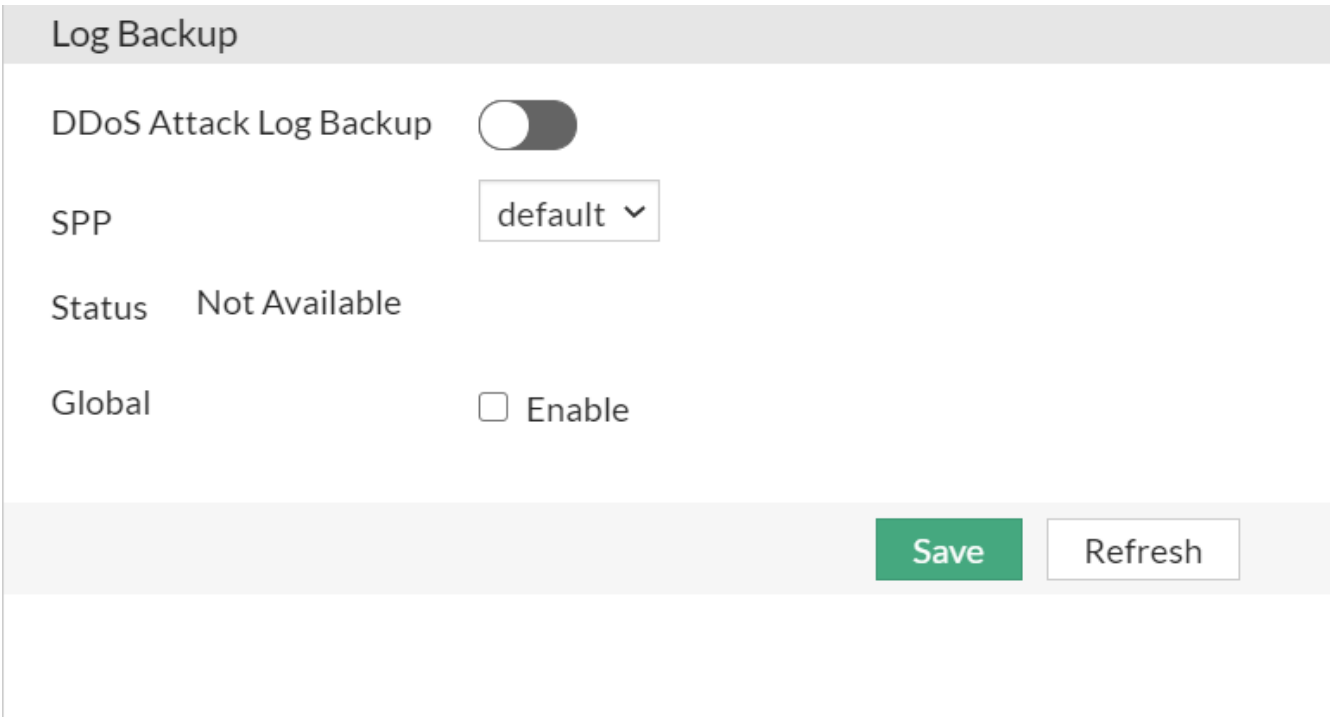
- You must have Read-Write permission for Log & Report settings.
- You must have SQL database expertise.

To download collected logs:

1. Go to *Log & Report* > *Log Access* > *Log Backup*.
2. Enable *DDoS Attack Log Backup*.
3. Select *SPP* from dropdown.
4. Click *Save* to start the backup process.
5. Click *Refresh* to check whether the backup is complete.
6. Click *Download*.

Note: For HA Active-Passive pairs, this procedure can be done on the Primary node. To do this on the Secondary node, you must change the Secondary from Active-Passive to Standalone mode, then follow the procedure above and return the Slave to Active-Passive Mode. Go to *System* > *High Availability* > *Configured HA Mode* setting to change Standalone/Active-Passive mode.

Log backup



Login Events

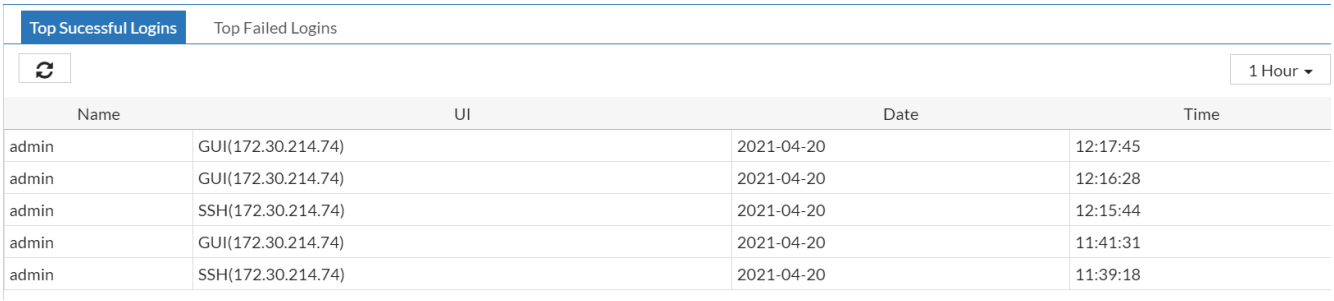
The Event Log dashboard which shows information about the following:

- Top Successful Logins
- Top Failed Logins

To view Event logs:

1. Go to *Log & Report* > *Log Access* > *Login Events*.

Login Events



Name	UI	Date	Time
admin	GUI(172.30.214.74)	2021-04-20	12:17:45
admin	GUI(172.30.214.74)	2021-04-20	12:16:28
admin	SSH(172.30.214.74)	2021-04-20	12:15:44
admin	GUI(172.30.214.74)	2021-04-20	11:41:31
admin	SSH(172.30.214.74)	2021-04-20	11:39:18

Reports

Reports Overview

FortiDDoS F-Series supports on-demand or on-schedule attack and event reports. The report content will look very similar to the *Dashboard* > *Top Attacks GUI* page.

Generated reports will be stored in the Report Browse page and can be simultaneously emailed, when scheduled.

Stored Reports can be automatically purged when storage reached a watermark or can be manually purged by start/end date.

All reports are currently Global – for all SPPs.

Configuring reports

The report generator enables you to configure report profiles that can be run on demand or automatically according to a schedule you specify. The report generator is typically used to generate reports that can be distributed to subscribers or similar stakeholders who do not have administrative access to the FortiDDoS system. You can configure profiles that include system event data, DDoS attack data, or both.

Top attack categories are ranked by drop count (highest to lowest).

The following attack categories are available within any Report:

- Top Attacks - Drop count by DDoS attack event type.
- Top ACL Attacks - Drop count by ACL rules.
- Top Attackers - Drop count by Source IP address.
- Top Attacked Subnets - Drop count by Protected Subnet.
- Top ACL Subnets - Drop count by ACLs associated with Protected Subnets.
- Top Attacked Protocols - Drop count by Protocol.
- Top Attacked TCP Ports - Drop count by TCP port.
- Top Attacked UDP Ports - Drop count by UDP port.
- Top Attacked ICMP Type Codes - Drop count by ICMP Type / Code.
- Top Attacked HTTP URLs - Drop count by HTTP URL (hash index).
- Top Attacked HTTP Methods - Drop count by HTTP method.
- Top Attacked HTTP Hosts - Drop count by Host header (hash index).
- Top Attacked HTTP Referers - Drop count by Referer header (hash index).
- Top Attacked HTTP Cookies - Drop count by Cookie header (hash index).
- Top Attacked HTTP User Agents - Drop count by User-Agent header (hash index).
- Top Attacked HTTP Servers - Drop count by HTTP server IP address.
- Top Attacked Destinations - Drop count by Destination IP address.
- Top Attacked SPPs - Drop count by SPPs.
- Top Attacked ACL SPPs - Drop count by ACL SPPs.
- Top Attacked DNS Servers - Drop count by DNS server IP address (destination Port 53).
- Top Attacked DNS Anomalies - Drop count due to anomalies by DNS server IP address (destination port 53).

Top Event Reports:

- Top Successful Logins
- Top Failed Logins

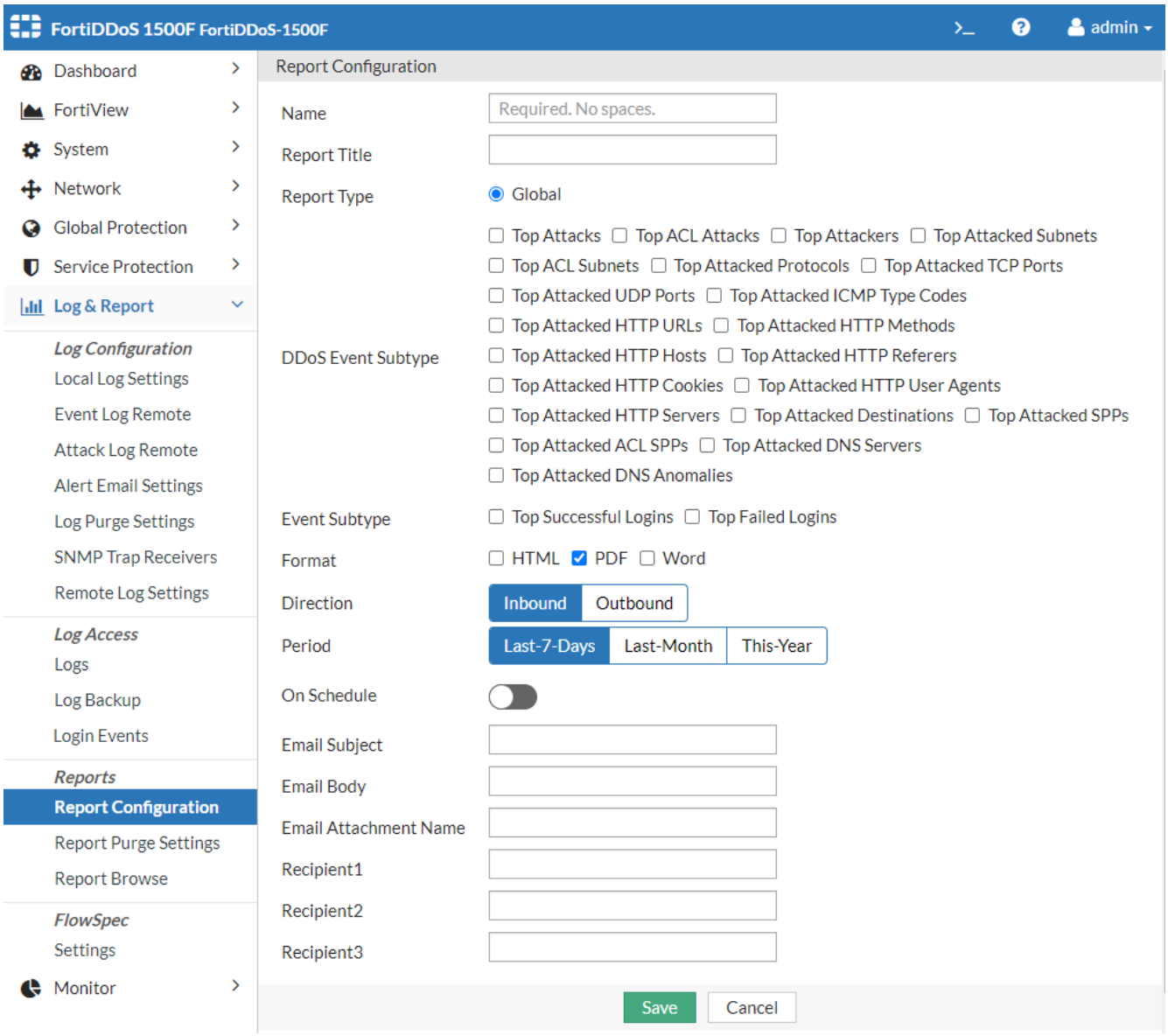
Before you begin:

- You must have Read-Write permission for Log & Report settings.
- You must have enabled local logging for system events if you want to generate system event reports.
- If you intend to email reports, you must have configured *Log & Report > Alert Email Settings*.

To configure Reports:

1. Go to *Log & Report > Report Configuration* and click *Create New*.
2. Configure the Report according to the table below.

Setting	Description
Name	Required. No spaces.
Report Title	Optional
Report Type	Global report type
DDos Event Subtype	Select at least one
Event Subtype	Optional
Format	Format of the report • HTML – Report saved as a web page • PDF - Report saved in PDF format • Word - Report saved in RTF format
Direction	Inbound (default) or outbound
Period	Last 7 days, last month, or last year
On Schedule	Enable if you want to make it a regular report. Schedule types: • Daily - Select the hour each day when you want the report to run • Weekdays - Select the day(s) of the week when you want the report to run • Dates - Select the day(s) of the month when you want the report to run • Hourly - Report will run every hour 7x24
Email settings	If you want to email the reports, complete the email fields: • Email subject • Email body (optional) • Email attachment name (optional) • Recipient 1, 2, 3 - you will need to use aliases to send to more than 3 recipients.


FortiDDoS 1500F FortiDDoS-1500F
admin
Dashboard
FortiView
System
Network
Global Protection
Service Protection
Log & Report
Log Configuration
Local Log Settings
Event Log Remote
Attack Log Remote
Alert Email Settings
Log Purge Settings
SNMP Trap Receivers
Remote Log Settings
Log Access
Logs
Log Backup
Login Events
Reports
Report Configuration
Report Purge Settings
Report Browse
FlowSpec
Settings
Monitor
Report Configuration
Name
Required. No spaces.
Report Title
Report Type
Global
DDoS Event Subtype
Top Attacks
Top ACL Attacks
Top Attackers
Top Attacked Subnets
Top ACL Subnets
Top Attacked Protocols
Top Attacked TCP Ports
Top Attacked UDP Ports
Top Attacked ICMP Type Codes
Top Attacked HTTP URLs
Top Attacked HTTP Methods
Top Attacked HTTP Hosts
Top Attacked HTTP Referers
Top Attacked HTTP Cookies
Top Attacked HTTP User Agents
Top Attacked HTTP Servers
Top Attacked Destinations
Top Attacked SPPs
Top Attacked ACL SPPs
Top Attacked DNS Servers
Top Attacked DNS Anomalies
Event Subtype
Top Successful Logins
Top Failed Logins
Format
HTML
PDF
Word
Direction
Inbound
Outbound
Period
Last-7-Days
Last-Month
This-Year
On Schedule
Email Subject
Email Body
Email Attachment Name
Recipient1
Recipient2
Recipient3
Save
Cancel

To configure with CLI:

```
config log report
   edit DailyLastMonth
      set title "FortiDDoS Report"
      set ddos-event-subtype top_attacks top_acl_attacks top_
           attackers
      top_attacked_http_methods top_attacked_tcp_ports top_attacked_
           udp_
      ports top_attacked_icmp_type_codes
      set event-subtype top_successful_logins top_failed_logins
      set direction
      set period-relative
      set email-subject "Report_111"
      set email-body "This is a report generated by FortiDDoS"
      set email-attachname FDD_111_report
      set recipient1 admin@abc.com
   next
end
```

Configuring report purge settings

Report purging is the deleting of report files to preserve log space and maintain log system performance. By default, DDoS report files are purged on a first-in, first-out basis when the disk allocation for reports reaches 10 GB.

Report purge settings are configurable. You can specify a different threshold, and you can purge reports manually.

Before you begin:

- You must have Read-Write permission for Log & Report settings.

To configure purge settings:

1. Go to *Log & Report* > *Report Purge Settings*.
2. Complete the configuration as described in the table below.
3. Save the configuration

Report purge settings configuration guidelines

Settings	Guidelines
Automatic Purge	Select to automatically purge reports when the disk allocation is reached.
Purge Watermark (in GB)	Purge the earliest reports when this limit is reached. The default is 10 GB. The valid range is 1-48 GB.
Manual Purge	Select to purge reports that were generated during the specified period manually.
Start Date / End Date	Specify a period when purging reports manually. The period begins at 0:00 on the start date and ends at 23:59 on the end date.

CLI commands:

```
config ddos global report-purge
   set automatic-report-purge {enable | disable}
   set report-purge-watermark <watermark_int>
   set purge-now {enable | disable}
   set purge-start-date <purge_date_str>
   set purge-end-date <purge_date_str>
end
```

Using Report Browse

Log & Report > *Report Browse* is a list of generated reports (scheduled or on demand). You can use the report browser to view the reports or delete them from the system. The attack categories and types reported correspond with the DDoS Attack log categories and event types. Refer to DDoS attack log table for descriptions.

Reports are named similarly to these examples:

- Global-On-Demand-[report Name]-2021-04-12-14-07-20
- Global-On-Scheduled-[report Name]-2021-04-11-00-00-00

Before you begin:

- You must have Read-Write permission for Log & Report settings.

To view or delete reports:

1. Go to **Log & Report** > **Report Browse**.
2. Select the device from the top-right device selection button.
3. Click the report title to view or the delete link to remove it.

Configuring Flowspec

FortiDDoS can create Flowspec configuration scripts based on FortiDDoS attack information. The Flowspec scripts can be entered in Cisco and Juniper routes to create Flowspec-based ACLs, which are more fine-grained than traditional Remotely-Triggered-Black-Hole IP Addresses. The standard scripts may also work with other routers supporting Flowspec.

Depending on the type of attack seen, the script may include Destination IP, Destination Port, Protocol, Fragment and/or ICMP Type/Code. The full list of supported items from RFC 5575 is detailed below.

Before you begin:

- You must have Read-Write permission for Log & Report.

To create a Flowspec script:

1. Go to **Log & Report** > **Flowspec Settings**.
2. Select the FortiDDoS device from the top-right device selection button.
3. Complete the configuration as described in the table below.
4. **Save** the configuration. The **Report Status** field displays the date and time this or last script was generated. **Note**: You must save the current setting before you download the script. Download without saving will download the previous script which remains in the memory until replaced.
5. Click **Download** under **Report Status** to save the generated script to the device.

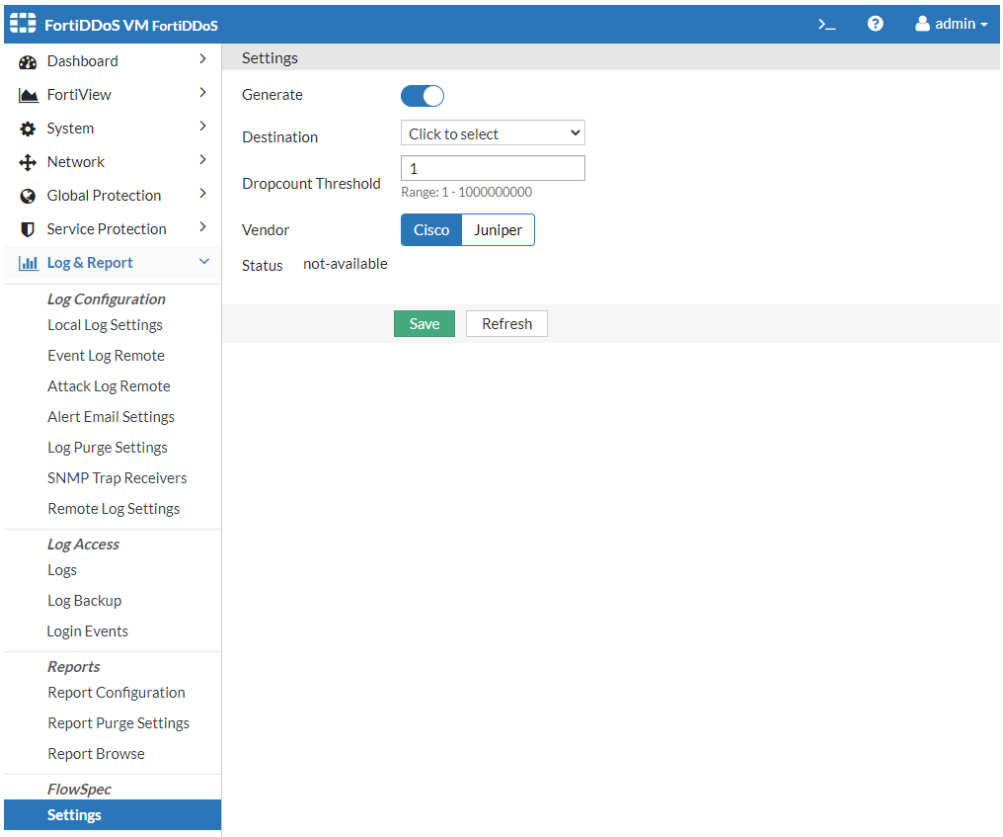
To use the generated Flowspec script:

- The script can be cut and pasted directly into the CLI of the edge/peering router to create a Flowspec ACL.
- You can determine whether the traffic filtering action will be rate-limit, re-direct or other action supported by the routers.

Flowspec configuration settings

Settings	Guidelines
Generate	Enable to allow script generation.
Destination	Select the protected Destination IP address from the drop-down.
Dropcount Threshold	Many large attacks are multi-vector. Since FortiDDoS sees even single-drop events, selecting a Destination IP address and creating a script for the last hour's attacks could result in very long and confusing scripts. The Dropcount Threshold limits the creation of scripts to only those attacks that exceed the entered Threshold. This Threshold should be set to a reasonably high number so you are generating scripts that make sense to use on the edge router – generally attacks that are exceeding the rate limits of the Internet links where FortiDDoS is mitigating. A reasonable Dropcount Threshold is 1,000,000. The Dropcount threshold value is in the range 1-1000000000. The default value is 10.
Vendor	Vendor - Cisco or Juniper
Report Status	Status of the Flowspec script.

Flowspec



Supported Flowspec Parameters

RFC 5575	Juniper	Available
Type 1	Destination prefix	Yes
	Destination prefix-offset	No
Type 2	Source prefix	Yes
Type 3	Protocol number	Yes
Type 5	Destination-port	Yes
Type 6	Source-port	No
	Source prefix-offset	No
Type 7	ICMP-v4/v6-code	Yes
Type 8	ICMP-v4/v-type	Yes
	Source-port	No
	Source prefix-offset	No
Type 9	TCP Flags	Yes
Type 10	Packet-length	Yes

RFC 5575	Juniper	Available
Type 11	DSCP	No
Type 12	**Fragment type**	
	dont-fragment	No
	first-fragment	No
	is-fragment	Yes
	last-fragment	No
	not-a-fragment	Not Explicit

Sample exported scripts:

Cisco

```
configure
class-map type traffic match all block-28.0.1.200-1
match source-address 28.0.0.6/32
match destination-address 28.0.1.200/32
end-class-map
configure
class-map type traffic match all block-28.0.1.200-2
match source-address 28.0.0.7/32
match destination-address 28.0.1.200/32
end-class-map
configure
class-map type traffic match all block-28.0.1.200-3
match source-address 28.0.0.9/32
match destination-address 28.0.1.200/32
end-class-map
```

Juniper

```
flow {
        term-order statndard;
        route block-28.0.1.200-1 {
                match {
                        tmatch source-address 28.0.0.6/32
                        match destination-address 28.0.1.200/32
                }
                then discard;
        }
 }
flow {
        term-order statndard;
        route block-28.0.1.200-2 {
                match {
                        tmatch source-address 28.0.0.7/32
                        match destination-address 28.0.1.200/32
                }
                then discard;
        }
 }
flow {
        term-order statndard;
        route block-28.0.1.200-3 {
                match {
                        tmatch source-address 28.0.0.9/32
                        match destination-address 28.0.1.200/32
```

```
                                }
                                then discard;
                        }
                }
```

Deployment Topologies

This section provides guidelines for basic and advanced deployments. It includes the following:

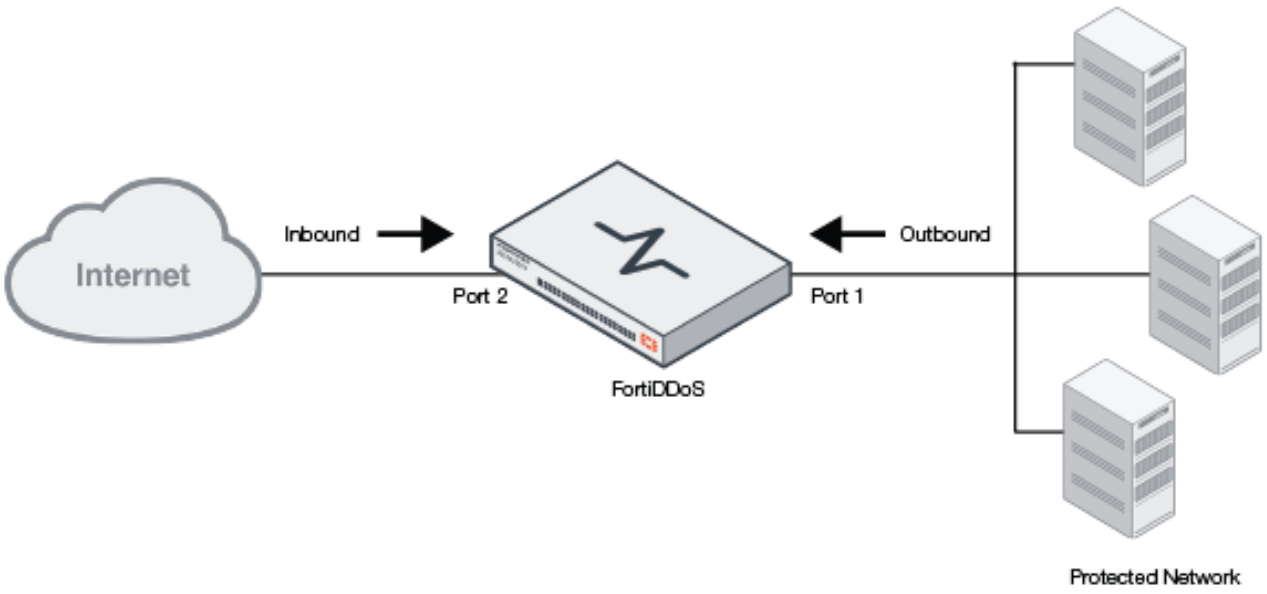
Basic Inline deployment

FortiDDoS is state-aware and bidirectional. The data packet traffic is described as either incoming (inbound) and/or outgoing (outbound).

FortiDDoS may be installed in asymmetric traffic situations where it sees only the inbound traffic for some TCP sessions or UDP flows and only the outbound traffic for others. The settings must be configured for this mode.

The figure below shows a basic inline deployment. The FortiDDoS-F appliance is positioned 'inline', meaning it is installed between the Internet and the protected network.

Basic topology



Built-in fail-open bypass

The following FortiDDoS-F network interface connections have a built-in bypass mechanism:

- Active copper fail-open bypass on copper (RJ-45) network connections 1-8 on FortiDDoS-200F. Fail-open is operation at any speed to 1Gbps but both link speeds must match.
- Active optical fail-open bypass on Ports 13-16 on the FortiDDoS-200F. Ports support GE Short-Range, Multi-Mode fiber only on LC connectors. SFPs are built-in to the chassis.
- Active optical fail-open bypass on Ports 5-8 on the FortiDDoS-1400F. Ports support 10GE Short-Range, Multi-Mode fiber only on LC connectors. SFP+s are built-in to the chassis.
- All other ports on any F-Series model do not support fail-open. An external bypass bridge/switch will be required if extra fail-open ports are needed.

You can use the *Global Protection > Deployment > Deployment tab* to configure the internal bypass mechanism to fail open or fail closed for F-Series appliances.

By default, the interfaces are configured to fail open. This means that interfaces pass traffic through without performing any monitoring or prevention tasks. Packets that arrive at ingress ports are simply transferred to the corresponding egress ports, just like a wire or optical cable.

If you use an external bypass solution, configure the interfaces to fail closed. This means traffic is not forwarded through the interfaces when FortiDDoS fails. An external bypass system detects the outage and routes traffic around the FortiDDoS.

If you deploy an active-passive cluster, configure the interfaces on the primary node to fail closed so the adjacent switches can select the secondary node. The secondary unit can be set to fail closed or fail open, depending on how you want to handle the situation if both FortiDDoS nodes are down.

The table below summarizes bypass behavior for a sequence of system states. During boot up, system processes are started. When boot up is complete the appliance exits the bypass state. Traffic is routed through the system, is monitored, and policies enforced.

In the event of failure, manual or system-caused reboot, system processes are unavailable because they are either being restarted or shut down, and the appliance enters the bypass state.

System state and bypass

User Option	State 1 Power Off	State 2 Just Powered Up	State 3 Boot Up Process	State 4 System Ready	State 5 Failure or Reboot	State 6 Power Off
Fail Open	Bypass	Bypass	Bypass	Traffic Processed	Bypass	Bypass
Fail Closed	Closed	Closed	Closed	Traffic Processed	Closed	Closed

In addition to the automatic bypass settings, the following models support manual bypass with the following CLI command:

```
execute bypass-traffic {enable | disable}
```

This command forces the appliance interfaces to fail open. This command does not have an option to force a fail closed.

Note: If you use the CLI command to initiate bypass, you must use the CLI command to disable that state.

Use carefully since there is currently no status check to confirm the bypass state.

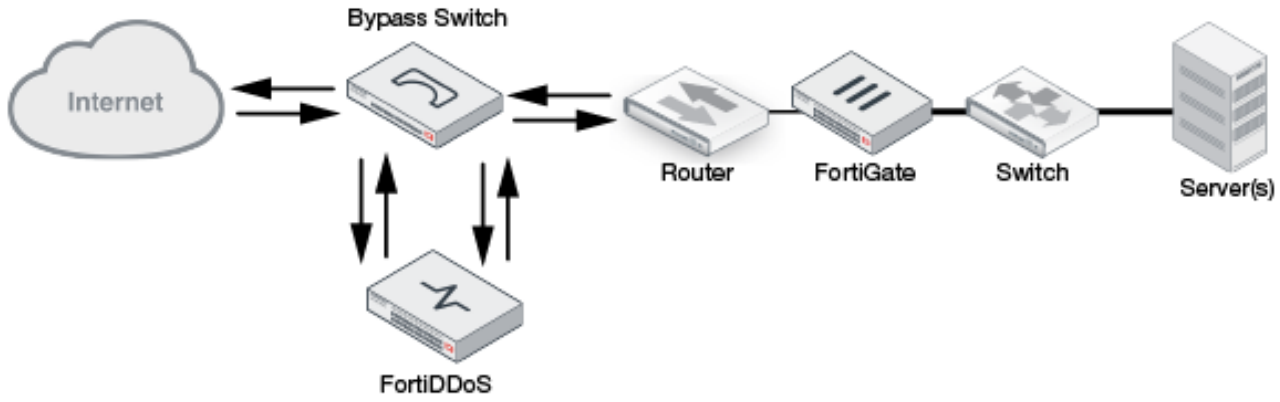
The manual bypass-traffic enable state is not persistent after reboot. If the appliance is rebooted, it will return inline.

External bypass

Most FortiDDoS models offer built-in bypass for at least 2 links. However, FortiDDoS can be deployed with an external bypass mechanism, such as a bypass switch. When both the FortiDDoS-F appliance and the failover switch share the same power supply, external connectivity is maintained during a power failure. Most bypass switches also employ a heartbeat monitor that checks for traffic flow through the FortiDDoS and fails open (fails to bypass) if the heartbeat fails.

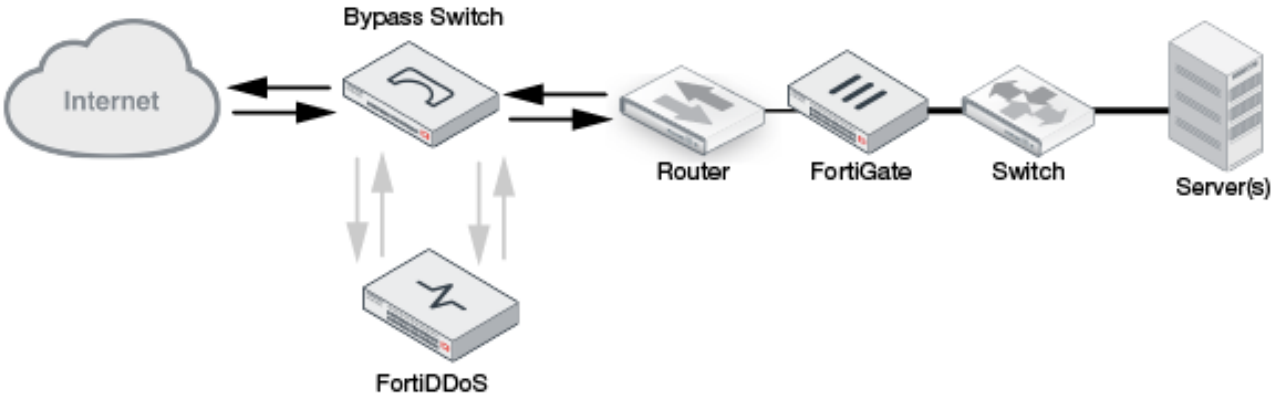
The following figure shows a bypass deployment when bypass is not active. The inline traffic flows through the FortiDDoS-F appliance.

Bypass ready but not active



The following figure shows a bypass deployment when bypass is active. All inline traffic is routed through the switch until FortiDDoS is back online.

Active bypass



When using an external bypass switch with heartbeat, obtain the MAC addresses of the Monitor ports (the ports facing the FortiDDoS) and add them to *Global Protections* > *Deployment* > *Bypass MAC*. This ensures that no heartbeat traffic from/to the bypass switch monitor ports is blocked by FortiDDoS, unless it is not processing any traffic (failure or power down).

Contact your Sales Engineer for recommendations on supported bypass switches.

Tap Mode deployments

This section provides the following information about FortiDDoS Tap Mode deployments:

- Overview
- Deployment Topology
- Requirements
- Limitations
- Configuration
- Best practices

Overview

The FortiDDoS appliance is a transparent Layer 2 bridge that could become a point-of-failure without proper bypass mechanisms. It is possible to deploy a Layer 1 bypass bridge in-path with the FortiDDoS appliance in an out-of-path monitor segment so that you are never faced with outages due to failure, maintenance, or replacement of a FortiDDoS appliance.

Most bypass bridge appliances support inline, bypass, and recovery features. Some bypass bridge appliances also support Tap Mode—a mode in which the Layer 2 bridge can simultaneously perform bypass through its network ports and mirroring through its monitor ports.

FortiDDoS appliances have a complementary Tap Mode setting that turns off the transmit (Tx) component of the FortiDDoS network interface cards. This ensures the FortiDDoS is a passive listener that cannot disrupt traffic or cause an outage.

In a Tap Mode deployment, FortiDDoS can use the mirrored packets to build the traffic history it uses to establish rate thresholds, and it can detect volumetric attacks (rate anomalies), but it does not take actions, like dropping traffic, blocking identified source attackers, or aggressively aging connections.

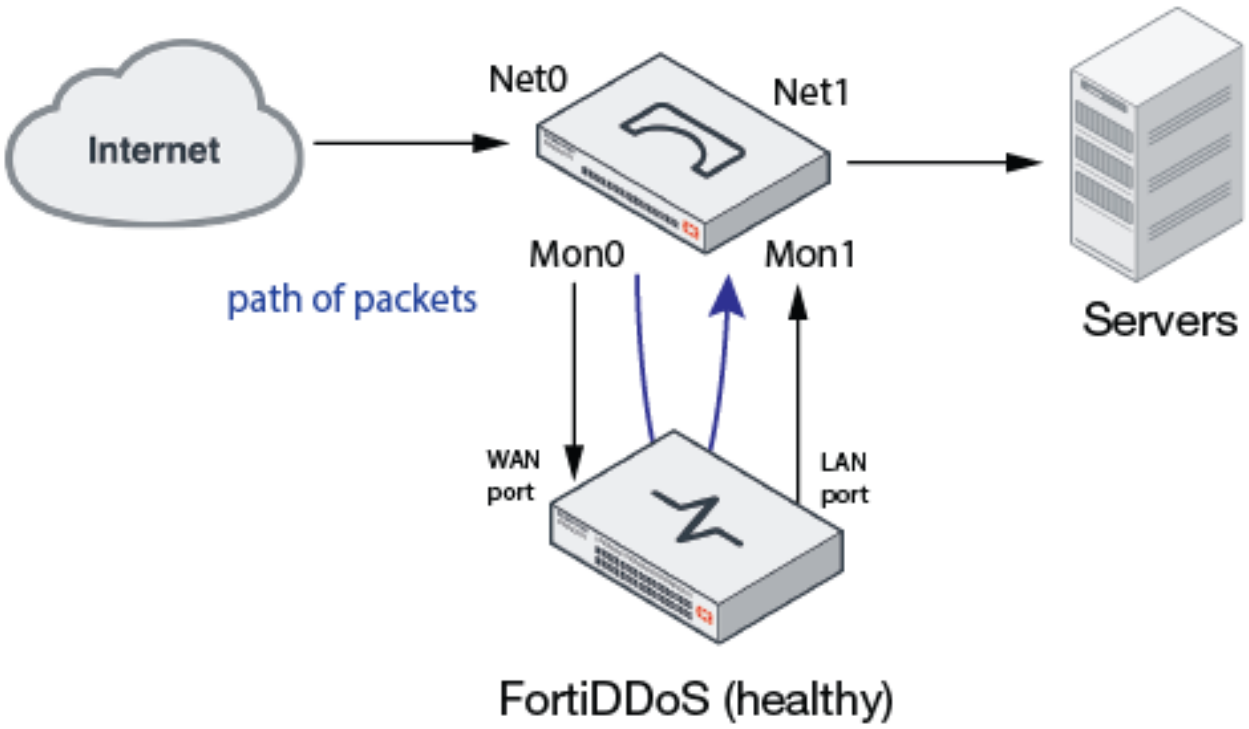
When an attack is detected, you can turn off Tap Mode on FortiDDoS and the FortiDDoS interfaces resume packet transmission. Bypass bridge probes will then pass through FortiDDoS successfully, the bridge will detect that the out-of-path segment is available, and it will switch to Inline Mode.

Deployment Topology

The figure below illustrates how bypass bridge deployment modes are used in a deployment with FortiDDoS. The bypass bridge is deployed in-path and FortiDDoS is deployed out-of-path.

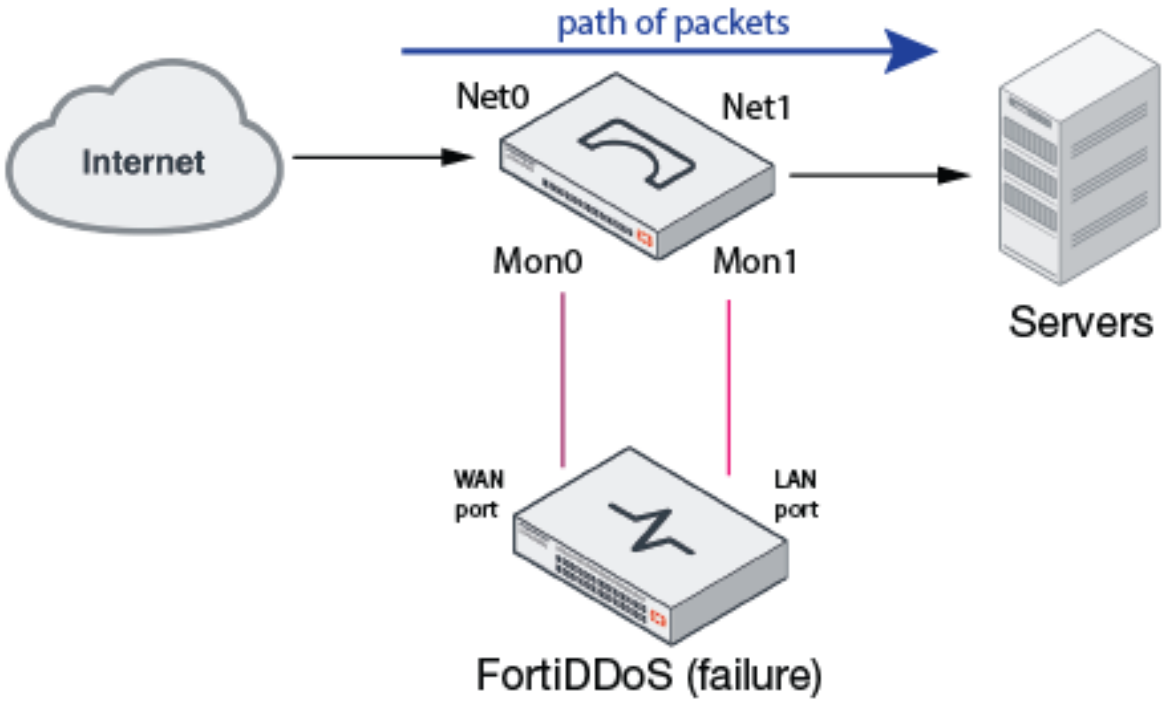
In Inline Mode, the bypass bridge passes heartbeat packets through its monitor ports to detect whether the out-of-path segment is available. When the health probes indicate the path is available, inbound traffic that is received by the bypass bridge Net0 interface is forwarded through the Mon0 interface to the FortiDDoS WAN port. FortiDDoS processes the traffic, takes action on attacks and passes non-attack traffic through its LAN port to the bypass bridge Mon1 interface. The traffic is passed through the bypass bridge Net1 interface towards its destination.

Inline Mode



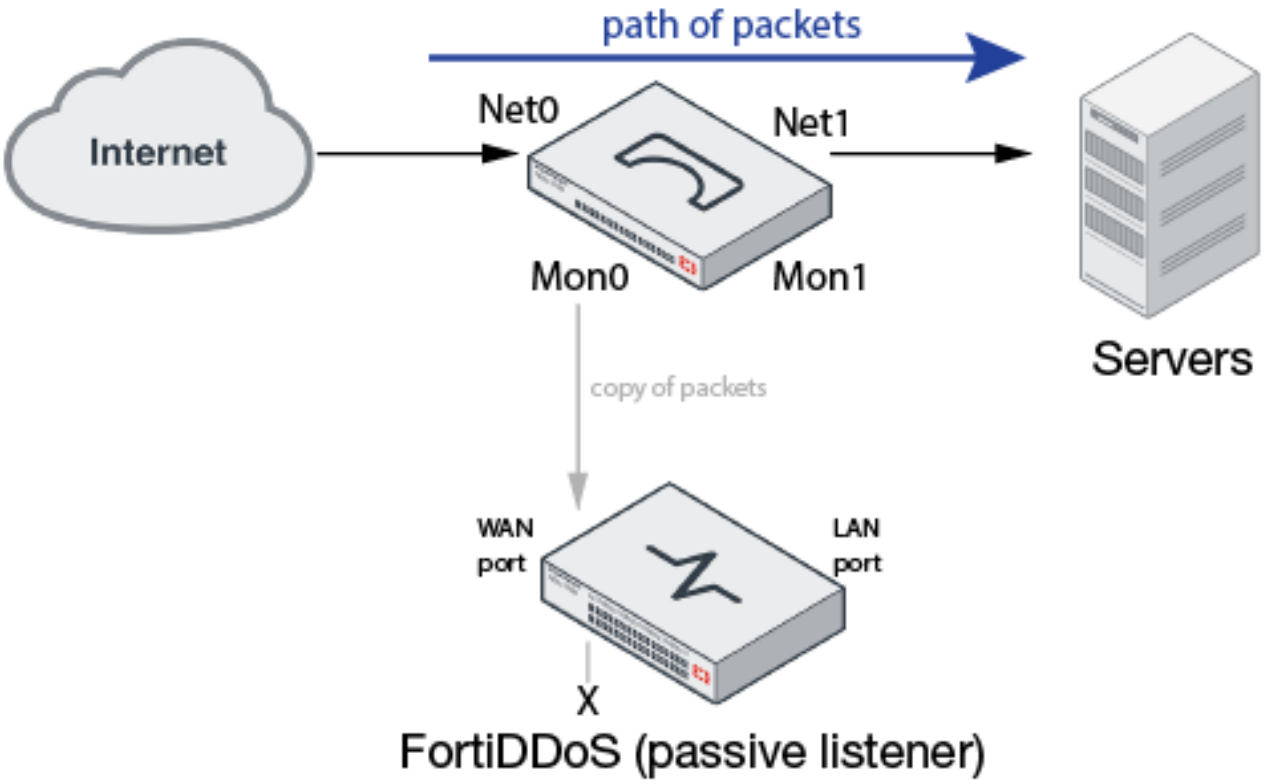
If the heartbeat probe fails due to FortiDDoS failure or maintenance, the bypass bridge can be set up to switch from Inline mode to Bypass mode. In Bypass Mode, traffic is not forwarded through the monitor ports. Instead, it is forwarded from Net0 to Net1, bypassing the out-of-path segment.

Bypass Mode



Alternatively, you can set up some bypass bridge to switch from Inline Mode to Tap Mode when probes fail. In bypass bridge Tap Mode, traffic is forwarded from Net0 to Net1, and it is also mirrored to Mon0. This is what you want when you want to deploy FortiDDoS as a passive listener.

Tap Mode



Although not shown in the illustrations, the reverse paths are processed the same way.

Note: When in Tap Mode, FortiDDoS discards packets after processing (noted by an X in Tap Mode). You should not expect to see egress traffic on the Monitor > Port Statistics graphs.

Requirements

Contact your Fortinet Sales Engineer to learn more about bypass bridges that can operate in this mode.

Fortinet does not support Tap Mode deployments with other bridge or tap devices. If you attempt a deployment with other devices, consider the following Tap Mode requirements:

- The bridge device must be deployed and configured to forward traffic along the data path and send mirrored traffic towards FortiDDoS on both its monitor ports (inbound traffic on one port and outbound on the other).
- The bridge must block any transmit packets from FortiDDoS on its monitor ports so that any traffic sent by FortiDDoS is blocked.
- The bridge device should have the ability to set inline/bypass/tap mode manually so that administrators take direct action when there is an attack.
- FortiDDoS passes heartbeat packets from its ingress to egress ports, so the bridge must not be affected by seeing these heartbeat packets (it will not switch to inline mode).

- Passive optical TAPs will generally not work since the TAPs usually have a single duplex monitor port output on 1 pair of fiber ports. FortiDDoS requires 2 separate monitor ports for inbound and outbound traffic on 2 separate fiber pairs. Custom cabling can support this, but FortiDDoS can never be switched inline using passive TAPs.

Limitations

In Tap Mode, FortiDDoS is a passive listener. It records actions it would have taken were it placed inline, so ACL, anomaly, rate threshold drops, source blocking, and aggressive aging events and statistics are just simulations.

However, some features cannot be simulated when FortiDDoS is a passive listener. The following Prevention Mode features depend on being deployed in-path and interacting with clients and servers to work correctly:

- SYN flood mitigation—With SYN validation enabled, FortiDDoS performs antispoofing tests to determine whether the source is legitimate. In Tap Mode, if the source was not already in the legitimate IP table, it will fail the test. As a result, the simulation is skewed, and the reports will show an inordinate spike in blocked sources.
- TCP state anomaly detection—With Foreign Packet Validation enabled, FortiDDoS drops unexpected packets (for example, if there is a sequence of events in which FortiDDoS drops inbound packets, it does not expect to receive corresponding outbound packets, so a foreign packet drop event is triggered).
- Aggressive aging—Aggressive aging resets are not actually sent when slow connection attacks and Layer 7 floods are detected, but the connections are cleared from the TCP state table. As a result, subsequent packets for the connection are treated as foreign packets.

Talk with your Fortinet CSE to make sure you thoroughly understand your choices, which include:

- Disabling TCP session feature control when FortiDDoS is deployed in Tap Mode. (But remember to enable it if you want its protections when you FortiDDoS is deployed inline.)
- Interpreting or disregarding the logs and graphs for these anomalies.

Tap Mode is not a perfect deployment simulation, but it does enable you prepare for volumetric attacks by building traffic history without risk of disruption or outage.

Configuration

We recommend you set up the bypass bridge to Inline Mode with action on failure set to Tap Mode; and then force a failure by turning on FortiDDoS Tap Mode.

FortiDDoS configuration guidelines

This section gives pointers for FortiDDoS configuration.

Before you begin:

- Physically connect FortiDDoS to the bypass bridge.

You must add the MAC addresses for the bypass bridge Monitor ports (if available) so that FortiDDoS accepts heartbeats from them. Heartbeats are used when the bypass bridge is in Inline Mode.

To configure bypass MAC addresses:

1. Go to *Global Protection* > *Deployment* > *Bypass MAC*.
2. Click *Add*, and then enter a name for the MAC address and the address.
3. Save the configuration.

To enable Tap Mode:

1. Go to *Global Protection* > *Deployment*.
2. Enable *Tap Mode*.
3. Save the configuration.

Note: The system reboots when you enable/disable Tap Mode.

```
config ddos global deployment
   set tap-mode {enable|disable}
end
```

Best practices

The following are recommended best practices:

- Do not set the bypass bridge Tap Mode manually. Set it up as the action on failure for the bypass bridge Inline Mode and then force a failure of the out-of-path segment by turning on FortiDDoS Tap Mode.
- In a FortiDDoS Tap Mode deployment, you can set SPPs in Detection Mode or Prevention Mode. Set it to whichever mode you want enabled when you toggle off Tap Mode and put FortiDDoS inline.

Troubleshooting

This section includes the following information:

Logs

Log messages often contain clues that can aid you in determining the cause of a problem.

Depending on the type, log messages may appear in either the system event logs or the DDoS attack logs. To enable logging of different categories of system events, go to Log & Report > Log Configuration > Local Log Settings. All DDoS attack log categories are enabled automatically and cannot be disabled.

During troubleshooting, you might find it useful to lower the logging severity threshold for more verbose logs, to include more information on less severe events. To configure the log level, go to Log & Report > Log Configuration > Local Log Settings.

Tools

This section describes the following troubleshooting tools:

- execute commands
- diagnose commands
- Special Fortinet Support commands
- get command

execute commands

You can use the command-line interface (CLI) execute commands to run diagnostic utilities, such as nslookup, ping, and traceroute.

Execute Commands	Description
`backup`	Backup: • system configuration • Domain Blocklist • IPv4 Blocklist • diagnostics information • mysql database to a tftp server
`backupextdisk`	Backup FortiDDoS information to external USB disk
`bypass-traffic`	Enable or Disable internal bypass data traffic
`checklogdisk`	Find and correct errors on the log disk
`cleanup-db-transaction-log`	Cleanup database transaction log files
`date`	Set system date and time
`domain-blocklist` (6.2.0)	Domain-blocklist related operations such as upload/download domain-blocklist file, append/delete/search/merge domain-blocklist, and reset
`factoryreset`	Reset system to factory default
`formatextdisk`	Format external USB disk
`formatlogdisk`	Format log disk to enhance performance
`fortiguard-database-update`	Update fortiguard-database
`generate-traffic-stats`	SPP generate traffic statistics
`global-rrd-reset`	Reset global RRDs in case of Interface and other global related chart mismatch
`ipv4-blocklist` (6.2.0)	IPv4-blocklist related operations such as upload/download IPv4-blocklist file, append/delete/search/merge IPv4-blocklist, and reset
`mountextdisk`	Mount external USB disk
`nslookup`	Test DNS server to obtain domain name or IP address mapping
`passphrase`	Generate backend password
`ping`	Send ICMP ECHO_REQUEST to network hosts with IPv4 address: ping <host name | host ipv4>
`ping-option`	ping option settings
`ping6`	Send ICMP6_ECHO_REQUEST to network hosts with IPv6 address: ping6 <host ipv6>
`ping6-option`	ping6 option settings
`reboot`	Reboot the system

Execute Commands	Description
`reload`	Reload appliance
`repair-database-tables`	Repair database tables
`reset` (6.1.1) Replaced with `domain-blocklist` in 6.2.0	Clear/delete: • IPv4 Blocklist • Domain Blocklist
`restore`	Restore image or configuration from tftp or ftp server
`restoreextdisk`	Restore from external USB disk
`rrd-reset`	Reset all global and SPP RRDs
`shutdown`	Shutdown appliance
`spp-factory-reset`	Reset the threshold configuration and clear traffic history for an SPP
`spp-rrd-reset`	Reset RRDs of a specific SPP in case of SPP related chart mismatch
`telnet`	Simple telnet client
`telnettest`	Test if we can telnet to a server
`thresholds-emergency-setup`	SPP emergency setup thresholds to adjust only certain key thresholds based on empirical knowledge
`thresholds-factory-defaults`	Reset the threshold configuration for an SPP
`traceroute`	Display possible routes (paths) to destination host
`unmountextdisk`	Unmount external USB disk
`vmware`	Upload license file from tftp server only for VM

diagnose commands

You can use the CLI diagnose commands to gather diagnostic information that can be useful to Fortinet Customer Care when diagnosing any issues with your system.

The following examples show the lists of diagnose commands:

```
FIVM08TM20090022 # diagnose
blocklisted blocklisted
dataplane dataplane
debug debug
hardware hardware
netlink netlink
sniffer sniffer
system system

FIVM08TM20090022 # diagnose debug
rrd_cmd_check Perform RRD commands check
rrd_cmd_recreate Re-create RRD commands
```

```
FIVM08TM20090022 # diagnose hardware get
deviceinfo list device status and information

FIVM08TM20090022 # diagnose sniffer packet any
interfaces=[any]
filters=[none]
pcap_lookupnet: any: no IPv4 address assigned
0.000000 172.30.144.11.62729 -> 172.30.153.113.22: ack 1556045916
0.000000 172.30.144.11.62729 -> 172.30.153.113.22: ack 1556046032
0.000000 172.30.153.17.68 -> 255.255.255.255.67: udp 300
```

Special Fortinet Support commands

The commands described in this section are useful when you are troubleshooting an issue with the help of Fortinet Technical Support. Your Fortinet contact might ask you to run these commands to gather data they need to troubleshoot system issues.

execute backup diag_info

This command exports diagnostic information to a remote TFTP server. The following information is exported:

- System status
- Current configuration
- Hardware register values
- Event and DDoS attack log database

Use the following command syntax:

execute backup diag_info tftp <tftp_server_ipaddress>

The filename generated stems from the appliance serial number and date. For example, `diag_info-FIVM08TM20090022-2015-03-07-16-57.tgz`.

The archive includes four files with filenames similar to the following:

back_status-FIVM08TM20090022-2015-03-07-16-57

back_cfg-FIVM08TM20090022-2015-03-07-16-57

back_hw_reg-FIVM08TM20090022-2015-03-07-16-57

back_logs-FIVM08TM20090022-2015-03-07-16-57.tgz

The logs archive includes four files with filenames similar to the following:

elog@002e0000000001.MAI

elog@002e0000000001.MAD

dlog.MAI

dlog.MAD

Solutions by issue type

This section includes the following topics:

Management Port Connectivity issues

One of your first tests when configuring a new FortiDDoS should be to determine whether management device can reach FortiDDoS management ports.

If your management device cannot reach FortiDDoS and you have followed the Quick Start Guide instructions to set Management Port IP addresses, static-routes/gateway and DNS, first check hardware connectivity.

- Ensure the network cables are properly plugged into the correct management port(s) on the FortiDDoS appliance.
- Ensure there are connection lights for the management port(s) on the appliance.
  - If not, change the cable if the cable or its connector are damaged or you are unsure about the cable's type or quality.
  - Ensure the attached device Ethernet port is set to AUTO
  - Connect the FortiDDoS-F appliance to different hardware to see if that makes a difference.
- In the web UI, select Network > Interface > Management Ports tab and ensure that the Config Status and Link Status indicators for the ports that are in use are green (indicating that physical connections are present

If the hardware connections are correct, and the appliance is powered on but you cannot connect using the CLI or web UI, check routing policies.

You can ping and traceroute to FortiDDoS or from a FortiDDoS management port(s) to check routing paths.

CLI commands:

```
execute ping | ping6 | ping-option | ping6-option
```

- Use ping-option to set the management port IP you wish to ping from. By default system will ping from management port 1.

```
execute traceroute
diagnose sniffer packet {any|mgmt1|mgmt2}
```

- Allows you to watch packets to and from the management ports

```
diagnose netlink route list
```

- Show you current routing table.

Data path connectivity issues

FortiDDoS data ports have no IP nor MAC addresses in the data path. Ping and Traceroute will not work to or from these ports.

Ping or Traceroute through the FortiDDoS from an outside client to inside server (or the reverse) should be totally transparent. (See bypass/fail-open below.)

For connectivity issues, first check that front panel port LEDs are green and flashing(?) when connected. If not, there is a physical connectivity issue or the appliance is in forced bypass/fail-open mode. Use CLI execute bypass-traffic disable to ensure the appliance is inline.

Check the FortiDDoS GUI *Network* > *Interfaces* > *Traffic Ports* to confirm that the traffic ports are configured “up” and the link status is “up” (connected).

Check that FortiDDoS and the connected devices are all set the same where there are speed/duplex settings. For example, the upstream and downstream devices and both traffic ports on the FortiDDoS must be set to Auto for 1000BT copper ports. If an attached device port is set to 1000Full, for example, the connection will revert to half-duplex, which may not exhibit problems until traffic becomes high. Also, remember that in bypass/fail-open mode the attached equipment is now negotiating directly, without FortiDDoS in the path. To test this and to test that FortiDDoS is not impeding traffic use CLI execute-bypass enable to remove FortiDDoS from that path of 1000BT GE links and the GE Optical LC links. If connectivity still fails the issue is in the physical cabling or the port settings on the connected devices.

Resource issues

If the system resource usage appears to be abnormally high according to the *Dashboard* > *Status: System Resource* widget or the CLI command `get system status`, you can view the current consumption by each process by entering this CLI command:`diagnose system top delay 10`.

The above command generates a list of processes every 10 seconds. It includes the process names, their process ID (pid), status, CPU usage, and memory usage.

The report continues to refresh and display in the CLI until you press `q` (quit).

If the issue recurs, and corresponds with a hardware or configuration change, you might need to change the configuration. Look especially into reducing frequent logging. If the issue persists, contact Fortinet Technical Support.

Resetting profile data or the system configuration

The following table summarizes 'factory reset' options.

'Factory reset' options

Task	Menu
Reset the threshold configuration for an SPP but do not clear traffic history. You might do this if you are conducting a demonstration or test, or you are troubleshooting an issue; or if you want to start over with a new learning period in Detection Mode and start with high thresholds that will not drop traffic.	See Restoring factory default threshold settings.
Reset the threshold configuration for an SPP and clear its traffic history. You might do this if characteristics of the traffic protected by an SPP change significantly (for example, you change which server or protocol that it protects).	See Performing a factory reset of SPP settings.
Reset the system to the factory state. All SPPs, statistics, and logs will be deleted. You might do this if you are selling your FortiDDoS appliance.	See Resetting the system.

Important: Before you perform a factory reset:

- Make a backup of the current configuration.
- Be ready to reconfigure the default gateway and IP address of the network interface that is used for connections to the web UI and CLI.
- Do not shut down the appliance while it is resetting.

Restoring firmware ('clean install')

Restoring (also called re-imaging) the firmware can be useful in the following cases:

- You are unable to connect to the FortiDDoS-F appliance using the web UI or the CLI
- You want to install firmware *without* preserving any existing configuration (that is, perform a “clean install”)

Unlike updating firmware, restoring firmware re-images the boot device. Also, restoring firmware can only be done during a boot interrupt, before network connectivity is available, and therefore requires a local console connection to the CLI. It cannot be done through an SSH or Telnet connection.

Note: This is only valid for hardware models and not for VM. If VM is unresponsive and all troubleshooting steps fail, user can deploy new VM and load the license file.

Alternatively, if you cannot physically access the appliance’s local console connection, connect the appliance’s local console port to a terminal server to which you have network access. Once you have used a client to connect to the terminal server over the network, you will be able to use the appliance’s local console through it. However, be aware that from a remote location, you may not be able to power cycle the appliance if abnormalities occur.

Important: Back up the configuration before completing a clean install.

To restore the firmware

1. Download the firmware file from the Fortinet Technical Support website.
2. Connect your management computer to the FortiDDoS-F console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.
3. Initiate a local console connection from your management computer to the CLI of the FortiDDoS-F appliance, and log in as the `admin` administrator.
4. Connect the MGMT1 port of the FortiDDoS-F appliance directly or to the same subnet as a TFTP server.
5. Copy the new firmware image file to the root directory of the TFTP server.
6. If necessary, start your TFTP server. (If you do not have one, you can temporarily install and run one such as `tftpd` on your management computer.)

TFTP is not secure, and it does not support authentication. You should run it only on trusted administrator-only networks, and never on computers directly connected to the Internet. Turn off tftpd off immediately after completing this procedure.

7. Verify that the TFTP server is currently running, and that the FortiDDoS-F appliance can reach the TFTP server. To use the FortiDDoS-F CLI to verify connectivity, enter the following command:
   `execute ping 192.168.1.168`
   where `192.168.1.168` is the IP address of the TFTP server.
8. Enter the following command to restart the FortiDDoS-F appliance: `execute reboot`
   As the FortiDDoS-F appliances starts, a series of system startup messages appear.
   `Press any key to display configuration menu.....`
9. Immediately press a key to interrupt the system startup.

You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiDDoS-F appliance reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the start-up process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.

Enter G,F,B,Q,or H:

Please connect TFTP server to Ethernet port "1".
```

10. If the firmware version requires that you first format the boot device before installing firmware, type `F`. Format the boot disk before continuing.
11. Type `G` to get the firmware image from the TFTP server. The following message appears:
    `Enter TFTP server address [192.168.1.168]:`
12. Type the IP address of the TFTP server and press Enter. The following message appears:
    `Enter local address [192.168.1.188]:`

13. Type a temporary IP address that can be used by the FortiDDoS-F appliance to connect to the TFTP server. The following message appears:
    `Enter firmware image file name [image.out]:`
14. Type the file name of the firmware image and press Enter. The FortiDDoS-F appliance downloads the firmware image file from the TFTP server and displays a message similar to the following:

    ```
    MAC:00219B8F0D94
    ##########################
    Total 28385179 bytes data downloaded.
    Verifying the integrity of the firmware image..
    Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?
    ```

15. Type `D`.
    The FortiDDoS-F appliance downloads the firmware image file from the TFTP server. The FortiDDoS-F appliance installs the firmware and restarts. The time required varies by the size of the file and the speed of your network connection.
    The FortiDDoS-F appliance reverts the configuration to default values for that version of the firmware.
16. To verify that the firmware was successfully installed, log in to the CLI and type: `get system status`
    The firmware version number is displayed.
17. Either reconfigure the FortiDDoS-F appliance or restore the configuration file.

- If you are *downgrading* the firmware to a previous version, and the settings are not fully backwards compatible, the FortiDDoS-F appliance either removes incompatible settings, or uses the feature's default values for that version of the firmware. You might need to reconfigure some settings.
- Installing firmware overwrites any FortiGuard IP Reputation Service definitions and disables the service. After any firmware update, re-enable the IP Reputation feature. FortiDDoS downloads current definitions as part of the enabling process.

Additional resources

Fortinet also provides these resources:

- Release Notes provided with your firmware
- Technical documentation (references, installation guides, and other documents)
- Knowledge base (technical support articles)
- Forums
- Online campus (tutorials and training materials)

Check within your organization. You can save time and effort during the troubleshooting process by checking if other FortiDDoS-F administrators experienced a similar problem before.

If you cannot resolve the issue on your own, contact Fortinet Technical Support.

Appendix

This section includes the following reference information:

Appendix A: DDoS Attack Log Reference

The following table provides the description of the fields in the Log Reference table.

Fields and description

Field	Description
Event code	1 - Layer 3, 2 - Layer 4, 4 - Layer 7
Subcode	Internal reference only.
Trap Attack Type	Attack Event identifier included in Attack SNMP Traps sent (instead of Event Name).
Event Name	Event Type in the web UI Attack Logs and Graphs, description field in syslog.
Category	Filter category in web UI Attack Logs.
Period	**Interrupt**: Rate Flood means the first event is logged within two minutes after the start of an attack and reported every minute thereafter. **Periodic**: Events other than Rate Flood means events are logged every 5 minutes.
Note: Source IP address is reported only for drops due to per-source thresholds (see Source tracking table).	

Log reference

Log reference

Event code	Subcode	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
1	0	1000	Protocol Flood	Rate Flood	Interrupt	Effective rate limit	Service	Monitor >

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
						for the protocol (0-255) has been reached. Protocols are rate-limited at the Threshold. Protocols 6 (TCP) and 17 (UDP) do not normally have Thresholds.	Protection > Service Protection Policy (List)> Service Protection Policy > Thresholds > Protocols	Drops Monitor > Flood Drops > Layer 3 > Protocols Monitor > Layer 3/4/7> Layer 3 > Protocols
1	1	1001	Other Protocols Fragment Flood	Rate Flood	Interrupt	Effective rate limit for fragments in Protocols other than TCP, UDP and DNS has been reached. Fragments are rate-limited at the Threshold.	Service Protection > Service Protection Policy (List)> Service Protection Policy > Thresholds > Scalars > OTH Fragment	Monitor > Drops Monitor >Flood Drops > Layer 3 > Fragmented Packets (aggregate of all Protocol fragments) Monitor > Layer 3/4/7> Layer 3 > Other > Fragmented Packets > Other Fragmented Packets
1	8	1008	Source Flood	Rate Flood	Interrupt	Effective rate limit for the most-active-source threshold has been reached. Source IP address is reported.	Service Protection > Service Protection Policy (List)> Service Protection Policy > Thresholds > Scalars > Most Active Source	Monitor > Drops Monitor >Flood Drops > Layer 3 > Source Flood Monitor > Layer 3/4/7> Layer 3 > Sources > Most Active Source

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
1	9	1009	Destination Flood	Rate Flood	Interrupt	Effective rate limit for the most-active-destination threshold has been reached. **Note:** This Threshold is not set by System Recommendations. You may manually add a Threshold if desired.	Service Protection > Service Protection Policy (List)> Service Protection Policy > Thresholds > Scalars > Most Active Destination	Monitor > Drops Monitor > Flood Drops > Layer 3 > Destinnation Flood Monitor > Layer 3/4/7> Layer 3 > Sources > Most Active Destination
1	14	1014	IP Header checksum error	Header anomaly	Periodic	Invalid IP header checksum.	Service Protection > IP Profile > IP Strict Anomalies. IP Profile must be assigned to an SPP.	Monitor >Drops Monitor >Anomaly Drops >Layer 3 > IP Header Checksum
1	15	1015	Source IP==dest IP	Header anomaly	Periodic	Identical source and protected IP addresses (LAND attack).	Service Protection > IP Profile > IP Strict Anomalies IP Profile must be assigned to an SPP.	Monitor >Drops Monitor >Anomaly Drops >Layer 3 > Source and Destination Address Match
1	16	1016	Source/dest IP==localhost	Header anomaly	Periodic	Source/destination address is the local host (loopback address spoofing).	Service Protection > IP Profile > IP Strict Anomalies IP Profile must be assigned to an SPP.	Monitor >Drops Monitor >Anomaly Drops >Layer 3 > Source/ Destination as Localhost

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
1	17	1017	L3 anomalies	Header anomaly	Periodic	Drops due to predefined Layer 3 rules: - IP version other than IPv4 or IPv6. - EOP (End of Packet) before 20 bytes of IPv4 data. -EOP comes before the length specified by Total Length. -Reserved Flag set. -More Frag and Don't Frag Flags set. -Added Anomaly for DSCP and ECN.	Service Protection > IP Profile > IP Strict Anomalies IP Profile must be assigned to an SPP.	Monitor >Drops Monitor >Anomaly Drops >Layer 3 > Layer 3
1	23	1023	TCP Fragment Flood	Rate Flood	Interrupt	Effective rate limit for the TCP fragment has been reached. **Note**: Use with care. Miss-configured clients can result in TCP fragmentation. Unless you are sure there can be no TCP Fragmentation, it is better to use the TCP Fragment Threshold than an ACL.	Service Protection > Service Protection Policy (List)> Service Protection Policy > Thresholds >Scalars > TCP Fragment	Monitor > Drops Monitor > Flood Drops > Layer 3> Fragmented Packets Monitor > Layer 3/4/7> Layer 3 > Other > Fragmented Packets > TCPFragmented Packets

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
1	24	1024	UDP Fragment Flood	Rate Flood	Interrupt	Effective rate limit for the UDP fragment has been reached. **Note**: Use with care. Miss-configured clients can result in UDP fragmentation. Unless you are sure there can be no UDP Fragmentation, it is better to use the UDP Fragment Threshold than an ACL.	Service Protection > Service Protection Policy (List)> Service Protection Policy > Thresholds >Scalars > UDP Fragment	Monitor > Drops Monitor > Flood Drops > Layer 3> Fragmented Packets Monitor > Layer 3/4/7> Layer 3 > Other > Fragmented Packets > UDPFragmented Packets
1	54	1054	Other Protocols Fragment denied	ACL	Periodic	Fragments for Protocols other than TCP, UDP, DNS, denied by an SPP IP Profile Fragment Check setting. **Note**: Use with care. Miss-configured clients can result in fragmentation for Protocols like GRE (47) and IPSEC (50). Unless you are sure there can be no Other Protocol Fragmentation, it is better to use the Other Protocol Fragment Threshold than an ACL.	Service Protection > IP Profile > IP Fragment Check > Other Protocol Fragment IP Profile must be assigned to an SPP.	Monitor > Drops Monitor > ACL Drops > Layyer 3 > Fragmented Packet Denied Drops Monitor > Layer 3/4/7> Layer 3 > Other > Fragmented Packets > OtherFragmented Packets blocked
1	60	1060	Denied: IP	ACL	Period	Denied by Global	Global	Monitor >

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
			address		ic	Blocklist	Protection > Blocklist > Blocklisted IPv4	Drops Monitor >ACL Drops > Layer 3 > Address Denied: Denied Address Drops
1	61	1061	Denied: IP reputation	ACL	Periodic	Denied by the IP Reputation ACL based on IP Profile per SPP.	IP Reputation is an optional subscription which must be current for this ACL to work. System > FortiGuard. For IP Reputation settings, subscription confirmation Service Protection > IP Profile > IP Reputation categories to enable when that IP Profile is assigned to an SPP.	Monitor > Drops Monitor > ACL Drops > Layer 3 > Address Denied: IP Reputation Denied Drops
1	63	1063	Denied: IP Multicast	ACL	Periodic	Denied by IP profile per SPP.	Service Protection > IP Profile > IP Multicast Check IP Profile must be assigned to an SPP.	Monitor > Drops Monitor > ACL Drops > Layer 3 > IP Multicast Denied Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
1	64	1064	Denied: Private IP	ACL	Periodic	Denied by IP profile per SPP.	Service Protection > IP Profile > IP Private Check IP Profile must be assigned to an SPP.	Monitor > Drops Monitor > ACL Drops >Layer 3 >Private IP Denied Drops
1	71	1071	TCPFragment denied	ACL	Periodic	TCP Fragments denied by an SPP IP Profile Fragment Check setting. **Note**: Miss-configured clients can send TCP Fragments. Use with care. It is better to use the TCP Fragment Threshold than an ACL.	Service Protection > IP Profile > IP Fragment Check >TCP Fragment IP Profile must be assigned to an SPP.	Monitor > Drops MonitoACL Drops > Layer 3 > Fragmented Packet Denied Drops Monitor > Layer 3/4/7> Layer 3 > Other > Fragmented Packets > TCPFragmented Packets blocked
1	72	1072	UDPFragment denied	ACL	Periodic	UDP Fragments denied by an SPP IP Profile Fragment Check setting. **Note**: Miss-configured clients can send UDP Fragments. Use with care. It is better to use the TCP Fragment Threshold than an ACL.	Service Protection > IP Profile > IP Fragment Check >UDP Fragment IP Profile must be assigned to an SPP.	Monitor > Drops Monitor >ACL Drops > Layer 3 > Fragmented Packet Denied Drops Monitor > Layer 3/4/7> Layer 3 > Other > Fragmented Packets > UDPFragmented Packets blocked

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
2	0	2000	SYN Flood	Rate Flood	Interrupt	Effective rate limit for the SYN Threshold has been reached. **Note**: **1.** Crossing the SYN Threshold initiates SYN Validation of the Source IPs. If TCP Profile > SYN Validation is not enabled, no SYN Validation will be done over-threshold (no SYN or Source blocking). **2.** SYN Validation reports SYNs initially dropped by the system while validating the Sources. Valid Sources are then allowed to exceed the SYN per Destination Threshold. Check the SYN per Destination graph, and Established Connections graph to view how many SYNs and Connections are allowed after validation.	Service Protection > Service Protection Policy > Thresholds > Scalars >: SYN Service Protection > TCP Profile >TCP Packets Validation > SYN Validation. **Note**: If SYN Validation is not enabled no SYN validation nor rate limiting is done.	Monitor > Drops Monitor >Flood Drops > Layer 3> SYN Monitor > Layer 3/4/7> Layer 4 > SYN
2	6	2006	State Anomalies: Foreign packet (Out of State)	State anomaly	Periodic	A foreign packet is a TCP packet that does not belong to any known	Service Protection > TCP Profile > TCP	Monitor > Drops Monitor > Anomaly Drops > Layer 4 > State

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
						connections. Tracked when TCP Profile for an SPP has Foreign Packet Validation enabled.	Packets Validation > Foreign Packet Validation TCP profile must be assignd to an SPP.	
2	7	2007	State Anomalies: Outside window	State anomaly	Periodic	Sequence number of a packet was outside the acceptable window. Tracked when TCP Profile for an SPP has Sequence Validation enabled.	Service Protection > TCP Profile > TCP Packets Validation > Sequence Validation. TCP profile must be assignd to an SPP.	Monitor > Drops Monitor > Anomaly Drops > Layer 4 > State
2	12	2012	State Anomalies: State transition error	State anomaly	Periodic	State of the TCP packet received was not consistent with the expected state. Tracked when TCP Profile for an SPP has State Transition Validation enabled.	Service Protection > TCP Profile > TCP Packets Validation > State Transition Anomalies Validation TCP profile must be assignd to an SPP.	Monitor > Drops Monitor > Anomaly Drops > Layer 4 > State
2	13	2013	SPP Rule Deny	ACL	Periodic	Global or SPP-based IPv4, IPv6, Geolocation, Service ACL drops. **Note:**	Global Protection > Access Control List >IPv4 or Global	Monitor > Drops Monitor > ACL Drops > Layer 4

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
						1. In Release 6.1.1, Global ACL drops will be shown in the default SPP graphs. SPP-based ACL drops will be shown in the SPP graphs. **2.** Global ACLs are always on - there is no Detection/Preventi onn Mode for Global ACLs.	Protection > Access Control List >IPv6 or Service Protection > Service Protection Policy > Service Protection Policy Rule > ACL	
2	16	2016	TCP zombie Flood	Rate Flood	Interrupt	Effective rate limit for the new-connections Thres hold has been reached. **Note:** this Threshold is set to maximum by System Recommendations to avoid rate-limiting new connections. You can add a manual Threshold if desired.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > New Connections	Monitor > Drops Monitor> Flood Drops >Layer 4 > Zombie Flood Monitor > Layer 3/4/7 > Layer 4 > Other > New Connections
2	17	2017	TCP Port Flood	Rate Flood	Periodic	Effective rate limit for the port has been reached.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds >TCP Ports	Monitor > Drops Monitor > Flood Drops > Layer 4> TCP Ports Monitor > Layer 3/4/7 > Layer 4 > Ports > TCP

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
						Note: Several TCP Ports like 80, 443 are set to system maximum (no thresholds) by System Recommendations. Other parameters (like the various SYN thresholds and Foreign Packet Validation) mitigate DDoS Floods to these Ports. You can add a Threshold for these ports if desired.		
2	18	2018	UDP Port Flood	Rate Flood	Periodic	Effective rate limit for the port has been reached. **Note**: No Threshold is set for UDP 53 where DNS mitigations are expected to be used. You can add a Threshold if desired.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > UDP Ports	Monitor > Drops Monitor > Flood Drops >Layer 4> UDP Ports Monitor > Layer 3/4/7 > Layer 4 > Ports > UDP
2	19	2019	ICMP Flood	Rate Flood	Periodic	Effective rate limit for the ICMP Type/Code has been reached. Type/Codes will be rate-limited to the Threshold.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > ICMP Types and Codes	Monitor > Drops Monitor >Flood Drops >Layer 4> ICMP Types/Codes Monitor > Layer 3/4/7 > Layer 4 > Other > ICMP

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
2	20	2020	Foreign Packets (Aggressive Aging and Slow Connections)	State anomaly	Periodic	Foreign (out-of-state) Packets seen after Slow Connection Aggressive Aging (RST to server)	Service Protection > TCP Profile > TCP Packets Validation > Foreign Packet Validation Service Protection > TCP Profile > TCP Session Settings > Aggressive Aging Feature Control > Slow TCP Connections	Monitor > Drops Monitor >Anomaly Drops >Layer 4> State
2	22	2022	Slow Connection: Source Flood	Rate Flood	Interrupt	Slow connection attack detected and “Source blocking for slow connections” enabled. Source IP address is reported.	Service Protection > TCP Profile > TCP Slow Connection Protection > Block Sources With Slow TCP Connections	Monitor > Drops Monitor >Flood Drops > Layer 4> Slow Connection
2	24	2024	TCP checksum error	Header anomaly	Periodic	Invalid TCP checksum.	Service Protection > TCP Profile > Strict Anomalies TCP Profile must be assigned to the SPP.	Monitor > Drops Monitor > Anomaly Drops > Layer 4> Header > TCP Checksum Error
2	26	2026	ICMP checksum	Header	Period	Invalid ICMP	Service	Monitor >

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
			error	anomaly	ic	checksum.	Protection > ICMP Profile > ICMP Strict Anomalies ICMP Profile must be assigned to the SPP.	Drops Monitor > Anomaly Drops > Layer 4 > Header > ICMP Checksum Error
2	27	2027	TCP invalid flag combination	Header anomaly	Periodic	Invalid TCP flag combination. If the urgent flag is set, then the urgent pointer must be non-zero. SYN, FIN or RST is set for fragmented packets, no flags, all flags and others.	Service Protection > TCP Profile > Strict Anomalies TCP Profile must be assigned to the SPP.	Monitor > Drops Monitor >Anomaly Drops > Layer 4 > Header > TCP Invalid Flag Combination
2	28	2028	L4 anomalies	Header anomaly	Periodic	Drops due to predefined Layer 4 header rules: Data offset is less than 5 for a TCP packet; EOP (End of packet) is detected before the 20 bytes of TCP header; EOP before the data offset indicated data offset; Length field in TCP window scale option is a value other than 3; Length field in TCP window scale option is a value other than 3: Missing UDP payload; Missing ICMP payload,TCP	Service Protection > TCP Profile >Strict Anomalies Service Protection > TCP Profile > SYN with Payload Service Protection > ICMP Profile >Strict Anomalies ICMP and TCP Profiles must be assigned to the SPP.	Monitor > Drops Monitor > Anomaly Drops > Layer 4 > Header > Anomaly Detected

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
						Option Anomaly based on Option Type; and others. SYN with Payload if SPP Option in TCP Profile is set.		
2	54	2054	ICMP Type/Code denied	ACL	Periodic	Denied by an ICMP Profile TypeCode ACL	Service Protection > ICMP Profile > ICMP Type Code ACL ICMP Profile must be assigned to the SPP.	Monitor > Drops Monitor > ACL Drops > Layer 4 > Aggregate > ICMP Type/Code Denied Drops
2	56	2056	SYN Flood from source	Rate Flood	Interrupt	Effective rate limit for the syn-per-src threshold from a single Source IP has been reached. Source IP address is reported. **Note**: No SYN Validation is done on SYNperSource Floods. The Source is rate-limited to the Threshold	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > SYN Per Source	Monitor > Drops Monitor >Flood Drops > Layer 4 > SYN Per Source Monitor > Layer 3/4/7 > Layer 4 > SYN per Source
2	61	2061	Excessive Concurrent Connections Per Source Flood	rate Flood	interrupt	Effective rate limit for the concurrent-connections-per-source threshold has been reached. Source IP address is reported. Per-Source Connections are rate-limited to the Threshold.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > Concurrent-Connections-per-	Monitor > Drops Monitor >L4> Flood Drops > Concurrent Connection per Source Monitor > Layer 3/4/7 > Layer 4 >Other > Concurrent Connections per Source

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							Source	
2	62	2062	SYN per Destination Flood	rate Flood	interrupt	Effective rate limit for the SYN per Destination threshold has been reached. **Note**: **1.** Crossing the SYN per Destination Threshold initiates SYN validation of the Source IPs. If TCP Profile > SYN Validation is not enabled, no SYN Validation will be done over-threshold (no SYN or Source blocking). **2.** SYN Validation reports SYNs initially dropped by the system while validating the Sources. Valid Sources are then alllowed to exceed the SYN per Destination Threshold. Check the SYN per Destination graph, and Established Connections graph to view how many SYNs and Connections are allowed after validation.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > SYN-per-Destination	Monitor > Drops Monitor >Flood Drops > Layer 4 > SYN per Destination Monitor > Layer 3/4/7 > Layer 4 >SYN per Destination

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
2	82	2082	DNS Query Flood from Source	rate Flood	Periodic	Effective rate limit for the DNS-Query-per-Source threshold has been reached. **Note**: **1.** No Source Validation (Anti-Spoofing) is attempted for DNS Query per Source. Queries from Sources are rate-limited to the Threhsold. **2.** DNS Query per Source Threshold is not set by System Recommendations. A manual Threshold can be added if desired.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds >Scalars > DNS-Query-per-Source	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Query per Source Monitor > Layer 3/4/7 > Layer 7 > DNS > Query per Source
2	83	2083	DNS Packet Track Flood from Source	rate Flood	Periodic	Effective rate limit for the DNS-Packet-Track-per-Source (Suspicious Sources) threshold has been reached. **Note:**	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds >Scalars > DNS Packet Track per Source	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Suspicious Sources Monitor > Layer 3/4/7 > Layer 7 > DNS > DNS Packet Track per Source

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
						1. No Source Validation (Anti-Spoofing) is attempted for DNS Packet Track per Source (Suspicious Sources). Queries from Sources are rate-limited to the Threhsold. **2.** DNS Packet Track per Source (Suspicious Sources) Threshold is not set by System Recommendations. A manual Threshold can be added if desired.		
2	86	2086	Invalid ICMP Type/Code	Header Anomaly	Periodic	Invalid ICMP Type/Code.	Service Protection > ICMP Profile > ICMP Type Code Anomaly ICMP Profile must be assigned to an SPP	Monitor > Drops Monitor >Anomaly Drops > Layer 4 > Header > Invalid ICMPv4 Type/Code or Invalid ICMPv6 Type/Code
2	87	2087	HTTP Method Flood from source	rate Flood	Interrupt	Effective rate limit for the HTTP-Method-per-Source threshold has been reached.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars >	Monitor > Drops Monitor > Flood Drops > Layer 7 > HTTP > Method Per Source Monitor > Layer 3/4/7 > Layer 7 >

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							HTTP Method Per Source	HTTP > Method per Source
4	0	4000	HTTP Method Flood	Rate Flood	Interrupt	Effective rate limit for a particular HTTP method threshold has been reached.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > HTTP Methods	Monitor > Drops Monitor >Flood Drops > Layer 7 > HTTP > Method Flood Monitor > Layer 3/4/7 > Layer 7 > HTTP > Methods (Select Method from drop-down)
4	1	4001	Known HTTP Method Anomaly	Header anomaly	Periodic	HTTP Known Method anomaly as defined in an HTTP Profile.	Service Protection > HTTP Profile > Known Method Anomaly HTTP Profile must be assigned to the SPP	Monitor > Drops Monitor >L7>Anomaly Drops > HTTP > Known Method
4	2	4002	Invalid HTTP Version Anomaly	Header anomaly	Periodic	Packets dropped due to the HTTP Profile version anomaly option	Service Protection > HTTP Profile > Version Anomaly HTTP Profile must be assigned to the SPP	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > HTTP > Invalid HTTP Version
4	3	4003	URL denied	ACL	Periodic	Denied by an HTTP Profile ACL rule.	Service Protection > HTTP Profile > HTTP Param ACL	Monitor > Drops Monitor > ACL Drops > Layer 7 > HTTP > URL

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							HTTP Profile must be assigned to the SPP	Denied Drops Monitor > Layer 3/4/7 > Layer 7 > HTTP > URL: Packets Blocked
4	4	4004	URL Flood	Rate Flood	Periodic	Effective rate limit for a particular URL threshold has been reached.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > URLs	Monitor > Drops Monitor >L7> Flood Drops > HTTP > URL Flood Monitor > Layer 3/4/7 > Layer 7 > HTTP > URLs
4	5	4005	Unknown HTTP Method Anomaly	Header Anomaly	Periodic	HTTP Profile Unknown HTTP Method.	Service Protection > HTTP Profile > Unknown Method Anomaly HTTP Profile must be assigned to the SPP	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > HTTP > Unknown Method
4	6	4006	HTTP L7 Host Flood	Rate Flood	Interrupt	Effective rate limit for a particular Host threshold has been reached.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Hosts	Monitor > Drops Monitor >Flood Drops > Layer 7 > HTTP > Host Flood Monitor > Layer 3/4/7 > Layer 7 > HTTP > Hosts
4	7	4007	HTTP L7 Host Deny	ACL	Periodic	Denied by an HTTP Profile ACL rule.	Service Protection > HTTP Profile > HTTP	Monitor > Drops Monitor > ACL Drops > Layer 7 >

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							Param ACL HTTP Profile must be assigned to the SPP	HTTP > Host Denied Drops Monitor > Layer 3/4/7 > Layer 7 > HTTP > Hosts: Packets Blocked
4	8	4008	HTTP L7 Referer Flood	Rate Flood	Interrupt	Effective rate limit for a particular Referer header threshold has been reached.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds >Referers	Monitor > Drops Monitor > Flood Drops > Layer 7 > HTTP > Referer Flood Monitor > Layer 3/4/7 > Layer 7 > HTTP > Referers
4	9	4009	HTTP L7 Referer Deny	ACL	Periodic	Denied by an HTTP Profile ACL rule.	Service Protection > HTTP Profile > HTTP Param ACL HTTP Profile must be assigned to the SPP	Monitor > Drops Monitor > ACL Drops > HTTP > Layer 7 > Referer Denied Drops Monitor > Layer 3/4/7 > Layer 7 > HTTP > Referers: Packets Blocked
4	10	4010	HTTP L7 Cookie Flood	Rate Flood	Interrupt	Effective rate limit for a particular Cookie header threshold has been reached.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds >Cookies	Monitor > Drops Monitor > Flood Drops > Layer 7 > HTTP > Cookie Flood Monitor > Layer 3/4/7 > Layer 7 > HTTP >

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
								Cookies
4	11	4011	HTTP L7 Cookie Deny	ACL	Periodic	Denied by an HTTP Profile ACL rule.	Service Protection > HTTP Profile > HTTP Param ACL HTTP Profile must be assigned to the SPP	Monitor > Drops Monitor > ACL Drops > Layer 7 > HTTP > Cookie Denied Drops Monitor > Layer 3/4/7 > Layer 7 > HTTP > Cookies: Packets Blocked
4	12	4012	HTTP L7 User Agent Flood	Rate Flood	Interrupt	Effective rate limit for a particular User-Agent threshold has been reached.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds> User Agents	Monitor > Drops Monitor >Flood Drops > Layer 7 > HTTP > User Agent Flood Monitor > Layer 3/4/7 > Layer 7 > HTTP > User Agents
4	13	4013	HTTP L7 User Agent Deny	ACL	Periodic	Denied by an HTTP Profile ACL rule.	Service Protection > HTTP Profile > HTTP Param ACL HTTP Profile must be assigned to the SPP	Monitor > Drops Monitor > ACL Drops > Layer 7 > HTTP > User Agent Denied Drops Monitor > Layer 3/4/7 > Layer 7 > HTTP > User Agents: Packets Blocked
4	37	4037	DNS Fragment Deny	ACL	Periodic	Denied by an DNS Profile DNS fragment option	Service Protection >	Monitor > Drops Monitor

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							DNS Profile > DNS Fragment	> ACL Drops > Layer 7 >DNS > Frag Drops
4	41	4041	DNS Rcode Flood	Rate Flood	Interrupt	Effective rate limit for the DNS Rcode threshold has been reached.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > DNS Rcode	Monitor > Drops Monitor > Flood Drops > Layer 7 >DNS:Response Code Drop Monitor > Layer 3/4/7 >L7> DNS > DNS Response Code
4	42	4042	DNS Header Anomaly: Invalid Opcode	DNS Anomaly	Periodic	Invalid value in the DNS OpCode field., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > Invalid Op Code DNS Profile must be assigned to SPP.	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > DNS > Header
4	43	4043	DNS Header Anomaly: Illegal Flag Combination	DNS Anomaly	Periodic	Invalid combination in the flags field., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > Illegal Flag Combination DNS Profile must be assigned to SPP.	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > DNS > Header
4	44	4044	DNS	DNS Anomal	Periodic	DNS Header	Service	Monitor >

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
			Header Anomaly: Same Source/Destination Port	y		where Source Port==Destination Port == 53., selected in DNS Profile.	Protection > DNS Profile > DNS Anomaly Feature Controls > SP,DP Both 53 DNS Profile must be assigned to SPP.	Drops Monitor > Anomaly Drops > Layer 7 > DNS > Header
4	45	4045	DNS Query Anomaly: Query Bit Set	DNS Anomaly	Periodic	(QR) bit set to 1., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > Query Bit Set DNS Profile must be assigned to SPP.	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > DNS > Query
4	46	4046	DNS Query Anomaly: RA Bit Set	DNS Anomaly	Periodic	recursion allowed (RA) bit set., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > RA Bit Set DNS Profile must be assigned to SPP.	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > DNS > Query
4	47	4047	DNS Query Anomaly: Null Query	DNS Anomaly	Periodic	DNS query with count 0., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls >	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > DNS > Query

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							Null Query DNS Profile must be assigned to SPP.	
4	48	4048	DNS Query Anomaly: QD Count not One in query	DNS Anomaly	Periodic	Question count not 1., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > DNS Query Anomaly: QD Count not One in query DNS Profile must be assigned to SPP.	Monitor > Drops Monitor >Anomaly Drops > Layer 7 > DNS > Query
4	50	4050	DNS Reply Anomaly: Qclass in reply	DNS Anomaly	Periodic	DNS response with QCLASS., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > QCLASS in Reply	Monitor > Drops Monitor >Anomaly Drops > Layer 7 > DNS > Response
4	51	4051	DNS Reply Anomaly: Qtype in reply	DNS Anomaly	Periodic	DNS response with a resource specifying a TYPE ID., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > QType in Reply DNS Profile must be assigned to SPP.	Monitor > Drops Monitor >Anomaly Drops > Layer 7 > DNS > Response

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
4	52	4052	DNS Reply Anomaly: Query bit not set	DNS Anomaly	Periodic	(QR) bit set to 0., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > Query Bit not Set DNS Profile must be assigned to SPP.	Monitor > Drops Monitor >Anomaly Drops > Layer 7 > DNS > Response
4	53	4053	DNS Reply Anomaly: QD count not 1 in response	DNS Anomaly	Periodic	DNS Response where QD count is not 1., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > QDCOUNT not One in Response DNS Profile must be assigned to SPP.	Monitor > Drops Monitor >Anomaly Drops > Layer 7 > DNS > Response
4	54	4054	DNS Buffer Overflow Anomaly: Message too long	DNS Anomaly	Periodic	DNS Query or Response message that exceeds the maximum header length., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > TCP Message too Long/UDP Message too Long DNS Profile must be assigned to SPP.	Monitor > Drops Monitor >Anomaly Drops > Layer 7 > DNS > Buffer Overflow

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
4	55	4055	DNS Buffer Overflow Anomaly: Name too long	DNS Anomaly	Periodic	DNS name that exceeds 255 characters., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > Name too Long DNS Profile must be assigned to SPP.	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > DNS > Buffer Overflow
4	56	4056	DNS Buffer Overflow Anomaly:Label length too large	DNS Anomaly	Periodic	Query or response with a label that exceeds the maximum length (63)., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > Label Length too Large DNS Profile must be assigned to SPP.	Monitor > Drops Monitor >Anomaly Drops > Layer 7 > DNS > Buffer Overflow
4	57	4057	DNS Exploit Anomaly: Pointer loop	DNS Anomaly	Periodic	DNS message with a pointer that points beyond the end of data., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > Pointer Loop DNS Profile must be assigned to SPP.	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > DNS > Exploit
4	58	4058	DNS Exploit Anomaly: Zone Transfer	DNS Anomaly	Periodic	An asynchronous Transfer Full Range (AXFR) request (QTYPE=252).,	Service Protection > DNS Profile > DNS Anomaly	Monitor > Drops Monitor >L7> Anomaly Drops > DNS > Exploit

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
						selected in DNS Profile.	Feature Controls > Zone transfer DNS Profile must be assigned to SPP.	
4	59	4059	DNS Exploit Anomaly: Class is not IN	DNS Anomaly	Periodic	A query/response in which the question/resource address class is not IN., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > Class not IN DNS Profile must be assigned to SPP.	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > DNS > Exploit
4	60	4060	DNS Exploit Anomaly: Empty UDP message	DNS Anomaly	Periodic	UDP DNS Query has no data., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > Empty UDP DNS Profile must be assigned to SPP.	Monitor > Drops Monitor >Anomaly Drops > Layer 7 > DNS > Exploit
4	61	4061	DNS Exploit Anomaly: Message ends prematurely	DNS Anomaly	Periodic	DNS message ends before proper EOP info., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > Message Ends Prematurely DNS Profile	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > DNS > Exploit

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							must be assigned to SPP.	
4	62	4062	DNS Exploit Anomaly: TCP Buffer Underflow	DNS Anomaly	Periodic	A query/response with less than two bytes of data specified in the two-byte prefix field., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > TCP Buffer Underflow DNS Profile must be assigned to SPP.	Monitor > Drops Monitor >Anomaly Drops > Layer 7 > DNS > Exploit
4	63	4063	DNS Info Anomaly:DNS type all used	DNS Anomaly	Periodic	DNS request with request type set to ALL (QTYPE=255)., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > Info Anomaly enable DNS Profile must be assigned to SPP.	Monitor > Drops Monitor >Anomaly Drops > Layer 7 > DNS > Info
4	64	4064	DNS Data Anomaly: Invalid type class	DNS Anomaly	Periodic	A query/response with TYPE or CLASS reserved values., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > Invalid Class Type DNS Profile must be assigned to SPP.	Monitor > Drops Monitor >Anomaly Drops > Layer 7 > DNS > Data

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
4	65	4065	DNS Data Anomaly: Extraneous data	DNS Anomaly	Periodic	A query/response with excess data., selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > Extraneous Data DNS Profile must be assigned to SPP.	Monitor > Drops Monitor >Anomaly Drops > Layer 7 > DNS > Data
4	66	4066	DNS Data Anomaly: TTL too long	DNS Anomaly	Periodic	TTL value is greater than 7 days, selected in DNS Profile. **Note:** Some services (Yahoo Mail for example) have TTLs lnger than 7 days.This Anomaly should remain disabled.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > TTL too Long DNS Profile must be assigned to SPP.	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > DNS > Data
4	67	4067	DNS Data Anomaly: Name length too short	DNS Anomaly	Periodic	A query/response with a null DNS name or lacking a TLD, selected in DNS Profile.	Service Protection > DNS Profile > DNS Anomaly Feature Controls > Name Length too Short DNS Profile must be assigned to SPP.	Monitor > Drops Monitor >Anomaly Drops > Layer 7 > DNS > Data
4	68	4068	DNS UDP Unsolicited Response	Rate Flood	Periodic	UDP Drops due to a response with no matching query, selected in DNS Profile.	Service Protection > DNS Profile > DNS Feature	Monitor > Drops Monitor >Flood Drops > Layer 7 > DNS:Unsolicit

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							Controls > Match Response With Queries (DQRM). DNS Profile must be assigned to SPP.	ed DNS Response Drops
4	69	4069	DNS TCP Unsolicited Response	Rate Flood	Periodic	TCP Drops due to a response with no matching query, selected in DNS Profile.	Service Protection > DNS Profile > DNS Feature Controls >Match Response With Queries (DQRM). DNS Profile must be assigned to SPP.	Monitor > Drops Monitor >Flood Drops > Layer 7 > DNS:Unsolicited DNS Response Drops
4	71	4071	DNS DQRM Out of Memory	-	Periodic	An issue with DQRM table internal logic or memory. Contact Fortinet.	None. Internal Table issue. Report to Fortinet.	Monitor > Drops Monitor >Out of Memory Drops > Layer 7 > DNS
4	72	4072	DNS UDP Response same direction	Rate Flood	Periodic	Drops due to UDP DNS Response sent to port 53.	Service Protection > DNS Profile > DNS Feature Controls > Match Response With Queries (DQRM) DNS Profile must be assigned to	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Unsolicited DNS Response Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							SPP.	
4	73	4073	DNS TCP Response same direction	Rate Flood	Periodic	Drops due to TCP DNS Response sent to port 53	Service Protection > DNS Profile > DNS Feature Controls > Match Response With Queries (DQRM) DNS Profile must be assigned to SPP.	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Unsolicited DNS Response Drops
4	74	4074	DNS LQ: UDP Query Flood	Rate Flood	Periodic	Drops due to LQ check during UDP DNS QG88:G94uery Flood	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNS Query UDP and Service Protection > DNS Profile > DNS Feature Controls > Allow Only Valid Queries Under Flood (LQ) DNS Profile must be assigned to SPP.	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > LQ Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
4	75	4075	DNS LQ: UDP Question Flood	Rate Flood	Periodic	Drops due to LQ check during UDP DNS Question Flood	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNS > Question Count UDP and Service Protection > DNS Profile > DNS Feature Controls > Allow Only Valid Queries Under Flood (LQ) DNS Profile must be assigned to SPP.	Monitor > Drops Monitor >Flood Drops > Layer 7 > DNS > LQ Drops
4	76	4076	DNS LQ: UDP Qtype All Flood	Rate Flood	Periodic	UDP drops due to LQ check during UDP Qtype All (ANY/*) Flood, selected in DNS Profile.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNS All UDP and Service Protection > DNS Profile > DNS	Monitor > Drops Monitor >Flood Drops > Layer 7 > DNS > LQ Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							Feature Controls > Allow Only Valid Queries Under Flood (LQ) DNS Profile must be assigned to SPP.	
4	78	4078	DNS LQ: UDP Qtype MX Flood	Rate Flood	Periodic	Drops due to LQ check during UDP DNS Qtype MX Flood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNSMX Count UDP and Service Protection > DNS Profile > DNS Feature Controls > Allow Only Valid Queries Under Flood (LQ)	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > LQ Drops
4	80	4080	DNS LQ: UDP Query Flood due to Negative Response	Rate Flood	Periodic	UDP drops due to LQ check during Flood.	Service Protection > Service Protection Policy > Service Protection Policy Rule > Scalars >	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > LQ Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							DNS UDP Query and Service Protection > DNS Profile > DNS Feature Controls > Allow Only Valid Queries Under Flood (LQ)	
4	81	4081	DNS TTL: UDP Query Flood	Rate Flood	Periodic	Drops due to TTL check during UDP DNS Query Flood	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNS QueryUDP and Service Protection > DNS Profile > DNS Feature Controls >Validate TTL For Queries From The Same IP DNS Profile must be assigned to the SPP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > TTL Drops
4	82	4082	DNS TTL: UDP Question Flood	Rate Flood	Periodic	Drops due to TTL check during UDP DNS Question	Service	Monitor > Drops Monitor

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
						Flood.	Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNSQuestion Count UDP and Service Protection > DNS Profile > DNS Feature Controls >Validate TTL For Queries From The Same IP DNS Profile must be assigned to the SPP	> Flood Drops > Layer 7 > DNS > TTL Drops
4	83	4083	DNS TTL: UDP Qtype All Flood	Rate Flood	Periodic	Drops due to TTL check during UDP DNS Qtype ALL (ANY/*) Flood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNS All UDP and Service Protection > DNS Profile > DNS	Monitor > Drops Monitor >Flood Drops > Layer 7 > DNS > TTL Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							Feature Controls >Validate TTL For Queries From The Same IP DNS Profile must be assigned to the SPP	
4	85	4085	DNS TTL: UDP Qtype MX Flood	Rate Flood	Periodic	Drops due to TTL check during UDP DNS Qtype MX Flood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNSMX Count UDP and Service Protection > DNS Profile > DNS Feature Controls > Validate TTL For Queries From The Same IP DNS Profile must be assigned to the SPP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > TTL Drops
4	87	4087	DNS Spoofed IP: UDP Query Flood drop during TC=1 check	Rate Flood	Periodic	Drops due to TC=1 antispoofing check during UDP DNS Query Flood	Service Protection > Service Protection	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Spoofed IP

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							Policy (List) > Service Protection Policy > Thresholds >Scalars > DNS UDP Query and Service Protection > DNS Profile > DNS Feature Controls > Flood Mitigation Mode: TC Equal One DNS Profile must be assigned to the SPP	Drops
4	88	4088	DNS Spoofed IP: UDP Question Flood drop during TC=1 check	Rate Flood	Periodic	Drops due to TC=1 antispoofing check during UDP DNS Question Flood	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNSQuestion Count UDP and Service Protection > DNS Profile > DNS Feature Controls >Flood Mitigation	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Spoofed IP Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							Mode: TC Equal One DNS Profile must be assigned to the SPP	
4	89	4089	DNS Spoofed IP: UDP Qtype All Flood drop during TC=1 check	Rate Flood	Periodic	Drops due to TC=1 antispoofing check during UDP DNS Qtype All (ANY/*) Flood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNSAll UDP and Service Protection > DNS Profile > DNS Feature Controls >Flood Mitigation Mode: TC Equal One DNS Profile must be assigned to the SPP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Spoofed IP Drops
4	91	4091	DNS Spoofed IP: UDP Qtype MX Flood drop during TC=1 check	Rate Flood	Periodic	Drops due to TC=1 antispoofing check during UDP DNS Qtype MXFlood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNSMX	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Spoofed IP Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							Count UDP and Service Protection > DNS Profile > DNS Feature Controls > Flood Mitigation Mode: TC Equal One DNS Profile must be assigned to the SPP	
4	93	4093	DNS Spoofed IP: UDP Query Flood Drop during Retransmission Check	Rate Flood	Periodic	Drops due to Retransmission antispoofing check during UDP DNS Query Flood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds >Scalars > DNS UDP Query and Service Protection > DNS Profile > DNS Feature Controls >Flood Mitigation Mode: Retransmission DNS Profile must be assigned to the SPP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Spoofed IP Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
4	94	4094	DNS Spoofed IP: UDP Question Flood Drop during Retransmission Check	Rate Flood	Periodic	Drops due to Retransmission antispoofing check during UDP DNS Question Flood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds >Scalars > DNSQuestion Count UDP and Service Protection > DNS Profile > DNS Feature Controls >Flood Mitigation Mode: Retransmission DNS Profile must be assigned to the SPP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Spoofed IP Drops
4	95	4095	DNS Spoofed IP: UDP Qtype All Flood Drop during Retransmission Check	Rate Flood	Periodic	Drops due to Retransmission antispoofing check during UDP DNS Qtype All (ANT/*) Flood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds >Scalars > DNSAll UDP and Service Protection > DNS Profile > DNS Feature	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Spoofed IP Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							Controls > Flood Mitigation Mode: Retransmission DNS Profile must be assigned to the SPP	
4	96	4096	DNS Spoofed IP: UDP Qtype Zone Transfer Flood Drop during Retransmission Check	Rate Flood	Periodic	Drops due to Retransmission antispoofing check during UDP DNS Qtype Zone Transfer Flood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds >Scalars > DNSQuery UDP and Service Protection > DNS Profile > DNS Feature Controls > Flood Mitigation Mode: Retransmission DNS Profile must be assigned to the SPP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Spoofed IP Drops
4	97	4097	DNS Spoofed IP: UDP Qtype MX Flood Drop during Retransmission Check	Rate Flood	Periodic	Drops due to Retransmission antispoofing check during UDP Qtype MX Flood.	Service Protection > Service Protection Policy (List) > Service Protection	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Spoofed IP Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							Policy > Thresholds > Scalars > DNSMX Count UDP and Service Protection > DNS Profile > DNS Feature Controls > Flood Mitigation Mode: Retransmission DNS Profile must be assigned to the SPP	
4	99	4099	DNS Cache: UDP Query Flood Drop Due To Response From Cache	Rate Flood	Periodic	DNS Query drops because the response was served from the cache during a UDP DNS Query Flood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNS UDP Query and Service Protection > DNS Profile > DNS Feature Controls > Generate Response From Cache Under Flood DNS Profile must be	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Cache Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							assigned to the SPP	
4	100	4100	DNS Cache: UDP Question Flood Drop Due To Response From Cache	Rate Flood	Periodic	DNS Query drops because the response was served from the cache during a UDP DNA Question Flood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNSQuestion Count UDP and Service Protection > DNS Profile > DNS Feature Controls >Generate Response From Cache Under Flood DNS Profile must be assigned to the SPP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Cache Drops
4	101	4101	DNS Cache: UDP Qtype All Flood Drop Due To Response From Cache	Rate Flood	Periodic	DNS Query drops because the response was served from the cache during a UDP DNS Qtype All (ANY/*) Flood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNSAll UDP and Service Protection >	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Cache Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							DNS Profile > DNS Feature Controls > Generate Response From Cache Under Flood DNS Profile must be assigned to the SPP	
4	103	4103	DNS Cache: UDP Qtype MX Flood Drop Due To Response From Cache	Rate Flood	Periodic	DNS Query drops because the response was served from the cache during a UDP DNS Qtype MX Flood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNSMX Count UDP and Service Protection > DNS Profile > DNS Feature Controls > Generate Response From Cache Under Flood DNS Profile must be assigned to the SPP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Cache Drops
4	105	4105	DNS Cache: UDP Query Flood Drop Due To No Response From Cache	Rate Flood	Periodic	DNS Query drops because the response was not served from the cache during a	Service Protection > Service	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Cache

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
						UDP DNS Query Flood.	Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNS UDP Query and Service Protection > DNS Profile > DNS Feature Controls > Generate Response From Cache Under Flood DNS Profile must be assigned to the SPP	Drops
4	106	4106	DNS Cache: UDP Question Flood Drop Due To No Response From Cache	Rate Flood	Periodic	DNS Query drops because the response was not served from the cache during a UDP DNS Question Flood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNSQuestion Count UDP and Service Protection > DNS Profile > DNS Feature Controls > Generate	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Cache Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							Response From Cache Under Flood DNS Profile must be assigned to the SPP	
4	107	4107	DNS Cache: UDP Qtype All Flood Drop Due To No Response From Cache	Rate Flood	Periodic	DNS Query dropss because the response was not served from the cache during a UDP DNS Qtype All (ANY/*) Flood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNSAll UDP and Service Protection > DNS Profile > DNS Feature Controls > Generate Response From Cache Under Flood DNS Profile must be assigned to the SPP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Cache Drops
4	109	4109	DNS Cache: UDP Qtype MX Flood Drop Due To No Response From Cache	Rate Flood	Periodic	DNS Query dropss because the response was not served from the cache during a UDP DNS Qtype MX Flood.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars >	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Cache Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							DNSMX Count UDP and Service Protection > DNS Profile > DNS Feature Controls > Generate Response From Cache Under Flood DNS Profile must be assigned to the SPP	
4	111	4111	DNS TCP Query Flood	Rate Flood	Interrupt	Effective rate limit for the dns-query threshold has been reached. Queries are rate-limited with no Query validations. Source validation is done at Layer 4.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > DNS Query TCP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > TCP Query Drops
4	112	4112	DNS TCP Question Flood	Rate Flood	Interrupt	Effective rate limit for the dns-question-count threshold has been reached. Queries are rate-limited with no Query validations. Source validation is done at Layer 4.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds >> Scalars > DNS Question Count TCP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > TCP Question Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
4	113	4113	DNS TCP Fragment Flood	Rate Flood	Interrupt	Effective rate limit for the dns-fragment threshold has been reached. Queries are rate-limited with no Query validations. Source validation is done at Layer 4.	Service Protection > Service Protection Policy > Service Protection Policy Rule > Thresholds > Scalars > DNS Fragment TCP	Monitor > Drops Monitor >Flood Drops > Layer 7 > DNS > Fragment Drops
4	114	4114	DNS TCP Zone Transfer Flood	Rate Flood	Interrupt	Effective rate limit for the dns-zone-xfer threshold has been reached. Queries are rate-limited with no Query validations. Source validation is done at Layer 4.	Service Protection > Service Protection Policy > Service Protection Policy Rule > Thresholds > Scalars > DNS Zone Transfer TCP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > TCP Zone Transfer Drops
4	115	4115	DNS TCP MX Flood	Rate Flood	Interrupt	Effective rate limit for the dns-mx threshold has been reached. Queries are rate-limited with no Query validations. Source validation is done at Layer 4.	Service Protection > Service Protection Policy > Service Protection Policy Rule > Thresholds > Scalars > DNS MX Count TCP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > TCP MX Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
4	116	4116	DNS TCP All Flood	Rate Flood	Interrupt	Effective rate limit for the dns-all threshold has been reached. Queries are rate-limited with no Query validations. Source validation is done at Layer 4.	Service Protection > Service Protection Policy > Service Protection Policy Rule > Thresholds > Scalars > DNS All TCP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > TCP ALL Drops
4	117	4117	DNS UDP Unexpected Query before Response	Rate Flood	Periodic	UDP Drops due to DQRM duplicate query check (more then 3 identical Queries (Source, XID) per second	Service Protection > DNS Profile > DNS Feature Controls > Duplicate Query Check DNS Profile must be assigned to the SPP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Unexpected Query Drops
4	118	4118	DNS TCP Unexpected Query before Response	Rate Flood	Periodic	TCP Drops due to DQRM duplicate query check.	Service Protection > DNS Profile > DNS Feature Controls > Duplicate Query Check DNS Profile must be assigned to the SPP	Monitor > Drops Monitor > Flood Drops > Layer 7 > DNS > Unexpected Query Drops
4	120	4120	DNS Query Blocked (Blocklisted Domains)	ACL	Periodic	DNS Query or Response ACL Drops due to Blocklisted Domains and Domain	Global Protection > Blocklist > Blocklisted Domains Service	Monitor > Drops Monitor > ACL Drops > Layer 7 > DNS > Query Blocked Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
						Reputation	Protection > DNS Profile > DNS Feature Controls > Domain Reputation	
4	121	4121	DNS Resource Record Type Deny	ACL	Periodic	DNS Query ACL drops due to Resource Record ACL	Service Protection > DNS Profile > DNS Feature Controls > DNS Resource Record Type ACL DNS Profile must be assigned to the SPP	Monitor > Drops Monitor >ACL Drops > Layer 7 > DNS > DNS Resource Record Type Drops
4	122	4122	DNS Query Anomaly: UDP Session Reuse	Anomaly	Periodic	DNS UDP Query reuse session within one second	Service Protection > DNS Profile	Monitor > Drops Monitor >L7> Anomaly Drops > DNS > Query
4	201	4201	HTTP Header Range Present Anomaly	Header anomaly	Periodic	Drops due to packets with a header range request.	Service Protection > HTTP Profile > Drop Range Header DNS Profile must be assigned to the SPP	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > HTTP > Range Present
4	203	4203	Incomplete HTTP Request	Header anomaly	Periodic	Drops due to HTTP requests that do not end in the correct end-of-packet information.	Service Protection > HTTP Profile > Incomplete Request Action = Drop or	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > HTTP > Incomplete HTTP Request

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							Aggressive Aging DNS Profile must be assigned to the SPP	
4	204	4204	SSL Renegotiation	Anomaly	Periodic	Drop due to SSL/TLS Renegotiation Check	Service Protection > SSL/TLS Profile > Renegotiation Check DNS Profile must be assigned to the SPP	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > SSL > SSL Renegotiation
4	205	4205	NTP Request Flood	Rate Flood	Interrupt	Rate Threshold for NTP Requests has been exceeded.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > NTP Request Flood	Monitor > Drops Monitor > Flood Drops > Layer 7 > NTP > Request Flood Drops
4	206	4206	NTP Response Flood	Rate Flood	Interrupt	Rate Threshold for NTP Responses has been exceeded.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > NTP Response Flood	Monitor > Drops Monitor > Flood Drops > Layer 7 > NTP > Response Flood Drops

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
4	207	4207	NTP Broadcast Flood	Rate Flood	Interrupt	Rate Threshold for NTP Broadcasts has been exceeded.	SeService Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > NTP Broadcast Flood	Monitor > Drops Monitor > Flood Drops > Layer 7 > NTP > Broadcast Flood Drops
4	208	4208	NTP Reflection ACL	ACL	Periodic	Drops due to NTP Reflection Deny option. Blocks NTP Mode 6 (varlist) and Mode 7 (monlist) Queries or Responses.	Service Protection > NTP Profile > Reflection Deny NTP Profile must be assigned to the SPP	Monitor > Drops Monitor > ACL Drops > Layer 7 > NTP > NTP Reflection ACL Drops
4	209	4209	NTP Version Anomaly	NTP Header Anomaly	Periodic	NTP Version and Modes must match currently ratified versions (Version =1-4 and Mode >0 if Version =1).	Service Protection > NTP Profile > Version Anomaly Check NTP Profile must be assigned to the SPP	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > NTP > Header
4	210	4210	NTP Stratum Anomaly	NTP Header Anomaly	Periodic	Stratum must be 1-16 (17-255 are invalid). If Stratum >2, Refence ID cannot be null/empty.	Service Protection > NTP Profile > Stratum Anomaly Check NTP Profile must be assigned to the SPP	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > NTP > Header
4	211	4211	NTP Data Length Anomaly	NTP Header Anomal	Periodic	Enforces minimum and maximum data lengths defined in	Service Protection >	Monitor > Drops Monitor

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
				y		NTP Versions 1-4)	NTP Profile > Data Length Anomaly Check NTP Profile must be assigned to the SPP	>Anomaly Drops > Layer 7 > NTP > Header
4	212	4212	NTP Control Header Anomaly	NTP Header Anomaly	Periodic	Examines Control Header for 10 different Anomalies and drops if seen.	Service Protection > NTP Profile > Control Header Anomalies Check NTP Profile must be assigned to the SPP	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > NTP > Header
4	213	4213	NTP Duplicate Request Before Response	Anomaly	Periodic	Drops identical requests in a few seconds before a reply (mini-Flood).	Service Protection > NTP Profile > Retransmission Check NTP Profile must be assigned to the SPP	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > NTP > State
4	214	4214	NTP Unsolicited Response	Rate Flood treated like Anomaly	Periodic	Drops Responses where the Query was not recorded in NTP Response Matching (NRM)table. Use ONLY with symmetric traffic or asymmetric traffic where both links traverse FortiDDoS.	Service Protection > NTP Profile > Unsolicited Response Check NTP Profile must be assigned to the SPP	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > NTP > State
4	215	4215	NTP State	State Anomal	Periodic	Drops Queries	Service	Monitor >

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
			Anomalies: Sequence mismatch	y		where Sequence number is incorrect. Normally only used when hosting NTP Servers	Protection > NTP Profile > Sequence Mismatch Check NTP Profile must be assigned to the SPP	Drops Monitor > Anomaly Drops > Layer 7 > NTP > State
4	218	4218	NTP State Anomalies: Mode Mismatch	State Anomaly	Periodic	Client Query/Server Response Modes do not match 1/2 or 3/4. If NTP Reflection ACL not enabled, then also checks or not matching Modes 6/6 or 7/7. Anything other than the above mode pairs is dropped as mismatched.	Service Protection > NTP Profile > Mode Mismatch Check NTP Profile must be assigned to the SPP	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > NTP > State
4	219	4219	NTP Response Per Destination	Rate Flood	Interrupt	Rate Threshold for NTP Responses Per Destination has been exceeded. This inidcates a reflected NTP Response Flood towards a single destination.	Service Protection > Service Protection Policy (List) > Service Protection Policy > Thresholds > Scalars > NTP Response Per Destination	Monitor > Drops Monitor > Flood Drops > Layer 7 > NTP > Response Per Destination Flood Drops
4	224	4224	SSL/TLS Protocol Anomaly	Anomaly	Periodic	Drop due to SSL/TLS profile's Procotol Anomaly check	Service Protection > SSL/TLS Profile > Procotol	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > SSL > SSL

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							Anomaly SSL/TLS Profile must be assigned to the SPP	Protocol
4	225	4225	SSL/TLS Version Anomaly	Anomaly	Periodic	Drop due to SSL/TLS profile's Version Anomaly check	Service Protection > SSL/TLS Profile > Version Anomaly SSL/TLS Profile must be assigned to the SPP	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > SSL > SSL Version
4	226	4226	SSL/TLS Cipher Anomaly	Anomaly	Periodic	Drop due to SSL/TLS profile's Cipher Anomaly check	Service Protection > SSL/tLS Profile > Cipher Anomaly SSL/TLS Profile must be assigned to the SPP	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > SSL > SSL Cipher
4	227	4227	SSL/TLS Incomplete Request Anomaly	Anomaly	Periodic	Drop due to SSL/TLS profile's Block Incomplete Request check	Service Protection > SSL/TLS Profile > Block Incomplete Request SSL/TLS Profile must be assigned to the SPP	Monitor > Drops Monitor > Anomaly Drops > Layer 7 > SSL > SSL Incomplete Request
4	228	4228	SSL/TLS Incomplete Request: Source Flood	Rate Flood	Interrupt	Drop due to SSL/TLS profile's Block Source With Incomplete Request	Service Protection > SSL/TLS Profile > Block	Monitor > Drops Monitor > Flood Drops > Layer 7 > SSL >

Event code	Sub-code	Trap attack type	Event name	Category	Period	Description	Parameter	Graph
							Source With Incomplete Request SSL/TLS Profile must be assigned to the SPP	SSL/TLS Incomplete Request Source Flood

DDoS Attack log Directionality for TCP

Setup	Traffic Direction	Source	Destination	Source Port	Destination Port	Attack Log Direction	Protected IP
SYN	Outbound	Inside	Outside	High	Low	Outbound	Inside
ACK	Inbound	Outside	Inside	Low	High	Outbound	Inside
SYN	Inbound	Outside	Inside	High	Low	Inbound	Inside
ACK	Outbound	Inside	Outside	Low	High	Inbound	Inside
SYN	Outbound	Inside	Outside	High	High	Outbound	Inside
ACK	Inbound	Outside	Inside	High	High	Outbound	Inside
SYN	Inbound	Outside	Inside	High	High	Inbound	Inside
ACK	Outbound	Inside	Outside	High	High	Inbound	Inside
SYN	Outbound	Inside	Outside	Low	Low	Outbound	Inside
ACK	Inbound	Outside	Inside	Low	Low	Outbound	Inside
SYN	Inbound	Outside	Inside	Low	Low	Inbound	Inside
ACK	Outbound	Inside	Outside	Low	Low	Inbound	Inside

DDoS Attack log Directionality for UDP

Traffic Direction	Source	Destination	Source Port	Destination Port	Attack Log Direction	Protected IP
Outbound	Inside	Outside	High	Low	Outbound	Inside

Traffic Direction	Source	Destination	Source Port	Destination Port	Attack Log Direction	Protected IP
Inbound	Outside	Inside	Low	High	Inbound	Inside
Inbound	Outside	Inside	High	Low	Inbound	Inside
Outbound	Inside	Outside	Low	High	Outbound	Inside
Outbound	Inside	Outside	High	High	Outbound	Inside
Inbound	Outside	Inside	High	High	Inbound	Inside

Appendix B: Remote Syslog Reference

FortiDDoS Syslog

FortiDDoS supports Syslog features for the following:

- **Event Logs:** Refer to Configuring remote log server settings for event logs for more details about configuration.
- **Attack Logs:** Whenever a FortiDDoS appliance records an attack event in its own internal database for reporting, it also sends a Syslog event to an external Syslog server. The purpose of this logging is to have a persistent storage for or further analysis or future access. This feature can also be used for integrating with log analysis tools. The following sections describe about the Data path Syslog.

Configuration

FortiDDoS allows each SPP to send Attack Logs to 1 or 2 separate Syslog Servers. All DDoS attack events are sent to these individual Syslog servers. For each SPP, you can configure the IPv4 address of the Syslog server, the Syslog port on which the Syslog server listens, default being (UDP) 514. All SPPs can send to the same Syslog Servers but these must be configured per-SPP. See **Log & Report > Attack Log Remote**.

Remote attack log syslog limiting

Remote Attack Logs can be suppressed when the number of drops associated with the log is below a specific threshold. This threshold can be set via Log & Report > Log Configuration > Remote Log Settings. Please see here.

Format of the Syslog messages

FortiDDoS Syslog messages have a name/value based format. The following example shows the log messages received on a server: FortiDDoS uses the FortiAnalyzer syslog format which may not be completely compatible with RFCs.

Syslog for attack log

```
devid=FI200B3914000081 date=2017-10-18 time=11:10:00 tz=PDT.type=attack spp=1
evecode=2 evesubcode=18 description="UDP.port.flood" dir=1 protocol=17 sip=0.0.0.0
dip=61.255.0.253 dport=19160 dropcount=188 subnetid=61 facility=Local0 level=Notice
```

Syslog for event log

```
Facility kernel (0), Severity info (6) Msg: date=2017-10-18 time=14:27:36 tz=PDT
devid=FI200B3914000081 log_id=0000001065 type=event subtype=config
level=information msg_id=76823 user=admin ui=ssh(172.30.153.16) action=none
status=success reason=none msg="changed settings 'network-76' for 'ddos global spp-
policy spp'"
```

Field Names and their Interpretations

Name	Interpretation
devid	Device serial number
date	Event date
time	Event time
tz	Event time zone
type	This field describes type of event. Possible values: a string
subtype	This field describes sub type of event. Possible values: a string
spp	Service Protection Profile on which the attack was observed. Possible values: 0-7.
evecode	Event code. Possible values: 0-4 For description, refer to the Event code and description table.
evesubcode	Event sub-code. Possible values: 0-85. For description, refer to the Event code and description table.
dir	Direction of the event. Possible values are: 1 – Inbound, 0 – Outbound
protocol	This is the protocol field of the attack event. If the protocol of the attack was distinct in all the attack packets under this event, this field will have a numeric value. Possible values: 0-255
sip	Source IP of the packet if it was identified. Possible values: IP address in string format
dip	Destination IP of the packet if it was identified. Possible values: IP address in string format

Name	Interpretation
dport	Destination Port (for TCP or UDP protocols) of the packet if it was identified. Possible values: 0-65535
dropCount	The number of packets dropped due to this event. Possible values are: a number
log_id	Log id of the event. Possible values: a string
msg_id	Message id of the event. Possible values: 0-255
user	User name associated with the event. Possible values: a string
ui	This describes from where user logged in or changed settings. Possible values: a string
action	This describes user action like login, logout or so on. Possible values: a string
status	Status message of the event like success, failed or so on. Possible values: a string
reason	Reason message of the event. Possible values: a string
msg	Detailed message of the event. Possible values: a string
description	This field further describes the event. Possible values: a string
facility	For attack logs, FortiDDoS sends an attack log message with facility value 'local0'. For event logs, you can configure the **Facility** from FortiDDoS GUI under Log & Report > Event Log Remote.
level	For attack logs, FortiDDoS sends an attack log message with log level value 'notice'. For event logs, you can configure the **Log Level** from FortiDDoS GUI under Log & Report > Event Log Remote.

Event code (evecode) description

Event code	Description
0	Layer 2
1	Layer 3
2	Layer 4
3	Device events
4	Layer 7

Refer to the Event code and Subcode columns in the 'Log Reference' table under Appendix A for all attack events sent by Syslog.

Appendix C: Management Information Base (MIB)

The FortiDDoS-F SNMP agent supports a few management information blocks (MIBs).

Supported MIBs

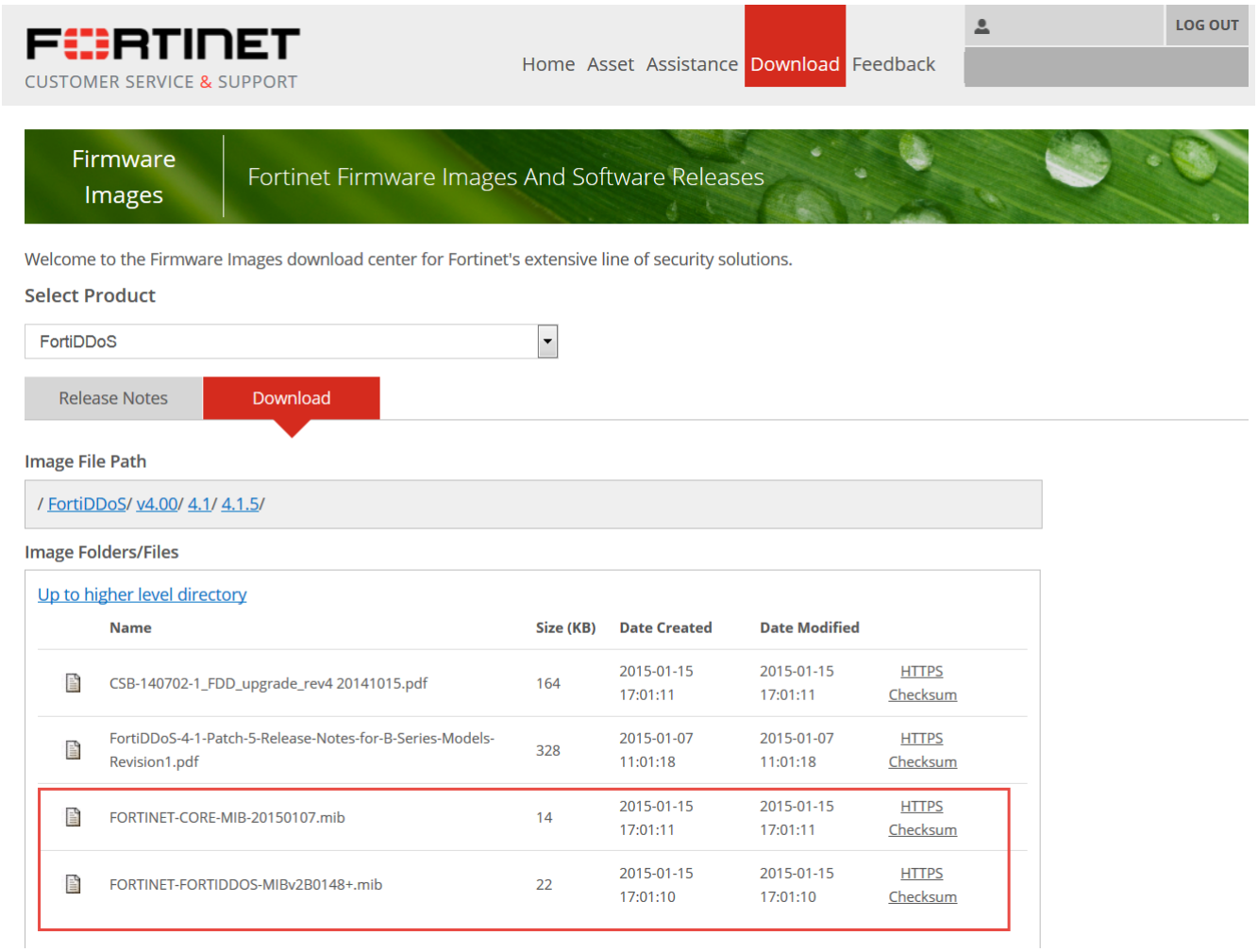
MIB or RFC	Description
Fortinet Technologies Inc. Core MIB	This Fortinet Technologies Inc.-proprietary MIB enables your SNMP manager to query for system information and to receive traps that are common to multiple Fortinet Technologies Inc. devices.
FortiDDoS-F MIB	This Fortinet Technologies Inc.-proprietary MIB enables your SNMP manager to query for FortiDDoS-F-specific information and to receive FortiDDoS-F-specific traps.
RFC 1213 (MIB II)	The FortiDDoS-F SNMP agent supports MIB II groups, except: • There is no support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). • Protocol statistics returned for MIB II groups (IP, ICMP, TCP, UDP, and so on) do not accurately capture all FortiDDoS-F traffic activity. More accurate information can be obtained from the information reported by the FortiDDoS-F MIB.
RFC 2665 (Ethernet-like MIB)	The FortiDDoS-F SNMP agent supports “Ethernet-like MIB information,” except the dot3Tests and dot3Errors groups.
RFC 2863 (IF-MIB)	FortiDDoS-F SNMP uses the linkDown and linkUP traps from IF-MIB, RFC 2863, section 6.
RFC 3411	“An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks”
RFC 3414	Partial support for “User-based Security Model (USM).”

To communicate with the FortiDDoS-F SNMP agent, you must first compile these MIBs into your SNMP manager. If the standard MIBs used by the SNMP agent are already compiled into your SNMP manager, you do not have to compile them again. The FortiDDoS-F SNMP implementation is read-only.

To view a trap or query’s name, object identifier (OID), and description, open its MIB file in a plain text editor. All traps sent include the message, the FortiDDoS-F appliance’s serial number, and hostname.

You can obtain the Fortinet MIB files from the Fortinet Technologies Inc. Service & Support website in the same section where you download firmware images. Go to Fortinet Support site.

Download MIB files from the Fortinet Service & Support website



Appendix D: Port Numbers

Communications between the FortiDDoS-F appliance, clients, servers, and FortiGuard Distribution Network (FDN) require that any routers and firewalls between them permit specific protocols and port numbers.

The following tables list the default port assignments used by FortiDDoS-F.

Default ports used by FortiDDoS-F for incoming traffic (listening)

Port Number	Protocol / Service	Purpose
N/A	ICMP	`ping` and `traceroute` responses.
22	TCP	SSH administrative CLI access.
23	TCP	Telnet administrative CLI access.
80	TCP	HTTP administrative web UI access.

Port Number	Protocol / Service	Purpose
161	UDP	SNMP queries.
443	TCP	HTTPS administrative web UI access FortiDDoS REST API Cloud Signaling REST API
6065	UDP	HA heartbeat. Multicast.
6066	UDP	HA configuration synchronization. Multicast.

Default ports used by FortiDDoS-F for outgoing traffic

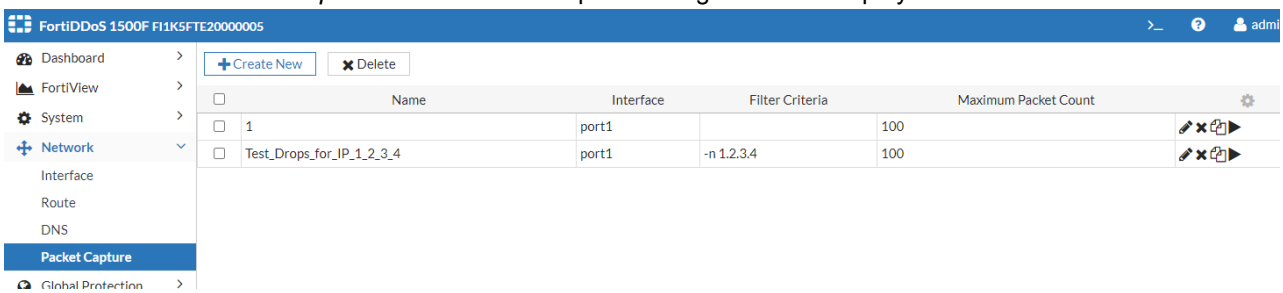
Port Number	Protocol / Service	Purpose
20, 21	TCP	FTP client.
25	TCP	SMTP for alert email.
49	TCP	TACAS+
53	UDP	DNS client.
69	UDP	TFTP client for backups, restoration, and firmware updates. See commands such as `execute backup` or `execute restore`.
123	UDP	NTP client.
162	UDP	SNMP traps.
389	TCP	LDAP authentication.
443	TCP	FortiGuard polling and update downloads. FortiDDoS REST API. Cloud Signaling REST API.
514	UDP	Syslog.
1812	TCP	RADIUS authentication.
6055	UDP	HA heartbeat. Multicast.
6056	UDP	HA configuration synchronization. Multicast.

Appendix E: Capturing Packets

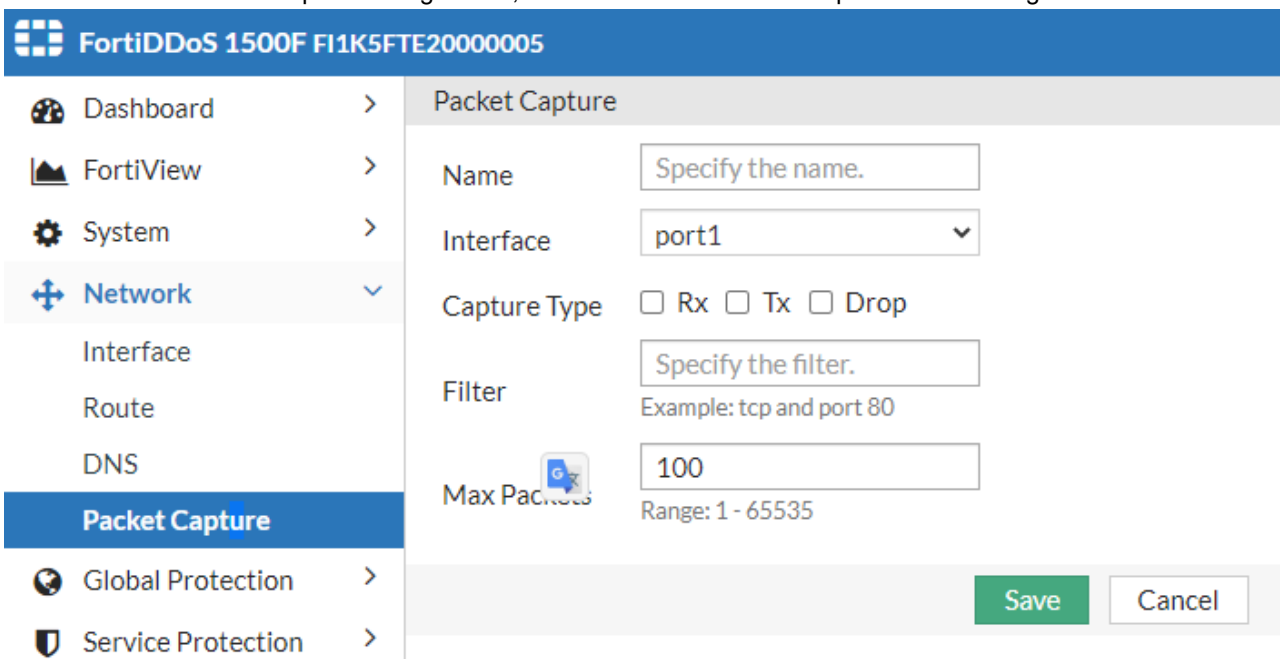
FortiDDoS allows you to capture packets via a GUI-based *tcpdump* function.

To configure Packet Capture:

1. Go to *Network* > *Packet Capture*. A list of saved capture configurations is displayed.



2. From that list, the right-side icons allow you to:
   - *Edit* - Edit that Packet Capture configuration. Note the Name cannot be edited after saving.
   - *Delete* - Delete that Packet Capture configuration. You may also select the checkbox to the left of each row and click Delete to remove one or more existing configurations.
   - *Clone* - Clone that Packet Capture configuration to create a new one with the same configuration.
   - *Run* - Run the Packet Capture.
   - *Stop* - Manually stops the Packet Capture if it is running.
   - *Download* - Download the resulting pcap after completion
3. To use an existing configuration, click *Run*.
4. To create a new Packet Capture configuration, click *+Create New* and complete the following fields:



Setting	Description
Name	a-Z, 0-9, “-“, “_” only, no spaces, 35 character maximum
Interface	Dropdown menu for the traffic interface from which to capture. For example, if looking or inbound Drops, capture from ports 2, 4 or 6.

Setting	Description
Capture Type	Rx – all received packets Tx – all transmitted packets Drops – dropped packets only
Filter	tcpdump filters such as src/dst, host, port, protocol name or proto #, and/or/not, etc.
Max Packets	Maximum (to 65535) packets to capture. During capture, the capture can be stopped manually.
Save	Save the configuration.

5. Onced saved, select the configuration to run from the displayed list.

Appendix F: Deleting Service Protection Policies (SPPs)