

F5[®] DDoS Hybrid Defender[™] : Setup

Version 13.1.0.3



Table of Contents

| | |
|--|-----------|
| Introducing DDoS Hybrid Defender..... | 5 |
| Introduction to DDoS Hybrid Defender..... | 5 |
| DDoS deployments | 5 |
| Example DDoS Hybrid Defender deployment..... | 7 |
| Installing DDoS Hybrid Defender for High Availability..... | 9 |
| Overview: Installing DDoS Hybrid Defender for High Availability..... | 9 |
| Performing initial setup..... | 9 |
| Manually licensing DDoS Hybrid Defender..... | 10 |
| Connecting two DDoS Hybrid Defender devices..... | 11 |
| Installing DDoS Hybrid Defender on device 1..... | 11 |
| Connecting with F5 Silverline..... | 12 |
| Configuring high availability on device 1..... | 12 |
| Checking the status of DDoS Hybrid Defender on device 2..... | 13 |
| Configuring the network on the high availability systems..... | 13 |
| Setting up remote logging..... | 15 |
| Installing a Stand-alone DDoS Hybrid Defender..... | 17 |
| Overview: Installing a Stand-alone DDoS Hybrid Defender..... | 17 |
| Performing initial setup..... | 17 |
| Manually licensing DDoS Hybrid Defender..... | 18 |
| Installing DDoS Hybrid Defender..... | 19 |
| Configuring the network for an inline stand-alone device..... | 19 |
| Configuring the network for out-of-band deployment..... | 21 |
| Setting up remote logging..... | 21 |
| Connecting with F5 Silverline..... | 22 |
| Protecting Against DDoS Attacks..... | 23 |
| Overview: Protecting against DDoS attacks..... | 23 |
| Protecting the network from DDoS attacks..... | 23 |
| Automatically setting system-wide DDoS vector thresholds..... | 24 |
| Manually setting system-wide DDoS vector thresholds..... | 25 |
| Bypassing DDoS checks..... | 27 |
| Configuring network bandwidth and scrubbing..... | 27 |
| Protecting network objects from DDoS attacks..... | 28 |
| How to protect different network objects from DDoS attacks..... | 30 |
| DDoS protected object attack types..... | 31 |
| DDoS device attack types..... | 35 |
| Preventing DDoS Flood and Sweep Attacks..... | 43 |
| About DoS sweep and flood attack prevention..... | 43 |
| Protecting against single-endpoint flood and sweep attacks..... | 43 |
| Protecting objects system-wide from flood attacks..... | 44 |
| Viewing DDoS Reports, Statistics, and Logs..... | 47 |
| Investigating DoS attacks and mitigation..... | 47 |

| | |
|---|-----------|
| Sample DoS Dashboards..... | 49 |
| Displaying DDoS Event logs..... | 50 |
| Displaying DoS Application Events logs..... | 51 |
| Creating customized DoS reports..... | 51 |
| Adjusting Global Settings..... | 53 |
| Overview: Adjusting global settings..... | 53 |
| Adjusting global settings..... | 53 |
| Global Settings..... | 53 |
| Sending the blacklist to a next-hop router..... | 55 |
| Updating DDoS Hybrid Defender..... | 57 |
| Overview: Updating DDoS Hybrid Defender..... | 57 |
| Downloading DDoS Hybrid Defender..... | 57 |
| Updating DDoS Hybrid Defender..... | 57 |
| Legal Notices..... | 59 |
| Legal notices..... | 59 |

Introducing DDoS Hybrid Defender

Introduction to DDoS Hybrid Defender

F5® DDoS Hybrid Defender™ protects your organization against a wide range of DDoS attacks using a multi-pronged approach. By combining on-premises and cloud technologies, analytics, and advanced methods, DDoS Hybrid Defender is a hybrid solution that detects network and application layer attacks, and is easy to deploy and manage.

DDoS Hybrid Defender mitigates against the full spectrum of DDoS attacks including:

- Network capacity attacks
- DNS and SIP protocol volumetric attacks
- HTTP and HTTPS volumetric attacks
- HTTP and HTTPS CPU-based (heavy URL) attacks

You can specify which objects to protect on the network, assigning the appropriate protections to network devices and application servers, and prevent attackers from exhausting network resources and impacting application availability. DDoS Hybrid Defender can be installed for high availability (two systems) or as a stand-alone system.

DDoS deployments

The deployment you use for DDoS Hybrid Defender™ depends on the needs of your organization. For maximum DDoS protection, it is recommended that you deploy DDoS Hybrid Defender inline. However, it can also be deployed out of band, or in locations where symmetric data flows are not guaranteed. Typical locations for the placement of DDoS Hybrid Defender are at the edge of the network or at the edge of the data center as shown in the figure.

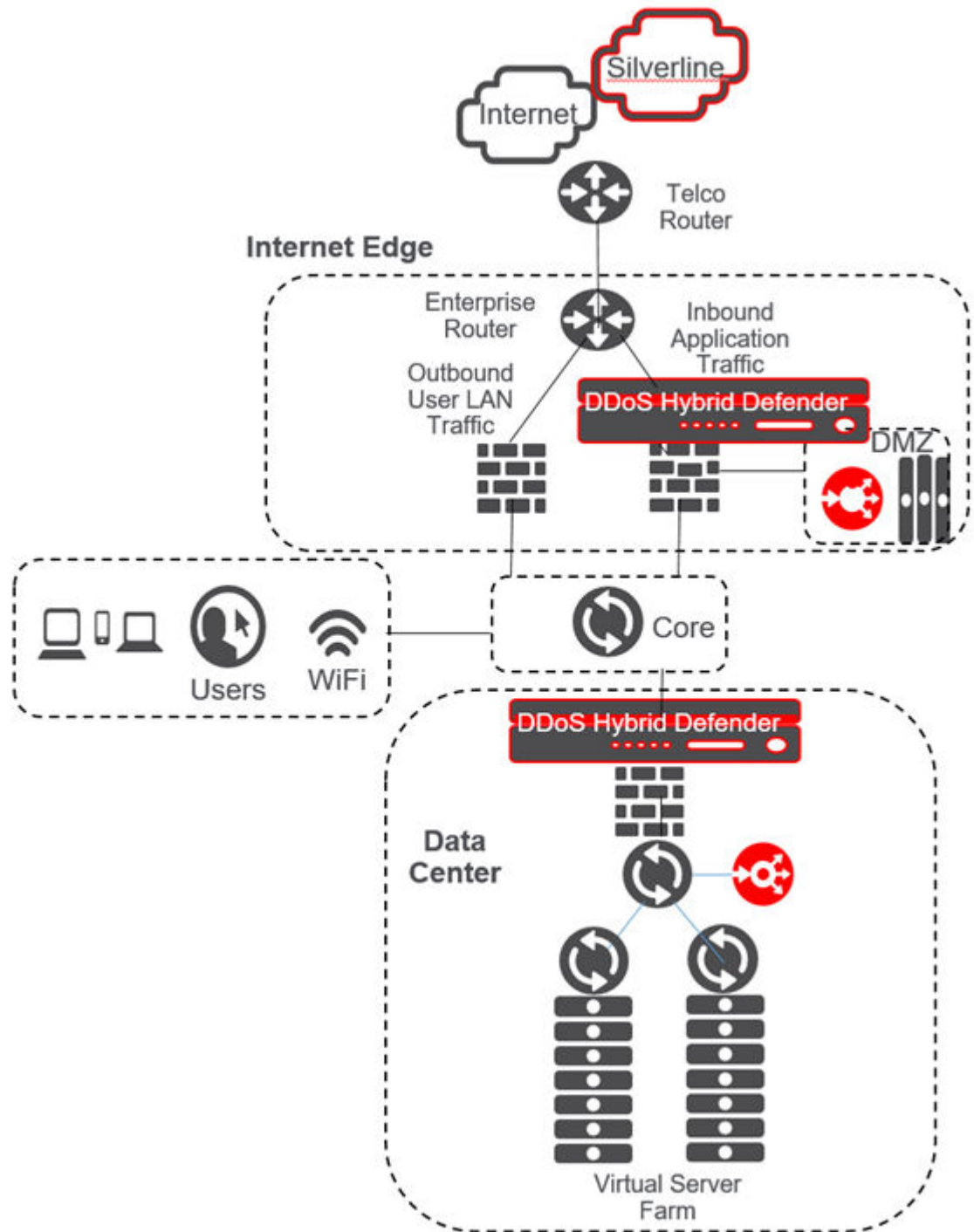


Figure 1: Points in the network for DDoS defense

Inline deployment

DDoS Hybrid Defender provides maximum protection when deployed inline in one of two ways:

- Bridged mode with VLAN groups
- Routed mode

For bridged mode, you can place DDoS Hybrid Defender in transparent mode on a link between two Layer 3 devices. This way, the IP addresses on each end of the link do not have to change. You do this by

creating VLAN groups on DDoS Hybrid Defender. The VLANs and the VLAN group configured are purely internal, and are used to bridge traffic from one port to another within DDoS Hybrid Defender.

For routed mode, you can insert DDoS Hybrid Defender at the edge of the network without disturbing the current configuration. It is possible to pick and choose the networks whose traffic goes through the DDoS Hybrid Defender, and let the rest continue to follow the path it was previously taking.

Step by step instructions are provided in the installation chapter.

Out of band deployment

You can deploy DDoS Hybrid Defender out of band in two ways:

- Set up a Layer 2 switch with span ports so that it mirrors traffic onto DDoS Hybrid Defender.
- Configure network devices so that they send Netflow data to DDoS Hybrid Defender.

If using span ports, you can configure DDoS Hybrid Defender to perform DDoS detection by listening to traffic that is mirrored from a Layer 2 switch. Of the various ports that can be mirrored on the DDoS Hybrid Defender, it is usually best to mirror the Layer 2 switch ports that connect to the firewall. Since firewalls are stateful devices, traffic typically flows through them in a symmetric fashion. Thus, mirroring the ports connected to the firewalls is a good way to send all the packets in a session directed through the firewall and on to DDoS Hybrid Defender. Using span ports, DDoS Hybrid Defender can use all L2 to L7 DDoS detection mechanisms.

Alternatively, you can configure DDoS Hybrid Defender to detect DDoS attacks by examining Netflow traffic sent to it. In this case, you can deploy DDoS Hybrid Defender anywhere in the network and configure it to receive Netflow streams on a Netflow listener IP address and port. Netflow traffic should be allowed through any firewalls that are in the path from devices sending Netflow data to the DDoS Hybrid Defender.

Step by step instructions are provided in the installation chapter.

Example DDoS Hybrid Defender deployment

DDoS Hybrid Defender™ guards against multiple types of attacks including protection for the device, protection for the data center, networks, and, optionally, offloading using F5 Silverline® cloud-based services.

Here is how it works: A DDoS Hybrid Defender™ system that is deployed in your network defends against DDoS Layer 3 through Layer 7 attacks as long the upstream Internet pipe is not saturated. When the upstream pipe is flooded, DDoS Hybrid Defender can signal the F5 Silverline Cloud Platform to help mitigate the attack. DDoS Hybrid Defender sends Silverline Cloud Platform the information that an attack was detected, and provides the application or CIDR definition, destination subnet, attack type, and the attack size.

The Hybrid Signaling feature enables enterprises with DDoS Hybrid Defender to integrate with F5 Silverline to divert traffic during large attacks. The F5 Silverline Cloud Platform scrubs the volumetric attack traffic and forwards the clean traffic to the customer's networks. The clean traffic is sent through GRE tunnels that were set up between the Silverline scrubbing centers and the customer's networks.

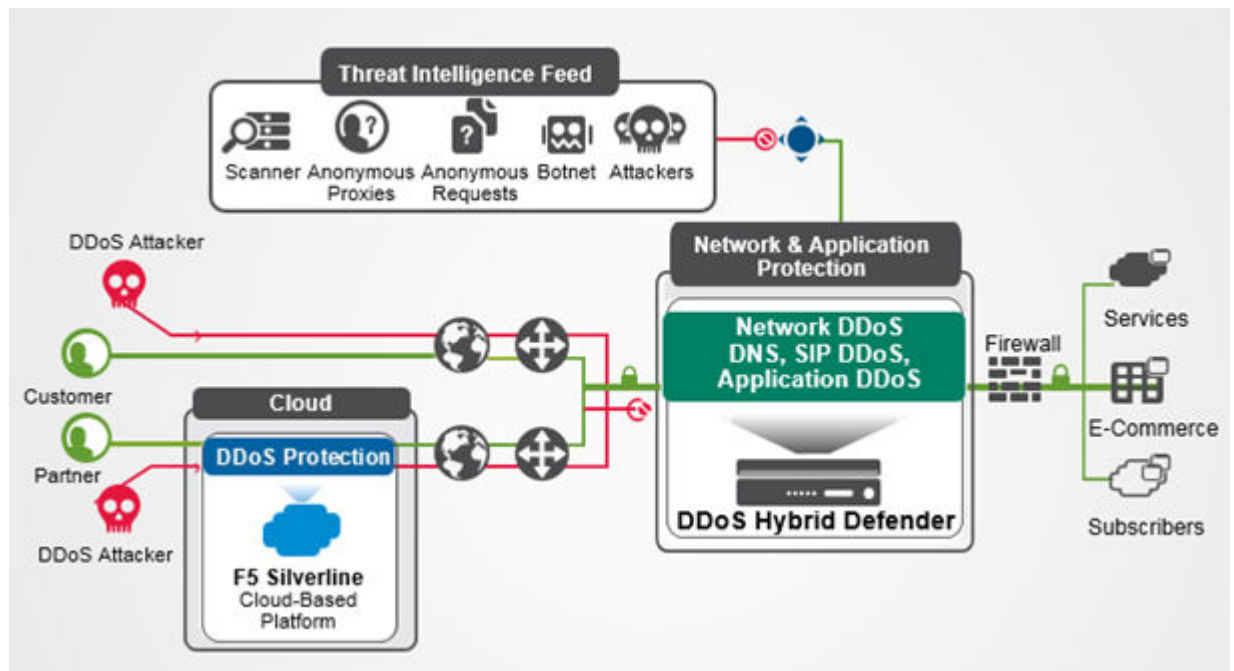


Figure 2: Example DDoS Hybrid Defender deployment

Installing DDoS Hybrid Defender for High Availability

Overview: Installing DDoS Hybrid Defender for High Availability

You can install DDoS Hybrid Defender™ onto a dedicated system (device 1) and set up a failover system that automatically takes over in case of system failure (device 2). The system processing traffic is called the *active system*. A second system is set up as a *standby system*, and data is synchronized between the active and standby systems. If the active system goes offline, the standby system become active, and begins processing traffic and protecting against DDOS attacks.

Note: To set up two DDoS Hybrid Defender devices for high availability, you need to follow the steps outlined in this section exactly in the order shown.

You can assign the management IP addresses from the LCD panel of the devices, or with a hypervisor if you are using the Virtual Edition.

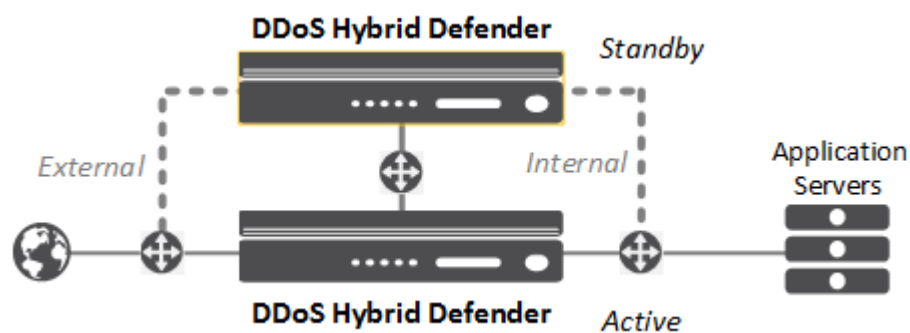


Figure 3: DDoS Hybrid Defender High-Availability deployment

You must have two DDoS Hybrid Defender systems to set up high availability. Before you begin, make sure you have this information for both devices:

- Base registration key
- Internal and external self-IP addresses
- Management IP address, network mask, and management route IP address
- Passwords for the root and admin accounts
- NTP server IP address (optional)
- Remote DNS lookup server IP address (required for F5 Silverline® integration or if resolving host names)

Performing initial setup

Before you begin, be sure to have the base registration key.

You need to perform an initial setup on your system before you can start to use DDoS Hybrid Defender™. Some of the steps vary, depending on the state your system is in when you begin, and whether you are using a physical device or a virtual edition.

If setting up two systems for high availability, you need to perform initial setup on both systems.

1. If this is a new system, specify the management IP address using the LCD panel or command line on the physical device, or using the appropriate hypervisor on the virtual edition.

2. From a workstation browser on the network connected to the system, type: `https://<management_IP_address>`.
3. At the login prompt, type the default user name `admin`, and password `admin`, and click **Log in**. The Setup utility screen opens.
4. Click **Next**. The License screen opens.
5. In the **Base Registration Key** field, type or paste the registration key.
You receive the registration key when you purchase DDoS Hybrid Defender. If you also have the add-on IP Intelligence service, specify the key in the **Add-On Key** field.
6. For **Activation Method**, leave it set to **Automatic** unless the system does not have Internet access. In that case, click **Manual** and follow the instructions for manually licensing DDoS Hybrid Defender.
7. Click **Activate**. The license is activated.
8. Click **Next**; the device certificate is displayed, and click **Next** again. The Platform screen opens.
9. For the **Management Port Configuration** setting, click **Manual**.
10. The **Management Port** setting should include the management interface details that were previously set up.
11. In the **Host Name** field, type the name of this system.
For example, `ddosdefender1.example.com`.
12. In the User Administration area, we strongly recommend that you change the Root and Admin Account passwords from the defaults. Type and confirm the new passwords.
The Root account provides access to the command line, and the Admin account accesses the user interface.
13. Click **Next**. The NTP (Network Time Protocol) screen opens.
14. Optional: To synchronize the system clock with an NTP server, in the **Address** field, type the IP address of the NTP server, and click **Add**.
15. Click **Next**. The DNS (Domain Name Server) screen opens.
16. To resolve host names on the DDoS Hybrid Defender system, set up the DNS and associated servers (required for IP Intelligence):
 - a) For the **DNS Lookup Server List**, in the **Address** field, type the IP address of the DNS server, and click **Add**.
 - b) If you use BIND servers, add them to the **BIND Forwarder Server List**.
 - c) For doing local domain lookups to resolve local host names, add them to the **DNS Search Domain List**.
17. Click **Finished**.

If the system is connected to the Internet, it is now licensed and ready for you to install DDoS Hybrid Defender. If the system is not connected to the Internet, you have to manually activate the license.

Manually licensing DDoS Hybrid Defender

If the DDoS Hybrid Defender™ system is not connected to the Internet, use this procedure to manually activate the license. Otherwise, skip this task.

If setting up two systems for high availability, you have to activate the license on both systems.

1. From a workstation on the network connected to the system, type: `https://<management_IP_address>`.

2. At the login prompt, type the default user name `admin`, and password `admin`, and click **Log in**.
The Setup utility screen opens.
3. Click **Next**.
The License screen opens.
4. In the **Base Registration Key** field, type or paste the registration key.
You receive the registration key when you purchase DDoS Hybrid Defender. If you also have the add-on IP Intelligence service, specify the key in the **Add-On Key** field.
5. For the **Activation Method** setting, select **Manual** and click the **Generate Dossier** button.
The dossier is displayed in the **Device Dossier** field.
6. Select and copy the text displayed in the **Device Dossier** field, and click the **Click here to access F5 Licensing Server** link.
Alternatively, you can navigate to the F5 license activation portal at <https://activate.f5.com/license/>.
7. Click **Activate License**.
8. Into the **Enter your dossier** field, paste the dossier.
Alternatively, if you saved the file onto your system, click the **Choose File** button and navigate to the file.
The license key text is displayed.
9. Copy the license key, and paste it into the **License Text** field.
10. Continue with the Setup Utility.

Connecting two DDoS Hybrid Defender devices

For you to set up two DDoS Hybrid Defender™ devices for high availability, they need to be physically connected in the network.

1. Connect the two DDoS Hybrid Defender™ devices as required by your network configuration.
2. Note the interfaces and VLAN used to connect the devices.

The two systems are connected to each other and both systems are active, but not running the software yet.

Installing DDoS Hybrid Defender on device 1

Before you begin, you need to have access to the DDoS Hybrid Defender™ software from F5 (either on the system or by downloading it from F5), and have completed the initial setup on device 1, the one that will be the active device.

When installing two systems for high availability, you first install DDoS Hybrid Defender onto device 1, the system you want to set up as the active system. Device 1 must be the system with the highest management IP address.

1. Log in to DDoS Hybrid Defender device 1 using the administrator user name and password.
The system displays the Welcome screen.
2. On the Main tab, click **DoS Protection**.
Because the software has not yet been installed, the Import Package screen opens.
3. From the **Install Method** list, select **Use Onboard RPM**.
If the software is not on the device, you need to download the RPM onto your local system from F5 Downloads, then select **Upload RPM** to locate and upload that file.
4. Click **Install**.
The software is installed quickly, and the Protected Objects screen opens.

The DDoS Hybrid Defender software is installed on device 1, and the DoS configuration screens are now available.

Important: *If using Silverline DDoS protection with DDoS Hybrid Defender systems set up for high-availability, you next need to follow these same instructions to install DDoS Hybrid Defender on device 2. After that, you need to connect both devices to Silverline, and can proceed with setting up high availability.*

If not using Silverline, skip the next section, then proceed to set up high availability on device 1.

Connecting with F5 Silverline

Connecting with F5 Silverline® is optional, and is available for customers who have an active F5 Silverline DDoS Protection subscription.

To integrate the F5 Silverline Cloud Platform with DDoS Hybrid Defender™ as a way to mitigate DDoS attacks, you need to register DDoS Hybrid Defender with F5 Silverline.

If setting up high availability, you need to register with Silverline on both devices.

1. On the Main tab, click **DoS Protection > Quick Configuration**.
2. On the menu bar, click **Silverline**.
3. In the **Username** field, type the user name for an active Silverline DDoS Protection account. For example, `username@example.com`.
4. In the **Password** field, type the password for the Silverline DDoS Protection account.
5. In the **Service URL** field, type the URL or fully qualified domain name used to connect to the Silverline DDoS Protection service.
6. Click **Update** to save the credentials.
DDoS Hybrid Defender sends a registration request to the F5 Silverline Cloud Platform.
7. Log in to the F5 Silverline customer portal (<https://portal.f5silverline.com>) and specify DDoS Hybrid Defender as an **Approved Hybrid Signaling Device**.

Important: *Depending on your network configuration, you may need to add a VLAN and route to enable DDoS Hybrid Defender to communicate with Silverline.*

DDoS Hybrid Defender is now integrated with the Silverline Cloud Platform.

When configuring the device or objects to protect, you will need to select the **Silverline** check box to send information about DDoS attacks to the Silverline Cloud Platform.

Configuring high availability on device 1

Before you can set up a failover device, you must have installed DDoS Hybrid Defender™ on one of the two devices. That system must connect to a second system that uses the same hardware platform.

To ensure high availability, you can configure an HA VLAN that connects to and synchronizes data between the active and standby systems. You perform this task by logging in to device 1.

1. On the Main tab, click **DoS Protection > Quick Configuration**.
2. On the menu bar, click **High Availability**.
On the High Availability screen, the HA Cluster Configuration is displayed, and shows partial configuration of the device on which you are working (device 1).
3. Click the management IP address of device 1, and specify this information:
 - a) Type the **Username** and **Password** of the system administrator account on device 1.
 - b) If your network requires a **VLAN Tag**, type the number (1-4094). Otherwise, leave it blank.

- c) Click **Select Interface** and select the interface to connect to the standby system. If you specified a VLAN tag and want to accept only frames that contain VLAN tags, select **Tagged**; otherwise, leave it unselected.

You can associate multiple VLANs with tagged interfaces, but you can associate only one VLAN with untagged interfaces.

- d) In the **IP Address/Mask** field, type the IP address and netmask that specifies the HA interface.

4. Click Remote Device Management IP, and specify this information for the standby system:

- a) In the **Management IP Address** field, type the management IP address of the remote device (device 2) to use for high availability.
- b) Type the **Username** and **Password** of the system administrator account on device 2.
- c) If your network requires a **VLAN Tag**, type the number (1-4094). Otherwise, leave it blank.
- d) Click **Select Interface** and select the interface to connect to the active system. If you specified a VLAN tag and want to accept only frames that contain VLAN tags, select **Tagged**; otherwise, leave it unselected.
- e) In the **IP Address/Mask** field, type the IP address and netmask of the HA interface.

5. Click Submit.

Device 1 becomes the Active device and device 2 is the Standby device. In the upper left corner of the screen it says ONLINE (ACTIVE) on device 1.

You have set up the two systems for high availability. After you complete setting up the two systems and configuring DDoS, the standby or failover system will be able to automatically take over and handle DDoS protection if the active system goes offline.

Next, you need to install DDoS Hybrid Defender on the standby system.

Checking the status of DDoS Hybrid Defender on device 2

You can now check the status of DDoS Hybrid Defender on device 2, the system that is set up as the standby system.

In the upper left corner, if the two systems are configured properly, it says ONLINE (STANDBY). You can proceed to configure the network on both systems. However, note that you should configure DoS protection on the Active device.

Configuring the network on the high availability systems

You must configure the network to create the workflow on both the active and standby DDoS Hybrid Defender™ systems. You do this by configuring VLANs (virtual local area networks), and associating the physical interfaces on the system with them. The way you set up the system depends on your network organization. Here are some of the configurations to consider:

- Use the default VLAN setup (L2 bridge mode), for example, if you use switch topology
- Use Virtual Wire (L2Wire) to set up the system as an inline L2 transparent mode device
- Define VLANs, if the system uses routed technology
- Define routes as needed to direct traffic.

Note: If you are using the BIG-IP® Virtual Edition, to set up the network as described here, you must create a security policy on the vSwitch. Configure the security policy to accept the **Promiscuous Mode** and **Forged Transmits** policy exceptions. For details about these options, see the *VMware ESX or ESXi Configuration Guide*.

1. Log in to DDoS Hybrid Defender device 1 using the administrator user name and password.
2. On the Main tab, click **DoS Protection > Quick Configuration**.
3. On the menu bar, click **Network Configuration**.

4. If your network relies on switch topology and all traffic ingress to DDoS Hybrid Defender is from one VLAN and traffic egress is through another VLAN, you can use the **defaultVLAN** setup. Otherwise, skip this step and go to the next one.
 - a) Click **defaultVLAN**.

This default VLAN group contains two VLANs, one for external traffic and one for internal traffic.
 - b) For the **Internal** and **External** fields, type a tag number (from 1 to 4094) for the VLAN.

The system automatically assigns a tag number if you do not specify a value.
 - c) For each VLAN, select the interface to use for traffic management, leave **Untagged** unselected, and click **Add**.

Click **Untagged** to allow the interface to accept traffic only from that VLAN, instead of from multiple VLANs.
 - d) In the **IP Address/Mask (Port Lockdown)** field, type the IP address and mask.
 - e) After the IP address, select the Port Lockdown setting: Select **Allow None** to accept no traffic; **Allow Default** to accept default protocols and services only; and **Allow All** to allow full access to this IP address (all TCP and UDP services).
 - f) Because you are setting up two systems for high availability, in the **Floating IP** field, type the IP address (it must be in the same subnet as the IP address), and select the Port Lockdown setting.

The floating IP address must be the same on both devices, and you must configure it on both devices since it represents the active device.

Tip: Using a floating IP address makes it so the router always goes to the same address regardless of which system is active.

- g) Click **Done Editing** to save the default network configuration.

The system configures the default network in the background creating 2 VLANs, a VLAN group, and assigns a self IP address.

5. To operate DDoS Hybrid Defender as an inline L2 transparent mode device, create a Virtual Wire configuration. (The ingress and egress VLANs are the same.) Click **Create** and configure it as follows:
 - a) Type a name for the Virtual Wire configuration, then select unique interfaces (or trunks) for the ingress and egress ports on the system (Member 1 and Member 2).
 - b) In the Configuration section, for **Define VLANs** select **Add**.
 - c) Type a name for the VLAN group.
 - d) If using tagged VLANs, type a tag number for the VLANs (an integer from 1 to 4095), select the **Members Tagged** check box,
 - e) Click **Add**.
 - f) If using other VLAN tags, create additional VLANs following the same steps.

The system creates a Virtual Wire configuration.

6. If DDoS Hybrid Defender uses routed topology, instead of using the default network, configure the network in the VLAN area. Click **Create** and set up each VLAN as follows:
 - a) Type a name, VLAN tag, then select the interface for the VLAN, and click **Add**.
 - b) In the **IP Address/Mask (Port Lockdown)** field, type the IP address and mask that specifies a range of IP addresses spanning the hosts in the VLAN.
 - c) After the IP address, select the Port Lockdown setting: Select **Allow None** to accept no traffic; **Allow Default** to accept default protocols and services only; and **Allow All** to activate TCP and UDP services.
 - d) Optional: To share an IP address between two high availability devices (such as if data passes through a router on the way to DDoS Hybrid Defender), in the **Floating IP Address/Mask (Port**

Lockdown) field, type the floating IP address (it must be in the same subnet as the IP address), and select the Port Lockdown setting.

The floating IP address must be the same on both devices, and you must configure it on both devices since it represents the active device.

Tip: Using a floating IP address makes it so the router always goes to the same address regardless of which system is active.

- e) Click **Done Editing** to save the VLAN configuration.
- f) Create as many VLANs as you need to connect to DDoS Hybrid Defender.
- 7. If your system is configured using routed mode and connects to other networks through additional routers, add the required routes so the traffic can reach its destination:
 - a) Next to **Routes**, click **Create**.
 - b) Type a name, destination IP address, netmask, and gateway IP address (this is the next hop router address).
 - c) Click **Done Editing** to save the route.
- 8. Click **Update** to save the network configuration.
- 9. Log in to DDoS Hybrid Defender device 2 using the administrator user name and password.
- 10. Repeat the network configuration steps (2-8) on device 2, using a similar configuration.

Tip: The names of the VLANs (if you added new VLANs), VLAN tags, floating IP address, and routes (if added) should be the same on both systems.

The active and standby DDoS Hybrid Defender systems are set up to work within your network for most typical configurations. The network configurations are not synchronized between the two devices because they need to differ. However, other settings that you configure on the active device will be synchronized with the standby device.

At this point, you can start configuring DDoS Hybrid Defender on the active system. You can set up remote logging and Silverline, if you are using those features. Then you can begin setting up DDoS protection. All changes you make on the active system are synchronized automatically with the standby system.

Setting up remote logging

You can specify one remote logging destination on DDoS Hybrid Defender™. Set up remote logging if you want to consolidate statistics gathered from multiple appliances onto a Security Information and Event Management (SIEM) device, such as Arcsight or Splunk.

If setting up high availability, configure remote logging on the active device.

1. On the Main tab, click **DoS Protection > Quick Configuration**.
2. On the menu bar, click **Logging**.
3. In the Remote Logging area, from the **Format** list, select the log format used on the remote logging server: **Arcsight** or **Splunk**.
4. In the **Destination IP Address** field, type the IP address of the remote logging server.
5. In the **Port** field, type the port number used for the remote logging server.
6. Click **Commit Changes to System** to save the changes.

Important: Depending on your network configuration, you may need to add a VLAN and route to enable DDoS Hybrid Defender to communicate with the remote logging server.

Event logs from DDoS Hybrid Defender are sent to the remote logging server in the format you specified.

Installing a Stand-alone DDoS Hybrid Defender

Overview: Installing a Stand-alone DDoS Hybrid Defender

You can install DDoS Hybrid Defender™ onto a dedicated system approved for the software. You can deploy the system inline or out-of-band. For out-of-band deployments, you can set up the system in one of two ways: as a span port or using NetFlow. A span port analyzes mirrored packets, and NetFlow listens for and reviews metadata.

Before you start, you must have assigned the management IP address on the LCD panel of the device, or with a hypervisor if using the Virtual Edition. This procedure is for installing a single, stand-alone DDoS Hybrid Defender system to protect against DDoS attacks. If you have two systems and want to install them for high availability, follow the steps described in *Installing DDoS Hybrid Defender for High Availability*.

Make sure you have this information available:

- Base registration key
- Internal and external self-IP addresses
- Management IP address, network mask, and management route IP address
- Passwords for the root and admin accounts
- NTP server IP address (optional)
- Remote DNS lookup server IP address (required for F5 Silverline® integration or if resolving host names)

Performing initial setup

Before you begin, be sure to have the base registration key.

You need to perform an initial setup on your system before you can start to use DDoS Hybrid Defender™. Some of the steps vary, depending on the state your system is in when you begin, and whether you are using a physical device or a virtual edition.

If setting up two systems for high availability, you need to perform initial setup on both systems.

1. If this is a new system, specify the management IP address using the LCD panel or command line on the physical device, or using the appropriate hypervisor on the virtual edition.
2. From a workstation browser on the network connected to the system, type: `https://<management_IP_address>`.
3. At the login prompt, type the default user name `admin`, and password `admin`, and click **Log in**. The Setup utility screen opens.
4. Click **Next**. The License screen opens.
5. In the **Base Registration Key** field, type or paste the registration key.
You receive the registration key when you purchase DDoS Hybrid Defender. If you also have the add-on IP Intelligence service, specify the key in the **Add-On Key** field.
6. For **Activation Method**, leave it set to **Automatic** unless the system does not have Internet access. In that case, click **Manual** and follow the instructions for manually licensing DDoS Hybrid Defender.
7. Click **Activate**. The license is activated.

8. Click **Next**; the device certificate is displayed, and click **Next** again.
The Platform screen opens.
9. For the **Management Port Configuration** setting, click **Manual**.
10. The **Management Port** setting should include the management interface details that were previously set up.
11. In the **Host Name** field, type the name of this system.
For example, `ddosdefender1.example.com`.
12. In the User Administration area, we strongly recommend that you change the Root and Admin Account passwords from the defaults. Type and confirm the new passwords.
The Root account provides access to the command line, and the Admin account accesses the user interface.
13. Click **Next**.
The NTP (Network Time Protocol) screen opens.
14. Optional: To synchronize the system clock with an NTP server, in the **Address** field, type the IP address of the NTP server, and click **Add**.
15. Click **Next**.
The DNS (Domain Name Server) screen opens.
16. To resolve host names on the DDoS Hybrid Defender system, set up the DNS and associated servers (required for IP Intelligence):
 - a) For the **DNS Lookup Server List**, in the **Address** field, type the IP address of the DNS server, and click **Add**.
 - b) If you use BIND servers, add them to the **BIND Forwarder Server List**.
 - c) For doing local domain lookups to resolve local host names, add them to the **DNS Search Domain List**.
17. Click **Finished**.

If the system is connected to the Internet, it is now licensed and ready for you to install DDoS Hybrid Defender. If the system is not connected to the Internet, you have to manually activate the license.

Manually licensing DDoS Hybrid Defender

If the DDoS Hybrid Defender™ system is not connected to the Internet, use this procedure to manually activate the license. Otherwise, skip this task.

If setting up two systems for high availability, you have to activate the license on both systems.

1. From a workstation on the network connected to the system, type: `https://<management_IP_address>`.
2. At the login prompt, type the default user name `admin`, and password `admin`, and click **Log in**.
The Setup utility screen opens.
3. Click **Next**.
The License screen opens.
4. In the **Base Registration Key** field, type or paste the registration key.
You receive the registration key when you purchase DDoS Hybrid Defender. If you also have the add-on IP Intelligence service, specify the key in the **Add-On Key** field.
5. For the **Activation Method** setting, select **Manual** and click the **Generate Dossier** button.
The dossier is displayed in the **Device Dossier** field.
6. Select and copy the text displayed in the **Device Dossier** field, and click the **Click here to access F5 Licensing Server** link.
Alternatively, you can navigate to the F5 license activation portal at `https://activate.f5.com/license/`.

7. Click **Activate License**.
8. Into the **Enter your dossier** field, paste the dossier.
Alternatively, if you saved the file onto your system, click the **Choose File** button and navigate to the file.
The license key text is displayed.
9. Copy the license key, and paste it into the **License Text** field.
10. Continue with the Setup Utility.

Installing DDoS Hybrid Defender

Before you begin, you need to have access to the DDoS Hybrid Defender™ software from F5 (either on the system or downloaded from F5), and have completed the initial setup.

You can install DDoS Hybrid Defender on the system.

1. Log in to DDoS Hybrid Defender with the administrator user name and password.
The system displays the Welcome screen.
2. On the Main tab, click **DoS Protection**.
3. From the **Install Method** list, select **Use Onboard RPM**.
If the software is not on the device, you need to download the RPM onto your local system from F5 Downloads, then select **Upload RPM** to locate and upload that file.
4. Click **Install**.
The software is installed quickly, and the Protected Objects screen opens.

The DDoS Hybrid Defender software is installed. The next time you log in, you will be able to access the DoS Protection screens.

Next, you can begin configuring the network, then setting up DDoS Hybrid Defender to protect your networks and web applications from DoS attacks.

Configuring the network for an inline stand-alone device

You must first configure the network to create the workflow when installing DDoS Hybrid Defender™ as an inline device. You do this by creating VLANs (virtual local area networks), and associating the physical interfaces on the system with them. The way you set up the system depends on your network organization. Here are some of the configurations to consider:

- Use the default VLAN setup (L2 bridge mode), for example, if you use switch topology
- Use Virtual Wire (L2Wire) to set up the system as an inline L2 transparent mode device
- Define VLANs, if the system uses routed technology
- Define routes as needed to direct traffic.

Note: If using the BIG-IP Virtual Edition, to set up the network as described here, you must create a security policy on the vSwitch. Configure the security policy to accept the **Promiscuous Mode** and **Forged Transmits** policy exceptions. For details about these options, see the VMware ESX or ESXi Configuration Guide.

1. On the Main tab, click **DoS Protection > Quick Configuration**.
2. On the menu bar, click **Network Configuration**.
3. If your network relies on switch topology and all traffic ingress to DDoS Hybrid Defender is from one VLAN and traffic egress is through one VLAN, you can use the **defaultVLAN** setup. Otherwise, skip this step and go to step 4.
 - a) Click **defaultVLAN**.

This VLAN group contains two VLANs, one for external traffic and one for internal traffic.

- b) For the **Internal** and **External** fields, type a tag number (from 1 to 4094) for the VLAN.
The system automatically assigns a tag number if you do not specify a value.
- c) For each VLAN, select the interface to use for traffic management, leave **Untagged** unselected, and click **Add**.
- d) In the **IP Address/Mask (Port Lockdown)** field, type the IP address and mask.
- e) After the IP address, select the Port Lockdown setting: Select **Allow None** to accept no traffic; **Allow Default** to accept default protocols and services only; and **Allow All** to allow full access to this IP address (all TCP and UDP services).
- f) Click **Done Editing** to save the default network configuration.

The network is set up using the default network. You do not need to add VLANs. Skip steps 4 and 5 and continue.

- 4. To operate DDoS Hybrid Defender as an inline L2 transparent mode device, create a Virtual Wire configuration. (The ingress and egress VLANs are the same.) Click **Create** and configure it as follows:
 - a) Type a name for the Virtual Wire configuration, then select unique interfaces (or trunks) for the ingress and egress ports on the system (Member 1 and Member 2).
 - b) In the Configuration section, for **Define VLANs** select **Add**.
 - c) Type a name for the VLAN group.
 - d) If using tagged VLANs, type a tag number for the VLANs (an integer from 1 to 4095), select the **Members Tagged** check box,
 - e) Click **Add**.
 - f) If using other VLAN tags, create additional VLANs following the same steps.

The system creates a Virtual Wire configuration.

- 5. If DDoS Hybrid Defender uses routed topology, instead of using the default VLAN network, configure the network in the VLAN area. Click **Create** and set up the VLAN as follows:
 - a) Type a name, VLAN tag (from 1 to 4094), then select the interface for the VLAN and click **Add**.
 - b) In the **IP Address/Mask (Port Lockdown)** field, type the IP address and mask.
 - c) After the IP address, specify the protocols and services from which this system (self-IP address) can accept traffic (port lockdown).
Select **Allow None** to accept no traffic; **Allow Default** to accept default protocols and services only; and **Allow All** to activate TCP and UDP services.
 - d) No **Floating IP** is needed if you are configuring just one DDoS Hybrid Defender system for this network.
 - e) Click **Done Editing** to save the VLAN configuration.
 - f) Create as many VLANs as you need to connect to DDoS Hybrid Defender.
- 6. If your system is configured using routed mode and connects to other networks through additional routers, add the required routes so the traffic can reach its destination:
 - a) Next to **Routes**, click **Create**.
 - b) Type a name, destination IP address, netmask, and gateway IP address (this is the next hop router address).
 - c) Click **Done Editing** to save the route.

- 7. Click **Update** to save the network configuration.

DDoS Hybrid Defender is set up to work within your network for most typical inline configurations.

At this point, you can start configuring DDoS Hybrid Defender to protect against DDoS attacks. You can also set up remote logging and Silverline, if you are using those features.

Configuring the network for out-of-band deployment

When installing DDoS Hybrid Defender™ using an out-of-band deployment, you need to configure the network workflow. You can do this using span ports or NetFlow messaging.

Note: If using the BIG-IP Virtual Edition, to set up the network as described here, you must create a security policy on the vSwitch. Configure the security policy to accept the **Promiscuous Mode** and **Forged Transmits** policy exceptions. For details about these options, see the VMware ESX or ESXi Configuration Guide.

1. On the Main tab, click **DoS Protection > Quick Configuration**.
2. On the menu bar, click **Network Configuration**.
3. To allow traffic to reach the DDoS Hybrid Defender, you most likely need to create VLANs and possibly routes.
 - a) In the VLAN section, create the VLANs needed to direct traffic on the network.
This is required if using NetFlow messaging
 - b) In the Routes section, add routes as needed.
4. To detect attacks by passively observing mirrored traffic, configure Span Ports:
 - a) Next to Span Ports, click **Create**.
 - b) Select the interface from which to listen to traffic.
 - c) Click **Done Editing** to save the route.

Important: For port mirroring to work, the TCP Half Open vector must not be enforced. Click **Protected Objects > Device Configuration > Other > TCP Half Open** and set it to **Don't Enforce**.

The Span Ports that you configure have Span Mode (also called Tap Mode) enabled. The switch or router sends a copy of all network packets to DDoS Hybrid Defender for analysis. That's all you have to do. Click **Update** to finish.

5. To detect attacks by examining traffic metadata in NetFlow messages, create a NetFlow configuration:
 - a) Next to Netflow, click **Create**.
 - b) Type a name for the configuration.
 - c) Type the **IP Address/Mask** and **Port** for the NetFlow traffic.
 - d) Specify the **VLAN** on which to listen for NetFlow messages.
 - e) Select the **NetFlow Version** to listen for.
 - f) Click **Done Editing** to save the route.
6. Click **Update** to save the network configuration.

DDoS Hybrid Defender is configured for out-of band deployment using either span ports or NetFlow messages.

At this point, you can start configuring DDoS Hybrid Defender to protect against DDoS attacks. You can also set up remote logging and Silverline, if you are using those features.

Setting up remote logging

You can specify one remote logging destination on DDoS Hybrid Defender™. Set up remote logging if you want to consolidate statistics gathered from multiple appliances onto a Security Information and Event Management (SIEM) device, such as Arcsight or Splunk.

If setting up high availability, configure remote logging on the active device.

1. On the Main tab, click **DoS Protection > Quick Configuration**.

2. On the menu bar, click **Logging**.
3. In the Remote Logging area, from the **Format** list, select the log format used on the remote logging server: **Arcsight** or **Splunk**.
4. In the **Destination IP Address** field, type the IP address of the remote logging server.
5. In the **Port** field, type the port number used for the remote logging server.
6. Click **Commit Changes to System** to save the changes.

Important: Depending on your network configuration, you may need to add a VLAN and route to enable DDoS Hybrid Defender to communicate with the remote logging server.

Event logs from DDoS Hybrid Defender are sent to the remote logging server in the format you specified.

Connecting with F5 Silverline

Connecting with F5 Silverline® is optional, and is available for customers who have an active F5 Silverline DDoS Protection subscription.

To integrate the F5 Silverline Cloud Platform with DDoS Hybrid Defender™ as a way to mitigate DDoS attacks, you need to register DDoS Hybrid Defender with F5 Silverline.

If setting up high availability, you need to register with Silverline on both devices.

1. On the Main tab, click **DoS Protection > Quick Configuration**.
2. On the menu bar, click **Silverline**.
3. In the **Username** field, type the user name for an active Silverline DDoS Protection account. For example, `username@example.com`.
4. In the **Password** field, type the password for the Silverline DDoS Protection account.
5. In the **Service URL** field, type the URL or fully qualified domain name used to connect to the Silverline DDoS Protection service.
6. Click **Update** to save the credentials.
DDoS Hybrid Defender sends a registration request to the F5 Silverline Cloud Platform.
7. Log in to the F5 Silverline customer portal (<https://portal.f5silverline.com>) and specify DDoS Hybrid Defender as an **Approved Hybrid Signaling Device**.

Important: Depending on your network configuration, you may need to add a VLAN and route to enable DDoS Hybrid Defender to communicate with Silverline.

DDoS Hybrid Defender is now integrated with the Silverline Cloud Platform.

When configuring the device or objects to protect, you will need to select the **Silverline** check box to send information about DDoS attacks to the Silverline Cloud Platform.

Protecting Against DDoS Attacks

Overview: Protecting against DDoS attacks

You can easily set up DDoS Hybrid Defender™ to protect your networks and applications from DoS attacks. Once it is all set up, you can monitor the system to see whether there have been any attacks, and whether they are being handled properly.

***Note:** You configure DDoS Hybrid Defender by using the settings in **DoS Protection > Quick Configuration** > . F5 does not recommend making changes outside of the DDoS Hybrid Defender application.*

Protecting the network from DDoS attacks

DDoS Hybrid Defender™ detects and handles DDoS attacks using preconfigured responses. Here you can adjust the device configuration settings that apply to the DDoS Hybrid Defender device as a whole so that it protects the network.

1. On the Main tab, click **DoS Protection > Quick Configuration**.

2. In the Device Protection area, click **Device Configuration**.

The DoS Device Configuration screen opens.

3. For **Auto Threshold Sensitivity**, select **Low**, **Medium**, or **High**.

Low means the automatic threshold calculations are less sensitive to changes in traffic and CPU usage, and the system adjusts the thresholds more slowly over time. If traffic rates are consistent over time, set this to **Low**. If traffic patterns vary, set this to a higher number, such as **Medium** or **High**.

4. Optionally, set up a whitelist of IP addresses that should be allowed to bypass DDoS checks at the device level. See *Bypassing DDoS checks* for details.

5. If you are using Silverline DDoS Protection Services, select the **Silverline** check box.

The system reports DDoS attacks to F5 Silverline. For severe attacks, you can work with the F5 Silverline Security Operations Center (SOC) to migrate traffic to the F5 Silverline Cloud Platform for mitigation.

6. For **DDoS settings**, all the categories of protections are selected, and the associated vectors are enforced and preconfigured.

| Setting | Protects against: |
|------------------------|--|
| Bad Headers | DDoS attacks related to header fields. |
| DNS | DDoS attacks related to DNS queries. |
| Flood | DDoS flood attacks. |
| Fragmentation | Various types of ICMP and IP fragmentation errors. |
| Single Endpoint | Single endpoint flood and sweep DoS attacks. |
| SIP | SIP protocol DDoS vectors. |
| Behavioral | Dynamic signatures and scrubbing. |
| Other | Miscellaneous DDoS vectors. |

7. Click the + sign next to each category to display the attack vectors.

A table opens listing the associated attack vectors, the properties, and the current device statistics, if available.

8. Click the name of any vector to edit the settings as needed for your environment.

Configure the settings at a level that reflects the device and network capacity.

The configuration settings appear on the right side of the screen.

9. Configure the DDoS vector for automatic threshold configuration or manual thresholds.

- If the attack allows automatic threshold configuration, you can select **Auto-Threshold Configuration** for the system to set the thresholds. See *Automatically setting system-wide DDoS thresholds* for details.
- To configure thresholds manually, click **Manual Configuration**. See *Manually setting system-wide DDoS thresholds* for details.

10. Click the **Update** button.

The device configuration is updated, and the DoS Device Configuration screen opens again.

Now you have configured the device to respond to DoS and DDoS attacks, and to allow such attacks to be identified in system logs and reports.

Refer to the sections on automatically and manually setting system-wide DDoS vector thresholds for more details about adjusting the DDoS Hybrid Defender device configuration.

Automatically setting system-wide DDoS vector thresholds

DDoS Hybrid Defender™ handles DDoS attacks with preconfigured responses, but you might need to adjust the values for your environment. For some DDoS attack vectors in the device configuration, you can have the system automatically set detection thresholds and internal rate or leak limits. Use this task to configure individual DoS vectors that include the **Auto-Configuration** setting.

Note: *Not all settings apply to all DoS vectors. For example, some vectors do not use Auto-Thresholds.*

1. On the Main tab, click **DoS Protection > Quick Configuration**.
2. In the Device Protection area, click **Device Configuration**.
The DoS Device Configuration screen opens.
3. Click the + sign next to a category to display the attack vectors for any of the enabled DDoS settings. A table opens listing the associated attack vectors, the properties, and the current device statistics, if available.
4. Click the name of any vector to edit the settings.
The configuration settings appear on the right side of the screen.
5. By default, the system enforces all of the vectors at some level. If you do not want to enforce a particular vector, in the properties select **Don't Enforce**.
6. For vectors that are volumetric in nature, select **Auto-Threshold Configuration** (available for DNS, Flood, SIP, and some Fragmentation and other vectors).

Note: *This setting is not available for every DoS vector. In particular, for error packets that are broken by their nature, such as those listed under Bad Headers, you must configure them manually.*

7. In the **Attack Floor PPS** field, specify the minimum number of packets per second of the vector type for the calculated detection threshold.

Because automatic thresholds take time to be reliably established, this setting defines the minimum number of packets allowed until automatic thresholds are calculated and reported.

Below the attack floor value, attacks are not reported.

8. In the **Attack Ceiling PPS** field, specify the maximum number of packets per second that are allowed for the vector for the calculated detection threshold.

To set no hard limit, set this to **Infinite**.

Unless set to infinite, if the maximum number of packets exceeds the ceiling value, the system considers it to be an attack.

9. To detect IP address sources from which possible attacks originate, enable **Bad Actor Detection**.
10. To automatically blacklist bad actor IP addresses, select **Blacklist Attacking Address**.

***Note:** Automatic IP address blacklisting is enabled only when **Bad Actor Detection** is enabled.*

11. Specify the **Detection Time**, in seconds, after which an IP address is blacklisted.
12. To change the duration for which the address is blacklisted, specify the duration in seconds in the **Duration** field. The default duration for an automatically blacklisted item is 4 hours (14400 seconds).
After this time period, the IP address is removed from the blacklist.
13. To allow IP source blacklist entries to be advertised to edge routers so they will null route their traffic, select **Allow Advertisements**.

***Note:** To advertise to edge routers, you must configure a **Blacklist Publisher** for the **Advertisement Next-Hop** in the **Global Settings**.*

14. On the main screen, click the **Update** button.
The selected configuration is updated, and the DoS Protection Device Configuration screen opens again.
15. Repeat the previous steps for any other attack types for which you want to change the configuration.

Now you have configured the system to automatically determine DoS attack thresholds based on the characteristics of the traffic. The thresholds assigned are usually between the attack floor and attack ceiling values.

Manually setting system-wide DDoS vector thresholds

You manually configure thresholds for a DDoS vector when you want to configure specific settings, or when the vector does not allow for automatic threshold configuration.

***Note:** Not all settings apply to all DoS vectors. For example, some vectors allow **Leak Limits** instead of **Rate Limits**, and some vectors cannot be automatically blacklisted.*

1. On the Main tab, click **DoS Protection > Quick Configuration**.
2. In the Device Protection area, click **Device Configuration**.
The DoS Device Configuration screen opens.
3. Click the + sign next to a category to display the attack vectors for any of the enabled DDoS settings.
A table opens listing the associated attack vectors, the properties, and the current device statistics, if available.
4. Click the name of any vector to edit the settings.
The configuration settings appear on the right side of the screen.
5. In the configuration settings, select **Manual Configuration**.
6. From the **Detection Threshold PPS** list, select **Specify** or **Infinite**.
 - Use **Specify** to set a value (in packets per second) for the attack detection threshold. If packets of the specified types cross the threshold, an attack is logged and reported. The system continues to check every second, and registers an attack for the duration that the threshold is exceeded.
 - Use **Infinite** to set no value for the threshold.
7. From the **Detection Threshold Percent** list, select **Specify** or **Infinite**.

- Use **Specify** to set a value (in percentage of traffic) for the attack detection threshold. If packets of the specified types cross the percentage threshold, an attack is logged and reported. The system continues to check every second, and registers an attack for the duration that the threshold is exceeded.
- Use **Infinite** to set no value for the threshold.

8. For **Rate/Leak Limit**, set the value for the leak limit or the rate limit as follows:

- For **Bad Headers**, this value sets the leak limit. This is the maximum amount of traffic with bad header vectors that is allowed to pass through the system making the issue visible.

On platforms with hardware support for DoS protection, Bad Header packets are dropped in hardware (this provides better performance but limits visibility). The leak limit permits the specified packet rate to *leak* through to Hybrid DDoS Defender, which provides better visibility through statistics and reporting.

- For most of the other vectors, this value is the rate limit. It is the maximum number of packets that are allowed to go through the system. Excess packets are dropped.

9. To log traffic that the system identifies as a DoS attack according to the automatic thresholds, click **Log Auto Threshold Events**.

***Note:** This setting allows you to see the results of auto thresholds on the selected DoS vector without actually affecting traffic. The system displays the current computed thresholds for automatic thresholds for this vector. Automatic thresholds are computed and enforced only when you select **Auto-Threshold Configuration** for a vector.*

10. To detect IP address sources from which possible attacks originate, enable **Bad Actor Detection**.

11. In the **Per Source IP Detection (PPS)** field, specify the number of packets of this type per second from one IP address that identifies the IP source as a bad actor, for purposes of attack detection and logging.

12. In the **Per Source IP Rate Limit (PPS)** field, specify the number of packets of this type per second from one IP address, above which rate limiting or leak limiting occurs.

13. To automatically blacklist bad actor IP addresses, select **Blacklist Attacking Address**.

***Note:** Automatic IP address blacklisting is enabled only when **Bad Actor Detection** is enabled.*

14. Select the **Blacklist Category** to which blacklist entries generated by **Bad Actor Detection** are added.

15. Specify the **Detection Time**, in seconds, after which an IP address is blacklisted.

When a Bad Actor IP address exceeds the **Per Source IP Detection PPS** setting for the **Detection Time** period, that IP address is added to the blacklist.

16. To change the duration for which the address is blacklisted, specify the duration in seconds in the **Duration** field. The default duration for an automatically blacklisted item is 4 hours (14400 seconds).

After this time period, the IP address is removed from the blacklist.

17. To allow IP source blacklist entries to be advertised to edge routers so they will null route their traffic, select **Allow Advertisements**.

***Note:** To advertise to edge routers, you must configure a **Blacklist Publisher** for the **Advertisement Next-Hop** in the **Global Settings**.*

18. Click **Update**.

The selected configuration is updated, and the DoS Protection Device Configuration screen opens again.

19. Repeat the previous steps for any other attack types for which you want to manually configure thresholds.

Now you have configured the system to provide custom responses to possible DDoS attacks, and to allow such attacks to be identified in system logs and reports, rate-limited, and blacklisted when specified.

Bypassing DDoS checks

You can specify IP addresses on a whitelist that the system does not check for DDoS attacks. Addresses on the whitelist are trusted IP addresses that are never blocked.

1. On the Main tab, click **DoS Protection > Quick Configuration**.
2. In the Device Protection area, click **Device Configuration**.
The DoS Device Configuration screen opens.
3. In the Whitelist area, click **Create New**.
4. In the **Name** field, type a name for the whitelist entry.
5. In the Source area, specify the IP address and VLAN combination that serves as the source of traffic that the system recognizes as acceptable to pass the DoS checks.
The VLANs you can select from are specified on the Network Configuration screen. Use **Any** to specify any address or VLAN.

***Note:** Be careful not to allow all traffic.*

6. In the Destination area, specify the IP address and port combination that serves as the intended destination for traffic that the system recognizes as acceptable to pass DoS checks.
You can also use **Any** to specify any address or port.
7. From the **Protocol** list, select the protocol for the whitelist entry.
The options are **Any**, **TCP**, **UDP**, **ICMP**, or **IGMP**.
8. Click **Done Editing** to add the whitelist entry to the configuration.
You can add up to eight IP addresses to the DoS whitelist.

Traffic from the trusted IP addresses is allowed to pass through DDoS Hybrid Defender, and does not undergo DoS checks.

Configuring network bandwidth and scrubbing

You can configure general network protections, such as maximum bandwidth and scrubbing details, for all traffic on DDoS Hybrid Defender. When the maximum bandwidth and scrubbing thresholds are reached, you can configure the system so that traffic is scrubbed by sending it to a BGP router or, if you have an account, to Silverline.

1. On the Main tab, click **DoS Protection > Quick Configuration**.
2. In the Network Protection area, click **Create**.
3. For **Maximum Bandwidth**, specify the maximum allowed bandwidth on DDoS Hybrid Defender in Mbps. Use the **System Default** to have the system automatically assign a reasonable value, or click **Specify** and type a value from 10-1000000 for the maximum bandwidth.
If you use **System Default**,
4. For **VLANs**, specify which traffic to examine for DoS attacks. By default, the entire domain is protected (all configured VLANs are in the **Included** list), and all traffic is scrubbed. To exclude certain areas, move VLANs that do not need to be processed for DoS attacks into the **Excluded** list, and save the changes.

***Tip:** You can configure VLANs on the Network Configuration tab.*

5. For **Scrubbing Threshold**, specify the threshold above which excess traffic will be redirected:

- For **Type**, select **Absolute** or **Percentage** to specify how to express the threshold value. If using **System Default** for maximum bandwidth, only **Absolute** is allowed.
 - Set the **Value**. If the type is **Absolute**, the value is either **Infinite** (no limit so scrubbing never occurs) or a specific value (10-1000000) in Mbps (scrubbing occurs when traffic bandwidth reaches that number). If the type is **Percentage**, the threshold is a specific percent of Mbps (scrubbing occurs when traffic reaches this percentage of the maximum bandwidth).
6. From the **Advertisement Method** list, select how the system should reroute excess traffic: ask upstream **BGP** routers to reroute the traffic, let **Silverline** handle it, or don't reroute or scrub traffic (select **None**).
 7. In the **Scrubber Details** field, include the type of scrubbing and next hop address:
 - a) For **Type**, select how to advertise.

Select **Advertise All** to advertise all scrubbed IP addresses to a BGP router or to Silverline. For BGP, type the IPv4 or IPv6 address of the BGP router (the Silverline destination is configured elsewhere).

Select **Prefix Specific Advertisement** to advertise specific prefixes to a BGP router or to Silverline. In the **IP Address/Mask** field, type the IP address and mask of subnets to be scrubbed, in CIDR notation. For BGP only, in the **BGP Scrubber Destination** field, type the IP address of the scrubber. Click **Add** to add the entry to the list.
 8. Click **Save**.

Protecting network objects from DDoS attacks

With DDoS Hybrid Defender™, you can protect different types of network devices such as application servers, network hosts, DNS servers, routers, and so on against DDoS attacks. These network devices are called *protected objects*.

You need to create protected objects that represent the different types of device, and set up the DoS protections that are applicable to that device.

1. On the Main tab, click **DoS Protection > Quick Configuration**.
2. In the Protected Objects area, click **Create**.

The Create Protected Object screen opens.
3. In the **Name** field, type a name for the protected object.
4. In the **IP Address/Mask** field, type the IP address or network from which the protected object accepts traffic.

Specify the IP address in CIDR format: `address/prefix`, where the prefix length is in bits: for example, for IPv4: `10.0.0.1/32` or `10.0.0.0/24`, and for IPv6: `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`.
5. In the **Port** field, type the service port used by the protected object.
6. From the **Protocol** list, select the network protocol that the protected object uses. Options are: **TCP**, **UDP**, or **All Protocols**.
7. From the **VLAN** list, select the name of the virtual network available to this protected object. Options are: **Any**, and a list of VLANs that are defined on the system. The default is **Any**, meaning any VLAN.

Tip: You can create VLANs by clicking **Network Configuration**.

8. If the protected object manages SSL traffic (required for HTTPS), select the **SSL** check box, and configure these settings:
 - a) From the **SSL Certificate** list, select the SLL certificate and key for the server-side certificate that is presented to the client on the client-side flow.

***Note:** You need to have imported both an SSL certificate (signed by a certificate authority) and key onto the system in **System > File Management > SSL Certificate List**.*

- b) If you want to encrypt SSL traffic heading to the server, select the **Encrypt Connection to Server** check box.

9. From the **Deployment Model** list, select whether the traffic is **Symmetric** (connections from both sides) or **Asymmetric** (inbound connections only).
-

***Tip:** Some attacks (such as HTTP, HTTPS, SIP, or Syn Flood) may not be detected if you use **Asymmetric**.*

10. For the **Action**, select what you want to happen in case of a DDoS attack:

- To have the system detect, log, and mitigate DDoS attacks, select **Log And Mitigate**. The mitigating action rate-limits the attack. You can also select to detect bad actors, blacklist the bad actors, and advertise the bad actors.
- To have the system detect and log attacks only, select **Log Only**. To ensure that no mitigation takes place, you must set the rate-limit thresholds for all enabled vectors to **Infinite**.
- To disable system-level device protection and take no action, select **None**.

The selected action occurs when a DoS vector exceeds the detection (log) or rate-limit (mitigate) threshold.

11. If you are using Silverline DDoS Protection Services, select the **Silverline** check box.

The system reports DDoS attacks to F5 Silverline. For severe attacks, you can work with the F5 Silverline Security Operations Center (SOC) to migrate traffic to the F5 Silverline Cloud Platform for mitigation.

12. For **Default Whitelist**, one at a time, type trusted IP addresses or subnets (for all types of traffic) that do not need to be examined for DoS attacks, and click **Add**.

13. For **HTTP Whitelist**, select **Use Default** unless you want to create a new whitelist specifically for HTTP traffic. Select **Override Default** to create a new list and add the trusted IP addresses for HTTP traffic that should not be counted as part of DDoS attacks (never blocked).

14. To detect attacks using stress-based detection by measuring server latency, select the **Server Health** check box.

You must select this check box if you are using Behavioral DoS detection. You can clear it if using only HTTP or HTTPS L7 DoS detection.

If cleared, DDoS detection uses TPS to measure transaction rates with absolute thresholds. Behavioral DoS mitigation is disabled.

15. For **DDoS settings**, select the categories of protections to enforce at the device level.
-

***Note:** Some of the settings are mutually exclusive (SIP, DNS, HTTP, and HTTPS), and cause others to be unavailable. For example, if you are protecting an HTTP application server, you could select **IPv4** or **IPv6**, **TCP**, **HTTP**, and optionally, **Sweep**.*

| Setting | When to Use |
|-------------|---|
| IPv4 | The protected object uses 32-bit IP addressing, any protocol, any deployment model. |
| IPv6 | The protected object uses 64-bit IP addressing, any protocol, any deployment model. |
| TCP | The protected object uses TCP protocol. The protocol of the protected object must be set to TCP or All Protocols , any deployment model is allowed (SYN cookies disabled for Asymmetric). |
| UDP | The protected object uses UDP protocol. The protocol of the protected object must be set to UDP or All Protocols , any deployment model is allowed. |

| Setting | When to Use |
|-------------------|--|
| Sweep | To protect against single-endpoint flood and sweep DDoS attacks. |
| DNS | The protected object is one or more DNS servers. The port of the protected object must be set to one DNS port number, the protocol must be set to UDP or TCP , deployment model must be Symmetric . |
| SIP | The protected object is one or more SIP servers. The port of the protected object must be set to one SIP port number, the protocol must be set to UDP or TCP , deployment model must be Symmetric . |
| HTTP | The protected object is one or more HTTP application servers. The port of the protected object must be set to one port number, the protocol must be set to TCP , deployment model must be Symmetric . |
| HTTPS | The protected object is one or more HTTPS application servers. The port of the protected object must be set to one port number, the protocol must be set to TCP , deployment model must be Symmetric , and an SSL Certificate must be specified. |
| Behavioral | The system is using behavioral analysis of traffic to the protected object to discover patterns (dynamic signatures) that indicate DDoS attacks. |

The system pre-configures all of the vectors in each of the categories, but you might need to adjust the values to suit your environment.

16. Click the + sign next to the category to display the attack vectors.

A table opens listing the associated attack vectors, the properties, and the current device statistics, if available.

17. Click the name of any vector to edit the settings.

The configuration settings appear on the right side of the screen.

18. Configure the DDoS vector for automatic threshold configuration or manual thresholds.

- If the attack allows automatic threshold configuration, you can select **Auto-Threshold Configuration** to configure automatic thresholds. See *Automatically setting system-wide DDoS thresholds* for details.
- To configure thresholds manually, click **Manual Configuration**. See *Manually setting system-wide DDoS thresholds* for details.

19. Click the **Update** button.

The system creates the protected object.

Now you have configured the system to protect against DDoS attacks, and to allow such attacks to be identified in system logs and reports.

How to protect different network objects from DDoS attacks

Administrators often want to protect against a specific type of DDoS attack or to protect a particular type of protected object from attacks. This table gives you an idea of the types of protections you can set up.

| To protect this: | Set this in the protected object: |
|------------------|--|
| DNS Servers | <ul style="list-style-type: none"> • Set Port to the DNS port. • Set Protocol to All Protocols. • Set Deployment Model to Symmetric. • In DDoS Settings, click DNS. • Expand DNS, check threshold settings. |
| SIP Servers | <ul style="list-style-type: none"> • Set Port to the SIP port. |

| To protect this: | Set this in the protected object: |
|------------------------------------|---|
| | <ul style="list-style-type: none"> Set Protocol to TCP. Set Deployment Model to Symmetric. In DDoS Settings, click SIP. Expand SIP, check threshold settings. |
| Web applications | <ul style="list-style-type: none"> Set Port to the 80 for HTTP or 443 for HTTPS. Set Protocol to TCP. Set Deployment Model to Symmetric. In DDoS Settings, click HTTP or HTTPS. Expand HTTP or HTTPS, check threshold settings. |
| Backend servers from Syn Floods | <ul style="list-style-type: none"> Set IP Address to * for all addresses. Set Port to * for all ports. Set VLAN to defaultVLAN. Set Protocol to TCP. Set Deployment Model to Symmetric. In DDoS Settings, click TCP. Expand TCP, check the settings for TCP SYN Flood. |
| Backend servers from Sweep Attacks | <ul style="list-style-type: none"> Set IP Address to * for all addresses. Set Port to * for all ports. Set VLAN to defaultVLAN. Set Protocol to TCP. Set Deployment Model to Symmetric. In DDoS Settings, click Sweep. Expand Sweep, for Sweep set the packet types to check for sweep attacks. |

DDoS protected object attack types

For each protected object, you can specify specific threshold, rate increase, rate limit, and other parameters for supported DoS attack types, to more accurately detect, track, and rate limit attacks.

IPv4 Attack Vectors

| Vector | Information |
|-----------------------|---|
| Host Unreachable | The host cannot be reached. |
| ICMP Fragment | ICMP fragment flood. |
| ICMPv4 Flood | Flood with ICMPv4 packets. |
| IP Fragment Flood | Fragmented packet flood with IPv4. |
| IP Option Frames | IPv4 address packets that are part of an IP option frame flood. On the command line <code>option.db</code> variable <code>tm.acceptipsourceroute</code> must be enabled to receive IP options. |
| TIDCMP | ICMP type 4 error; can't accept queries. |
| TTL <= <i>tunable</i> | An IP packet with a destination that is not multicast has a Time to live (TTL) value less than or equal to the configured value. To tune this value, in <code>tmsh:</code> modify <code>sys db dos.iplowttl value</code> , where <i>value</i> is 1-4. 1 is default. |

IPv6 Attack Vectors

| Vector | Information |
|---------------------------------|--|
| Host Unreachable | The host cannot be reached. |
| ICMP Fragment | ICMP fragment flood. |
| ICMPv6 Flood | Flood with ICMPv6 packets. |
| IPv6 Extended Header Frames | IPv6 address contains extended header frames. |
| IPv6 extension header too large | An IPv6 extension header exceeds the limit in bytes set at DoS Protection > Quick Configuration > Global Settings , in the Too Large IPv6 Extension Header field. |
| IPv6 Fragment Flood | The IPv6 extended header hop count is less than or equal to the hop count limit set at DoS ProtectionQuick ConfigurationGlobal Settings , in the IPv6 Low Hop Count field. |
| IPv6 hop count <= <tunable> | The IPv6 extended header hop count is less than or equal to the hop count limit set at DoS ProtectionQuick ConfigurationGlobal Settings , in the IPv6 Low Hop Count field. |
| Too Many Extended Headers | For an IPv6 address, the extension headers exceed the limit set at DoS Protection > Quick Configuration > Global Settings , in the Too Many IPv6 Extension Header field. |

TCP Attack Vectors

| Vector | Information |
|------------------------------------|---|
| Option Present With Illegal Length | Packets contain an option with an illegal length. |
| TCP Bad URG | TCP header has a bad URG flag, this is likely malicious (flag is set and urgent pointer is 0). |
| TCP Option Overruns TCP Header | The TCP option bits overrun the TCP header. |
| TCP PSH Flood | Attackers send spoofed PUSH packets at very high rates; packets do not belong to any current session. |
| TCP RST Flood | TCP reset attack, also known as "forged TCP resets", "spoofed TCP reset packets" or "TCP reset attacks" is a method of tampering with Internet communications. |
| TCP SYN ACK Flood | An attack method that involves sending a target server spoofed SYN-ACK packets at a high rate. |
| TCP SYN Flood | Attackers send a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. |
| TCP SYN Oversize | Detects TCP data SYN packets larger than the maximum specified in the limit set at DoS Protection > Quick Configuration > Global Settings , in the Too Large TCP SYN Packet field. The default size in bytes is 64 and the maximum allowable value is 9216. |
| TCP Window Size | The TCP window size in packets is above the maximum size. To tune this setting, change the setting at Dos Protection > Quick Configuration > Global Settings , in the Too Low TCP Window Size field. |

| Vector | Information |
|-------------------------|----------------------------------|
| Unknown TCP Option Type | TCP option type is not standard. |

UDP Attack Vector

| Vector | Information |
|-----------|--|
| UDP Flood | The attacker sends UDP packets, typically large ones, to single destination or to random ports. |

Sweep Attack Vector

| Vector | Information |
|--------|---|
| Sweep | The attacker uses a network scanning technique that typically sweeps your network by sending packets, and using the packet responses to determine live hosts. |

DNS Attack Vectors

| Vector | How to identify it |
|---------------|--|
| a | UDP packet, DNS Qtype is A_QRY, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). |
| aaaa | UDP packet, DNS Qtype is AAAA, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). |
| any | UDP packet, DNS Qtype is ANY_QRY, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). |
| axfr | UDP packet, DNS Qtype is AXFR, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). |
| cname | UDP DNS query, DNS Qtype is CNAME, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). |
| dns-malformed | Malformed DNS packets. |
| ixfr | UDP DNS query, DNS Qtype is IXFR, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). |
| mx | UDP DNS query, DNS Qtype is MX, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). |
| ns | UDP DNS query, DNS Qtype is NS, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). |
| other | UDP DNS query, DNS Qtype is OTHER, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). |

| Vector | How to identify it |
|--------|--|
| ptr | UDP DNS query, DNS Qtype is PTR, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). |
| qdcoun | DNS QDCount limit. UDP packet, DNS qdcoun neq 1, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). |
| soa | UDP packet, DNS Qtype is SOA_QRY, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). |
| srv | UDP packet, DNS Qtype is SRV, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). |
| txt | UDP packet, DNS Qtype is TXT, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). |

SIP Attack Vectors

| Vector | Information |
|-----------|--|
| ack | SIP ACK packets. Used with invite request when establishing a call. |
| bye | SIP BYE packets. The attacker tries to terminate a communication session prematurely. |
| cancel | SIP CANCEL packets. Attackers prevent callers from establishing a session. |
| invite | SIP INVITE packets. Attackers send multiple invite packets to initiate call sessions. |
| message | SIP MESSAGE packets. Attackers send instant messages. |
| notify | SIP NOTIFY packets. Attackers send notifications, such as of voice mails. |
| options | SIP OPTIONS packets. Attackers send probes to determine capabilities of servers. |
| other | Other SIP method packets. |
| prack | SIP PRACK packets. Attackers send prack packets for provisional acknowledgements. |
| publish | SIP PUBLISH packets. Attackers publish messages to the server. |
| register | SIP REGISTER packets. Attackers register or unregister a phone address listed in the To header field with a SIP server. |
| subscribe | SIP SUBSCRIBE packets. Attackers send subscriber notification messages. |
| URI Limit | The SIP URI exceeds the limit set at Dos Protection > Quick Configuration > Global Settings , in the Too Long SIP URI field. This setting should be less than 1024, the maximum length for a SIP URI in bytes. |

Layer 7 HTTP and HTTPS Attack Vectors

| Protection | Description |
|---------------------|--|
| Behavioral | Attack indicates bad actors by their anomalous behavior based on deviation from baseline behavior. |
| Detection by Device | Attack indicates suspicious client devices tracked by fingerprinting and a high number of transactions per second. |

| Protection | Description |
|--------------------------|---|
| Detection by Geolocation | Attack indicates suspicious geographical locations identified by their IP range and an unusual traffic share. |
| Detection by Site | Attack indicates that the global traffic on the site (whole application) signifies an attack based on a high number of transactions per second. |
| Detection by Source-IP | Attack indicates suspicious clients identified by their IP address and a high number of transactions per second. |
| Detection by URL | Attack targets specific URLs in the web application by sending a high number of transactions per second to them. |
| Heavy URL | Attack focuses on URLs that consume considerable server resources thus can become tipping points in DoS attacks. The system automatically detects heavy URLs. |

HTTP and HTTPS Proactive Bot Defense Categories

| Category | Description/Category |
|-----------------------|---|
| Proactive Bot Defense | Attacks caused by web robots. The system uses JavaScript evaluations and bot signatures to ensure that browsers are legitimate not automated. |
| Crawler | Benign |
| HTTP Library | Benign |
| Search Bot | Benign |
| Search Engine | Benign |
| Service Agent | Benign |
| Site Monitor | Benign |
| Social Media Agent | Benign |
| Web Downloader | Benign |
| DoS Tool | Malicious |
| E-Mail Collector | Malicious |
| Exploit Tool | Malicious |
| Network Scanner | Malicious |
| Spam Bot | Malicious |
| Vulnerability Scanner | Malicious |
| Web Spider | Malicious |

DDoS device attack types

You can specify specific threshold, rate increase, rate limit, and other parameters for supported device-level DDoS attack types, to more accurately detect, track, and rate limit attacks. Broken packets, such as those with bad headers, should be severely rate limited

Bad Header attack types

| Vector | Information | Hardware accelerated |
|--------------------|---|----------------------|
| Bad ICMP Checksum | An ICMP frame checksum is bad. Reuse the TCP or UDP checksum bits in the packet. | Yes |
| Bad ICMP Frame | <p>The ICMP frame is either the wrong size or not one of the valid IPv4 or IPv6 types. Valid IPv4 types:</p> <ul style="list-style-type: none"> • 0 Echo Reply • 3 Destination Unreachable • 4 Source Quench • 5 Redirect • 8 Echo • 11 Time Exceeded • 12 Parameter Problem • 13 Timestamp • 14 Timestamp Reply • 15 Information Request • 16 Information Reply • 17 Address Mask Request • 18 Address Mask Reply <p>Valid IPv6 types:</p> <ul style="list-style-type: none"> • 1 Destination Unreachable • 2 Packet Too Big • 3 Time Exceeded • 4 Parameter Problem • 128 Echo Request • 129 Echo Reply • 130 Membership Query • 131 Membership Report • 132 Membership Reduction | Yes |
| Bad IGMP Frame | IPv4 IGMP packets should have a header ≥ 8 bytes. Bits 7:0 should be either 0x11, 0x12, 0x16, 0x22 or 0x17, or else the header is bad. Bits 15:8 should be non-zero only if bits 7:0 are 0x11, or else the header is bad. | Yes |
| Bad IP TTL Value | Time-to-live equals zero for an IPv4 address. | Yes |
| Bad IP Version | The IPv4 address version in the IP header is not 4. | Yes |
| Bad IPv6 Addr | IPv6 source IP = 0xff00:: | Yes |
| Bad IPV6 Hop Count | Both the terminated (cnt=0) and forwarding packet (cnt=1) counts are bad. | Yes |
| Bad IPV6 Version | The IPv6 address version in the IP header is not 6. | Yes |
| Bad SCTP Checksum | Bad SCTP packet checksum. | No |
| Bad Source | The IPv4 source IP = 255.255.255.255 or 0xe0000000U. | Yes |
| Bad TCP Checksum | The TCP checksum does not match. | Yes |

| Vector | Information | Hardware accelerated |
|--|--|----------------------|
| Bad TCP Flags (All Cleared) | Bad TCP flags (all cleared and SEQ#=0). | Yes |
| Bad TCP Flags (All Flags Set) | Bad TCP flags (all flags set). | Yes |
| Bad UDP Checksum | The UDP checksum is not correct. | Yes |
| Bad UDP Header (UDP Length > IP Length or L2 Length) | UDP length is greater than IP length or Layer 2 length. | Yes |
| DNS Malformed | Malformed DNS packet | Yes |
| DNS Oversize | Detects oversized DNS headers. To tune this value, set the Too Large DNS Packet setting at DoS Protection > Quick Configuration > Global Settings to the maximum value for a DNS header, from 256-8192 bytes. | Yes |
| DNS QDCount Limit | UDP packet, DNS qdcount neq 1, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). | Yes |
| Ethernet MAC Source Address == Destination Address | Ethernet MAC source address equals the destination address. | Yes |
| FIN Only Set | Bad TCP flags (only FIN is set). | Yes |
| Header Length > L2 Length | No room in Layer 2 packet for IP header (including options) for IPv4 address | Yes |
| Header Length Too Short | IPv4 header length is less than 20 bytes. | Yes |
| ICMP Frame Too Large | The ICMP frame exceeds the declared IP data length or the maximum datagram length set at DoS Protection > Quick Configuration > Global Settings , in the Too Large IPv6 Extension Header field. To tune this value, in tmsh: modify sys db dos.maxicmpframesize value, where value is <=65515. | Yes |
| IP Error Checksum | The header checksum is not correct. | Yes |
| IP Length > L2 Length | The total length in the IPv4 address header or payload length in the IPv6 address header is greater than the Layer 3 length in a Layer 2 packet. | Yes |
| IP Option Frames | IPv4 address packets that are part of an IP option frame flood. On the command line option.db variable tm.acceptipsourceroute must be enabled to receive IP options. | Yes |
| IP Option Illegal Length | Option present with illegal length. | No |
| IPv4 mapped *IPv6* | The IPv6 stack is receiving IPv4 address packets. | Yes |

| Vector | Information | Hardware accelerated |
|---|--|----------------------|
| IPv6 duplicate extension headers | An extension header should occur only once in an IPv6 packet, except for the Destination Options extension header. | Yes |
| IPv6 Extended Header Frames | IPv6 address contains extended header frames. | Yes |
| IPv6 extended headers wrong order | Extension headers in the IPv6 header are in the wrong order. | Yes |
| IPv6 extension header too large | An IPv6 extension header exceeds the limit in bytes set at DoS Protection > Quick Configuration > Global Settings , in the Too Large IPv6 Extension Header field. | Yes |
| IPv6 hop count <= <tunable> | The IPv6 extended header hop count is less than or equal to the hop count limit set at DoS Protection > Quick Configuration > Global Settings , in the IPv6 Low Hop Count field. | Yes |
| IPv6 Length > L2 Length | IPv6 address length is greater than the Layer 2 length. | Yes |
| L2 Length >> IP Length | Layer 2 packet length is much greater than the payload length in an IPv4 address header, and the Layer 2 length is greater than the minimum packet size. | Yes |
| No L4 | No Layer 4 payload for IPv4 address. | Yes |
| No L4 (Extended Headers Go To Or Past End of Frame) | Extended headers go to the end or past the end of the L4 frame. | Yes |
| Option Present With Illegal Length | Packets contain an option with an illegal length. | Yes |
| Payload Length < L2 Length | Specified IPv6 payload length is less than the L2 packet length. | Yes |
| SYN && FIN Set | Bad TCP flags (SYN and FIN set). | Yes |
| TCP Flags - Bad URG | Packet contains a bad URG flag; this is likely malicious. | Yes |
| TCP Header Length > L2 Length | The TCP header length exceeds the Layer 2 length. | Yes |
| TCP Header Length Too Short (Length < 5) | The Data Offset value in the TCP header is less than five 32-bit words. | Yes |
| TCP Option Overruns TCP Header | The TCP option bits overrun the TCP header. | Yes |
| Too Many Extended Headers | For an IPv6 address, the extension headers exceed the limit set at DoS Protection > Quick Configuration > Global Settings , in the Too Many IPv6 Extension Header field. | Yes |
| TTL <= <tunable> | An IP packet with a destination that is not multicast has a TTL greater than 0 and less than the value set at DoS Protection > Quick Configuration > Global Settings , in the IPv4 Low TTL field. The range for this setting is 1–4. | Yes |
| Unknown Option Type | Unknown IP option type. | No |

| Vector | Information | Hardware accelerated |
|-------------------------|--------------------------|----------------------|
| Unknown TCP Option Type | Unknown TCP option type. | Yes |

DNS attack vectors

| Vector | Information | Hardware accelerated |
|-----------------|--|----------------------|
| DNS A Query | UDP packet, DNS Qtype is A_QRY, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). | Yes |
| DNS AAAA Query | UDP packet, DNS Qtype is AAAA, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). | Yes |
| DNS Any Query | UDP packet, DNS Qtype is ANY_QRY, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). | Yes |
| DNS AXFR Query | UDP packet, DNS Qtype is AXFR, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). | Yes |
| DNS CNAME Query | UDP DNS query, DNS Qtype is CNAME, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). | Yes |
| DNS IXFR Query | UDP DNS query, DNS Qtype is IXFR, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). | Yes |
| DNS MX Query | UDP DNS query, DNS Qtype is MX, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). | Yes |
| DNS NS Query | UDP DNS query, DNS Qtype is NS, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). | Yes |
| DNS OTHER Query | UDP DNS query, DNS Qtype is OTHER, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). | Yes |
| DNS PTR Query | UDP DNS query, DNS Qtype is PTR, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). | Yes |

| Vector | Information | Hardware accelerated |
|--------------------|--|----------------------|
| DNS Response Flood | UDP DNS Port=53, packet and DNS header flags bit 15 is 1 (response), VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). | Yes |
| DNS SOA Query | UDP packet, DNS Qtype is SOA_QRY, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). | Yes |
| DNS SRV Query | UDP packet, DNS Qtype is SRV, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). | Yes |
| DNS TXT Query | UDP packet, DNS Qtype is TXT, VLAN is <tunable>. To tune this value, set the DNS VLAN setting at DoS Protection > Quick Configuration > Global Settings to the DNS VLAN (0-4094). | Yes |

Flood attack vectors

| Vector | Information | Hardware accelerated |
|---------------------------|--|----------------------|
| Flood | ARP packet flood | Yes |
| Ethernet Broadcast Packet | Ethernet broadcast packet flood | Yes |
| Ethernet Multicast Packet | Ethernet destination is not broadcast, but is multicast. | Yes |
| ICMPv4 Flood | Flood with ICMPv4 packets | Yes |
| ICMPv6 Flood | Flood with ICMPv6 packets | Yes |
| IGMP Flood | Flood with IGMP packets (IPv4 packets with IP protocol number 2) | Yes |
| IGMP Fragment Flood | Fragmented packet flood with IGMP protocol | Yes |
| IP Fragment Flood | Fragmented packet flood with IPv4 | Yes |
| IPv6 Fragment Flood | Fragmented packet flood with IPv6 | No |
| Routing Header Type 0 | Routing header type zero is present in flood packets | Yes |
| TCP BADACK Flood | TCP ACK packet flood | No |
| TCP PUSH Flood | TCP PUSH flood | Yes |
| TCP RST Flood | TCP RST flood | Yes |
| TCP SYN ACK Flood | TCP SYN/ACK flood | Yes |
| TCP SYN Flood | TCP SYN flood | Yes |
| TCP SYN Oversize | Detects TCP data SYN packets larger than the maximum specified in the limit set at DoS Protection > Quick Configuration > Global Settings , in the Too Large TCP | Yes |

| Vector | Information | Hardware accelerated |
|-----------------|---|----------------------|
| TCP Window Size | <p>SYN Packet field. The default size in bytes is 64 and the maximum allowable value is 9216.</p> <p>The TCP window size in packets is above the maximum size. To tune this setting, change the setting at Dos Protection > Quick Configuration > Global Settings, in the Too Low TCP Window Size field.</p> | Yes |
| UDP Flood | UDP flood attack | Yes |

Fragmentation attack vectors

| Vector | Information | Hardware accelerated |
|-------------------------|---|----------------------|
| ICMP Fragment | ICMP fragment flood | Yes |
| IP Fragment Error | Other IPv4 fragment error | Yes |
| IP Fragment Overlap | IPv4 overlapping fragment error | No |
| IP Fragment Too Small | IPv4 short fragment error | Yes |
| IPV6 Atomic Fragment | IPv6 Frag header present with M=0 and FragOffset =0 | Yes |
| IPV6 Fragment Error | Other IPv6 fragment error | Yes |
| IPv6 Fragment Overlap | IPv6 overlapping fragment error | No |
| IPv6 Fragment Too Small | IPv6 short fragment error | Yes |

Single Endpoint attack vectors

| Vector | Information | Hardware accelerated |
|-----------------------|--|----------------------|
| Single Endpoint Flood | Flood to a single endpoint and can come from many sources. You can configure packet types to check for, and packets per second for both detection and rate limiting. | No |
| Single Endpoint Sweep | Sweep on a single endpoint. You can configure packet types to check for, and packets per second for both detection and rate limiting. | No |

SIP attack vectors

| Vector | Information | Hardware accelerated |
|--------------------|-----------------------|----------------------|
| SIP ACK Method | SIP ACK packets | Yes |
| SIP BYE Method | SIP BYE packets | Yes |
| SIP CANCEL Method | SIP CANCEL packets | Yes |
| SIP INVITE Method | SIP INVITE packets | Yes |
| SIP Malformed | Malformed SIP packets | Yes |
| SIP MESSAGE Method | SIP MESSAGE packets | Yes |

| Vector | Information | Hardware accelerated |
|----------------------|--|----------------------|
| SIP NOTIFY Method | SIP NOTIFY packets | Yes |
| SIP OPTIONS Method | SIP NOTIFY packets | Yes |
| SIP OTHER Method | Other SIP method packets | Yes |
| SIP PRACK Method | SIP PRACK packets | Yes |
| SIP PUBLISH Method | SIP PUBLISH packets | Yes |
| SIP REGISTER Method | SIP REGISTER packets | Yes |
| SIP SUBSCRIBE Method | SIP SUBSCRIBE packets | Yes |
| SIP URI Limit | The SIP URI exceeds the limit set at Dos Protection > Quick Configuration > Global Settings , in the Too Long SIP URI field. This setting should be less than 1024, the maximum length for a SIP URI in bytes. | Yes |

Behavioral

Behavioral DDoS protection is enabled, by default, and all thresholds and threshold actions are applied. You can initiate leaning or relearning of dynamic signatures, adjust mitigation sensitivity, and enable redirection and scrubbing of IP addresses identified by the dynamic signatures. You also have the option of selecting **Learn Only** to track dynamic vector statistics, without enforcing any thresholds or limits.

In the case of an attack, the system dynamically creates signatures that characterize the attack. During the attack, you see them listed as behavioral vectors (starting with Sig). They are removed when the attack is over.

Other attack vectors

| Vector | Information | Hardware accelerated |
|---------------------|--|----------------------|
| Host Unreachable | Host unreachable error | Yes |
| IP Unknown protocol | Unknown IP protocol | No |
| LAND Attack | Source IP equals destination IP address | Yes |
| TCP Half Open | TCP connection whose state is out of synchronization between the two communicating hosts | Yes |
| TIDCMP | ICMP source quench attack | Yes |

Preventing DDoS Flood and Sweep Attacks

About DoS sweep and flood attack prevention

A *sweep attack* is a network scanning technique that typically sweeps your network by sending packets, and using the packet responses to determine live hosts. Typical attacks use ICMP to accomplish this.

The Sweep vector tracks packets by source address. Packets from a specific source that meet the defined single endpoint Sweep criteria, and exceed the rate limit, are dropped. You can also configure the Sweep vector to automatically blacklist an IP address from which the Sweep attack originates.

Important: *The sweep mechanism protects against a flood attack from a single source, whether that attack is to a single destination host, or multiple hosts.*

A *flood attack* is an attack technique that floods your network with packets of a certain type, in an attempt to overwhelm the system. A typical attack might flood the system with SYN packets without then sending corresponding ACK responses. UDP flood attacks flood your network with a large number of UDP packets, requiring the system to verify applications and send responses.

The Flood vector tracks packets per destination address. Packets to a specific destination that meet the defined Single Endpoint Flood criteria, and exceed the rate limit, are dropped. The system can detect such attacks with a configurable detection threshold, and can rate limit packets from a source when the detection threshold is reached.

You can configure DoS sweep and flood prevention to detect and prevent floods and sweeps of ICMP, UDP, TCP SYN without ACK, or any IP packets that originate from a single source address, according to the threshold setting. Both IPv4 and IPv6 are supported. The sweep vector acts first, so a packet flood from a single source address to a single destination address is handled by the sweep vector.

Sweep and flood is the first prevention that is limited to the affected hosts. For example, the Flood TCP SYN flood vector rate limits all TCP SYNs, good and bad, once the rate limit threshold is reached. Sweep protection detects and rate limits just the bad guys. Flood detects and limits just the traffic to the targeted host. Collateral damage is much lower by mitigating these vectors. You can set the limits lower than would be reasonable for the indiscriminate vectors.

Protecting against single-endpoint flood and sweep attacks

You can protect against DDoS single-endpoint attacks to protect a specific server from flood and sweep attacks.

1. On the Main tab, click **DoS Protection > Quick Configuration**.

2. In the Device Protection area, click **Device Configuration**.

The DoS Device Configuration screen opens.

3. Specify the **Auto Threshold Sensitivity**.

A lower number means the automatic threshold algorithm is less sensitive to changes in traffic and CPU usage.

4. Expand the **Single-Endpoint** category, and click **Single Endpoint Flood**.

The settings appear on the right.

5. From the **Detection Threshold PPS** list, select **Specify** or **Infinite**.

- Use **Specify** to set a value (in packets per second) for the attack detection threshold. If packets of the specified types cross the threshold, an attack is logged and reported. The system continues to check every second, and registers an attack for the duration that the threshold is exceeded.
 - Use **Infinite** to set no value for the threshold.
6. From the **Rate/Leak Limit** list, select **Specify** or **Infinite**.
 - Use **Specify** to set a value (in packets per second), which cannot be exceeded by packets of this type. All packets of this type over the threshold are dropped. Rate limiting continues until the rate no longer exceeds.
 - Use **Infinite** to set no value for the threshold.
 7. In the **Packet Types** area, move the packet types you want to detect into the **Selected** list.
 8. On the left, under the **Single-Endpoint** category, click **Single Endpoint Sweep**.

The settings appear on the right, and are the same as for the flood, so you complete them the same way. Additional blacklist settings are available.
 9. In the **Per Source IP Rate Limit (PPS)** field, specify the number of packets of this type per second from one IP address, above which rate limiting or leak limiting occurs.
 10. To automatically blacklist bad actor IP addresses, select **Blacklist Attacking Address**.

***Note:** Automatic IP address blacklisting is enabled only when **Bad Actor Detection** is enabled.*

11. Select the **Blacklist Category** to which blacklist entries generated by **Bad Actor Detection** are added.
12. Specify the **Detection Time**, in seconds, after which an IP address is blacklisted.

When a Bad Actor IP address exceeds the **Per Source IP Detection PPS** setting for the **Detection Time** period, that IP address is added to the blacklist.
13. To change the duration for which the address is blacklisted, specify the duration in seconds in the **Duration** field. The default duration for an automatically blacklisted item is 4 hours (14400 seconds).

After this time period, the IP address is removed from the blacklist.
14. To allow IP source blacklist entries to be advertised to edge routers so they will null route their traffic, select **Allow Advertisements**.

***Note:** To advertise to edge routers, you must configure a **Blacklist Publisher** for the **Advertisement Next-Hop** in the **Global Settings**.*

15. From the **Detection Threshold PPS** list, select **Specify** or **Infinite**.
 - Use **Specify** to set a value (in packets per second) for the attack detection threshold. If packets of the specified types cross the threshold, an attack is logged and reported. The system continues to check every second, and registers an attack for the duration that the threshold is exceeded.
 - Use **Infinite** to set no value for the threshold.
16. Click the **Update** button.

The flood and sweep attack configurations are updated.

Now you have configured the system to provide protection against DoS flood and sweep attacks on a single server, and to allow such attacks to be identified in system logs and reports.

Protecting objects system-wide from flood attacks

You can use DDoS Hybrid Defender™ to protect all objects system-wide from flood attacks.

1. On the Main tab, click **DoS Protection > Quick Configuration**.
2. In the Device Protection area, click **Device Configuration**.

The DoS Device Configuration screen opens.

3. Specify the **Auto Threshold Sensitivity**.

A lower number means the automatic threshold algorithm is less sensitive to changes in traffic and CPU usage.

4. Expand the **Flood** category, and review the settings for the different types of floods.

5. Click the type of flood for which you want to change the settings.

The settings appear on the right.

6. Adjust the settings as needed.

Tip: In the settings that allow it, click **Auto-Threshold Configuration** to have the system determine the thresholds based on traffic.

7. Click the **Update** button.

The flood attack configuration is updated.

Now you have configured the system to provide protection against DDoS flood attacks, to allow such attacks to be identified in system logs and reports, and to automatically add such attackers to a blacklist of your choice.

Viewing DDoS Reports, Statistics, and Logs

Investigating DoS attacks and mitigation

You can use the DoS Dashboard screen for an overview of DoS attack activity on your BIG-IP® system, and corresponding system information during DoS attacks.

1. On the Main tab, click **Security > Reporting > DoS > Dashboard**.

Tip: For quick navigation to the DoS Dashboard screen, on the Main tab to go **Statistics > DoS Visibility**.

The DoS Dashboard screen opens and displays system information about all DoS attacks over a default time range.

2. Use the time settings at the top of the screen to set a time range or refresh the information on screen. To immediately update the statistics on screen, adjust the time range or refresh settings.

| | |
|------------|--|
| Time Focus | Select the time range of the displayed data. |
|------------|--|

Note: Additional time options become available as your system gathers more data.

| | |
|-------------------------------|--|
| Currently Selected Time Range | Displays the current time range of the displayed data. |
|-------------------------------|--|

| | |
|--------------------------------|---|
| Auto-Refresh Interval Selector | Select how frequently the data on this screen is refreshed. |
|--------------------------------|---|

| | |
|----------------|---|
| Manual Refresh | Click Refresh to trigger an immediate refresh of the displayed data. |
|----------------|---|

| | |
|--------------------------------|---|
| Manual Time Adjustment Handles | Set the data to a specific window of time within the currently selected time range. Use the handles at either end of the time line to define the specific time you want to examine. Use the handle above the time line to display data that is outside the selected time range. |
|--------------------------------|---|

Note: Adjusting the time range to display previous data stops the auto-refresh so you can focus on a specific data point.

You can zoom into a specific time range within a chart. Select an area within the chart and then click the magnifying glass icon.

Note: Selecting a time range within the chart stops the screen's auto-refresh settings.

3. Review the charts and tables that provide high-level information about your system's status.

Tip: You can filter the entire screen's displayed data to correspond with a specific data point by selecting entities in the charts, tables or map.

4. Review the Attack Duration and Attacks areas for recent or ongoing DoS attacks.
5. Review the Attack Duration area to determine the duration of each DoS attack over the selected time period, including ongoing attacks. In the Attack Duration chart, each horizontal bar represents an individual attack and indicates the start and end time of the attack, and the severity.

An ongoing attack extends to the end of the chart.

You can view additional attack information in the chart:

- Hover over an individual attack to view attack details, including Attack ID, Mitigation, Severity, Trigger and Vector.
- Hover over the chart area to view the number of attacks that occurred at a specific time in the chart legend.

6. Review the Attacks area to determine the distribution of DoS attacks over the selected time period.

- Use the # of Attacks table to view a breakdown of the number of attacks according to the attack severity.

Note: You can select one or more values in this table to filter the entire screen according to an attack severity level.

- Use the # of Attacks per Protocol chart to view the breakdown of attacks according to severity of attack and transaction protocol.
- Use the table in this area to examine the details of each attack, according to Attack ID.

Note: You can view more information by hovering over the table's data.

7. Review the Virtual Servers area to determine the impact of DoS attack's on your system's virtual servers.

- Use the # of Virtual Servers table to view a breakdown of your virtual servers health status according to each virtual server's latency, client concurrent connections and throughput.
- Use the Virtual Servers Health chart to view a breakdown of virtual servers according to health score for each performance indicator that is used to evaluate health status.
- Use the table in this area to examine the health and corresponding attack details for each virtual server.

8. Review the tiles in the System Health area for a quick view of your BIG-IP system's health status. Each health tile is color coded according to the overall severity of each parameter for the entire system. Severity ranges are as follows: Good, Moderate, Unhealthy and Critical.

Note: In a multi-blade system, each health parameter also displays the slots with the highest system activity.

- Use the TMM CPU Usage tile to determine the status of the TMM's CPU usage, and if the system has crossed any critical thresholds.

Note: You can select from the drop-down icon to view a list of the busiest cores. For a multi-blade system, a list of the busiest cores is available for each slot.

- Use the Memory Usage tile to determine your system's average TMM memory usage (out of total RAM allocated to TMM processes), and if the system has crossed any critical thresholds.
- Use the Client Throughput tile to determine the average rate of bits per seconds transmitted during client-side transactions with your BIG-IP system.
- Use the Client Connections tile to determine the average number of client concurrent connections with your BIG-IP system over the selected time period.

9. Review the Countries area for information about the geolocation of traffic handled by your BIG-IP system.


- Filter location information by client IP or the intended destination IP. Select Source to filter by client IP/country or Destination(Network) to filter by the server IP/country.

- Use the map to evaluate the global distribution of traffic, and the frequency of attacks from a country origin or destination. Countries are color-coded according to the frequency of attacks. You can select a country within the map to filter the entire screen by IPs from that destination or origin.

Note: Countries in grey do not have sufficient traffic information.

- Use the table in this area to examine the traffic information by country.

10. To view more details of your DoS activity, click **Security > Reporting > DoS > Analysis**.

Tip: From the Dashboard, you can automatically filter specific Attack IDs or Virtual Servers in the DoS Analysis screen, by selecting the chart icon () from a table row.

You can continue to review the system snapshot using the DoS Dashboard screen. As a result, you become more familiar with you system's activities during DoS attacks. You can also view the statistics in graphical charts and in tables, focusing on the specific data you need using attack and dimension filters.

Sample DoS Dashboards

This figure shows a sample DoS Dashboard on a system that is having a low-level DoS attack now.

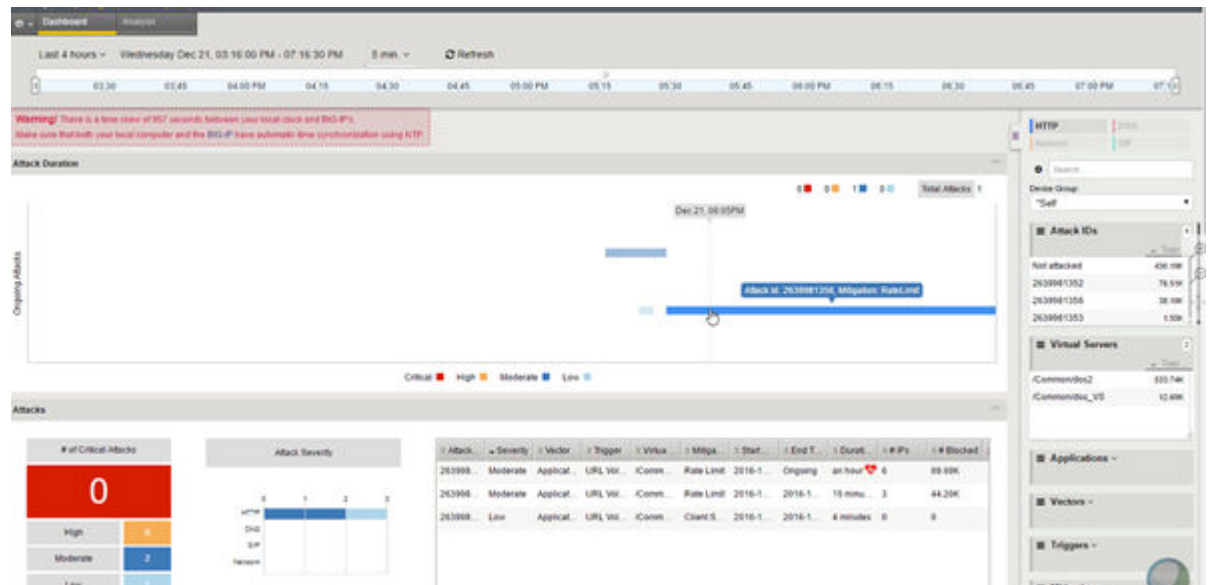


Figure 4: Sample DoS Dashboard

This figure shows a sample DoS Dashboard showing DoS attacks that occurred during the last week. Three of the attacks were critical but all were mitigated within minutes.

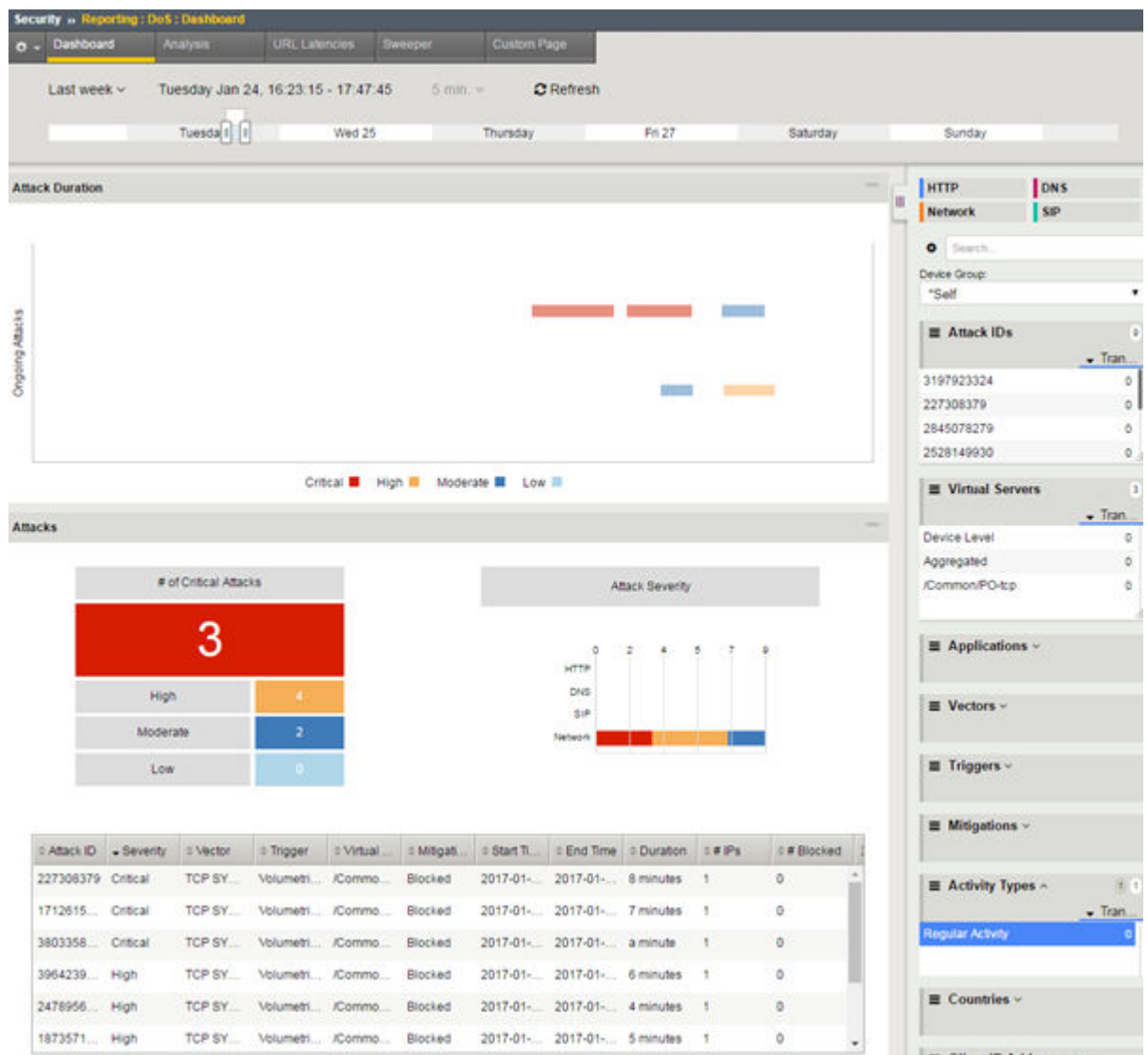


Figure 5: Sample DoS Dashboard showing attacks

Displaying DDoS Event logs

You can display DoS Event logs to see whether DDoS attacks have occurred, and view information about the attacks. The logs show details about the DDoS events.

1. On the Main tab, click **Security > Event Logs > DoS**.
The DoS Application Events screen opens, and if Layer 7 DoS attacks were detected, it lists the details about the DoS attack such as the start and end times, how it was detected and mitigated, the attack ID, and so on.
2. If DoS attacks are listed, review the list of attacks to see what has occurred, when it occurred, the mitigation, and the severity of the attack.
3. From the event log, click the **Attack ID** link for an attack or event to display information about the attack in a graphical chart.
4. To view information about other types of DoS attacks, from the DoS menu, choose another event log to view:

- For DNS DoS event logs, click **DNS Protocol**.
- For SIP DoS event logs, click **SIP Protocol**.
- For network firewall DoS event logs, click **Network**.
- To view event logs if you are using **Auto-Threshold Configuration** and have selected **Log Auto Threshold Events**, click **Auto Threshold**.

Many of the vectors set using device configuration, or when creating a protected object, include a setting for Auto-Threshold Configuration. You can log the auto-threshold events to see what values the system is setting based on the traffic it is handling.

Displaying DoS Application Events logs

You can display DoS Application Events logs to see whether L7 DoS attacks have occurred, and view information about the attacks. The logs show details about the DoS events.

1. On the Main tab, click **Security > Event Logs > DoS > Application Events**.
The DoS Application Events screen opens, and if Layer 7 DoS attacks were detected, it lists the details about the DoS attack such as the start and end times, how it was detected and mitigated, the attack ID, and so on.
2. If DoS attacks are listed, review the list of attacks to see what has occurred, when it occurred, the mitigation, and the severity of the attack.
3. From the event log, click the **Attack ID** link for an attack or event to display information about the attack in a graphical chart.

Creating customized DoS reports

You can create a customized DoS reporting screen so that it shows the specific data you are interested in, such as the top DoS attacks and server latency.

1. On the Main tab, click **Security > Reporting > DoS > Application > Custom Page**.
The DoS Custom Page screen opens, and shows default widgets (sections) you may find useful.
2. Review the charts and tables provided, and click the configuration icon to adjust or delete them, as needed.
 - To modify the widget and change what it displays, click the gear icon and select **Settings**. On the popup screen, adjust the values that control what is displayed.
 - To remove the widget from the custom page, click the gear icon and select **Delete**.
3. To create a new widget to your specifications, click **Add Widget**.
The Add New Widget popup screen opens where you can select custom options for what to include, the time frame, and how to display the information.
4. Continue adjusting the custom page so that it shows the information you want.
You can drag and drop the widgets to change the order in which they are displayed. You can set the time range for all widgets or for each one separately.
5. To save the information shown in the custom report to a file or email attachment, click **Export** and choose your options.

You can also export the data from a single widget by selecting **Export** from the configuration icon.

You have created a custom page that includes the information you need to monitor your system. As you use the reports to investigate DoS attacks, you can adjust the custom page to include additional data that you need. You can save the reports or send them to others who want to review the data.

Adjusting Global Settings

Overview: Adjusting global settings

DDoS Hybrid Defender™ uses reasonable default settings for the global system settings. Some environments may require adjustments to port numbers, allowed protocols, or thresholds that signal an attack. For example, you may use a different DNS or SIP port number from the one that is configured. In that case, you can change it.

Many of the thresholds indicate the value at which a packet, header, URI, or other setting is considered too large, too small, or not typical. This does not necessarily indicate an attack. It means that the value is unusual enough that you should take a look at what's happening on the system. You may want to change the global settings because the traffic should be allowed and should not cause alarm.

However, note that adjusting these settings should be needed only in rare cases. The changes should be made only by an administrator familiar with the applications, servers, or other network objects that DDoS Hybrid Defender is protecting.

Adjusting global settings

You can adjust global settings on DDoS Hybrid Defender™ if the default values are not right for your environment.

1. On the Main tab, click **DoS Protection > Quick Configuration**.
2. On the menu bar, click **Global Settings**.
3. Review the global settings to see if they are appropriate for your system.
A reference table or the help describes the settings.
4. Adjust the value of the setting you want to change.
5. Click **Update**.

The global settings are applied at the system level.

Global Settings

You need to adjust the global settings only if something is not working correctly. For example, if your systems use a DNS port other than 53.

Flow Eviction Policy

| Setting | Default Value | What It Specifies |
|---------------------------|--|--|
| Trigger Thresholds | High water mark 95%; Low water mark 85% | Specifies a high and low water mark that is a percentage of the quota of flows before flow eviction starts (high water mark) and ends (low water mark). |
| Strategies | None | Specifies which traffic flows to drop as much as possible: <ul style="list-style-type: none">• Oldest: Drops the oldest existing flows.• Idle: Drops the flows that have been the least busy the longest. |

| Setting | Default Value | What It Specifies |
|----------------------------|--|---|
| Slow Flow Detection | <ul style="list-style-type: none"> Not enabled Max Slow Flows: 100 Slow Threshold: 32 | <ul style="list-style-type: none"> Busiest: Drops the flows that have been busiest the longest. <p>Enables the features and specifies what constitutes slow flows:</p> <ul style="list-style-type: none"> Max Slow Flows: Specifies the maximum percentage of slow flows allowed on the system. Slow Threshold: Specifies the rate (bytes/sec) below which a flow is considered slow. |

Ports & VLANs

| Setting | Default Value | What It Specifies |
|--|---------------|---|
| UDP Port Inclusion/Exclusion List | Exclude | Specifies UDP ports to analyze for DDoS attacks (Include) or exclude from analysis (Exclude) for all protected objects. One at a time, type the port number, select source and/or destination, and click Add . |
| DNS Port | 53 | Specifies which port to use for DNS traffic, if the default of 53 is not correct. |
| DNS VLAN | 0 | Specifies which VLAN should receive external DNS responses. The default is 0, all VLANs. |
| SIP Port | 5060 | Specifies which port to use for SIP traffic, if the default of 5060 is not correct. |

Allowed Protocols & Options

| Setting | Default Value | What It Specifies |
|--|---------------------|---|
| Allowed non-Standard IP Protocols | Protocol 1 & 2: 255 | Specifies the protocol number of one or two IP protocols that the Unknown IP Protocol DoS vector should treat as known (that is, ignored). Note: Though valid values are 0-255, IP protocols 0-142 are already known by the vector so specifying an IP protocol number in that range has no effect on the behavior of the vector. |
| Allowed non-Standard ICMPv6 Types | Type 1 & 2: 158 | Specifies one or two additional ICMPv6 message types for the Unknown ICMPv6 Message Type vector to treat as known (that is, ignored). The allowed values are 0-254. However, ICMPv6 message types 0-132, 134, and 135 are already ignored by the vector so specifying one of those message types has no effect on the behavior of the vector. |
| Allowed non-Standard TCP Types | Type 1 & 2: 0 | Specifies one or two TCP option types for the Unknown TCP Option Type vector to treat as known (that is, ignored). Though valid values are 0-255, option types 0-5, 8, 19-21, 30, 34, 128, and 254 are allowed and have no effect on the behavior of the vector. |

Thresholds

| Setting | Default Value | What It Specifies |
|---|---------------|--|
| IPv6 Single Endpoint Prefix Length | 128 | Specifies whether a single endpoint in IPv6 is /64 or /128 (or some other prefix). |
| IPv4 Low TTL | 1 | Defines the minimum acceptable value for TTL (time to live) in the IPv4 header. |
| IPv6 Low Hop Count | 1 | Specifies the minimum acceptable value for IPv6 Hop Count. |
| Too Large DNS Packet | 4096 | Specifies the size at which a DNS packet is considered oversized. |
| Too Large ICMPv4 Packet | 1480 | Specifies the size at which an ICMPv4 packet is considered oversized. |
| Too Large ICMPv6 Packet | 1460 | Specifies the size at which an ICMPv6 packet is considered oversized. |
| Too Large IPv6 Extension Header | 128 | Specifies the size at which an IPv6 Extension Header is considered oversized. |
| Too Many IPv6 Extension Headers | 4 | Specifies the number of IPv6 Extension Headers that are considered too many. |
| Too Long SIP URI | 1024 | Specifies the length at which a SIP URI is considered too long. |
| Too Small TCP Window Size | 0 | Specifies the window size that is considered too small. |
| Too Large TCP SYN Packet | 64 | Specifies the size at which a TCP SYN packet is considered oversized. |

Blacklist Publisher

| Setting | Default Value | What It Specifies |
|-------------------------------------|---------------|--|
| Blacklist Publisher Next-Hop | Any | Specifies the next hop address of the BGP router to which you want to advertise blacklisted addresses. |
| Scrubbing | None | Specifies the type of scrubbing: BGP (specify IPv4 or IPv6 address), Silverline, or none. |

Sending the blacklist to a next-hop router

DDoS Hybrid Defender™ detects bad actors, adding their IP addresses to a blacklist temporarily. You can specify an edge router to which to advertise the blacklist, so it can stop the traffic causing a DoS attack.

1. On the Main tab, click **DoS Protection > Quick Configuration**.
2. On the menu bar, click **Global Settings**.
3. In the Blacklist Publisher area, in the **Advertisement Next-Hop** field, type the IP address of a next-hop router to which to send the blacklist.
4. Click **Update**.

The router you configured will drop traffic from IP addresses on the blacklist until the blacklist entry is automatically removed.

Updating DDoS Hybrid Defender

Overview: Updating DDoS Hybrid Defender

As product updates for DDoS Hybrid Defender™ become available, you can download and install them on the system. The existing configuration is retained.

Downloading DDoS Hybrid Defender

DDoS Hybrid Defender™ software updates are available from the F5 downloads web site. You need to download it onto your computer so you can install it onto the DDoS Hybrid Defender system.

1. Log in to the F5 Downloads site, <https://downloads.f5.com>, and click the **Find a Download** button.
2. In the Security F5 Product Family, locate the DDoS Hybrid Defender software, and click it.
3. Select the product version and click **DDoS_Hybrid_Defender**.
4. Read the End User Software License, and click the **I Accept** button if you agree with the terms.
5. Click the `f5-ddos-hybrid-defender rpm` file to download it.
6. Click the closest geographical location, and save the file on your local system.
The software package is downloaded onto your system.
7. Optionally, you can download the `md5` file to verify the integrity of the rpm file.

The DDoS Hybrid Defender software package is now available on your local computer, and is ready for you to install onto the DDoS Hybrid Defender system. If setting up two systems for high availability, you should use the same package on both systems.

Updating DDoS Hybrid Defender

You need to have downloaded the DDoS Hybrid Defender™ update from F5.

You can update DDoS Hybrid Defender.

1. Log in to DDoS Hybrid Defender with the administrator user name and password.
The Welcome screen of the system is displayed.
2. On the Main tab, click **DoS Protection > Quick Configuration**.
3. On the menu bar, click **About**.
The About screen opens and shows the version of the product that is running.
4. In the **File Name** setting, click **Choose File** and navigate to the DDoS Hybrid Defender update that you previously downloaded from F5, and click **Install**.
5. From the **Install Method** list, select **Choose File**, navigate to the DDoS Hybrid Defender update that you previously downloaded from F5, and click **Install**.

The DDoS Hybrid Defender update is installed, and the configuration from the previous version is preserved on the system.

Look over the configuration screens to see if there are new features that you want to use.

Legal Notices

Legal notices

Publication Date

This document was published on February 27, 2018.

Publication Number

MAN-0622-03

Copyright

Copyright © 2018, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

For a current list of F5 trademarks and service marks, see <http://www.f5.com/about/guidelines-policies/trademarks>.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at: <https://f5.com/about-us/policies/patents>.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

Index

A

attack types 35

B

bandwidth 27

bypass DDoS checking 27

C

custom reports

creating for DoS 51

D

DDoS attacks

detecting at the device level 23

viewing event logs 50

DDoS checking

bypassing 27

DDoS device configuration

detecting DDoS flood attacks 43

DDoS Hybrid Defender

about 5

adjusting global settings 53

downloading the software 57

example: deployment 7

installing 19

installing high availability overview 9

installing on device 1 11

installing overview 17

performing initial setup 9, 17

performing network configuration 13, 19, 21

setting up remote logging 15, 21

setup overview 23, 53

specifying Silverline credentials 12, 22

updating 57

updating overview 57

DDoS protection

summary table 30

deployments 5

device configuration

automatically setting thresholds 24

detecting DDoS attacks 23

manually setting thresholds 25

device configuration attack types 35

DoS

about blacklisting sweep attack IP addresses 43

about preventing flood attacks 43

about preventing sweep attacks 43

protected object attack types 31

DoS attacks

automatically setting thresholds for the device 24

investigating 47

protecting network objects 28

viewing DoS Overview 47

DoS attacks (*continued*)

viewing event logs 51

DoS device configuration

detecting DDoS flood attacks 44

DoS Overview Summary

viewing 47

DoS protection

installing overview 17

setup overview 23, 53

DoS reports

creating custom 51

sample Dashboard 49

DoS vectors

setting thresholds manually 25

E

event logs

viewing for DDoS 50

viewing for DoS 51

F

failover 12

flood attack

defined 43

flood attacks

detecting at the device level 43

protecting all objects 44

G

global settings

descriptions of 53

H

high availability

configuring 12

connecting devices 11

installing overview 9

I

initial configuration

licensing DDoS Hybrid Defender 10, 18

initial setup

of DDoS Hybrid Defender 9, 17

inline deployment 5

installation

of DDoS Hybrid Defender 11, 19

L

license activation

for DDoS Hybrid Defender 10, 18

logging

Index

logging (*continued*)
 setting up for DDoS Hybrid Defender 15, 21, 53

N

network configuration
 out-of-band 21
 setting up for DDoS Hybrid Defender 19
 setting up on high-available systems 13

O

out-of-band deployment 5

P

protected object
 attack vectors 31
protected objects
 creating 28

R

router
 specifying next hop address 55

S

scrubbing 27
self IP address
 configuring 13, 19
Silverline
 setting up authentication 12, 22
software download 57
standby status 13
sweep attack
 defined 43
sweep attacks
 detecting at the device level 43

U

update
 of DDoS Hybrid Defender 57
 overview 57

V

vectors
 device configuration 35
VLAN
 configuring 19

W

whitelist
 allowing addresses to bypass DDoS checks 27