F5® DDoS Hybrid Defender™: Setup

Version 12.1.0

Table of Contents

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.

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.

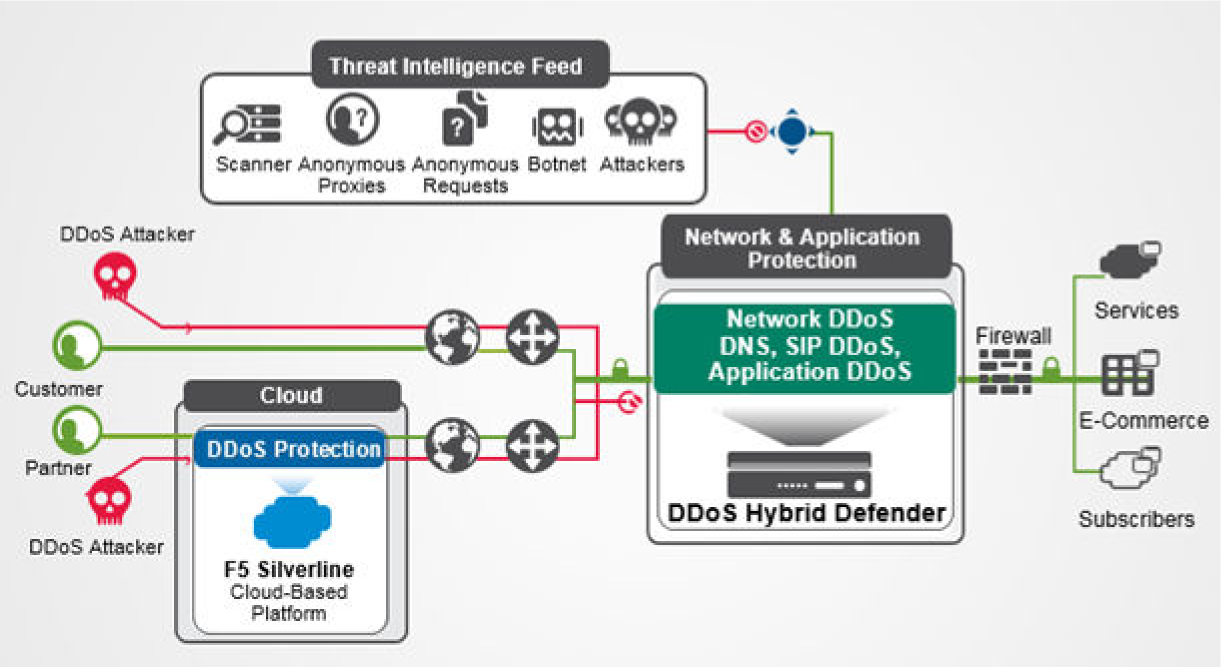


Figure 1: Example DDoS Hybrid Defender deployment

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.

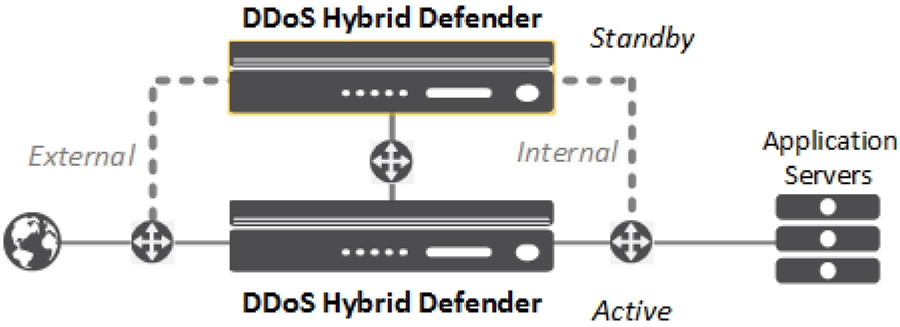


Figure 2: DDoS Hybrid Defender High-Availability deployment

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)

Task Summary

Downloading DDoS Hybrid Defender
Performing initial setup
Manually licensing DDoS Hybrid Defender
Connecting two DDoS Hybrid Defender devices
Installing DDoS Hybrid Defender on device 1
Configuring high availability on device 1
Installing DDoS Hybrid Defender on device 2
Configuring the network on the high availability systems
Setting up remote logging
Connecting with F5 Silverline

Downloading DDoS Hybrid Defender

DDoS Hybrid Defender™ software is 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.

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

You need to have downloaded the DDoS Hybrid Defender™ software from F5, and completed the initial setup before you can install DDoS Hybrid Defender.

You can 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. If you are installing on systems with management IP addresses of `10.192.19.24` and `10.192.19.25`, consider `10.192.19.25` to be device 1.

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. In the **File Name** setting, click **Choose File** and navigate to the DDoS Hybrid Defender software that you previously downloaded from F5, and click **Open**.

The DDoS Hybrid Defender software is now installed on device 1. The next time you log in, you will be able to access the DoS Protection screens.

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.

Installing DDoS Hybrid Defender on device 2

Before you begin, you need to have access to the DDoS Hybrid Defender™ software from F5, and have completed the initial setup on device 2, the standby device. The active device (device 1) must be set up for high availability.

You can now install DDoS Hybrid Defender onto device 2, the system that is set up as the standby system. Device 2 must be the system with the lower management IP address. If you are installing on systems with management IP addresses of `10.192.19.24` and `10.192.19.25`, consider `10.192.19.24` to be device 2.

1. Log in to DDoS Hybrid Defender device 2 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. In the **File Name** setting, click **Choose File** and navigate to the DDoS Hybrid Defender software that you previously downloaded from F5, and click **Open**.

The DDoS Hybrid Defender software is now installed on device 2. The next time you log in, you can access the DoS Protection screens. In the upper left corner, it says ONLINE (STANDBY). 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.

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 one VLAN, you can use the **defaultVLAN** setup. Otherwise, skip this step and go to the next one.
   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**.

      Click **Untagged** to allow the interface to accept traffic only from that VLAN, instead of from multiple VLANs.
   d) In the **IP Address/Mask** field, type either an IPv4 or an IPv6 address.

      The self IP address is the address of the system on the internal interface that provides access to the internal network.
   e) 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.
5. If DDoS Hybrid Defender connects to multiple VLANs or uses routed topology, instead of using the default network, configure the network in the VLAN area. Click **Create** and set up the 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.
   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.

      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.
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.
8. Log in to DDoS Hybrid Defender device 2 using the administrator user name and password.
9. 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 to 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.

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, register with Silverline on the active device.

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 Address** field, type the IP address 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**.

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.

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 must have assigned the management IP address on the LCD panel of the device, or with a hypervisor if you are 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*.

Before you begin, make sure you have this information:

- 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)

Task Summary

Downloading DDoS Hybrid Defender
Performing initial setup
Manually licensing DDoS Hybrid Defender
Installing DDoS Hybrid Defender
Configuring the network for a stand-alone device
Setting up remote logging
Connecting with F5 Silverline

Downloading DDoS Hybrid Defender

DDoS Hybrid Defender™ software is 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.

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

You need to have downloaded the DDoS Hybrid Defender™ software from F5, and 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**.
   Because the software has not yet been installed, the Import Package screen opens.
3. In the **File Name** setting, click **Choose File** and navigate to the DDoS Hybrid Defender software that you previously downloaded from F5, and click **Open**.

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 a stand-alone device

You must first configure the network to create the workflow for DDoS Hybrid Defender™. You do this by configuring VLANs (virtual local area networks), and associating the physical interfaces on the system with them.

***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 the next one.
   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**.

      Click **Untagged** to allow the interface to accept traffic only from that VLAN, instead of from multiple VLANs.
   d) In the **IP Address/Mask** field, type either an IPv4 or an IPv6 address.

      The self IP address is the address of the system on the internal interface that provides access to the internal network.
   e) 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.
4. If DDoS Hybrid Defender connects to multiple VLANs or uses routed topology, instead of using the default network, configure the network in the VLAN area. Click **Create** and set up the 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** field, type the IP address and mask in the form `10.10.10.10/22`.
   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 Address/Mask** 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.
5. 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.
6. Click **Update** to save the network configuration.

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

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.

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, register with Silverline on the active device.

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 Address** field, type the IP address 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**.

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.

Task Summary

Protecting the network from DDoS attacks

Automatically setting system-wide DDoS vector thresholds

Manually setting system-wide DDoS vector thresholds

Bypassing DDoS checks

Protecting network devices from DDoS attacks

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. Configure the **Auto Threshold Sensitivity** (`1-100`, default is `50`).

   A lower number 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.
4. Optionally, set up a whitelist of IP addresses that should be allowed to bypass DDoS checks. 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 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.

Setting	Protects against:
Single Endpoint	Single endpoint flood and sweep DoS attacks.
SIP	SIP protocol DDoS vectors.
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 system to respond to possible 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. 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.*
6. 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.

7. 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.
8. Click the **Update** button.
   The selected configuration is updated, and the DoS Protection Device Configuration screen opens again.
9. 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. 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.

Protecting network devices 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** 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 **Whitelisted IP Addresses**, one at a time, type trusted IP addresses or subnets that do not need to be examined for DoS attacks, and click **Add**.

13. If you want to detect attacks by considering server health using stress-based detection by measuring server latency, select the **Server Health** check box.

You can clear this check box if you are using HTTP or HTTPS L7 DoS detection. It must be set if you are using Behavioral DoS detection.

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

14. 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.

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.

15. 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.

16. Click the name of any vector to edit the settings.
The configuration settings appear on the right side of the screen.

17. 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.

18. 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	• 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	• Set **Port** to the SIP port. • Set **Protocol** to **TCP**. • Set **Deployment Model** to **Symmetric**. • In **DDoS Settings**, click **SIP**.

To protect this:	Set this in the protected object:
	- Expand **SIP**, check threshold settings.
Web applications	- 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	- 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	- 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 `option.db variable tm.acceptipsourceroute` must be enabled to receive IP options.
Option Present With Illegal Length	Packets contain an option with an illegal length.

IPv6 Attack Vectors

Vector	Information
ICMPv6 Flood	Flood with ICMPv6 packets.

Vector	Information
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
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.
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`).
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`).
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`).
qdcount	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`).

Vector	How to identify it
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 voicemails.
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.
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.

Protection	Description
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.
Proactive Bot Defense	Attacks caused by web robots. The system uses JavaScript evaluations and bot signatures to ensure that browsers are legitimate not automated.

HTTP and HTTPS Proactive Bot Defense Categories

Category	Description
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	The ICMP frame is either the wrong size or not one of the valid IPv4 or IPv6 types. Valid IPv4 types: • 0 Echo Reply • 3 Destination Unreachable	Yes

Vector	Information	Hardware accelerated
	• 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 Valid IPv6 types: • 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	
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
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

Vector	Information	Hardware accelerated
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
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

Vector	Information	Hardware accelerated
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
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

Vector	Information	Hardware accelerated
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
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**	Yes

Vector	Information	Hardware accelerated
	Protection > **Quick Configuration** > **Global Settings** to the DNS VLAN (`0-4094`).	
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 SYN Packet** field. The default size in bytes is `64` and the maximum allowable value is `9216`.	Yes
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.	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
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

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
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
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 a 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.

Task list

Protecting against single-endpoint flood and sweep attacks
Protecting objects system-wide from flood attacks

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 display a DoS Overview report that tells you whether or not a DoS attack is taking place, and shows information about the impact of DoS attacks on your system throughput and memory.

1. On the Main tab, click **Security** > **Reporting** > **DoS**.
   The DoS Overview screen opens and displays real-time information about all DoS attacks on the system. The system displays attacks that either started or ended during the last hour, by default.
2. Review the Recent Attacks log, Throughput, and RAM & CPU usage charts to see if there have been any recent DoS attacks.

   The Recent Attacks log lists recent DoS attacks and shows a flag for an attack in progress. The log includes the most recent 100 events per protocol for application and network attacks. So up to 200 attacks may be shown in the charts.
3. If the information you are looking for is not shown, next to **Logged Attacks**, try increasing the time period selected.

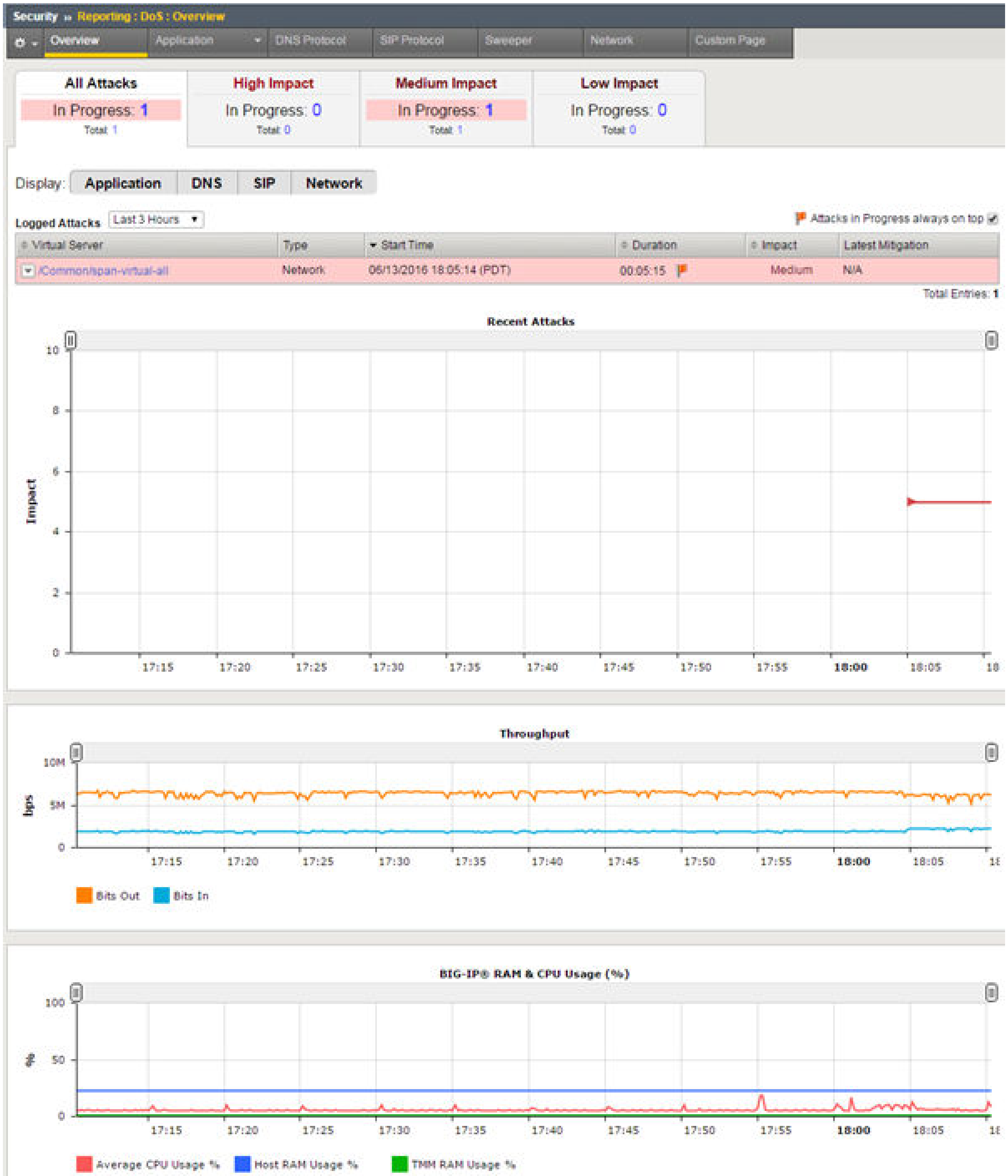
   You can also filter the attacks to view only those which have High, Medium, or Low Impact by clicking the appropriate tab.
4. To focus on specific details in the charts, point on the charts at the time you are interested in.
   The system displays the details about what was happening at that time in a tooltip. For example, pointing on the throughput chart at a specific time displays the number of bits in and bits out at that time.
5. To learn more about attacks that have occurred, in the Recent Attacks log, click the Attack ID number.
   The system displays events associated with the attack. If there are more than 100 events, you can see a link to the Event Log, which you can click to see more events.

You can review the details about DoS attacks on the DoS Overview screen and quickly see whether or not you are under attack.

Sample DoS Overview screen

This figure shows a sample DoS Overview screen on a system that is having an attack.

The Overview screen includes information on throughput and RAM and CPU usage. Because the statistics vary from system to system, it is a good idea to become familiar with typical memory and CPU usage and throughput on your system as well as checking for recent attacks.



All Attacks	High Impact	Medium Impact	Low Impact
In Progress: 1	In Progress: 0	In Progress: 1	In Progress: 0
Total: 1	Total: 0	Total: 1	Total: 0

Logged Attacks Last 3 Hours

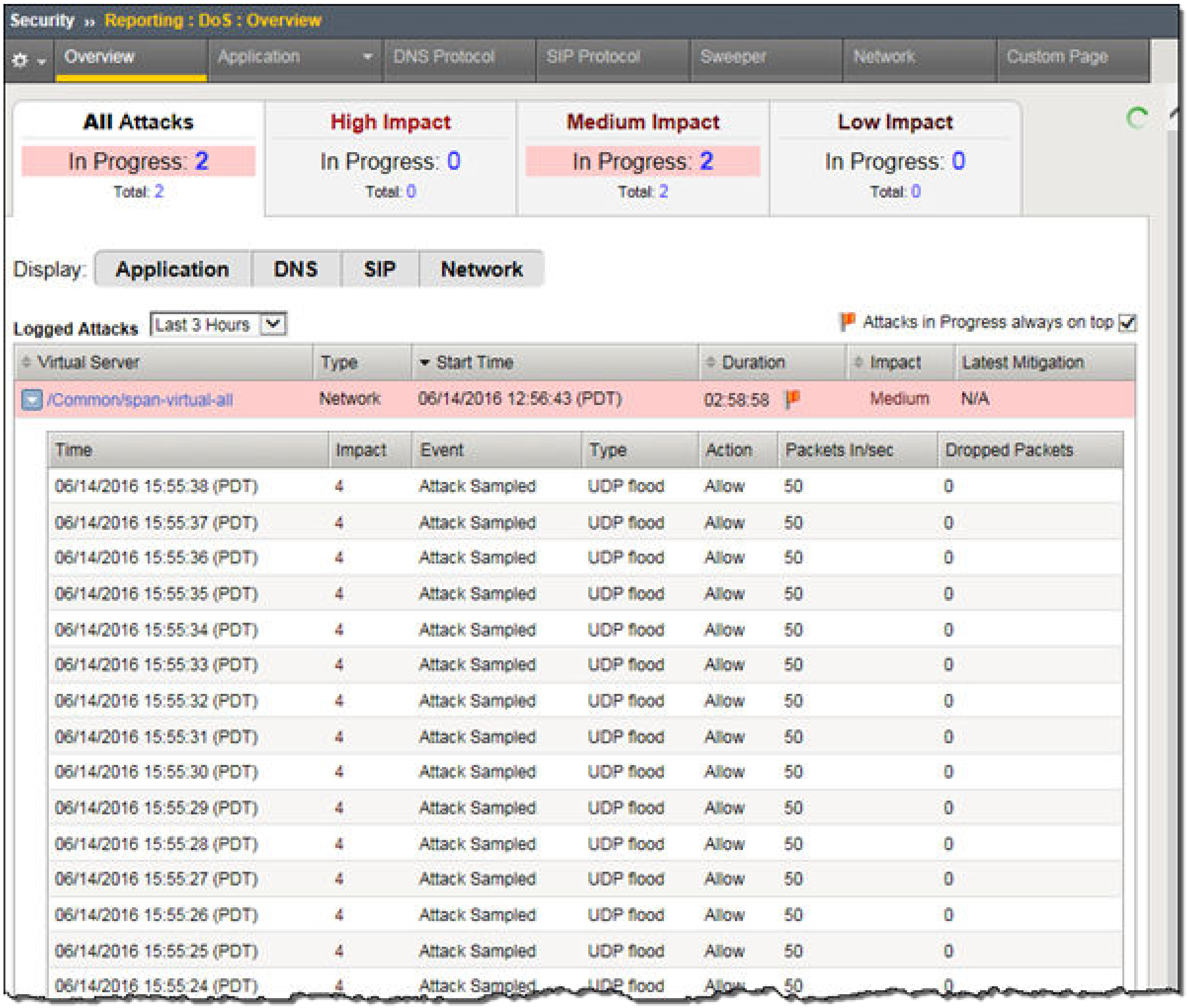
Attacks in Progress always on top ☑

Virtual Server	Type	Start Time	Duration	Impact	Latest Mitigation
/Common/span-virtual-all	Network	06/13/2016 18:05:14 (PDT)	00:05:15	Medium	N/A

Total Entries: 1

Figure 3: Sample DDoS Overview screen

Click the down arrow next to the protected object (in the Virtual Server column) to find out what type of attack it is. Here you can see the attack is a UDP flood attack.



All Attacks	High Impact	Medium Impact	Low Impact
In Progress: 2	In Progress: 0	In Progress: 2	In Progress: 0
Total: 2	Total: 0	Total: 2	Total: 0

Logged Attacks: Last 3 Hours

Virtual Server	Type	Start Time	Duration	Impact	Latest Mitigation
/Common/span-virtual-all	Network	06/14/2016 12:56:43 (PDT)	02:58:58	Medium	N/A

Time	Impact	Event	Type	Action	Packets In/sec	Dropped Packets
06/14/2016 15:55:38 (PDT)	4	Attack Sampled	UDP flood	Allow	50	0
06/14/2016 15:55:37 (PDT)	4	Attack Sampled	UDP flood	Allow	50	0
06/14/2016 15:55:36 (PDT)	4	Attack Sampled	UDP flood	Allow	50	0
06/14/2016 15:55:35 (PDT)	4	Attack Sampled	UDP flood	Allow	50	0
06/14/2016 15:55:34 (PDT)	4	Attack Sampled	UDP flood	Allow	50	0
06/14/2016 15:55:33 (PDT)	4	Attack Sampled	UDP flood	Allow	50	0
06/14/2016 15:55:32 (PDT)	4	Attack Sampled	UDP flood	Allow	50	0
06/14/2016 15:55:31 (PDT)	4	Attack Sampled	UDP flood	Allow	50	0
06/14/2016 15:55:30 (PDT)	4	Attack Sampled	UDP flood	Allow	50	0
06/14/2016 15:55:29 (PDT)	4	Attack Sampled	UDP flood	Allow	50	0
06/14/2016 15:55:28 (PDT)	4	Attack Sampled	UDP flood	Allow	50	0
06/14/2016 15:55:27 (PDT)	4	Attack Sampled	UDP flood	Allow	50	0
06/14/2016 15:55:26 (PDT)	4	Attack Sampled	UDP flood	Allow	50	0
06/14/2016 15:55:25 (PDT)	4	Attack Sampled	UDP flood	Allow	50	0
06/14/2016 15:55:24 (PDT)	4	Attack Sampled	UDP flood	Allow	50	0

Figure 4: Events related to an attack

Displaying DDoS Events logs

You can display DoS Events 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:

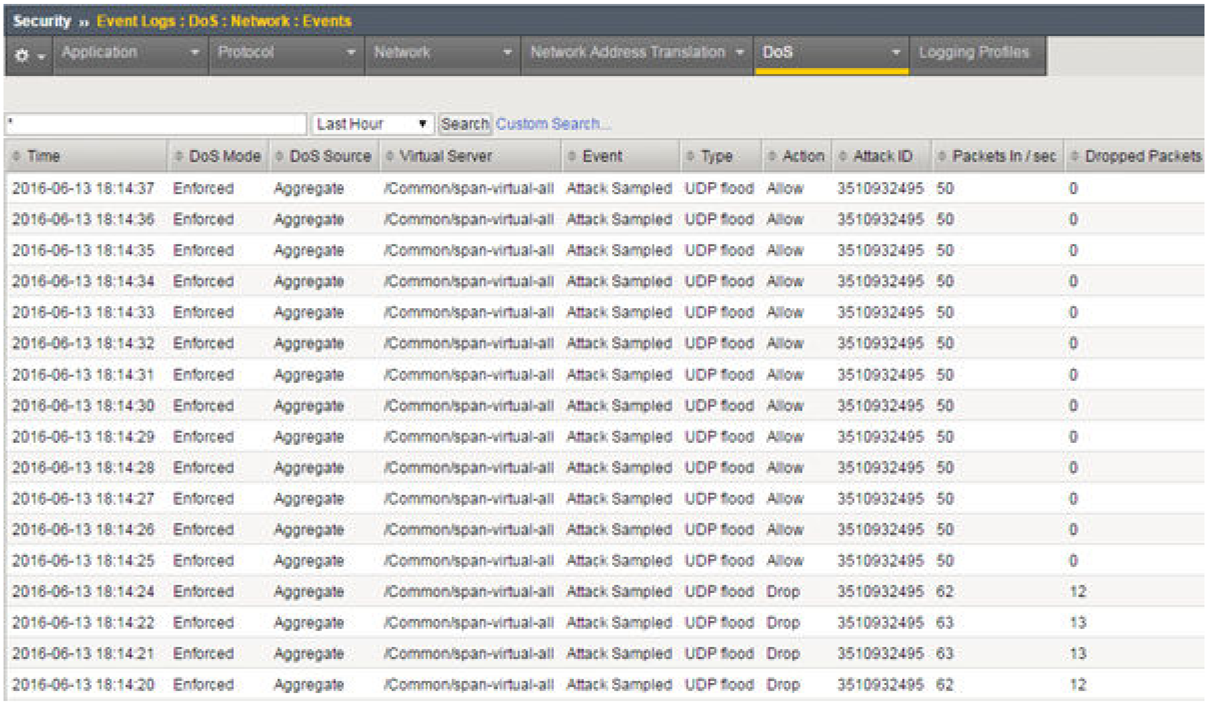
   - For DNS DoS event logs, click **DNS Protocol**.
   - For SIP DoS event logs, click **SIP Protocol**.
   - For network firewall DoS event logs, click **Network**.

- 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.

Sample DDoS event log

This figure shows a sample DDoS event log on a system that is experiencing UDP flood attack. When the attack exceeds the maximum packets per seconds (50 pps), excess packets are dropped.



Time	DoS Mode	DoS Source	Virtual Server	Event	Type	Action	Attack ID	Packets In / sec	Dropped Packets
2016-06-13 18:14:37	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495	50	0
2016-06-13 18:14:36	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495	50	0
2016-06-13 18:14:35	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495	50	0
2016-06-13 18:14:34	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495	50	0
2016-06-13 18:14:33	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495	50	0
2016-06-13 18:14:32	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495	50	0
2016-06-13 18:14:31	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495	50	0
2016-06-13 18:14:30	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495	50	0
2016-06-13 18:14:29	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495	50	0
2016-06-13 18:14:28	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495	50	0
2016-06-13 18:14:27	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495	50	0
2016-06-13 18:14:26	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495	50	0
2016-06-13 18:14:25	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495	50	0
2016-06-13 18:14:24	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Drop	3510932495	62	12
2016-06-13 18:14:22	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Drop	3510932495	63	13
2016-06-13 18:14:21	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Drop	3510932495	63	13
2016-06-13 18:14:20	Enforced	Aggregate	/Common/span-virtual-all	Attack Sampled	UDP flood	Drop	3510932495	62	12

Figure 5: Sample DDoS event log

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.

Viewing DoS transaction outcomes

You can display graphic charts that show transaction outcomes for DoS attacks on web applications that were detected on your system. The charts provide visibility into what caused the attack, IP addresses of the attackers, which applications are being attacked, and how the attacks are being mitigated.

1. On the Main tab, click **Security** > **Reporting** > **DoS** > **Application** > **Transaction Outcomes**.
   The Transaction Outcomes screen opens and displays a graphical chart showing cumulative statistics about DoS attacks detected by the system.
2. If you want to change the time frame for information shown in the chart, adjust the **Display .. during** settings.

   You can focus in on requests or responses only, and for the period of time you are interested in.
3. To see the statistics for a specific time, point anywhere on the chart.
   Information about the transactions at that time pops up on the screen.
4. If you want to view additional information, under the chart, from **Drilldown to** select the option for the details you want to see.

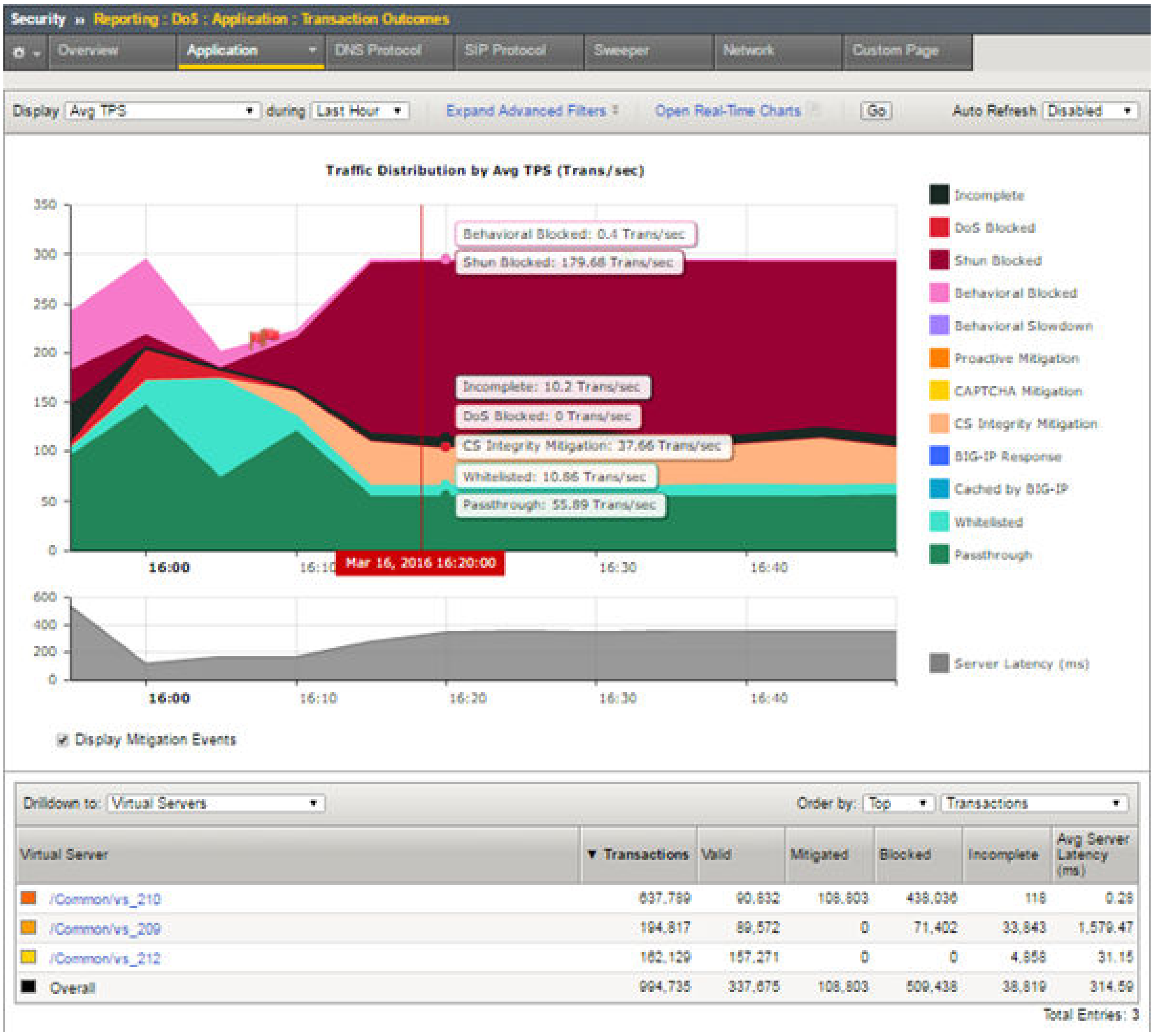
   For example, select **Client IP Addresses** to see the list of IP addresses involved in the attack, the number of transactions initiated by each one, and those which were valid, mitigated, and blocked.
5. To view a report showing live traffic, click **Open Real-Time Charts**.
   A popup screen shows DoS statistics in real-time, and it is updated every 10 seconds.

By reviewing DoS Application Statistics, you can investigate the details of an attack. You can become more familiar with what caused the attacks, what applications are most vulnerable, and you see the mitigation methods that are in place. As a result of your investigation, you have more information to help you decide whether you need to tune the DoS configuration and add more protections, or change the thresholds in the DoS profile.

To get additional information if you are recording traffic during attacks, you can view the TCP dumps related to the DoS attacks in `/shared/dosl7/tcpdumps`.

Sample DoS Transaction Outcomes report

This figure shows a sample Transaction Outcomes report for a system on which there have been DoS attacks. The chart shows how the traffic has been handled by the system. It shows aggregated data that is updated every few minutes.



Display: Avg TPS during: Last Hour

Auto Refresh: Disabled

☑ Display Mitigation Events

Drilldown to: Virtual Servers

Order by: Top Transactions

	Virtual Server	▼ Transactions	Valid	Mitigated	Blocked	Incomplete	Avg Server Latency (ms)
🟧	/Common/vs_210	637,789	90,832	108,803	438,036	118	0.28
🟧	/Common/vs_209	194,817	89,572	0	71,402	33,843	1,579.47
🟨	/Common/vs_212	162,129	157,271	0	0	4,858	31.15
⬛	Overall	994,735	337,675	108,803	509,438	38,819	314.59

Total Entries: 3

Figure 6: Sample DoS Transaction Outcomes report

You can adjust which elements are listed in the table below the chart. This figure lists the virtual servers that traffic is attempting to access. By clicking one of the virtual servers (or other objects listed), you can drill down to see what is happening with that specific traffic. For example, here attacks are primarily taking place on `vs_210`, and much of the traffic is being blocked.

You can also open a real-time chart that is constantly updated by clicking the **Open Real-Time Charts** link. It is a popup screen that you can leave displayed on your computer. It shows the traffic distribution on the system.

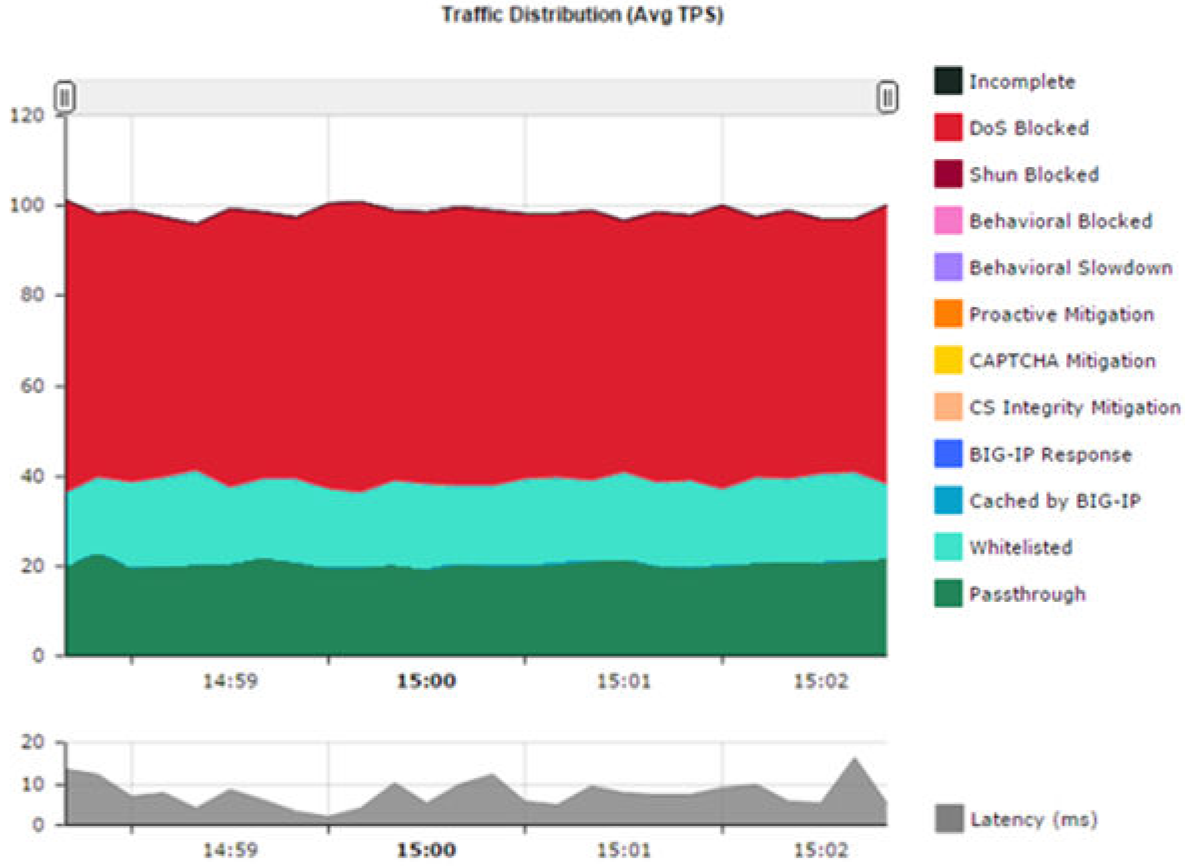


Figure 7: Sample DoS real-time chart

You can go back to the DoS Statistics report and change the values for what is displayed using the **Display** and **during** settings to see additional information. Viewing different statistical views is useful to understanding and tracking DoS attacks.

In the lower table on the screen, Latency (ms) indicates how long it takes (in milliseconds) from the time a request reaches the system, for it to proceed to the web application server, and return a response. Note that dropped or blocked requests that do not reach the server, do not register latency because there is no full request-response cycle.

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 **Commit Changes to System** to save the changes.

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 33.

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: • **Oldest**: Drops the oldest existing flows. • **Idle**: Drops the flows that have been the least busy the longest.

Setting	Default Value	What It Specifies
		- **Busiest**: Drops the flows that have been busiest the longest.
Slow Flow Detection	- Not enabled - Max Slow Flows: 100 - Slow Threshold: 32	Enables the features and specifies what constitutes slow flows: - **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 (0-255) of one or two IP protocols to allow in addition to the standard ones (TCP and UDP).
Allowed non-Standard ICMPv6 Types	Type 1 & 2: 158	Specifies one or two ICMPv6 types (0-255) to allow.
Allowed non-Standard TCP Types	Type 1 & 2: 0	Specifies one or two TCP types (0-255) to allow.

Thresholds

Setting	Default Value	What It Specifies
SYN Cookie Activation Threshold	2048	Specifies the number of SYN requests the system can receive until the SYN Cookie protection mechanism kicks in (protecting against SYN flood attacks).
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.

Setting	Default Value	What It Specifies
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
Advertisement Next-Hop	none	Specifies the next hop address of the BGP router to which you want to advertise blacklisted addresses.

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 **Commit Changes to System** to save the changes.

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.

Task Summary

Downloading DDoS Hybrid Defender
Updating DDoS Hybrid Defender

Downloading DDoS Hybrid Defender

DDoS Hybrid Defender™ software is 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**.

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

Legal Notices

Legal notices

Publication Date

This document was published on November 2, 2016.

Publication Number

MAN-0622-00

Copyright

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