Platform Settings

Platform settings for Firewall Threat Defense devices configure a range of unrelated features whose values you might want to share among several devices. Even if you want different settings per device, you must create a shared policy and apply it to the desired device.

> **Note** In 7.4 and later, the Management and Diagnostic interfaces are merged. If Platform Settings for syslog servers or SNMP hosts specify the Diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices (7.3 and earlier, and some upgraded 7.4 devices).

Introduction to Platform Settings

A platform settings policy is a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in your deployment, such as time settings and external authentication.

A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device.

For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy.

You can also benefit from having multiple platform settings policies on a single Firewall Management Center. For example, if you have different mail relay hosts that you use under different circumstances or if you want to test different access lists, you can create several platform settings policies and switch between them, rather than editing a single policy.

Requirements and Prerequisites for Platform Settings Policies

Supported Domains

Any

User Roles

Admin

Access Admin

Network Admin

Manage Platform Settings Policies

Use the **Platform Settings** page (**Devices** > **Platform Settings**) to manage platform settings policies. This page indicates the type of device for each policy. The **Status** column shows the device targets for the policy.

Procedure

Step 1   Choose **Devices** > **Platform Settings**.

Step 2   For an existing policy, you can **Copy** ( ), **Edit** ( ), or **Delete** ( ) the policy.

Caution
You should not delete a policy that is the last-deployed policy on any of its target devices, even if it is out of date. Before you delete the policy completely, it is good practice to deploy a different policy to those targets.

Step 3   To create a new policy, click **New Policy**.

    a) Choose a device type from the drop-down list:

> • **Firepower Settings** to create a shared policy for managed Classic devices.
>
> • **Threat Defense Settings** to create a shared policy for managed Firewall Threat Defense devices.
>
> • **Chassis Platform Settings** to create a shared policy for managed Firewall Threat Defense chassis in multi-instance mode.

    b) Enter a **Name** for the new policy and optionally, a **Description**.

    c) Optionally, choose the **Available Devices** or **Available Chassis** where you want to apply the policy and click **Add** (or drag and drop) to add the selected devices. You can enter a search string in the **Search** field to narrow the list of devices.

    d) Click **Save**.

        The system creates the policy and opens it for editing.

Step 4   To change the target devices for a policy, click **Edit** (✎) next to the platform settings policy that you want to edit.

    a) Click **Policy Assignment**.

    b) To assign a device, high-availability pair, or device group to the policy, select it in the **Available Devices** or **Available Chassis** list and click **Add**. You can also drag and drop.

    c) To remove a device assignment, click **Delete** (🗑) next to a device, high-availability pair, or device group in the **Selected Devices** or **Selected Chassis** list.

    d) Click **OK**.

What to do next

> • Deploy configuration changes; see Deploy Configuration Changes.

Chassis Platform Settings

Chassis Platform Settings apply to multiple-instance mode chassis. For details on these settings, see Configure Chassis Platform Settings.

ARP Inspection

By default, all ARP packets are allowed between bridge group members. You can control the flow of ARP packets by enabling ARP inspection.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a "man-in-the-middle" attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router.

ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, so long as the correct MAC address and the associated IP address are in the static ARP table.

When you enable ARP inspection, the Firewall Threat Defense device compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.

- If there is a mismatch between the MAC address, the IP address, or the interface, then the Firewall Threat Defense device drops the packet.

- If the ARP packet does not match any entries in the static ARP table, then you can set the Firewall Threat Defense device to either forward the packet out all interfaces (flood), or to drop the packet.

Note The dedicated Management interface never floods packets even if this parameter is set to flood.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **ARP Inspection**.

Step 3 Add entries to the ARP inspection table.

a) Click **Add** to create a new entry, or click **Edit** if the entry already exists.

b) Select the desired options.

- **Inspect Enabled**—To perform ARP inspection on the selected interfaces and zones.

- **Flood Enabled**—Whether to flood ARP requests that do not match static ARP entries out all interfaces other than the originating interface or the dedicated management interface. This is the default behavior.

  If you do not elect to flood ARP requests, then only those requests that exactly match static ARP entries are allowed.

- **Security Zones**—Add the zones that contain the interfaces on which to perform the selected actions. The zones must be switched zones. For interfaces not in a zone, you can type the interface name into the field below the Selected Security Zone list and click **Add**. These rules will be applied to a device only if the device includes the selected interfaces or zones.

c) Click **OK**.

Step 4 Add static ARP entries according to Add a Static ARP Entry.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Banner

You can configure messages to show users when they connect to the device command line interface (CLI).

Procedure

Step 1   Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2   Select **Banner**.

Step 3   Configure the banner.

Following are some tips and requirements for banners.

- Only ASCII characters are allowed. You can use line returns (press Enter), but you cannot use tabs.

- You can dynamically add the hostname or domain name of the device by including the variables **$(hostname)** or **$(domain)**.

- Although there is no absolute length restriction on banners, Telnet or SSH sessions will close if there is not enough system memory available to process the banner messages.

- From a security perspective, it is important that your banner discourage unauthorized access. Do not use the words "welcome" or "please," as they appear to invite intruders in. The following banner sets the correct tone for unauthorized access:

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk criminal charges.
```

Step 4   Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

DNS

The Domain Name System (DNS) servers are used to resolve hostnames to IP addresses. There are two DNS server settings that apply to different types of traffic: data and special management traffic. Data traffic includes any services that use FQDNs for which a DNS lookup is necessary, such as access control rules and remote access VPN. Special management traffic includes traffic originating on the Management interface such as configuration and database updates. This procedure only applies to *data* DNS servers. For *management* DNS settings, see the CLI **configure network dns servers** and **configure network dns searchdomains** commands.

To determine the correct interface for DNS server communications, the managed device uses a routing lookup, but which routing table is used depends on the interfaces for which you enable DNS. See the interface settings below for more information.

You can optionally configure multiple DNS server groups and use them to resolve different DNS domains. For example, you could have a catch-all default group that uses public DNS servers, for use with connections to the Internet. You could then configure a separate group to use internal DNS servers for internal traffic, for example, any connection to a machine in the example.com domain. Thus, connections to an FQDN using your organization's domain name would be resolved using your internal DNS servers, whereas connections to public servers use external DNS servers. These resolutions are used by any feature that uses data DNS resolution, such as NAT and access control rules.

You can configure trusted DNS services for DNS snooping using the Trusted DNS Servers tab. DNS snooping is used to map the application domains to IPs in order to detect the application on the first packet. Apart from configuring the trusted DNS servers, you can include the already configured servers in DNS group, DHCP pool, DHCP relay and DHCP client as trusted DNS servers.

Note   For an application-based PBR, you must configure trusted DNS servers. You must also ensure that the DNS traffic passes through Firewall Threat Defense in a clear-text format (encrypted DNS is not supported) so that domains can be resolved to detect applications.

Before you begin

- Ensure you have created one or more DNS server groups. For more information, see Creating DNS Server Group Objects.

- Ensure you have created interface objects to connect to the DNS servers.

- Ensure that the managed device has appropriate static or dynamic routes to access the DNS servers.

Procedure

Step 1   Choose **Devices** > **Platform Settings** and create or edit a Threat Defense policy.

Step 2   Click **DNS**.

Step 3   Click the **DNS Settings** tab.

Step 4   Check **Enable DNS name resolution by device**.

Step 5   Configure the DNS server groups.

a) Do any of the following in the DNS server group list:

- To add a group to the list, click **Add**. You cannot add another group once there are 30 filter domains configured within the existing list of server groups.

- To edit the settings for a group, click **Edit** (✏) next to the group.

- To remove a group, click **Delete** (🗑) next to the group. Removing a group does not delete the DNS server group object, it simply removes it from this list.

b) When adding or editing a group, configure the following settings, then click **OK**:

- **Select DNS Group**—Select an existing DNS server group object, or click + to create a new one.

- **Make as default**—Select this option to make this group the default group. Any DNS resolution request that does not match the filters for other groups will be resolved using the servers in this group.

- **Filter Domains**—For non-default groups only, a comma-separated list of domain names, such as example.com,example2.com. Do not include spaces.

  The group will be used for DNS resolutions for these domains only. You can enter a maximum of 30 separate domains across all groups added to this DNS platform settings policy. Each name can be a maximum of 127 characters.

  Note that these filter domains are not related to the default domain name for the group. The filter list can be different from the default domain.

Step 6 (Optional) Enter the **Expiry Entry Timer** and **Poll Timer** values in minutes.

These options apply to FQDNs that are specified in network objects only. These do not apply to FQDNs used in other features.

- **Expire Entry Timer** specifies the minimum time-to-live (TTL) for the DNS entry, in minutes. If the expiration timer is longer than the entry's TTL, the TTL is increased to the expire entry time value. If the TTL is longer than the expiration timer, the expire entry time value is ignored: no additional time is added to the TTL in this case. Upon expiration, the entry is removed from the DNS lookup table. Removing an entry requires that the table be recompiled, so frequent removals can increase the processing load on the device. Because some DNS entries can have very short TTL (as short as three seconds), you can use this setting to virtually extend the TTL. The default is 1 minute (that is, the minimum TTL for all resolutions is 1 minute). The range is 1 to 65535 minutes.

  Note that for systems running 7.0 or earlier, the expiration time is actually added to the TTL: it does not specify a minimum value.

- **Poll Timer** specifies the time limit after which the device queries the DNS server to resolve the FQDN that was defined in a network object. An FQDN is resolved periodically either when the poll timer has expired, or when the TTL of the resolved IP entry has expired, whichever occurs first.

Step 7 Enable DNS lookups on all interfaces or on specific interfaces. These choices also affect which routing tables are used.

Note that enabling DNS lookups on an interface is not the same as specifying the source interface for lookups. The Firewall Threat Defense always uses a route lookup to determine the source interface. Management-only interfaces other than the dedicated Management interface cannot be used.

- No interfaces selected—Enables DNS lookups on all interfaces. The Firewall Threat Defense checks the data routing table only.

- Specific interfaces selected but not the **Enable DNS Lookup via diagnostic/management interface also** option—Enables DNS lookups on the specified interfaces. The Firewall Threat Defense checks the data routing table only.

- Specific interfaces selected plus the **Enable DNS Lookup via diagnostic/management interface also** option—Enables DNS lookups on the specified interfaces and the Management interface. The Firewall Threat Defense checks the data routing table, and if no route is found, falls back to the management-only routing table.

- Only the **Enable DNS Lookup via diagnostic/management interface also** option—Enables DNS lookups on Management. The Firewall Threat Defense checks only the management-only routing table.

Step 8   To configure the trusted DNS servers, click the **Trusted DNS Servers** tab.

Step 9   By default, the existing DNS servers that are configured in DHCP pool, DHCP relay, DHCP client, or DNS server group are included as trusted DNS servers. If you want to exclude any of them, uncheck the appropriate check boxes.

Step 10   To add trusted DNS servers, under **Specify DNS Servers**, click **Edit**.

Step 11   In the **Select DNS Servers** dialog box, either choose a host object as the trusted DNS server or directly specify the IP address of the trusted DNS server:

    a) To choose existing host objects, under **Available Host Objects**, select the required host object and click **Add** to include it to **Selected DNS Servers**. For information on adding the host objects, see Creating Network Objects.

    b) To directly provide the IP address(IPv4 or IPv6) of the trusted DNS server, enter the address in the given text field, and click **Add** to include it to **Selected DNS Servers**.

    c) Click **Save**. The added DNS servers are displayed in the **Trusted DNS Servers** page.

Note
You can configure a maximum of 12 DNS servers per policy.

Step 12   (Optional) To search for a DNS server that was added, using either the host name or the IP address, use the search field under **Specify DNS Servers**.

Step 13   Click **Save**.

What to do next

To use FQDN objects for access control rules, create an FQDN network object which can then be assigned to an access control rule. For instructions see, Creating Network Objects.

External Authentication

Note   You must have administrator privileges to perform this task.

When you enable external authentication for management users, the Firewall Threat Defense verifies the user credentials with an LDAP or RADIUS server as specified in an external authentication object.

Sharing External Authentication Objects

External authentication objects can be used by the Firewall Management Center and Firewall Threat Defense devices. You can share the same object between the Firewall Management Center and devices, or create separate objects. Note that the Firewall Threat Defense supports defining users on the RADIUS server, while the Firewall Management Center requires you to predefine the user list in the external authentication object. You can choose to use the predefined list method for the Firewall Threat Defense, but if you want to define users on the RADIUS server, you must create separate objects for the Firewall Threat Defense and the Firewall Management Center.

Note   The timeout range is different for the Firewall Threat Defense and the Firewall Management Center, so if you share an object, be sure not to exceed the Firewall Threat Defense's smaller timeout range (1-30 seconds for LDAP, and 1-300 seconds for RADIUS). If you set the timeout to a higher value, the Firewall Threat Defense external authentication configuration will not work.

Assigning External Authentication Objects to Devices

For the Firewall Management Center, enable the external authentication objects directly on **System** (⚙) > **Users** > **External Authentication**; this setting only affects Firewall Management Center usage, and it does not need to be enabled for managed device usage. For Firewall Threat Defense devices, you must enable the external authentication object in the platform settings that you deploy to the devices, and you can only activate one external authentication object per policy. An LDAP object with CAC authentication enabled cannot also be used for CLI access. Be sure that both the Firewall Threat Defense and the Firewall Management Center can reach the LDAP server, even if you are not sharing the object. The Firewall Management Center is essential to retrieving the user list and downloading it to the device.

Firewall Threat Defense Supported Fields

Only a subset of fields in the external authentication object are used for Firewall Threat Defense SSH access. If you fill in additional fields, they are ignored. If you also use this object for the Firewall Management Center, those fields will be used. This procedure only covers the supported fields for the Firewall Threat Defense. For other fields, see *Configure External Authentication for the Firewall Management Center* in the Cisco Secure Firewall Management Center Administration Guide.

Usernames

Usernames must be Linux-valid usernames and be lower-case only, using alphanumeric characters plus period (.) or hyphen (-). Other special characters such as at sign (@) and slash (/) are not supported. You cannot add the **admin** user for external authentication. You can only add external users (as part of the External Authentication object) in the Firewall Management Center; you cannot add them at the CLI. Note that internal users can only be added at the CLI, not in the Firewall Management Center.

If you previously configured the same username for an internal user using the **configure user add** command, the Firewall Threat Defense first checks the password against the internal user, and if that fails, it checks the AAA server. Note that you cannot later add an internal user with the same name as an external user; only pre-existing internal users are supported. For users defined on the RADIUS server, be sure to set the privilege level to be the same as any internal users; otherwise you cannot log in using the external user password.

Privilege Level

LDAP users always have Config privileges. RADIUS users can be defined as either Config or Basic users.

Before you begin

- SSH access is enabled by default on the management interface. To enable SSH access on data interfaces, see SSH Access, on page 19.

- Inform RADIUS users of the following behavior to set their expectations appropriately:

  - The first time an external user logs in, Firewall Threat Defense creates the required structures but cannot simultaneously create the user session. The user simply needs to authenticate again to start the session. The user will see a message similar to the following: "New external username identified. Please log in again to start a session."

- If the user's Service-Type attribute is not defined or incorrectly configured in the RADIUS server, and when using the RADIUS-defined users for authentication, the user will see a message similar to the following: "Your username is not defined with a service type that is valid for this system. You are not authorized to access the system?.

  In some cases, the SSH clients close the CLI window on an unsuccessful SSH connection, even before displaying the failure message. Hence, ensure that the user's Service-Type attribute is correctly defined in the RADIUS server.

- Similarly, if the user's Service-Type authorization was changed since the last login, the user will need to re-authenticate. The user will see a message similar to the following: "Your authorization privilege has changed. Please log in again to start a session."

Procedure

Step 1   Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2   Click **External Authentication**.

Step 3   Click the **Manage External Authentication Server** link.

You can also open the External Authentication screen by clicking **System** > **Users** > **External Authentication**.

Step 4   Configure an LDAP Authentication Object.

a) Click **Add External Authentication Object**.

b) Set the **Authentication Method** to **LDAP**

c) Enter a **Name** and optional **Description**.

d) Choose a **Server Type** from the drop-down list.

e) For the **Primary Server**, enter a **Host Name/IP Address**.

Note
If you are using a certificate to connect via TLS or SSL, the host name in the certificate must match the host name used in this field. In addition, IPv6 addresses are not supported for encrypted connections.

f) (Optional) Change the **Port** from the default.

g) (Optional) Enter the **Backup Sever** parameters.

h) Enter **LDAP-Specific Parameters**.

- **Base DN**—Enter the base distinguished name for the LDAP directory you want to access. For example, to authenticate names in the Security organization at the Example company, enter `ou=security,dc=example,dc=com`. Alternatively click **Fetch DNs**, and choose the appropriate base distinguished name from the drop-down list.

- (Optional) **Base Filter**—For example, if the user objects in a directory tree have a `physicalDeliveryOfficeName` attribute and users in the New York office have an attribute value of `NewYork` for that attribute, to retrieve only users in the New York office, enter `(physicalDeliveryOfficeName=NewYork)`.

- **User Name**—Enter a distinguished name for a user who has sufficient credentials to browse the LDAP server. For example, if you are connecting to an OpenLDAP server where user objects have a `uid` attribute, and the object for the administrator in the Security division at our example company

has a `uid` value of `NetworkAdmin`, you might enter
`uid=NetworkAdmin,ou=security,dc=example,dc=com`.

- **Password** and **Confirm Password**—Enter and confirm the password for the user.

- (Optional) **Show Advanced Options**—Configure the following advanced options.

  - **Encryption**—Click **None**, **TLS**, or **SSL**.

    Note
    If you change the encryption method after specifying a port, you reset the port to the default
    value for that method. For **None** or **TLS**, the port resets to the default value of 389. If you choose
    SSL encryption, the port resets to 636.

  - **SSL Certificate Upload Path**—For SSL or TLS encryption, you must choose a certificate by
    clicking **Choose File**.

  - (Not Used) **User Name Template**—Not used by the Firewall Threat Defense.

  - **Timeout**—Enter the number of seconds before rolling over to the backup connection between
    1 and 30. The default is 30.

    Note
    The timeout range is different for the Firewall Threat Defense and the Firewall Management
    Center, so if you share an object, be sure not to exceed the Firewall Threat Defense's smaller
    timeout range (1-30 seconds). If you set the timeout to a higher value, the Firewall Threat
    Defense external authentication configuration will not work.

i) (Optional) Set the **CLI Access Attribute** if you want to use a shell access attribute other than the user
distinguished type. For example, on a Microsoft Active Directory Server, use the `sAMAccountName` shell
access attribute to retrieve shell access users by typing `sAMAccountName` in the **CLI Access Attribute**
field.

j) Set the **CLI Access Filter**.

Choose one of the following methods:

- To use the same filter you specified when configuring authentication settings, choose **Same as Base
  Filter**.

- To retrieve administrative user entries based on attribute value, enter the attribute name, a comparison
  operator, and the attribute value you want to use as a filter, enclosed in parentheses. For example, if
  all network administrators have a `manager` attribute which has an attribute value of `shell`, you can
  set a base filter of `(manager=shell)`.

The names on the LDAP server must be Linux-valid usernames:

- Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)

- All lowercase

- Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash
  (/)

k) Click **Save**.

Step 5 For LDAP, if you later add or delete users on the LDAP server, you must refresh the user list and redeploy the Platform Settings.

a) Choose **System** (⚙) > **Users** > **External Authentication**.

b) Click **Refresh** (↻) next to the LDAP server.

If the user list changed, you will see a message advising you to deploy configuration changes for your device. The Firepower Theat Defense Platform Settings will also show that it is "Out-of-Date on x targeted devices."

c) Deploy configuration changes; see Deploy Configuration Changes.

Step 6 Configure a RADIUS Authentication Object.

a) Define users on the RADIUS server using the Service-Type attribute.

The following are supported values for the Service-Type attribute:

- Administrator (6)—Provides Config access authorization to the CLI. These users can use all commands in the CLI.

- NAS Prompt (7) or any level other than 6—Provides Basic access authorization to the CLI. These users can use read-only commands, such as **show** commands, for monitoring and troubleshooting purposes.

The names must be Linux-valid usernames:

- Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)

- All lowercase

- Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)

Alternatively, you can predefine users in the external authentication object (see Step 6.j, on page 13). To use the same RADIUS server for the Firewall Threat Defense and Firewall Management Center while using the Service-Type attribute method for the Firewall Threat Defense, create two external authentication objects that identify the same RADIUS server: one object includes the predefined **CLI Access Filter** users (for use with the Firewall Management Center), and the other object leaves the **CLI Access Filter** empty (for use with Firewall Threat Defenses).

b) In Firewall Management Center, click **Add External Authentication Object**.

c) Set the **Authentication Method** to **RADIUS**.

d) Enter a **Name** and optional **Description**.

e) For the **Primary Server**, enter a **Host Name/IP Address**.

Note

If you are using a certificate to connect via TLS or SSL, the host name in the certificate must match the host name used in this field. In addition, IPv6 addresses are not supported for encrypted connections.

f) (Optional) Change the **Port** from the default.

g) Enter a **RADIUS Secret Key**.

h) (Optional) Enter the **Backup Sever** parameters.

i) Enter **RADIUS-Specific Parameters**.

- **Timeout (Seconds)**—Enter the number of seconds before rolling over to the backup connection. The default is 30.

> - **Retries**—Enter the number of times the primary server connection should be tried before rolling over to the backup connection. The default is 3.

> j) (Optional) Instead of using RADIUS-defined users, under **CLI Access Filter**, enter a comma-separated list of usernames in the **Administrator CLI Access User List** field. For example, enter **jchrichton, aerynsun, rygel**.
>
> You may want to use the **CLI Access Filter** method for Firewall Threat Defense so you can use the same external authentication object with Firewall Threat Defense and other platform types. Note that if you want to use RADIUS-defined users, you must leave the **CLI Access Filter** empty.
>
> Make sure that these usernames match usernames on the RADIUS server. The names must be Linux-valid usernames:
>
> > - Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)
> >
> > - All lowercase
> >
> > - Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)
>
> > **Note**
> > If you want to only define users on the RADIUS server, you must leave this section empty.

> k) Click **Save**.

Step 7 Return to **System** (⚙) > **Users** > **External Authentication**.

Step 8 Click **Refresh** (↻) to view any newly-added objects.

For LDAP when you specify SSL or TLS encryption, you must upload a certificate for the connection; otherwise, the server will not be listed on this window.

Step 9 Click **Slider enabled** (⬤) next to the External Authentication object you want to use. You can only enable one object.

Step 10 Click **Save**.

Step 11 Deploy configuration changes; see Deploy Configuration Changes.

Fragment Settings

By default, the Firewall Threat Defense device allows up to 24 fragments per IP packet, and up to 200 fragments awaiting reassembly. You might need to let fragments on your network if you have an application that routinely fragments packets, such as NFS over UDP. However, if you do not have an application that fragments traffic, we recommend that you do not allow fragments by setting **Chain** to 1. Fragmented packets are often used as Denial of Service (DoS) attacks.

Note These settings establish the defaults for devices assigned this policy. You can override these settings for specific interfaces on a device by selecting **Override Default Fragment Setting** in the interface configuration. When you edit an interface, you can find the option on **Advanced** > **Security Configuration**. Select **Devices** > **Device Management**, edit a Firewall Threat Defense device, and select **Interfaces** to edit interface properties..

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Fragment Settings**.

Step 3 Configure the following options. Click **Reset to Defaults** if you want to use the default settings.

- **Size (Block)**—The maximum number of packet fragments from all connections collectively that can be waiting for reassembly. The default is 200 fragments.
- **Chain (Fragment)**—The maximum number of packets into which a full IP packet can be fragmented. The default is 24 packets. Set this option to 1 to disallow fragments.
- **Timeout (Sec)**—The maximum number of seconds to wait for an entire fragmented packet to arrive. The default is 5 seconds. If all fragments are not received within this time, all fragments are discarded.

Step 4 Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

HTTP Access

You can enable the HTTPS server to provide a health check mechanism for a cloud load balancer, for example, for the Firewall Threat Defense Virtual on AWS using an Application Load Balancer.

Other uses for HTTPs on the Firewall Threat Defense are not supported; for example, the Firewall Threat Defense does not have a web interface for configuration in this management mode.

This configuration only applies to data interfaces, including any you have configured as management-only. It does not apply to the dedicated Management interface. The Management interface is separate from the other interfaces on the device. It is used to set up and register the device to the Firewall Management Center. It has a separate IP address and static routing.

To use HTTPS, you do not need an access rule allowing the host IP address. You only need to configure HTTPS access according to this section.

You can only use HTTPS to a reachable interface; if your HTTPS host is located on the outside interface, you can only initiate a management connection directly to the outside interface.

Before you begin

- You cannot configure both HTTPS and AnyConnect VPN module of Cisco Secure Client on the same interface for the same TCP port. For example, if you configure remote access SSL VPN on the outside

interface, you cannot also open the outside interface for HTTPS connections on port 443. If you must configure both features on the same interface, use different ports. For example, open HTTPS on port 4443.

- You need network objects that define the hosts or networks you will allow to make HTTPS connections to the device. You can add objects as part of the procedure, but if you want to use object groups to identify a group of IP addresses, ensure that the groups needed in the rules already exist. Select **Objects** > **Object Management** to configure objects.

✎

Note   You cannot use the system-provided **any** network object group. Instead, use **any-ipv4** or **any-ipv6**.

Procedure

Step 1   Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2   Select **HTTP Access**.

Step 3   Check the **Enable HTTP Server** check box to enable the HTTP server.

Step 4   (Optional) Change the HTTP port. The default is 443.

Step 5   Identify the interfaces and IP addresses that allow HTTP connections.

Use this table to limit which interfaces will accept HTTP connections, and the IP addresses of the clients who are allowed to make those connections. You can use network addresses rather than individual IP addresses.

a)   Click **Add** to add a new rule, or click **Edit** to edit an existing rule.

b)   Configure the rule properties:

- **IP Address**—The network object or group that identifies the hosts or networks you are allowing to make HTTP connections. Choose an object from the drop-down menu, or click + to add a new network object.

- **Available Zones/Interfaces**—Add the zones that contain the interfaces to which you will allow HTTP connections. For interfaces not in a zone, you can type the interface name into the field below the **Selected Zones/Interfaces** list and click **Add**. These rules will be applied to a device only if the device includes the selected interfaces or zones.

c)   Click **OK**.

Step 6   Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

ICMP Access

By default, you can send ICMP packets to any interface using either IPv4 or IPv6, with these exceptions:

• The Firewall Threat Defense does not respond to ICMP echo requests directed to a broadcast address.

• The Firewall Threat Defense only responds to ICMP traffic sent to the interface that traffic comes in on; you cannot send ICMP traffic through an interface to a far interface.

To protect the device from attacks, you can use ICMP rules to limit ICMP access to interfaces to particular hosts, networks, or ICMP types. ICMP rules function like access rules, where the rules are ordered, and the first rule that matches a packet defines the action.

If you configure any ICMP rule for an interface, an implicit deny ICMP rule is added to the end of the ICMP rule list, changing the default behavior. Thus, if you want to simply deny a few message types, you must include a permit any rule at the end of the ICMP rule list to allow the remaining message types.

We recommend that you always grant permission for the ICMP unreachable message type (type 3). Denying ICMP unreachable messages disables ICMP path MTU discovery, which can halt IPsec and PPTP traffic. Additionally ICMP packets in IPv6 are used in the IPv6 neighbor discovery process.

Before you begin

Ensure that the objects needed in the rules already exist. Select **Objects** > **Object Management** to configure objects. You need network objects or groups that define the desired hosts or networks, and port objects that define the ICMP message types you want to control.

Procedure

Step 1   Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2   Select **ICMP Access**.

Step 3   Configure ICMP rules.

a) Click **Add** to add a new rule, or click **Edit** to edit an existing rule.

b) Configure the rule properties:

• **Action**—Whether to permit (allow) or deny (drop) matching traffic.

• **ICMP Service**—The port object that identifies the ICMP message type.

• **Network**—The network object or group that identifies the hosts or networks whose access you are controlling.

• **Available Zones/Interfaces**—Add the zones that contain the interfaces that you are protecting. For interfaces not in a zone, you can type the interface name into the field below the **Selected Zones/Interfaces** list and click **Add**. These rules will be applied to a device only if the device includes the selected interfaces or zones.

c) Click **OK**.

Step 4   (Optional.) Set rate limits on ICMPv4 Unreachable messages.

• **Rate Limit**—Sets the rate limit of unreachable messages, between 1 and 100 messages per second. The default is 1 message per second.

• **Burst Size**—Sets the burst rate, between 1 and 10. The system sends this number of replies, but subsequent replies are not sent until the rate limit is reached.

Step 5   Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

NetFlow

The NetFlow feature enables you to collect IP network traffic information as it enters or exits an interface. The collected traffic information is sent as collected records to a NetFlow Collector server or NetFlow Analyzer. You can analyze the data from NetFlow and determine information, such as source and destination of traffic, class of service, traffic pattern, bandwidth usage, type of traffic, traffic volume, and the causes of the congestion.

With the native NetFlow configuration support, the traffic information collection that was enabled through syslogs flow exports has to be disabled.

The NetFlow provides the option to configure the flow exporter and collectors along with flow event types that must be monitored.

Procedure

Step 1   Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2   Select **NetFlow**.

Step 3   Enable the **Enable Flow Export** toggle to enable NetFlow data export.

Step 4   Configure the general NetFlow parameters that controls the frequency of events pushed to the collector.

   a) **Active Refresh Interval**—For active connections, specify the time interval (in minutes) between flow-update events.
   b) **Delay Flow Create**—Specify the delay (in seconds) before sending a flow-create event. If you do not enter any value, there is no delay and the flow-create event is exported as soon as the flow is created.
   c) **Template Timeout Rate**—Specify the time interval (in minutes) at which the template records are sent to the collectors.

Step 5   Click **Add Collector** to configure the collector. See Add Collector in NetFlow, on page 18.

Step 6   Click **Add Traffic Class** to configure the traffic class. See Add Traffic Class to NetFlow, on page 18.

Step 7   Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Add Collector in NetFlow

Procedure

Step 1	Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.
Step 2	Choose **NetFlow**.
Step 3	Enable the **Enable Flow Export** toggle to enable NetFlow data export.
Step 4	Click **Add Collector** to configure the collector. You can configure a maximum of five collectors.
Step 5	From the **Host** dropdown list, choose the collector host IP address (IPv4 only) of the NetFlow event collector or server to which the NetFlow packets must be sent. Alternatively, you can click the (➕) icon to create a new network host.
Step 6	In the **Port** field, enter the UDP port on the collector to which the NetFlow packets must be sent.
Step 7	From **Available Interfaces or Interface Groups**, choose the interface or interface group through which the collector must be reached. You can choose multiple interfaces or interface groups. The Interface Group object can contain only one interface for a given device. A collector can be reached only through one interface. The object can include a virtual-router-aware interface. You can click the (➕) icon to create a new interface group.
Step 8	Click **Add** to add the interfaces you chose.
Step 9	You can also enter the interface name and click **Add** to add the interface.
Step 10	Click **OK**.

Add Traffic Class to NetFlow

Procedure

Step 1	Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.
Step 2	Select **NetFlow**.
Step 3	Enable the **Enable Flow Export** toggle to enable NetFlow data export.
Step 4	Click **Add Traffic Class** to configure the traffic class.
Step 5	In the **Name** field, enter the name of the traffic class that must match the NetFlow events.
Step 6	In the **Type** field, choose the traffic class to filter the type of traffic you want to capture: • **Default**—The traffic class that is matched if none of the traffic classes matches the traffic. • **Access List**—The specific traffic class that must match the traffic captured for the NetFlow events.
Step 7	If you chose **Access List** as the **Type**, then you must choose the access list object from the **Access List Object** dropdown list. **Note**

You can also click the (＋) icon to create a new extended access list object. See Configure Extended ACL Objects.

Step 8   In **Event Types**, check the checkboxes for the different NetFlow events that you want to capture and send to the collectors.

Step 9   Click **OK**.

SSH Access

If you enabled Firewall Management Center access on a data interface, such as outside, you should enable SSH on that interface using this procedure. This section describes how to enable SSH connections to one or more *data* interfaces on the Firewall Threat Defense.

The Firewall Threat Defense uses the CiscoSSH stack, which is based on OpenSSH. CiscoSSH supports FIPS compliance and regular updates, including updates from Cisco and the open source community.

Note   SSH is enabled by default on the Management interface; however, this screen does not affect Management SSH access.

The Management interface is separate from the other interfaces on the device. It is used to set up and register the device to the Firewall Management Center. SSH for data interfaces shares the internal and external user list with SSH for the Management interface. Other settings are configured separately: for data interfaces, enable SSH and access lists using this screen; SSH traffic for data interfaces uses the regular routing configuration, and not any static routes configured at setup or at the CLI.

For the Management interface, to configure an SSH access list, see the **configure ssh-access-list** command in the Cisco Secure Firewall Threat Defense Command Reference. To configure a static route, see the **configure network static-routes** command. By default, you configure the default route through the Management interface at initial setup.

To use SSH, you do not also need an access rule allowing the host IP address. You only need to configure SSH access according to this section.

You can SSH only to a reachable interface (including an interface in a user-defined virtual router); if your SSH host is located on the outside interface, you can only initiate a management connection directly to the outside interface. When you enable SSH in a user-defined virtual router, and you want VPN users to access SSH, be sure to terminate the VPN on the same virtual router. If the VPN is terminated on another virtual router, then you must configure route leaks between the virtual routers.

SSH supports the following ciphers and key exchange:

- Encryption—aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
- Integrity—hmac-sha2-256
- Key exchange—dh-group14-sha256

Note After you make three consecutive failed attempts to log into the CLI using SSH, the device terminates the SSH connection.

Before you begin

- You can configure SSH internal users at the CLI using the **configure user add** command; see Add an Internal User at the CLI. By default, there is an **admin** user for which you configured the password during initial setup. You can also configure external users on LDAP or RADIUS by configuring **External Authentication** in platform settings. See External Authentication, on page 8.

- You need network objects that define the hosts or networks you will allow to make SSH connections to the device. You can add objects as part of the procedure, but if you want to use object groups to identify a group of IP addresses, ensure that the groups needed in the rules already exist. Select **Objects** > **Object Management** to configure objects.

Note You cannot use the system-provided **any** network object. Instead, use **any-ipv4** or **any-ipv6**.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **SSH Access**.

Step 3 Identify the interfaces and IP addresses that allow SSH connections.

Use this table to limit which interfaces will accept SSH connections, and the IP addresses of the clients who are allowed to make those connections. You can use network addresses rather than individual IP addresses.

a) Click **Add** to add a new rule, or click **Edit** to edit an existing rule.

b) Configure the rule properties:

- **IP Address**—The network object or group that identifies the hosts or networks you are allowing to make SSH connections. Choose an object from the drop-down menu, or click + to add a new network object.

- **Available Zones/Interfaces**—Add the zones that contain the interfaces to which you will allow SSH connections. For interfaces not in a zone, you can type the interface name into the field below the **Selected Zones/Interfaces** list and click **Add**. You can also add loopback interfaces and virtual-router-aware interfaces. These rules will be applied to a device only if the device includes the selected interfaces or zones.

c) Click **OK**.

Step 4 Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

SMTP Server

You must identity an SMTP server if you configure email alerts in the Syslog settings. The source email address you configure for Syslog must be a valid account on the SMTP servers.

Before you begin

Ensure that the network objects that define the host address of the primary and secondary SMTP servers exist. Select **Objects** > **Object Management** to define the objects. Alternatively, you can create the objects while editing the policy.

Procedure

Step 1   Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2   Click **SMTP Server**.

Step 3   Select the network objects that identify the **Primary Server IP Address** and optionally, the **Secondary Server IP Address**.

Step 4   Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

SNMP

Simple Network Management Protocol (SNMP) defines a standard way for network management stations running on PCs or workstations to monitor the health and status of many types of devices, including switches, routers, and security appliances. You can use the SNMP page to configure a firewall device for monitoring by SNMP management stations.

The Simple Network Management Protocol (SNMP) enables monitoring of network devices from a central location. Cisco security appliances support network monitoring using SNMP versions 1, 2c, and 3, as well as traps and SNMP read access; SNMP write access is not supported.

SNMPv3 supports read-only users and encryption with DES (deprecated), 3DES, AES256, AES192, and AES128.

Note The DES option has been deprecated. If your deployment includes SNMP v3 users using DES encryption that were created using a version previous to 6.5, you can continue to use those users for Firewall Threat Defenses running versions 6.6 and previous. However, you cannot edit those users and retain DES encryption, or create new users with DES encryption. If your Firewall Management Center manages any Firewall Threat Defenses running Versions 7.0+, deploying a platform settings policy that uses DES encryption to those Firewall Threat Defenses will fail.

Note SNMP configuration supports Routed and Diagnostic interface only.

Note To create an alert to an external SNMP server, access **Policies** > **Actions** > **Alerts**

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **SNMP**.

Step 3 Enable SNMP and configure basic options.

- **Enable SNMP Servers**—Whether to provide SNMP information to the configured SNMP hosts. You can deselect this option to disable SNMP monitoring while retaining the configuration information.
- **Read Community String**, **Confirm**—Enter the password used by a SNMP management station when sending requests to the Firewall Threat Defense device. The SNMP community string is a shared secret among the SNMP management stations and the network nodes being managed. The security device uses the password to determine if the incoming SNMP request is valid. The password is a case-sensitive alphanumeric string of up to 32 characters; spaces and special characters are not permitted.
- **System Administrator Name**—Enter the name of the device administrator or other contact person. This string is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
- **Location**—Enter the location of this security device (for example, Building 42,Sector 54). This string is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
- **Port**—Enter the UDP port on which incoming requests will be accepted. The default is 161.

Step 4 (SNMPv3 only.) Add SNMPv3 Users, on page 28.

Step 5 Add SNMP Hosts, on page 31.

Step 6 Configure SNMP Traps, on page 33.

Step 7 Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

About SNMP

SNMP is an application-layer protocol that facilitates the exchange of management information between network devices and is part of the TCP/IP protocol suite. Firewall Threat Defense provides support for network monitoring using SNMP Versions 1, 2c, and 3, and support the use of all three versions simultaneously. The SNMP agent running on the Firewall Threat Defense interface lets you monitor the network devices through network management systems (NMSes), such as HP OpenView. Firewall Threat Defense supports SNMP read-only access through issuance of a GET request. SNMP write access is not allowed, so you cannot make changes with SNMP. In addition, the SNMP SET request is not supported.

You can configure the Firewall Threat Defense to send traps, which are unsolicited messages from the managed device to the management station for certain events (event notifications) to an NMS, or you can use the NMS to browse the Management Information Bases (MIBs) on the security devices. MIBs are a collection of definitions, and the Firewall Threat Defense maintain a database of values for each definition. Browsing a MIB means issuing a series of GET-NEXT or GET-BULK requests of the MIB tree from the NMS to determine values.

An SNMP agent notifies the designated management stations if events occur that are predefined to require a notification, for example, when a link in the network goes up or down. The notification it sends includes an SNMP OID, which identifies itself to the management stations. The agent also replies when a management station asks for information.

SNMP Terminology

The following table lists the terms that are commonly used when working with SNMP.

Table 1: SNMP Terminology

Term	Description
Agent	The SNMP server running on the Secure Firewall Threat Defense. The SNMP agent has the following features: • Responds to requests for information and actions from the network management station. • Controls access to its Management Information Base, the collection of objects that the SNMP manager can view or change. • Does not allow SET operations.
Browsing	Monitoring the health of a device from the network management station by polling required information from the SNMP agent on the device. This activity may include issuing a series of GET-NEXT or GET-BULK requests of the MIB tree from the network management station to determine values.
Management Information Bases (MIBs)	Standardized data structures for collecting information about packets, connections, buffers, failovers, and so on. MIBs are defined by the product, protocols, and hardware standards used by most network devices. SNMP network management stations can browse MIBs and request specific data or events be sent as they occur.
Network management stations (NMSs)	The PCs or workstations set up to monitor SNMP events and manage devices.
Object identifier (OID)	The system that identifies a device to its NMS and indicates to users the source of information monitored and displayed.

Term	Description
Trap	Predefined events that generate a message from the SNMP agent to the NMS. Events include alarm conditions such as linkup, linkdown, coldstart, warmstart, authentication, or syslog messages.
	coldStart—The coldStart trap occurs when the SNMP agent starts after the SNMP configuration. This trap also occurs when the agent starts after a system reboot.
	Note For cluster and HA nodes, post a reload, if the interfaces reboot time exceeds 5 minutes (preset threshold), the trap is dropped. When the cluster and HA nodes have rebooted sucessfully, all other traps are sent as expected.
	The **snmp-server enable traps snmp coldstart** command is used to enable and disable transmission of these traps.

MIBs and Traps

MIBs are either standard or enterprise-specific. Standard MIBs are created by the IETF and documented in various RFCs. A trap reports significant events occurring on a network device, most often errors or failures. SNMP traps are defined in either standard or enterprise-specific MIBs. Standard traps are created by the IETF and documented in various RFCs. SNMP traps are compiled into the ASA software.

If needed, you can also download RFCs, standard MIBs, and standard traps from the following locations:

http://www.ietf.org/

Browse the SNMP Object Navigator to look up Cisco MIBs, traps, and OIDs from the following location:

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

In addition, download Cisco OIDs by FTP from the following location:

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

Supported Tables and Objects in MIBs

The following sections list the supported tables and objects for the specified MIBs.

Remote Access VPN Polling

Table 2: CISCO-REMOTE-ACCESS-MONITOR-MIB

Counter	OID	Description
Active Sessions	crasNumSessions (1.3.6.1.4.1.9.9.392.1.3.1)	The number of currently active sessions.
Users	crasNumUsers (1.3.6.1.4.1.9.9.392.1.3.3)	The number of users who have active sessions.
Peak Sessions	crasNumPeakSessions (1.3.6.1.4.1.9.9.392.1.3.41)	The number of peak RA sessions since system up.

Site-to-Site VPN Tunnel Polling

Table 3: CISCO-REMOTE-ACCESS-MONITOR-MIB

Counter	OID	Description
LAN to LAN Sessions	crasL2LNumSessions (1.3.6.1.4.1.9.9.392.1.3.29)	The number of currently active LAN to LAN sessions.
Peak LAN to LAN Sessions	crasL2LPeakConcurrentSessions (1.3.6.1.4.1.9.9.392.1.3.31)	The number of peak concurrent LAN to LAN sessions since the system is up.

Connection Polling

Table 4: CISCO-FIREWALL-MIB

Counter	OID	Description
Active Connections	cfwConnectionActive (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.6)	The number of connections currently in use by the entire firewall.
Peak Connections	cfwConnectionPeak (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.7)	The highest number of connections in use at any one time since system startup.
Connections Per Second	cfwConnectionPerSecond (1.3.6.1.4.1.9.9.147.1.2.2.3)	The current connections per second rate on the firewall.
Peak Connections Per Second	cfwConnectionPerSecondPeak (1.3.6.1.4.1.9.9.147.1.2.2.4)	The highest number of connections per second on the firewall since system startup.

NAT Translation Polling

Table 5: CISCO-NAT-EXT-MIB

Counter	OID	Description
Active Translations	cneAddrTranslationNumActive (1.3.6.1.4.1.9.9.532.1.1.1.1)	The total number of address translation entries that are currently available in the NAT device. This indicates the aggregate of the translation entries created from both the static and dynamic address translation mechanisms.
Peak Active Translations	cneAddrTranslationNumPeak (1.3.6.1.4.1.9.9.532.1.1.1.2)	The maximum number of address translation entries that are active at any one time since the system startup. This indicates the high watermark of address translation entries that are active at any one time since the system startup. This object includes the translation entries created from both the static and dynamic address translation mechanisms.

Routing Table Entries Polling

Table 6: IP-FORWARD-MIB

Counter	OID	Description
Active Translations	inetCidrRouteNumber (1.3.6.1.2.1.4.24.6)	The total number of current inetCidrRouteTable entries that valid.

Interface Duplex Status Polling

Table 7: CISCO-IF-EXTENSION-MIB

Counter	OID	Description
Duplex Status	cieIfDuplexCfgStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.20)	This object specifies the configured duplex status on the given interface.
Detected Duplex Status	cieIfDuplexDetectStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.21)	This object specifies the detected duplex status on the given interface.

Snort 3 Intrusion Event Rate Polling

Table 8: CISCO-UNIFIED-FIREWALL-MIB

Counter	OID	Description
Snort 3 Intrusion Event Rate	cufwAaicIntrusionEvtRate (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	The rate at which intrusion events were recorded by Snort on this firewall averaged over the last 300 seconds.

BGP Peer-Flap Trap Notification

Table 9: BGP4-MIB

Counter	OID	Description
BGP Peer-flap	bgpBackwardTransition (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	The BGPBackwardTransition Event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.

CPU Utilization Polling

Table 10: CISCO-PROCESS-MIB

Counter	OID	Description
CPU Total Utilization	cpmCPUTotal1minRev (1.3.6.1.4.1.9.9.109.1.1.1.1.7.1)	Total system CPU utilization for the last one minute.

Counter	OID	Description
Individual CPU Core Utilization	Associated parameters and values of cpmCPUTotal1minRev 1.3.6.1.4.1.9.9.109.1.1.1.1.7.2 to 1.3.6.1.4.1.9.9.109.1.1.1.1.7.(n+1)	Individual CPU core utilization values for the last one minute, where 'n' represents the number of cores. Examples: • $3.6.1.4.1.9.9.109.1.1.1.1.7.(n+2)$ - Aggregate system CPU utilization % (This value is same as the system cpu usage from $3.6.1.4.1.9.9.109.1.1.1.1.7.1$ in single context mode). • $3.6.1.4.1.9.9.109.1.1.1.1.7.(n+3)$ - Snort average CPU utilization % (total aggregate value of all snort instances) • $3.6.1.4.1.9.9.109.1.1.1.1.7.(n+4)$ - System process average % (average of "Sysproc" cores)

Note The SNMP OIDs 1.3.6.1.2.1.25.3.3 and 1.3.6.1.2.1.25.3.4 pertaining to CPU monitoring (hrProcessorTable and hrNetworkTable) were removed on ASA FirePOWER. You can view and monitor the CPU health details of the device only through its device manager.

In ENTITY-MIB, two new vendor OIDs were added for the dual EPM 2X100G and 4X200G cards of Secure Firewall 4200 for slot 2 and slot 3—cevFPRNM4X200Gng and cevFPRNM2X100Gng.

Add SNMPv3 Users

Note You create users for SNMPv3 only. These steps are not applicable for SNMPv1 or SNMPv2c.

Note that SNMPv3 only supports read-only users.

SNMP users have a specified username, an authentication password, an encryption password, and authentication and encryption algorithms to use.

✎

Note   When using SNMPv3 with clustering or High Availability, if you add a new cluster unit after the initial cluster formation or you replace a High Availability unit, then SNMPv3 users are not replicated to the new unit. You must remove the users, re-add them, and then redeploy your configuration to force the users to replicate to the new unit.

Authentication algorithm options

For a successful SNMPv3 user authentication, the authentication key size should be equal to or larger than the encryption key size. For example, a user authentication using SHA-1 with AES256 fails, whereas authentication using SHA256 with AES256 succeeds.

The authentication algorithm options are MD5 (deprecated, pre-6.5 only), SHA, SHA224, SHA256, and SHA384.

✎

Note   The MD5 option has been deprecated. If your deployment includes SNMP v3 users using the MD5 authentication algorithm that were created using a version previous to 6.5, you can continue to use those users for FTDs running versions 6.7 and previous. However, you cannot edit those users and retain the MD5 authentication algorithm, or create new users with the MD5 authentication algorithm. If your management center manages any threat defenses running Versions 7.0+, deploying a platform settings policy that uses the MD5 authentication algorithm to those threat defenses will fail.

The encryption algorithm options are DES (deprecated, pre-6.5 only), 3DES, AES256, AES192, and AES128.

✎

Note   The DES option has been deprecated. If your deployment includes SNMP v3 users using DES encryption that were created using a version previous to 6.5, you can continue to use those users for threat defenses running versions 6.7 and previous. However, you cannot edit those users and retain DES encryption, or create new users with DES encryption. If your management center manages any threat defenses running Versions 7.0+, deploying a platform settings policy that uses DES encryption to those threat defenses will fail.

Procedure

Step 1   Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2   Click **SNMP** > **Users**.

Step 3   Click **Add**.

Step 4   Select the security level for the user from the **Security Level** drop-down list.

- **Auth**—Authentication but No Privacy, which means that messages are authenticated.

- **No Auth**—No Authentication and No Privacy, which means that no security is applied to messages.

- **Priv**—Authentication and Privacy, which means that messages are authenticated and encrypted.

Step 5   Enter the name of the SNMP user in the **Username** field. Usernames must be 32 characters or less.

Step 6   Select the type of password, you want to use in the **Encryption Password Type** drop-down list.

- **Clear text**—The Firewall Threat Defense device will still encrypt the password when deploying to the device.
- **Encrypted**—The Firewall Threat Defense device will directly deploy the encrypted password.

Step 7   In the **Auth Algorithm Type** drop-down list, select the type of authentication you want to use: SHA, SHA224, SHA256, or SHA384.

Note
The MD5 option has been deprecated. If your deployment includes SNMP v3 users using the MD5 authentication algorithm that were created using a version previous to 6.5, you can continue to use those users for FTDs running versions 6.7 and previous. However, you cannot edit those users and retain the MD5 authentication algorithm, or create new users with the MD5 authentication algorithm. If your Firewall Management Center manages any Firewall Threat Defenses running Versions 7.0+, deploying a platform settings policy that uses the MD5 authentication algorithm to those Firewall Threat Defenses will fail.

Step 8   In the **Authentication Password** field, enter the password to use for authentication. If you selected Encrypted as the Encrypt Password Type, the password must be formatted as xx:xx:xx..., where xx are hexadecimal values.

Note
The length of the password will depend on the authentication algorithm selected. For all passwords, the length must be 256 characters or less.

If you selected Clear Text as the Encrypt Password Type, repeat the password in the **Confirm** field.

Step 9   In the **Encryption Type** drop-down list, select the type of encryption you want to use: AES128, AES192, AES256, 3DES.

Note
To use AES or 3DES encryption, you must have the appropriate license installed on the device.

Note
The DES option has been deprecated. If your deployment includes SNMP v3 users using DES encryption that were created using a version previous to 6.5, you can continue to use those users for Firewall Threat Defenses running versions 6.7 and previous. However, you cannot edit those users and retain DES encryption, or create new users with DES encryption. If your Firewall Management Center manages any Firewall Threat Defenses running Versions 7.0+, deploying a platform settings policy that uses DES encryption to those Firewall Threat Defenses will fail.

Step 10   Enter the password to use for encryption in the **Encryption Password** field. If you selected Encrypted as the Encrypt Password Type, the password must be formatted as xx:xx:xx..., where xx are hexadecimal values. For encrypted passwords, the length of the password depends on the encryption type selected. The password sizes are as follows (where each xx is one octal):

- AES 128 requires 16 octals
- AES 192 requires 24 octals
- AES 256 requires 32 octals
- 3DES requires 32 octals
- DES can be any size

Note

For all passwords, the length must be 256 characters or less.

If you selected Clear Text as the Encrypt Password Type, repeat the password in the **Confirm** field.

Step 11   Click **OK**.

Step 12   Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Add SNMP Hosts

Use Host to add or edit entries in the SNMP Hosts table on the SNMP page. These entries represent SNMP management stations allowed to access the Firewall Threat Defense device.

You can add up to 8192 hosts. However, only 128 of this number can be for traps.

Note   In 7.4 and later, the Management and Diagnostic interfaces are merged. If Platform Settings for syslog servers or SNMP hosts specify the Diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices (7.3 and earlier, and some upgraded 7.4 FTDs).

Before you begin

Ensure that the network objects that define the SNMP management stations exist. Select **Device** > **Object Management** to configure network objects.

Note   The supported network objects include IPv6 hosts, IPv4 hosts, IPv4 range and IPv4 subnet addresses.

Procedure

Step 1   Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2   Click **SNMP** > **Hosts**.

Step 3   Click **Add**.

Step 4   In the **IP Address** field, either enter a valid IPv6 or IPv4 host or select the network object that defines the SNMP management station's host address.

The IP address can be an IPv6 host, IPv4 host, IPv4 range or IPv4 subnet.

Step 5   Select the appropriate SNMP version from the **SNMP version** drop-down list.

Step 6   (SNMPv3 only.) Select the username of the SNMP user that you configured from the **User Name** drop-down list.

Note
You can associate up to 23 SNMP users per SNMP host.

Step 7 (SNMPv1, 2c only.) In the **Read Community String** field, enter the community string that you have already configured, for read access to the device. Re-enter the string to confirm it.

> **Note**
> This string is required, only if the string used with this SNMP station is different from the one already defined in the **Enable SNMP Server** section.

Step 8 Select the type of communication between the device and the SNMP management station. You can select both types.

- **Poll**—The management station periodically requests information from the device.
- **Trap**—The device sends trap events to the management station as they occur.

> **Note**
> When the SNMP host IP address is either an IPv4 range or an IPv4 subnet, you can configure either **Poll** or **Trap**, not both.

Step 9 In the **Port** field, enter a UDP port number for the SNMP host. The default value is 162. The valid range is 1 to 65535.

Step 10 Select the interface type for communication between the device and the SNMP management station under the **Reachable By** options. You can select either the device's Management interface or an available security zone/named interface.

- **Device Management Interface**—Communication between the device and the SNMP management station occurs over the Management interface.

  - When you choose this interface for SNMPv3 polling, all configured SNMPv3 users are allowed to poll and are not restricted to the user chosen in Step 6, on page 31. Here, SNMPv1 and SNMPv2c are not allowed from an SNMPv3 host.

  - When you choose this interface for SNMPv1 and SNMPv2c polling, the polling is not restricted at all to the version selected in Step 5, on page 31.

- **Security Zones or Named Interface**—Communication between the device and the SNMP management station occurs over a security zone or interface.

  - Search for zones in the **Available Zones** field.

  - Add the zones that contain the interfaces through which the device communicates with the management station to the **Selected Zone/Interface** field. For interfaces not in a zone, you can type the interface name into the field below the **Selected Zone/Interface** list and click **Add**. You can also choose a loopback interface and virtual-router-aware interfaces. The host will be configured on a device only if the device includes the selected interfaces or zones.

Step 11 Click **OK**.

Step 12 Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure SNMP Traps

Use SNMP Traps to configure SNMP traps (event notifications) for the Firewall Threat Defense device. Traps are different from browsing; they are unsolicited "comments" from the Firewall Threat Defense device to the management station for certain events, such as linkup, linkdown, and syslog event generated. An SNMP object ID (OID) for the device appears in SNMP event traps sent from the device.

Some traps are not applicable to certain hardware models. These traps will be ignored if you apply the policy to one of these models. For example, not all models have field-replaceable units, so the **Field Replaceable Unit Insert/Delete** trap will not be configured on those models.

SNMP traps are defined in either standard or enterprise-specific MIBs. Standard traps are created by the IETF and documented in various RFCs. SNMP traps are compiled into the Firewall Threat Defense software.

If needed, you can download RFCs, standard MIBs, and standard traps from the following location:

http://www.ietf.org/

Browse the complete list of Cisco MIBs, traps, and OIDs from the following location:

SNMP Object Navigator

In addition, download Cisco OIDs by FTP from the following location:

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Click **SNMP** > **SNMP Traps** to configure SNMP traps (event notifications) for the Firewall Threat Defense device.

Step 3 Select the appropriate Enable Traps options. You can select either or both options.

   a) Check **Enable All SNMP Traps** to quickly select all traps in the subsequent four sections.

   b) Check **Enable All Syslog Traps** to enable transmission of trap-related syslog messages.

   Note

   SNMP traps are of higher priority than other notification messages from the Firewall Threat Defense as they are expected to be near real-time. When you enable all SNMP or syslog traps, it is possible for the SNMP process to consume excess resources in the agent and in the network, causing the system to hang. If you notice system delays, unfinished requests, or timeouts, you can selectively enable SNMP and syslog traps. You can also limit the rate at which syslog messages are generated by severity level or message ID. For example, all syslog message IDs that begin with the digits 212 are associated with the SNMP class; see Limit the Rate of Syslog Message Generation, on page 51.

Step 4 The event-notification traps in the **Standard** section are enabled by default for an existing policy:

   • **Authentication** – Unauthorized SNMP access. This authentication failure occurs for packets with an incorrect community string.

   • **Link Up** – One of the device's communication links has become available (it has "come up"), as indicated in the notification.

   • **Link Down** – One of the device's communication links has failed, as indicated in the notification.

- **Cold Start** – The device is reinitializing itself such that its configuration or the protocol entity implementation may be altered.

- **Warm Start** – The device is reinitializing itself such that its configuration and the protocol entity implementation is unaltered.

Step 5   Select the desired event-notification traps in the **Entity MIB** section:

- **Field Replaceable Unit Insert** – A Field Replaceable Unit (FRU) has been inserted, as indicated. (FRUs include assemblies such as power supplies, fans, processor modules, interface modules, etc.)

- **Field Replaceable Unit Delete** – A Field Replaceable Unit (FRU) has been removed, as indicated in the notification

- **Configuration Change** – There has been a hardware change, as indicated in the notification

Step 6   Select the desired event-notification traps in the **Resource** section:

- **Connection Limit Reached** – This trap indicates that a connection attempt was rejected because the configured connections limit has been reached.

Step 7   Select the desired event-notification traps in the **Other** section:

- **NAT Packet Discard** – This notification is generated when IP packets are discarded by the NAT function. Available Network Address Translation addresses or ports have fallen below configured threshold.

- **CPU Rising Threshold** – This notification is generated when rising CPU utilization exceeds a predefined threshold for a configured period of time. Check this option to enable CPU rising threshold notifications:

  - **Percentage** – The default value is 70 percent for the high threshold notification; the range is between 10 and 94 percent. The critical threshold is hardcoded at 95 percent.

  - **Period** – The default monitoring period is 1 minute; the range is between 1 and 60 minutes.

- **Memory Rising Threshold** – This notification is generated when rising memory utilization exceeds a predefined threshold, thus reducing available memory. Check this option to enable memory rising threshold notifications:

  - **Percentage** – The default value is 70 percent for the high threshold notification; the range is between 50 and 95 percent.

- **Failover** – This notification is generated when there is a change in the failover state as reported by the CISCO-UNIFIED-FIREWALL-MIB.

- **Cluster** – This notification is generated when there is a change in the cluster health as reported by the CISCO-UNIFIED-FIREWALL-MIB.

- **Peer Flap** – This notification is generated when there is BGP route flapping, a situation in which BGP systems send an excessive number of update messages to advertise network reachability information.

Step 8   Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

SSL

✎

Note   You must have administrator privileges and be in a leaf domain to perform this task.

You must make sure that you are running a fully licensed version of the Secure Firewall Management Center. The SSL Settings will be disabled if you are running Secure Firewall Management Center in evaluation mode. Additionally, the SSL Settings will be disabled when the licensed Secure Firewall Management Center version does not meet the export-compliance criteria. If you are using Remote Access VPN with SSL, your Smart Account must have the strong-crypto features enabled. For more information, see *License Types and Restrictions* in the Cisco Secure Firewall Management Center Administration Guide.

Procedure

Step 1   Select **Devices** > **Platform Settings** and create or edit a Firewall Threat Defense policy.

Step 2   Select **SSL**.

Step 3   Add entries to the **Add SSL Configuration** table.

a) Click **Add** to create a new entry, or click **Edit** if the entry already exists.

b) Select the required security configurations from the drop-down list .

- **Protocol Version**—Specifies the TLS protocols to be used while establishing remote access VPN sessions.
- **Security Level**—Indicates the kind of security positioning you would like to set up for the SSL.

Step 4   Select the **Available Algorithms** based on the protocol version that you select and click **Add** to include them for the selected protocol. For more information, see About SSL Settings, on page 35.

The algorithms are listed based on the protocol version that you select. Each security protocol identifies unique algorithm for setting up the security level.

Step 5   Click **OK** to save the changes.

What to do next

Select **Deploy** > **Deployment** and click **Deploy** to deploy the policy to the assigned devices.

About SSL Settings

The Firewall Threat Defense device uses the Secure Sockets Layer (SSL) protocol and Transport Layer Security (TLS) to support secure message transmission for Remote Access VPN connection from remote clients. The SSL Settings window lets you configure SSL versions and encryption algorithms that will be negotiated and used for message transmission during remote VPN access over SSL.

Note Though you configure Firewall Management Center and Firewall Threat Defense to operate in a security certifications (UCAPL, CC, or FIPS) compliance mode, the Firewall Management Center allows configuration of unsupported ciphers. For example, in a FIPS enabled mode, management center allows configuring DH Group 5 which is not FIPS-compliant. However, VPN tunnel does not negotiate due to the non-compliant cipher usage.

Configure the SSL Settings at the following location:

Devices > **Platform Settings**, and then click **SSL**.

Fields

Minimum SSL Version as Server—Specify the minimum SSL/TLS protocol version that the Firewall Threat Defense device uses when acting as a server. For example, when it functions as a Remote Access VPN Gateway.

TLS Version—Select one of the following TLS versions from the drop-down list:

TLS V1	Accepts SSLv2 client hellos and negotiates TLSv1 (or greater).
TLSV1.1	Accepts SSLv2 client hellos and negotiates TLSv1.1 (or greater).
TLSV1.2	Accepts SSLv2 client hellos and negotiates TLSv1.2 (or greater).
TLSV1.3	Accepts SSLv2 client hellos and negotiates TLSv1.3 (or greater).

Note TLS 1.3 in remote access VPN requires Cisco Secure Client, Version 5.0 and above.

DTLS Version—Select the DTLS versions from the drop-down list, based on the selected TLS version. By default, DTLSv1 is configured on Firewall Threat Defense devices, you can choose the DTLS version as per your requirement.

Note Ensure that the TLS protocol version is higher than or equal to the DTLS protocol version selected. TLS protocol versions support the following DTLS versions:

TLS V1	DTLSv1
TLSV1.1	DTLSv1
TLSV1.2	DTLSv1, DTLSv1.2
TLSV1.3	DTLSv1, DTLSv1.2

Diffie-Hellman Group—Choose a group from the drop-down list. Available options are Group1 - 768-bit modulus, Group2 - 1024-bit modulus, Group5 - 1536-bit modulus, Group14 - 2048-bit modulus, 224-bit prime order, and Group24 - 2048-bit modulus, 256-bit prime order. The default is Group1.

Elliptical Curve Diffie-Hellman Group—Choose a group from the drop-down list. Available options are Group19 - 256-bit EC, Group20 - 384-bit EC, and Group21 - 521-bit EC. The default value is Group19.

TLSv1.2 adds support for the following ciphers:

- ECDHE-ECDSA-AES256-GCM-SHA384

- ECDHE-RSA-AES256-GCM-SHA384

- DHE-RSA-AES256-GCM-SHA384

- AES256-GCM-SHA384

- ECDHE-ECDSA-AES256-SHA384

- ECDHE-RSA-AES256-SHA384

- ECDHE-ECDSA-AES128-GCM-SHA256

- ECDHE-RSA-AES128-GCM-SHA256

- DHE-RSA-AES128-GCM-SHA256

- RSA-AES128-GCM-SHA256

- ECDHE-ECDSA-AES128-SHA256

- ECDHE-RSA-AES128-SHA256

Note   ECDSA and DHE ciphers are the highest priority.

TLSv1.3 adds support for the following ciphers:

- TLS_AES_128_GCM_SHA256

- TLS_CHACHA20_POLY1305_SHA256

- TLS_AES_256_GCM_SHA384

The SSL configuration table can be used to specify the protocol version, security level, and Cipher algorithms that you want to support on the Secure Firewall Threat Defense devices.

Protocol Version—Lists the protocol version that the Secure Firewall Threat Defense device supports and uses for SSL connections. Available protocol versions are:

- Default

- TLSV1

- TLSV1.1

- TLSV1.2

- TLSV1.3

- DTLSv1

- DTLSv1.2

Security Level—Lists the cipher security levels that Firewall Threat Defense device supports and uses for SSL connections.

If you have Firewall Threat Defense devices with evaluation license, the security level is Low by default. With Firewall Threat Defense smart license, the default security level is High. You can choose one of the following options to configure the required security level:

- **All** includes all ciphers, including NULL-SHA.

- **Low** includes all ciphers, except NULL-SHA.

- **Medium** includes all ciphers, except NULL-SHA, DES-CBC-SHA, RC4-SHA, and RC4-MD5 (this is the default).

- **Fips** includes all FIPS-compliant ciphers, except NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA, and DES-CBC3-SHA, TLS_CHACHA20_POLY1305_SHA256.

- **High** includes only AES-256 with SHA-2 ciphers and applies to TLS version 1.2 and the *default* version.

- **Custom** includes one or more ciphers that you specify in the Cipher algorithms/custom string box. This option provides you with full control of the cipher suite using OpenSSL cipher definition strings.

Cipher Algorithms/Custom String—Lists the cipher algorithms that the Firewall Threat Defense device supports and uses for SSL connections. For more information about ciphers using OpenSSL, see https://www.openssl.org/docs/apps/ciphers.html

Ciphers supported by TLSv1.2 only

ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256

AES128-SHA256

✎

Note   ECDSA and DHE ciphers are the highest priority.

Ciphers not supported by TLSv1.1 or TLSv1.2

RC4-SHA
RC4-MD5
DES-CBC-SHA
NULL-SHA

Syslog

You can enable system logging (syslog) for Firewall Threat Defense devices. Logging information can help you identify and isolate network or device configuration problems. You can also send some security events to a syslog server. The following topics explain logging and how to configure it.

About Syslog

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. Cisco devices can send their log messages to a UNIX-style syslog service. A syslog service accepts messages and stores them in files, or prints them according to a simple configuration file. This form of logging provides protected long-term storage for logs. Logs are useful both in routine troubleshooting and in incident handling.

Table 11: System Logs for Secure Firewall Threat Defense

Logs Related To	Details	Configure In
Device and system health, network configuration	This syslog configuration generates messages for features running on the data plane, that is, features that are defined in the CLI configuration that you can view with the **show running-config** command. This includes features such as routing, VPN, data interfaces, DHCP server, NAT, and so forth. Data plane syslog messages are numbered, and they are the same as those generated by devices running ASA software. However, Secure Firewall Threat Defense does not necessarily generate every message type that is available for ASA Software. For information on these messages, see *Cisco Secure Firewall Threat Defense Syslog Messages* at https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html. This configuration is explained in the following topics.	**Platform Settings**

Logs Related To	Details	Configure In
Security events	This syslog configuration generates alerts for file and malware, connection, Security Intelligence, and intrusion events. For details, see *About Sending Syslog Messages for Security Events* and subtopics in the Cisco Secure Firewall Management Center Administration Guide.	**Platform Settings** and the **Logging** in an access control policy
(All devices) Policies, rules, and events	This syslog configuration generates alerts for access control rules, intrusion rules, and other advanced services as described in *Configurations Supporting Alert Responses* in the Cisco Secure Firewall Management Center Administration Guide. These messages are not numbered. For information on configuring this type of syslog, see *Creating a Syslog Alert Response* in the Cisco Secure Firewall Management Center Administration Guide.	**Alert Responses** and the **Logging** in an access control policy

You can configure more than one syslog server, and control the messages and events sent to each server. You can also configure different destinations, such as console, email, internal buffer, and so forth.

Severity Levels

The following table lists the syslog message severity levels.

Table 12: Syslog Message Severity Levels

Level Number	Severity Level	Description
0	**emergencies**	System is unusable.
1	**alert**	Immediate action is needed.
2	**critical**	Critical conditions.
3	**error**	Error conditions.
4	**warning**	Warning conditions.
5	**notification**	Normal but significant conditions.
6	**informational**	Informational messages only.
7	**debugging**	Debugging messages only. Log at this level only temporarily, when debugging issues. This log level can potentially generate so many messages that system performance can be affected.

Note ASA and Firewall Threat Defense do not generate syslog messages with a severity level of zero (emergencies).

Syslog Message Filtering

You can filter generated syslog messages so that only certain syslog messages are sent to a particular output destination. For example, you could configure the Firewall Threat Defense device to send all syslog messages to one output destination and to send a subset of those syslog messages to a different output destination.

Specifically, you can direct syslog messages to an output destination according to the following criteria:

- Syslog message ID number

  (This does not apply to syslog messages for security events such as connection and intrusion events.)

- Syslog message severity level

- Syslog message class (equivalent to a functional area)

  (This does not apply to syslog messages for security events such as connection and intrusion events.)

You customize these criteria by creating a message list that you can specify when you set the output destination. Alternatively, you can configure the Firewall Threat Defense device to send a particular message class to each type of output destination independently of the message list.

(Message lists do not apply to syslog messages for security events such as connection and intrusion events.)

Syslog Message Classes

Note This topic does not apply to messages for security events (connection, intrusion, etc.)

You can use syslog message classes in two ways:

- Specify an output location for an entire category of syslog messages.

- Create a message list that specifies the message class.

The syslog message class provides a method of categorizing syslog messages by type, equivalent to a feature or function of the device. For example, the rip class denotes RIP routing.

All syslog messages in a particular class share the same initial three digits in their syslog message ID numbers. For example, all syslog message IDs that begin with the digits 611 are associated with the vpnc (VPN client) class. Syslog messages associated with the VPN client feature range from 611101 to 611323.

In addition, most of the ISAKMP syslog messages have a common set of prepended objects to help identify the tunnel. These objects precede the descriptive text of a syslog message when available. If the object is not known at the time that the syslog message is generated, the specific heading = value combination does not appear.

The objects are prefixed as follows:

Group = *groupname*, Username = *user*, IP = *IP_address*

Where the group is the tunnel-group, the username is the username from the local database or AAA server, and the IP address is the public IP address of the remote access client or Layer 2 peer.

The following table lists the message classes and the range of message IDs in each class.

Table 13: Syslog Message Classes and Associated Message ID Numbers

Class	Definition	Syslog Message ID Numbers
access-list*	Access Lists	106
application-firewall*	Application Firewall	415
auth	User Authentication	109, 113
botnet-traffic-filtering*	Botnet Traffic Filtering	338
bridge	Transparent Firewall	110, 220
ca	PKI Certification Authority	717
card-management*	Card Management	323
citrix	Citrix Client	723
clustering*	Clustering	747
config	Command Interface	111, 112, 208, 308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	Dynamic Access Policies	734
eap, eapoudp	EAP or EAPoUDP for Network Admission Control	333, 334
eigrp	EIGRP Routing	336
email	E-mail Proxy	719
environment-monitoring*	Environment Monitoring	735
ha	Failover	101, 102, 103, 104, 105, 210, 311, 709
identity-based-firewall*	Identity-based Firewall	746
ids	Intrusion Detection System	400, 733
ikev2-toolkit*	IKEv2 Toolkit	750, 751, 752
ip	IP Stack	209, 215, 313, 317, 408
ipaa	IP Address Assignment	735
ips	Intrusion Protection System	400, 401, 420
ipv6*	IPv6	325
licensing*	Licensing	444

Class	Definition	Syslog Message ID Numbers
mdm-proxy	MDM Proxy	802
nac	Network Admission Control	731, 732
nacpolicy	NAC Policy	731
nacsettings	NAC Settings to apply NAC Policy	732
nat-and-pat*	NAT and PAT	305
network-access-point*	Network Access Point	713
np	Network Processor	319
np-ssl*	NP SSL	725
ospf	OSPF Routing	318, 409, 503, 613
password-encryption*	Password Encryption	742
phone-proxy*	Phone Proxy	337
rip	RIP Routing	107, 312
rm	Resource Manager	321
scansafe*	ScanSafe	775
session	User Session	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
smart-call-home*	Smart Call Home	120
snmp	SNMP	212
ssl	SSL Stack	725
svc	SSL VPN Client	722
sys	System	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711, 741
tag-switching	Service Tag Switching	779
threat-detection*	Threat Detection	733
transactional-rule-engine-tre*	Transactional Rule Engine	780
uc-ims*	UC-IMS	339
vm	VLAN Mapping	730

Class	Definition	Syslog Message ID Numbers
vpdn	PPTP and L2TP Sessions	213, 403, 603
vpn	IKE and IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	VPN Client	611
vpnfo	VPN Failover	720
vpnlb	VPN Load Balancing	718
vxlan*	VXLAN	778
webfo	WebVPN Failover	721
webvpn	WebVPN and Secure Client	716

*These classes are provisioned in the management center web interface to facilitate creation of event lists. These classes are not displayed on the device console.

Guidelines for Logging

This section includes guidelines and limitations that you should review before configuring logging.

IPv6 Guidelines

- IPv6 is supported. Syslogs can be sent using TCP or UDP.

- Ensure that the interface configured for sending syslogs is enabled, IPv6 capable, and the syslog server is reachable through the designated interface.

- Secure logging over IPv6 is not supported.

Additional Guidelines

- Do not configure Firewall Management Center as a primary syslog server. The Firewall Management Center can log some syslogs. However, it does not have adequate storage provision to accommodate voluminous information from connection events for every sensor, especially when multiple sensors are used and all send syslogs.

- The syslog server must run a server program called syslogd. Windows provides a syslog server as part of its operating system.

- The syslog server operates based on the syslog-ng process of the firewall system. Do not use external configuration files, like the *scwx.conf* file from SecureWorks. Such files are not compatible with the device. Using them will lead to parsing error and eventually the syslog-ng process will fail.

- To view logs generated by the Firewall Threat Defense device, you must specify a logging output destination. If you enable logging without specifying a logging output destination, the Firewall Threat Defense device generates messages but does not save them to a location from which you can view them. You must specify each different logging output destination separately.

- If you use TCP as the transport protocol, the system opens 4 connections to the syslog server to ensure that messages are not lost. If you are using the syslog server to collect messages from a very large number of devices, and the combined connection overhead is too much for the server, use UDP instead.

- It is not possible to have two different lists or classes being assigned to different syslog servers or same locations.

- You can configure up to 16 syslog servers.

- The syslog server should be reachable through the Firewall Threat Defense device. You should configure the device to deny ICMP unreachable messages on the interface through which the syslog server is reachable and to send syslogs to the same server. Make sure that you have enabled logging for all severity levels. To prevent the syslog server from crashing, suppress the generation of syslogs 313001, 313004, and 313005.

- The number of UDP connections for syslog is directly related to the number of CPUs on the hardware platform and the number of syslog servers you configure. At any point in time, there can be as many UDP syslog connections as there are CPUs times the number of configured syslog servers. This is the expected behavior. Note that the global UDP connection idle timeout applies to these sessions, and the default is 2 minutes. You can adjust that setting if you want to close these session more quickly, but the timeout applies to all UDP connections, not just syslog.

- When the Firewall Threat Defense device sends syslogs via TCP, the connection takes about one minute to initiate after the syslogd service restarts.

- When the TCP logging host goes down, it takes approximately 6 minutes to change its connection status from *Connected* to *Not connected*. Logging relies on TCP to detect the channel state; until then, logging sends the logs through the channel. During this time, when you execute the **show log**, the output would display the TCP logging host as connected. Once the TCP channel is closed, the TCP logging host state is updated to *Not connected*.

Configure Syslog Logging for Firewall Threat Defense Devices

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense Platform Settings That Apply to Security Event Syslog Messages, on page 46.

To configure syslog settings, perform the following steps:

Before you begin

See requirements in Guidelines for Logging, on page 44.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Click **Syslog** from the table of contents.

Step 3   Click **Logging Setup** to enable logging, specify FTP Server settings, and specify Flash usage. For more information, see

Step 4   Click **Logging Destinations** to enable logging to specific destinations and to specify filtering on message severity level, event class, or on a custom event list. For more information, see

You must enable a logging destination to see messages at that destination.

Step 5   Click **E-mail Setup** to specify the e-mail address that is used as the source address for syslog messages that are sent as e-mail messages. For more information, see

Step 6   Click **Events List** to define a custom event list that includes an event class, a severity level, and an event ID. For more information, see

Step 7   Click **Rate Limit** to specify the volume of messages being sent to all configured destinations and define the message severity level to which you want to assign rate limits. For more information, see

Step 8   Click **Syslog Settings** to specify the logging facility, enable the inclusion of a time stamp, and enable other settings to set up a server as a syslog destination. For more information, see

Step 9   Click **Syslog Servers** to specify the IP address, protocol used, format, and security zone for the syslog server that is designated as a logging destination. For more information, see .

Firewall Threat Defense Platform Settings That Apply to Security Event Syslog Messages

"Security events" include connection, Security Intelligence, intrusion, and file and malware events.

Some of the syslog settings configured on the **Syslog** page (**Devices** > **Platform Settings**, edit Threat Defense Policy, and then click **Syslog**) and its tabs apply to syslog messages for security events, but most apply only to messages for events related to system health and networking.

The following settings apply to syslog messages for security events:

- **Logging Setup** tab:

  - **Send syslogs in EMBLEM format**

- **Syslog Settings** tab:

  - **Enable Timestamp on Syslog Messages**

  - **Timestamp Format**

  - **Enable Syslog Device ID**

- **Syslog Servers** tab:

  - All options on the **Add Syslog Server** form (and the list of configured servers).

Enable Logging and Configure Basic Settings

Enable logging and configure the basic settings for the system to generate syslog messages for data plane events. You can also set up archiving on flash or an FTP server as a storage location when the local buffer

becomes full. You can manipulate logging data after it is saved. For example, you could specify actions to be executed when certain types of syslog messages are logged, extract data from the log and save the records to another file for reporting, or track statistics using a site-specific script.

The following procedure explains some of the basic syslog settings.

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense Platform Settings That Apply to Security Event Syslog Messages, on page 46.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Logging Setup**.

Step 3 Enable logging and configure basic logging settings.

- **Enable Logging**—Turns on the data plane system logging for the Firewall Threat Defense device.
- **Enable Logging on the Failover Standby Unit**—Turns on logging for the standby for the Firewall Threat Defense device, if available.
- **Send syslogs in EMBLEM format**—Enables EMBLEM format logging for every logging destination. If you enable EMBLEM, you must use the UDP protocol to publish syslog messages; EMBLEM is not compatible with TCP.

  The EMBLEM syslog format is a Cisco-specific convention that is built upon the RFC 3164 and RFC 5424 standards. Hence, when EMBLEM is enabled, the syslog message prints colon (:) after <PRI> field in contrast to the RFC 5424 format.

  Note
  Syslog messages in RFC5424 format, typically displays the priority value (PRI). However, in Firewall Management Center, if you want to display the PRI value in the syslog messages of the managed Firewall Threat Defense device, ensure to enable the EMBLEM format. Also, the device ID does not appear in EMBLEM-formatted syslog messages.

- **Send debug messages as syslogs**—Redirects all the debug trace output to the syslog. The syslog message does not appear in the console if this option is enabled. Therefore, to see debug messages, you must enable logging at the console and configure it as the destination for the debug syslog message number and logging level. The syslog message number used is 711001. The default logging level for this syslog is debug.
- **Memory Size of Internal Buffer**—Specify the size of the internal buffer to which syslog messages are saved if the logging buffer is enabled. When the buffer fills up, it is overwritten. The default is 4096 bytes. The range is 4096 to 52428800.

Step 4 (Optional) Configure the syslog message logging to the Firewall Management Center.

a) Enable VPN logging by checking the **Enable Logging to Secure Firewall Management Center** check box.

b) Choose the syslog severity level for the logging messages from the **Logging Level** drop-down list.

- The logging level for the VPN messages is set to **errors** by default.

VPN troubleshooting syslogs can add excessive load on the Firewall Management Center. Hence, enable this option with caution. Also, when you configure a device with site-to-site or remote access VPN, it automatically enables sending VPN syslogs to the management center by default. We recommend that you limit the logging level to **error** and above to restrict the excessive flow of syslogs to the Firewall Management Center, especially in case of RAVPN, where multiple devices are involved.

For information on the levels, see Severity Levels, on page 40.

Step 5 (Optional) Configure an FTP server if you want to save log buffer contents to the server before the buffer is overwritten. Specify the FTP Server information.

- **FTP Server Buffer Wrap**—To save the buffer contents to the FTP server before it is overwritten, check this box and enter the necessary destination information in the following fields. To remove the FTP configuration, deselect this option.
- **IP Address**—Select the host network object that contains the IP address of the FTP server.
- **User Name**—Enter the username to use when connecting to the FTP server.
- **Path**—Enter the path, relative to the FTP root, where the buffer contents should be saved.
- **Password/ Confirm**—Enter and confirm the password used to authenticate the username to the FTP server.

Step 6 (Optional) Specify Flash size if you want to save log buffer contents to flash before the buffer is overwritten.

- **Flash**—To save the buffer contents to the flash memory before it is overwritten, check this box.
- **Maximum flash to be used by logging (KB)**—Specify the maximum space to be used in the flash memory for logging (in kilobytes). The range is 4-8044176 kilobytes.
- **Minimum free space to be preserved (KB)**—Specifies the minimum free space to be preserved in flash memory (in KB). The range is 0-8044176 kilobytes.

Step 7 Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Enable Logging Destinations

You must enable a logging destination to see messages at that destination. When enabling a destination, you must also specify the message filter for the destination.

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense Platform Settings That Apply to Security Event Syslog Messages, on page 46.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2   Select **Syslog** > **Logging Destinations**.

Step 3   Click **Add** to enable a destination and apply a logging filter, or edit an existing destination.

Step 4   In the **Logging Destinations** dialog box, select a destination and configure the filter to use for a destination:

a) Choose the destination you are enabling in the **Logging Destination** drop-down list. You can create one filter per destination: Console, E-Mail, Internal buffer, SNMP trap, SSH Sessions, and Syslog servers.

Note
Console and SSH session logging works in the diagnostic CLI only. Enter **system support diagnostic-cli**.

b) In **Event Class**, choose the filter that will apply to all classes not listed in the table.

You can configure these filters:

- **Filter on severity** —Select the severity level. Messages at this level or higher are sent to the destination

- **Use Event List** —Select the event list that defines the filter. You create these lists on the **Event Lists** page.

- **Disable Logging** —Prevents messages from being sent to this destination.

c) If you want to create filters per event class, click **Add** to create a new filter, or edit an existing filter, and select the event class and severity level to limit messages in that class. Click **OK** to save the filter.

For an explanation of the event classes, see Syslog Message Classes, on page 41.

d) Click **OK** .

Step 5   Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Send Syslog Messages to an E-mail Address

You can set up a list of recipients for syslog messages to be sent as e-mails.

Tip   If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense Platform Settings That Apply to Security Event Syslog Messages, on page 46.

Before you begin

- Configure an SMTP server on the SMTP Server platform settings page

- Enable Logging and Configure Basic Settings, on page 46

- Setup Email as the Logging Destination

Procedure

Step 1	Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.
Step 2	Select **Syslog** > **Email Setup**.
Step 3	Specify the e-mail address that is used as the source address for syslog messages that are sent as e-mail messages.
Step 4	Click **Add** to enter a new e-mail address recipient of the specified syslog messages.
Step 5	Choose the severity level of the syslog messages that are sent to the recipient from the drop-down list.
	The syslog message severity filter used for the destination e-mail address causes messages of the specified severity level and higher to be sent. For information on the levels, see Severity Levels, on page 40.
Step 6	Click **OK**.
Step 7	Click **Save**.
	You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Create a Custom Event List

An event list is a custom filter you can apply to a logging destination to control which messages are sent to the destination. Normally, you filter messages for a destination based on severity only, but you can use an event list to fine-tune which messages are sent based on a combination of event class, severity, and message identifier (ID).

Creating a custom event list is a two-step process. You create a custom list in the **Event Lists**, and then use the event list to define the logging filter for the various types of destination, in the **Logging Destinations**.

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense Platform Settings That Apply to Security Event Syslog Messages, on page 46.

Procedure

Step 1	Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.
Step 2	Select **Syslog** > **Events List**.
Step 3	Configure an event list.
	a) Click **Add** to add a new list, or edit an existing list.
	b) Enter a name for the event list in the **Name** field. Spaces are not allowed.
	c) To identify messages based on severity or event class, select the **Severity/Event Class** tab and add or edit entries.
	For information on the available classes see Syslog Message Classes, on page 41.

For information on the levels, see Severity Levels, on page 40.

Certain event classes are not applicable for the device in transparent mode. If such options are configured then they will be bypassed and not deployed.

d) To identify messages specifically by message ID, select the **Message ID** and add or edit the IDs.

You can enter a range of IDs using a hyphen, for example, 100000-200000. IDs are six digits. For information on how the initial three digits map to features, see Syslog Message Classes, on page 41.

For specific message numbers, see Cisco ASA Series Syslog Messages.

e) Click **OK** to save the event list.

Step 4 Click **Logging Destinations** and add or edit the destination that should use the filter.

See Enable Logging Destinations, on page 48.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Limit the Rate of Syslog Message Generation

You can limit the rate at which syslog messages are generated by severity level or message ID. You can specify individual limits for each logging level and each Syslog message ID. If the settings conflict, the Syslog message ID limits take precedence.

🔍

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense Platform Settings That Apply to Security Event Syslog Messages, on page 46.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Rate Limit**.

Step 3 To limit message generation by severity level, click **Logging Level** > **Add** and configure the following options:

- **Logging Level**—The severity level you are rate limiting. For information on the levels, see Severity Levels, on page 40.
- **Number of messages**—The maximum number of messages of the specified type allowed in the specified time period.
- **Interval**—The number of seconds before the rate limit counter resets.

Step 4 Click **OK**.

Step 5 To limit message generation by syslog message ID, click **Syslog Level** > **Add** and configure the following options:

- **Syslog ID**—The syslog message ID you are rate limiting. For specific message numbers, see Cisco ASA Series Syslog Messages.
- **Number of messages**—The maximum number of messages of the specified type allowed in the specified time period.
- **Interval**—The number of seconds before the rate limit counter resets.

Step 6   Click **OK**.

Step 7   Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure Syslog Settings

You can configure general syslog settings to set the facility code to be included in syslog messages that are sent to syslog servers, specify whether a timestamp is included in each message, specify the device ID to include in messages, view and modify the severity levels for messages, and disable the generation of specific messages.

If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), some settings on this page do not apply to these messages. See *Threat Defense Platform Settings That Apply to Security Event Syslog Messages* in the Cisco Secure Firewall Management Center Administration Guide.

Procedure

Step 1   Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2   Select **Syslog** > **Syslog Settings**.

Step 3   Select a system log facility for syslog servers to use as a basis to file messages in the **Facility** drop-down list.

The default is LOCAL4(20), which is what most UNIX systems expect. However, because your network devices share available facilities, you might need to change this value for system logs.

Facility values are not typically relevant for security events. If you need to include Facility values in messages, see *Facility in Security Event Syslog Messages* in the Cisco Secure Firewall Management Center Administration Guide.

Step 4   Select the **Enable timestamp on each syslog message** check box to include the date and time a message was generated in the syslog message.

Step 5   Select the **Timestamp Format** for the syslog message:

- The Legacy (MMM dd yyyy HH:mm:ss) format is the default format for syslog messages.

  When this timestamp format is selected, the messages do not indicate the time zone, which is always UTC.

- RFC 5424 (yyyy-MM-ddTHH:mm:ssZ) uses the ISO 8601 timestamp format as specified in the RFC 5424 syslog format.

  If you select the RFC 5424 format, a "Z" is appended to the end of each timestamp to indicate that the timestamp uses the UTC time zone.

Step 6 If you want to add a device identifier to syslog messages (which is placed at the beginning of the message), check the **Enable Syslog Device ID** check box and then select the type of ID.

- **Interface**—To use the IP address of the selected interface, regardless of the interface through which the appliance sends the message. Select the security zone that identifies the interface. The zone must map to a single interface.
- **User Defined ID**—To use a text string (up to 16 characters) of your choice.
- **Host Name**—To use the hostname of the device.

Step 7 Use the Syslog Message table to alter the default settings for specific syslog messages. You need to configure rules in this table only if you want to change the default settings. You can change the severity assigned to a message, or you can disable the generation of a message.

By default, Netflow is enabled and the entries are shown in the table.

a) To suppress syslog messages that are redundant because of Netflow, select **Netflow Equivalent Syslogs**.

This adds the messages to the table as suppressed messages.

Note
If any of these syslog equivalents are already in the table, your existing rules are not overwritten.

b) To add a rule, click **Add**.

c) You select the message number whose configuration you want to change, from the **Syslog ID** drop down list and then select the new severity level from the **Logging Level** drop down list, or select **Suppressed** to disable the generation of the message. Typically, you would not change the severity level and disable the message, but you can make changes to both fields if desired.

d) Click **OK** to add the rule to the table.

Step 8 Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Configure a Syslog Server

To configure a syslog server to handle messages generated from your system, perform the following steps.

If you want this syslog server to receive security events such as connection and intrusion events, see also Firewall Threat Defense Platform Settings That Apply to Security Event Syslog Messages, on page 46.

Note In 7.4 and later, the Management and Diagnostic interfaces are merged. If Platform Settings for syslog servers or SNMP hosts specify the Diagnostic interface by name, then you must use separate Platform Settings policies for merged and unmerged devices (7.3 and earlier, and some upgraded 7.4 Firewall Threat Defenses).

Before you begin

- See requirements in .

- Make sure your devices can reach your syslog collector on the network.

Procedure

Step 1   Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2   Select **Syslog** > **Syslog Server**.

Step 3   Check the **Allow user traffic to pass when TCP syslog server is down (Recommended)** check box, to allow traffic if any syslog server that is using the TCP protocol is down.

> **Note**
> - This option is enabled by default. Unless required, we recommend that you allow connections through the threat defense device when the external TCP syslog server is unreachable by the device.
>
> - When the **Allow user traffic to pass when TCP syslog server is down** option is disabled in Firewall Management Center version 6.2.x or earlier, it persist to be in the Disable state even after upgrading to version 6.3 or later. Ensure that you manually enable it.
>
> - With this option disabled, and when more than one TCP syslog server configured in the device, the user traffic is allowed to pass if atleast one of the servers is reachable by the threat defense device. Thus, the disabled option is applied only when none of the TCP syslog servers configured in the device are reachable. The device generates the following syslog that describes the root cause of the denied traffic through the device:
>
> ```
> %FTD-3-414003: TCP Syslog Server intf : IP_Address /port not responding. New connections
> are denied based on logging permit-hostdown policy
> ```

Step 4   In the **Message queue size (messages)** field, enter a size of the queue for storing syslog messages on the security appliance when syslog server is busy. The minimum is 1 message. The default is 512. Specify 0 to allow an unlimited number of messages to be queued (subject to available block memory).

When the messages exceed the configured queue size, they are dropped and result in missing syslog. To determine the ideal queue size, you need to identify the available block memory. Use the **show blocks** command to know the current memory utilization. For more information on the command and its attributes, see *Cisco Secure Firewall ASA Series Command Reference Guide*. For further assistance, contact Cisco TAC.

Step 5   Click **Add** to add a new syslog server.

a) In the **IP Address** drop-down list, select a network host object that contains the IP address of the syslog server.

b) Choose the protocol (either TCP or UDP) and enter the port number for communications between the Firewall Threat Defense device and the syslog server.

UDP is faster and uses less resources on the device than TCP.

The default port for UDP is 514. You must manually configure port 1470 for TCP. Valid non-default port values for either protocol are 1025 through 65535.

c) Check the **Log messages in Cisco EMBLEM format (UDP only)** check box to specify whether to log messages in Cisco EMBLEM format (available only if UDP is selected as the protocol).

The EMBLEM syslog format is a Cisco-specific convention that is built upon the RFC 3164 and RFC 5424 standards. Hence, when EMBLEM is enabled, the syslog message prints colon (:) after <PRI> field.

Note

Syslog messages in RFC5424 format, typically displays the priority value (PRI). However, in Firewall Management Center, only when you enable logging in Cisco EMBLEM format, the PRI value in the syslog messages of the managed Firewall Threat Defense is displayed. Also, the device ID does not appear in EMBLEM-formatted syslog messages.

d) Check the **Enable Secure Syslog** check box to encrypt the connection between the device and server using SSL/TLS over TCP.

Note

You must select TCP as the protocol and its port value ranging between 1025 and 65535 to use this option. You must also upload the certificate required to communicate with the syslog server on the **Devices** > **Certificates** page. Finally, upload the certificate from the Firewall Threat Defense device to the syslog server to complete the secure relationship and allow it to decrypt the traffic. The **Enable Secure Syslog** option is not supported on the device Management interface.

e) Select **Device Management Interface** or **Security Zones or Named Interfaces** to communicate with the syslog server.

- **Device Management Interface**: Send syslogs out of the Management interface. We recommend that you use this option when configuring syslog on Snort events.

  Note

  The **Device Management Interface** option does not support the **Enable Secure Syslog** option.

- **Security Zones or Named Interfaces**: Select the interfaces from the list of **Available Zones** and click **Add**. You can also add virtual-router-aware interfaces.

  Important

  The Firewall Threat Defense data plane (Lina) syslog messages cannot be sent out through the diagnostic interface. Configure other interfaces or the Management interface (Br1/Management0) to send out the data plane syslog messages.

f) Click **OK**.

Step 6   Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Timeouts

You can set the global idle timeout durations for the connection and translation slots of various protocols. If the slot has not been used for the idle time specified, the resource is returned to the free pool.

You can also set a time out for console sessions with the device.

Procedure

Step 1   Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2   Select **Timeouts**.

Step 3   Configure the timeouts you want to change.

For any given setting, select **Custom** to define your own value, **Default** to return to the system default value. In most cases, the maximum timeout is 1193 hours.

You can disable some timeouts by selecting **Disable**.

- **Console Timeout**—The idle time until a connection to the console is closed, range is 0 or 5 to 1440 minutes. The default is 0, which means the session does not time out. If you change the value, existing console sessions use the old timeout value. The new value applies to new connections only.

- **Translation Slot (xlate)**—The idle time until a NAT translation slot is freed. This duration must be at least 1 minute. The default is 3 hours.

- **Connection (Conn)**—The idle time until a connection slot is freed. This duration must be at least 5 minutes. The default is 1 hour.

- **Half-Closed**—The idle time until a TCP half-closed connection closes. A connection is considered half-closed if both the FIN and FIN-ACK have been seen. If only the FIN has been seen, the regular connection timeout applies. The minimum is 30 seconds. The default is 10 minutes.

- **UDP**—The idle time until a UDP connection closes. This duration must be at least 1 minute. The default is 2 minutes.

- **ICMP**—The idle time after which general ICMP states are closed. The default (and minimum) is 2 seconds.

- **RPC/Sun RPC**—The idle time until a SunRPC slot is freed. This duration must be at least 1 minute. The default is 10 minutes.

  In a Sun RPC-based connection, when the parent connection is deleted or timed-out, a new child connection may not be considered as a part of the parent-child connection, and thereby the new connection could be evaluated as per the policy or rules set in the system. After the parent connection has timed-out the existing child connections are valid only until the timeout value set is reached.

- **H.225**—The idle time until an H.225 signaling connection closes. The default is 1 hour. To close a connection immediately after all calls are cleared, a timeout of 1 second (0:0:1) is recommended.

- **H.323**—The idle time after which H.245 (TCP) and H.323 (UDP) media connections close. The default (and minimum) is 5 minutes. Because the same connection flag is set on both H.245 and H.323 media connections, the H.245 (TCP) connection shares the idle timeout with the H.323 (RTP and RTCP) media connection.

- **SIP**—The idle time until a SIP signaling port connection closes. This duration must be at least 5 minutes. The default is 30 minutes.

- **SIP Media**—The idle time until a SIP media port connection closes. This duration must be at least 1 minute. The default is 2 minutes. The SIP media timer is used for SIP RTP/RTCP with SIP UDP media packets, instead of the UDP inactivity timeout.

- **SIP Disconnect**—The idle time after which SIP session is deleted if the 200 OK is not received for a CANCEL or a BYE message, between 0:0:1 and 0:10:0. The default is 2 minutes (0:2:0).

- **SIP Invite**—The idle time after which pinholes for PROVISIONAL responses and media xlates will be closed, between 0:1:0 and 00:30:0. The default is 3 minutes (0:3:0).

- **SIP Provisional Media**—The timeout value for SIP provisional media connections, between 1 and 30 minutes. The default is 2 minutes.

- **Floating Connection**—When multiple routes exist to a network with different metrics, the system uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The default is 0 (the connection never times out). To make it possible to use better routes, set the timeout to a value between 0:0:30 and 1193:0:0. This timer does not apply to connections through virtual tunnel interfaces (VTI). If a connection through a VTI gets stuck, you must manually clear it.

- **Xlate PAT**—The idle time until a PAT translation slot is freed, between 0:0:30 and 0:5:0. The default is 30 seconds. You may want to increase the timeout if upstream routers reject new connections using a freed PAT port because the previous connection might still be open on the upstream device.

- **TCP Proxy Reassembly**—The idle timeout after which buffered packets waiting for reassembly are dropped, between 0:0:10 and 1193:0:0. The default is 1 minute (0:1:0).

- **ARP Timeout**—The number of seconds between ARP table rebuilds, from 60 to 4294967. The default is 14,400 seconds (4 hours).

Step 4   Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Time Synchronization

Use a Network Time Protocol (NTP) server to synchronize the clock settings on your devices. We recommend you configure all Firewall Threat Defenses managed by a Firewall Management Center to use the same NTP server as the Firewall Management Center. The Firewall Threat Defense gets its time directly from the configured NTP server. If the Firewall Threat Defense's configured NTP servers are not reachable for any reason, it synchronizes its time with the Firewall Management Center.

The device supports NTPv4.

Note   If you are deploying Firewall Threat Defense on the Firepower 4100/9300 chassis, you must configure NTP on the Firepower 4100/9300 chassis so that Smart Licensing will work properly and to ensure proper timestamps on device registrations. You should use the same NTP server for the Firepower 4100/9300 chassis and the Firewall Management Center.

Before you begin

- If your organization has one or more NTP servers that your Firewall Threat Defense can reach, use the same NTP server or servers for your devices that you have configured for Time Synchronization on the **System** (⚙) > **Configuration** page on your Firewall Management Center.

- If you selected **Use the authenticated NTP server only** when configuring NTP server or servers for the Firewall Management Center, for your devices use only the NTP server or servers that are configured to authenticate with the Firewall Management Center. (The managed devices will use the same NTP servers as the Firewall Management Center, but their NTP connections will not use authentication.)

- If your device cannot reach an NTP server or your organization does not have one, you must use the **Via NTP from Defense Center** option as discussed in the following procedure.

Procedure

Step 1   Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2   Select **Time Synchronization**.

Step 3   Configure one of the following clock options:

- **Via NTP from Defense Center**—(Default). The managed device gets time from the NTP servers you configured for the Firewall Management Center (except for authenticated NTP servers) and synchronizes time with those servers directly. However, if any of the following are true, the managed device synchronizes time from the Firewall Management Center:

    - The Firewall Management Center's NTP servers are not reachable by the device.

    - The Firewall Management Center has no unauthenticated servers.

- **Via NTP from**—If your Firewall Management Center is using NTP servers on the network, select this option and enter the fully-qualified DNS name (such as ntp.example.com), or IPv4 or IPv6 address, of the same NTP servers you specified in **System** (⚙) > **Configuration** > **Time Synchronization**. If the NTP servers are not reachable, the Firewall Management Center acts as an NTP server.

When multiple NTP servers are configured, the device uses the NTP server that is deemed appropriate based on the criteria defined in RFC. Thus, the status of "Being used" for a specific NTP server indicates that the server is currently used by the device.

Step 4   Click **Save**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Time Zone

By default, the system uses the UTC time zone. To designate a different time zone for a device, use this procedure.

The time zone you specify will be used only for time-based policy application in policies that support this functionality.

Note Time-based ACLs is supported in Snort 3 also from Firewall Management Center 7.0 onwards.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit an Firewall Threat Defense policy.

You can also create time zone objects from the **Objects** > **Object Management** > **Time Zone** page.

Step 2 Create a new time zone object by clicking +.

Step 3 Select the time zone.

Step 4 Click **Save**.

What to do next

- Create time range objects, select applicable time ranges in access control and prefilter rules, and assign the parent policies to devices associated with the correct time zone.

- Deploy configuration changes; see Deploy Configuration Changes.

UCAPL/CC Compliance

For more information about this setting and how to enable it for the Firewall Management Center, see the Cisco Secure Firewall Management Center Administration Guide.

Caution After you enable this setting, you cannot disable it. If you need to take the appliance out of CC or UCAPL mode, you must reimage.

Before you begin

- Secure Firewall Threat Defense devices cannot use an evaluation license; your Smart Software Manager account must be enabled for export-controlled features.

- Secure Firewall Threat Defense devices must be deployed in routed mode.

- You must be an Admin user to perform this task.

- Security certifications compliance mode cannot be changed if the Firewall Threat Defense device is in high availability. Modify the security certifications compliance mode before forming the high availability pair.

Procedure

Step 1   Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2   Click **UCAPL/CC Compliance**.

Step 3   To *permanently* enable security certifications compliance on the appliance, you have two choices:

- To enable security certifications compliance in Common Criteria mode, choose **CC** from the drop-down list.
- To enable security certifications compliance in Unified Capabilities Approved Products List mode, choose **UCAPL** from the drop-down list.

Step 4   Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Performance Profile

The performance profile determines how the CPU cores on the device are assigned to two of the main system processes: the data plane (Lina) and Snort. The data plane handles VPN connections, routing, and other basic layer 3/4 processing. Snort provides advanced inspection, including intrusion and malware prevention, URL filtering, application filtering, and other features that require deep packet inspection.

If you use a balance of basic and advanced features, do not change the performance profile. The system is designed to provide a balanced assignment of cores to these processes. The assignment differs based on the hardware model.

However, if you use the device primarily for VPN, or for intrusion and other advanced inspection, you can skew the performance profile so that more cores are assigned to the more heavily used features. This might improve system performance.

Before you begin

- These settings apply to systems running release 7.3+ only.

- Performance profile is supported on the following device types:

  - Firepower 4100/9300

  - Secure Firewall 3100/4200 (7.4+)

  - Secure Firewall Threat Defense Virtual

- Changing the performance profile is not supported on units in a cluster or high-availability group, or those configured for multi-instance. Deployment is blocked if you assign the profile to anything but standalone devices.

- The minimum number for core allocation is 2. Cores are assigned in even numbers based on the selected performance profile.

Procedure

Step 1	Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.
Step 2	Select **Performance Profile**.
Step 3	Select a profile:

- **Default**—This is the recommended setting and is the best option if you configure both VPN and intrusion inspection.

- **VPN Heavy with prefilter fastpath**—If you primarily use the device as a VPN endpoint or headend, and you configure rules in the prefilter policy to fastpath VPN traffic, you can choose this option to assign the majority of CPU cores to the data plane. The allocation is 90% data place, 10% Snort.

- **VPN Heavy with inspection**—If you primarily use the device as a VPN endpoint or headend, but do not use the prefilter policy to fastpath VPN traffic, you can choose this option to assign the majority of CPU cores to the data plane. This option assumes that you leave intrusion inspection, URL filtering, and other advanced functions that use Snort, to a different device in the network. The allocation is 60% data plane, 40% Snort.

- **IPS Heavy**—If you do not configure VPN, but you do use the device for intrusion prevention, you can choose this option to assign the majority of CPU core to the Snort process. The allocation is 30% data plane, 70% Snort.

Step 4	Click **Save**.
Step 5	Deploy the policy.
Step 6	After deployment completes, you must reboot each affected device so that the new core assignments can be made.

History for Platform Settings

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Device management services supported on user-defined VRF interfaces.	7.4.1	7.4.1	Device management services configured in the Firewall Threat Defense platform settings (NetFlow, SSH access, SNMP hosts, syslog servers) are now supported on user-defined Virtual Routing and Forwarding (VRF) interfaces. Platform restrictions: Not supported with container instances or clustered devices.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details

Chassis platform settings for the Secure Firewall 3100.	7.4.1	7.4.1	New platform settings for multi-instance chassis on the Secure Firewall 3100.
			
			New/modified screens:
			
			    • **Devices** > **Platform Settings** > **Add** > **Chassis Platform Settings**
			
			    • **Devices** > **Platform Settings** > **Edit** > **Chassis Platform Settings** > **DNS**
			
			    • **Devices** > **Platform Settings** > **Edit** > **Chassis Platform Settings** > **SSH**
			
			    • **Devices** > **Platform Settings** > **Edit** > **Chassis Platform Settings** > **Time Synchronization**
			
			    • **Devices** > **Platform Settings** > **Edit** > **Chassis Platform Settings** > **Time Zones**
			
			    • **Devices** > **Platform Settings** > **Edit** > **Chassis Platform Settings** > **Syslog**
			
			Supported platforms: Secure Firewall 3100

Performance profile support for the Secure Firewall 3100/4200.	7.4.0	7.4.0	The performance profile settings available in the platform settings policy now apply to Secure Firewall 3100/4200 devices.

Loopback interface support for DNS, HTTP, ICMP, NetFlow, SNMP and SSH.	7.4.0	7.4.0	You can create a loopback interface and use it for:
			
			    • DNS
			
			    • HTTP
			
			    • ICMP
			
			    • NetFlow
			
			    • SNMP
			
			    • SSH
			
			New/modified screens:
			
			    • **Devices** > **Platform Settings** > **DNS** > **DNS Settings**
			
			      Devices > **Platform Settings** > **HTTP Access** > **Add**
			
			      Devices > **Platform Settings** > **ICMP Access** > **Add**
			
			    • **Devices** > **Platform Settings** > **Network flow** > **Add Collector**
			
			    • **Devices** > **Platform Settings** > **SNMP** > **Hosts** > **Add**
			
			    • **Devices** > **Platform Settings** > **SSH Access** > **Add**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Merged Management and Diagnostic interfaces.	7.4.0	7.4.0	For new devices using 7.4 and later, you cannot use the legacy Diagnostic interface. Only the merged Management interface is available. If you upgraded to 7.4 or later, and you did not have any configuration for the Diagnostic interface, then the interfaces will merge automatically.
			If you upgraded to 7.4 or later, and you have configuration for the Diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate Diagnostic interface. Note that support for the Diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible.
			Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including Management) in the configuration.
			For platform settings, this means:
			• You can no longer enable HTTP, ICMP, or SMTP for Diagnostic.
			• For SNMP, you can allow hosts on Management instead of Diagnostic.
			• For Syslog servers, you can reach them on Management instead of Diagnostic.
			• If Platform Settings for syslog servers or SNMP hosts specify the Diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices.
			• DNS lookups no longer fall back to the management-only routing table if you do not specify interfaces.
			New/modified screens:
			• **Devices** > **Device Management** > **Interfaces**
			New/modified commands: **show management-interface convergence**
Performance profile for CPU core allocation.	7.3.0	7.3.0	You can adjust the percentage of system cores assigned to the data plane and Snort to adjust system performance. The adjustment is based on your relative use of VPN and intrusion policies. If you use both, leave the core allocation to the default values. If you use the system primarily for VPN (without applying intrusion policies), or as an IPS (with no VPN configuration), you can skew the core allocation to the data plane (for VPN) or Snort (for intrusion inspection).
			We added the **Performance Profile** page to the platform settings policy.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
TLS 1.3 in Remote Access VPN.	7.3.0	7.3.0	You can now use TLS 1.3 to encrypt remote access VPN connections. Use threat defense platform settings to specify that the device must use TLS 1.3 protocol when acting as a remote access VPN server. TLS 1.3 adds support for the following ciphers: • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 This feature requires Cisco Secure Client, Version 5.0 and above. New/modified screens: **Devices** > **Platform Settings** > **New Policy** > **Add/Edit Threat Defense Settings** > **SSL** > **TLS version**
Multiple DNS server groups for resolving DNS requests.	7.2.0	7.2.0	You can configure multiple DNS groups for the resolution of DNS requests from client systems. You can use these DNS server groups to resolve requests for different DNS domains. For example, you could have a catch-all default group that uses public DNS servers, for use with connections to the Internet. You could then configure a separate group to use internal DNS servers for internal traffic, for example, any connection to a machine in the example.com domain. Thus, connections to an FQDN using your organization's domain name would be resolved using your internal DNS servers, whereas connections to public servers use external DNS servers. We changed the **Platform Settings** > **DNS** page.
Network object support for HTTP, ICMP, and SSH platform settings.	7.1.0	7.1.0	You can now use network object groups that contain network objects for hosts or networks when configuring the IP addresses in the Threat Defense Platform Settings policy. Supported platforms: Firewall Threat Defense
Support to specify trusted DNS servers.	7.1.0	7.1.0	The option to specify DNS servers that you can trust for address resolution while using direct internet access was introduced. We added a tab for configuring the trusted DNS servers when configuring direct internet access: **Devices** > **Platform Settings** > **DNS** > **Trusted DNS Servers**. Supported platforms: Firewall Threat Defense

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Platform settings using the MD5 authentication algorithm or DES encryption for SNMPv3 users can not be deployed to Firewall Threat Defense devices running Versions 7.0+.	7.0.0	7.0.0	The MD5 authentication algorithm and DES encryption for SNMPv3 users on Firewall Threat Defense were deprecated in Version 6.5. If your deployment includes SNMPv3 users using the MD5 authentication algorithm or DES encryption that were created using Version 6.4 or earlier, you can continue to use those users for Firewall Threat Defense devices running Version 6.7 or earlier. However, you cannot edit those users and retain the MD5 or DES settings, and you cannot create new users with the MD5 or DES settings. If your Firewall Management Center manages any Firewall Threat Defenses running Versions 7.0+, deploying a platform settings policy with SNMP v3 users using the MD5 authentication algorithm or DES encryption to those Firewall Threat Defenses will fail. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Hosts** Supported platforms: Firewall Threat Defense
Specify SHA224 or SHA384 for SNMPv3 users' authorization algorithm.	7.0.0	7.0.0	You can now select SHA224 or SHA384 for SNMPv3 users' authorization algorithm. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Users** Supported platforms: Firewall Threat Defense
Specify time zone for device.	6.6.0	6.6.0	Specify a local time zone for a managed device, for use in time-based policy application. New/modified screens: **Devices** > **Platform Settings** > **Time Zone** Supported platforms: Firewall Threat Defense
Specify the Management interface for SNMP communication.	6.6.0	6.6.0	You can now select the Management interface for communication between the device and the SNMP management station. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Hosts** Supported platforms: Firewall Threat Defense
Specify SHA256 for SNMPv3 users' authorization algorithm.	6.6.0	6.6.0	You can now select SHA256 for SNMPv3 users' authorization algorithm. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Users** Supported platforms: Firewall Threat Defense

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
DES encryption and the MD5 authentication algorithm for SNMPv3 users on Firewall Threat Defense have been deprecated.	6.5.0	Any	We recommend that you not use the MD5 authentication algorithm or DES encryption for SNMPv3 users on Firewall Threat Defense devices, as these options have been deprecated. If your deployment includes SNMPv3 users using the MD5 authentication algorithm or DES encryption that were created using a Version 6.4 or earlier, you can continue to use those users. However, you cannot edit those users and retain the MD5 or DES settings, and you cannot create new users with the MD5 or DES settings. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Users** Supported platforms: Firewall Threat Defense
Allow user traffic to pass when TCP syslog server is down.	6.3.0	6.3.0	We recommend that you allow connections through the threat defense device when the external TCP syslog server is unreachable by the device. The **Allow user traffic to pass when TCP syslog server is down (Recommended to be enabled)** option in the Platform Settings is Enabled by default.
Limit number of SSH login failures.	6.3.0	6.3.0	When a user accesses any device via SSH and fails three successive login attempts, the device terminates the SSH session.
External authentication added for SSH.	6.2.3	6.2.3	You can now configure external authentication for SSH access to the Firewall Threat Defense using LDAP or RADIUS. New/modified screens: **Devices** > **Platform Settings** > **External Authentication** Supported platforms: Firewall Threat Defense
Support for UC/APPL compliance mode.	6.2.1	6.2.1	You can enable security certifications compliance in CC mode or UCAPL mode. Enabling security certifications compliance does not guarantee strict compliance with all requirements of the security mode selected. For more information on hardening procedures, refer to the guidelines for this product provided by the certifying entity. New/modified screens: **Devices** > **Platform Settings** > **UC/APPL Compliance** Supported platforms: Any device
SSL settings for remote access VPN.	6.2.1	6.2.1	The Firewall Threat Defense device uses the Secure Sockets Layer (SSL) protocol and Transport Layer Security (TLS) to support secure message transmission for Remote Access VPN connection from remote clients. You can configure SSL versions and encryption algorithms that will be negotiated and used for message transmission during remote VPN access over SSL. New/modified screens: **Devices** > **Platform Settings** > **SSL** Supported platforms: Firewall Threat Defense

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
External authentication for SSH and HTML removed.	6.1.0	6.1.0	Due to changes to support converged management access, only local users are supported for SSH and HTML to data interfaces. Also, you can no longer SSH to the logical Diagnostic interface; instead you can SSH to the logical Management interface (which shares the same physical port). Previously, only external authentication was supported for SSH and HTML access to Diagnostic and data interfaces, while only local users were supported to the Management interface. New/modified screens: **Devices** > **Platform Settings** > **External Authentication** Supported platforms: Firewall Threat Defense
Firepower Threat Defense support.	6.0.1	6.0.1	This feature was introduced. New/modified screens: **Devices** > **Platform Settings** Supported platforms: Firewall Threat Defense