Platform Settings for Firepower Threat Defense

Platform settings for Firepower 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.

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

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

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit the Firepower 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.

Configure Banners

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

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit the Firepower 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.

Configure 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 FMC management 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 FTD 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.

Before you begin

- Ensure you have created a DNS server group. For instructions, see Creating DNS Server Group Objects.
- Ensure that the FTD has appropriate static or dynamic routes to access the DNS servers.

Procedure

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

Step 2 Click **DNS**.

Step 3 Check **Enable DNS name resolution by device**.

Step 4 Choose the **DNS Server Group** that you have already created.

Step 5 (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 time limit to remove the IP address of a resolved FQDN from the DNS lookup table after its time-to-live (TTL) expires. Removing an entry requires the table to be recompiled, so frequent removals can increase the processing load on the device. This setting virtually extends the TTL.
- **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 6 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 FTD always uses a route lookup to determine the source interface.

- No interfaces selected—Enables DNS lookups on all interfaces, including Management and management-only interfaces. The FTD checks the data routing table, and if no route is found, falls back to the management-only routing table.
- Specific interfaces selected but not the **Enable DNS Lookup via diagnostic interface also** option—Enables DNS lookups on the specified interfaces. The FTD checks the data routing table only.
- Specific interfaces selected plus the **Enable DNS Lookup via diagnostic interface also** option—Enables DNS lookups on the specified interfaces and the interface. The FTD 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 interface also** option—Enables DNS lookups on . The FTD checks only the management-only routing table. Be sure to configure an IP address for the Diagnostic interface on the **Devices** > **Device Management** > **edit device** > **Interfaces** page.

Step 7 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.

Configure External Authentication for SSH

Note You must have administrator privileges to perform this task.

When you enable external authentication for management users, the Firepower 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 FMC and the Firepower Threat Defense devices. You can share the same object between the FMC and devices, or create separate objects. Note that the Firepower Threat Defense supports defining users on the RADIUS server, while the FMC requires you to predefine the user list in the external authentication object. You can choose to use the predefined list method for the Firepower Threat Defense, but if you want to define users on the RADIUS server, you must create separate objects for the Firepower Threat Defense and the FMC.

Note The timeout range is different for the Firepower Threat Defense and the FMC, so if you share an object, be sure not to exceed the Firepower 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 Firepower Threat Defense external authentication configuration will not work.

Assigning External Authentication Objects to Devices

For the FMC, enable the external authentication objects directly on **System** > **Users** > **External Authentication**; this setting only affects FMC usage, and it does not need to be enabled for managed device usage. For Firepower 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.

FTD Supported Fields

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

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 FMC; you cannot add them at the CLI. Note that internal users can only be added at the CLI, not in the FMC.

If you previously configured the same username for an internal user using the **configure user add** command, the Firepower 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 Configure Secure Shell, on page 16. SSH is not supported to the Diagnostic interface.
- Inform RADIUS users of the following behavior to set their expectations appropriately:
  - The first time an external user logs in, the Firepower 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."
  - 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 Select **Devices** > **Platform Settings** and create or edit the Firepower 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 Firepower 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 FTD and the FMC, so if you share an object, be sure not to exceed the FTD's smaller timeout range (1-30 seconds). If you set the timeout to a higher value, the FTD 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 Threat Defense Platform Setttings 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 9). To use the same RADIUS server for the Firepower Threat Defense and the FMC while using the Service-Type attribute method for the Firepower 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 FMC), and the other object leaves the **CLI Access Filter** empty (for use with the Firepower Threat Defenses).

b) In the FMC, 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 the Firepower Threat Defense so you can use the same external authentication object with the Firepower 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 **Devices** > > **Platform Settings** > **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.

Configure Fragment Handling

By default, the Firepower 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 Firepower Threat Defense device, and select **Interfaces** to edit interface properties..

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit the Firepower 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.

Configure HTTP

If you want to allow HTTPS connections to one or more interfaces on the Firepower Threat Defense device, configure HTTPS settings. You can use HTTPS to download packet captures for troubleshooting.

Before you begin

- When you manage the Firepower Threat Defense using the FMC, HTTPS access to the Firepower Threat Defense is only for viewing packet capture files. The Firepower Threat Defense does not have a web interface for configuration in this management mode.
- HTTPS local users can only be configured at the CLI using the **configure user add** command. By default, there is an **admin** user for which you configured the password during initial setup. AAA external authentication is not supported.
- The physical management interface is shared between the Diagnostic logical interface and the Management logical interface; this configuration applies only to the Diagnostic logical interface, if used, or to other data interfaces. The Management logical interface is separate from the other interfaces on the device. It is used to set up and register the device to the FMC. 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.
- You cannot configure both HTTPS and AnyConnect remote access SSL VPN 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.
- The device allows a maximum of 5 concurrent HTTPS connections.

- You need network objects that define the hosts or networks you will allow to make HTTPS connections to the device. 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 Select **Devices** > **Platform Settings** and create or edit the Firepower Threat Defense policy.

Step 2 Select **HTTP**.

Step 3 Enable the HTTPS server by clicking **Enable HTTP server**.

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

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

Use this table to limit which interfaces will accept HTTPS 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 that identifies the hosts or networks you are allowing to make HTTPS connections. Choose an object from the drop-down menu, or add a new network object by clicking +.
- **Security Zones**—Add the zones that contain the interfaces to which you will allow HTTPS connections. 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 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.

Configure ICMP Access Rules

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

- The FTD does not respond to ICMP echo requests directed to a broadcast address.
- The FTD 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 that define the desired hosts or networks, and port objects that define the ICMP message types you want to control.

Procedure

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

Step 2 Select **ICMP**.

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 that identifies the hosts or networks whose access you are controlling.
- **Security Zones**—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 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 (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.

Configure SSL Settings

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 Firepower Management Center. The SSL Settings will be disabled if you are running Firepower Management Center in evaluation mode. Additionally, the SSL Settings will be disabled when the licensed Firepower 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 FTD License Types and Restrictions.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit a Firepower 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, seeAbout SSL Settings, on page 13

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 Firepower 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.

Configure the SSL Settings at the following location:

Devices > Platform Settings > SSL

Fields

Minimum SSL Version as Server—Specify the minimum SSL/TLS protocol version that the Firepower 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).

DTLS Version—Select the DTLS versions from the drop-down list, based on the selected TLS version. By default, DTLSv1 is configured on the Firepower Threat Defense device, 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

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.

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

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

- Default
- TLSV1
- TLSV1.1
- TLSV1.2
- DTLSv1
- DTLSv1.2

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

If you have the Firepower Threat Defense devices with evaluation license, the security level is Low by default. With the Firepower 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.
- **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 Firepower 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

The Firepower Threat Defense device specifies the order of priority for supported ciphers as:

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

Ciphers not supported by TLSv1.1 or TLSv1.2

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

Configure Secure Shell

If you enabled the FMC 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 Firepower Threat Defense. SSH is not supported to the Diagnostic logical interface.

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 FMC. 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 Firepower 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 only SSH to a reachable interface; if your SSH host is located on the outside interface, you can only initiate a management connection directly to the outside interface.

The device allows a maximum of 5 concurrent SSH connections.

Note On all appliances, after a user makes three consecutive failed attempts to log into the CLI via SSH, the system 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 Configure External Authentication for SSH, on page 5.
- You need network objects that define the hosts or networks you will allow to make SSH connections to the device. 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 Select **Devices** > **Platform Settings** and create or edit the Firepower Threat Defense policy.

Step 2 Select **Secure Shell**.

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 that identifies the hosts or networks you are allowing to make SSH connections. Choose an object from the drop-down menu, or add a new network object by clicking +.

- **Security Zones**—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 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 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 SMTP

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 Select **Devices** > **Platform Settings** and create or edit the Firepower 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.

Configure SNMP for Threat Defense

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. However, you cannot edit those users and retain DES encryption, or create new users with DES encryption.

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

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit the Firepower 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 Firepower 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 20.

Step 5 Add SNMP Hosts, on page 22.

Step 6 Configure SNMP Traps, on page 23.

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 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.

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

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. However, you cannot edit those users and retain the MD5 authentication algorithm, or create new users with the MD5 authentication algorithm.

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. However, you cannot edit those users and retain DES encryption, or create new users with DES encryption.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit the Firepower 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 Firepower Threat Defense device will still encrypt the password when deploying to the device.
- **Encrypted**—The Firepower 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, SHA256.

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. However, you cannot edit those users and retain the MD5 authentication algorithm, or create new users with the MD5 authentication algorithm.

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. However, you cannot edit those users and retain DES encryption, or create new users with DES encryption.

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 Firepower Threat Defense device.

You can add up to 4000 hosts. However, only 128 of this number can be for traps.

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 Select **Devices** > **Platform Settings** and create or edit the Firepower 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 Step 6, on page 22. 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 Step 5, on page 22.
- **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**. 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 Firepower Threat Defense device. Traps are different from browsing; they are unsolicited "comments" from the Firepower 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 Firepower 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 Select **Devices** > **Platform Settings** and create or edit the Firepower Threat Defense policy.

Step 2 Click **SNMP** > **SNMP Traps** to configure SNMP traps (event notifications) for the Firepower 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 Firepower 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 36.

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.

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.

About Configuring Syslog

You can enable system logging (syslog) for Firepower 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 1: System Logs for Firepower 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, Firepower Threat Defense does not necessarily generate every message type that is available for ASA Software. For information on these messages, see *Cisco Firepower 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**
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.	**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. These messages are not numbered. For information on configuring this type of syslog, see Creating a Syslog Alert Response.	**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 2: 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.

Level Number	Severity Level	Description
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 FTD 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 FTD 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 FTD 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 3: Syslog Message Classes and Associated Message ID Numbers

Class	Definition	Syslog Message ID Numbers
auth	User Authentication	109, 113
—	Access Lists	106
—	Application Firewall	415
—	Botnet Traffic Filtering	338
bridge	Transparent Firewall	110, 220
ca	PKI Certification Authority	717
citrix	Citrix Client	723
—	Clustering	747
—	Card Management	323
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	735
ha	Failover	101, 102, 103, 104, 105, 210, 311, 709
—	Identity-based Firewall	746
ids	Intrusion Detection System	400, 733

Class	Definition	Syslog Message ID Numbers
—	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	325
—	Licensing	444
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	305
—	Network Access Point	713
np	Network Processor	319
—	NP SSL	725
ospf	OSPF Routing	318, 409, 503, 613
—	Password Encryption	742
—	Phone Proxy	337
rip	RIP Routing	107, 312
rm	Resource Manager	321
—	Smart Call Home	120
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
snmp	SNMP	212
—	ScanSafe	775
ssl	SSL Stack	725
svc	SSL VPN Client	722

Class	Definition	Syslog Message ID Numbers
sys	System	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711, 741
—	Threat Detection	733
tag-switching	Service Tag Switching	779
vm	VLAN Mapping	730
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	778
webfo	WebVPN Failover	721
webvpn	WebVPN and AnyConnect Client	716

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

- The syslog server must run a server program called syslogd. Windows provides a syslog server as part of its operating system.
- To view logs generated by the FTD device, you must specify a logging output destination. If you enable logging without specifying a logging output destination, the FTD 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 FTD 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 FTD device sends syslogs via TCP, the connection takes about one minute to initiate after the syslogd service restarts.

Configure Syslog Logging for FTD Devices

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most FTD platform settings do not apply to these messages. See FTD Platform Settings That Apply to Security Event Syslog Messages, on page 32.

To configure syslog settings, perform the following steps:

Before you begin

See requirements in Guidelines for Logging, on page 30.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit the Firepower 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 Enable Logging and Configure Basic Settings, on page 32

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 Enable Logging Destinations, on page 34

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 Send Syslog Messages to an E-mail Address, on page 35

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 Create a Custom Event List, on page 35

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 Limit the Rate of Syslog Message Generation, on page 36

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 Configure Syslog Settings, on page 37

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 Configure a Syslog Server, on page 39

FTD 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 on the **Devices > Platform Settings > Threat Defense Settings > Syslog** page 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).

See also Best Practices for Configuring Security Event Syslog Messaging.

Enable Logging and Configure Basic Settings

You must enable logging 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 FTD platform settings do not apply to these messages. See FTD Platform Settings That Apply to Security Event Syslog Messages, on page 32.

Procedure

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

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

Step 3 Enable logging and configure basic logging settings.

- **Enable Logging**—Turns on data plane system logging for the Firepower Threat Defense device.
- **Enable Logging on the Failover Standby Unit**—Turns on logging for the standby for the Firepower 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.

  Note Syslog messages in RFC5424 format, typically displays the priority value (PRI). However, in FMC, if you want to display the PRI value in the syslog messages of the managed FTD, ensure to enable the EMBLEM format. For more information on PRI, see RFC5424.

- **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 71101. 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) Enable VPN logging by checking the **Enable Logging to FMC** check box. Choose the syslog severity level for VPN messages from the **Logging Level** drop-down list.

For information on the levels, see Severity Levels, on page 26.

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 user name 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 user name 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 KB). 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 FTD platform settings do not apply to these messages. See FTD Platform Settings That Apply to Security Event Syslog Messages, on page 32.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit the Firepower 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 27.

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 FTD platform settings do not apply to these messages. See FTD Platform Settings That Apply to Security Event Syslog Messages, on page 32.

Before you begin

- Configure an SMTP server on the SMTP Server platform settings page
- Enable Logging and Configure Basic Settings, on page 32
- Enable Logging Destinations

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit the Firepower 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 26.

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 FTD platform settings do not apply to these messages. See FTD Platform Settings That Apply to Security Event Syslog Messages, on page 32.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit the Firepower 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 27.

For information on the levels, see Severity Levels, on page 26.

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 27.

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 34.

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 FTD platform settings do not apply to these messages. See FTD Platform Settings That Apply to Security Event Syslog Messages, on page 32.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit the Firepower 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 26.
- **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 FTD Platform Settings That Apply to Security Event Syslog Messages, on page 32.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit the Firepower 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.

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.

Related Topics

FTD Platform Settings That Apply to Security Event Syslog Messages, on page 32

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 FTD Platform Settings That Apply to Security Event Syslog Messages, on page 32.

Before you begin

- See requirements in Guidelines for Logging, on page 30.
- Make sure your devices can reach your syslog collector on the network.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit the Firepower 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 FTD device when the external TCP syslog server is unreachable by the device.
- When the FMC runs version 6.2.x or earlier and has the Platform Settings **Allow user traffic to pass when TCP syslog server is down** option disabled, this option persist to be in Disable state even after upgrading to version 6.3 or later.

Step 4 Enter a size of the queue for storing syslog messages on the security appliance when syslog server is busy in the **Message queue size (messages)** field. 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).

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 Firepower Threat Defense device and the syslog server.

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

The default ports are 514 for UDP, 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).

Note Syslog messages in RFC5424 format, typically displays the priority value (PRI). However, in FMC, only when you enable logging in Cisco EMBLEM format, the PRI value in the syslog messages of the managed FTD is displayed. For more information on PRI, see RFC5424.

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 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 Firepower 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**. If you type in the **diagnostic** interface name, you must also configure an IP address for the Diagnostic interface (edit the device settings from the **Device Management** page and select the **Interfaces** tab). For more information about the management/diagnostic interface, see Diagnostic Interface.

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.

Configure Global 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 Select **Devices** > **Platform Settings** and create or edit the Firepower 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.
- **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**—(Transparent mode only.) 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.

Configure NTP Time Synchronization for Threat Defense

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

The device supports NTPv4.

Note If you are deploying Firepower 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 FMC.

Before you begin

- If your organization has one or more NTP servers that your FTD 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 FMC.

- If you selected **Use the authenticated NTP server only** when configuring NTP server or servers for the FMC, for your devices use only the NTP server or servers that are configured to authenticate with the FMC. (The managed devices will use the same NTP servers as the FMC, 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 Select **Devices** > **Platform Settings** and create or edit the Firepower 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 FMC (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 FMC:
  - The FMC's NTP servers are not reachable by the device.
  - The FMC has no unauthenticated servers.
- **Via NTP from**—If your FMC 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 FMC acts as an NTP server.

Step 4 Click **Save**.

What to do next

- Make sure the policy is assigned to your devices. See Setting Target Devices for a Platform Settings Policy.
- Deploy configuration changes; see Deploy Configuration Changes.
- If your system includes Classic devices, set up time synchronization for those devices. See Synchronize Time on Classic Devices with an NTP Server.

Configure Device Time Zone for Policy Application

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.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit an Firepower 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

- Make sure the policy is assigned to your devices. See Setting Target Devices for a Platform Settings Policy.
- 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.

History for Firepower Threat Defense Platform Settings

Feature	Version	Details
Specify time zone for device	6.6	Specify a local time zone for a managed device, for use in time-based policy application. New screen: **Devices** > **Platform Settings** > **Time Zone** Supported platforms: Firepower Threat Defense
Specify the Management interface for SNMP communication	6.6	You can now select the Management interface for communication between the device and the SNMP management station. New/Modified screen: **Devices** > **Platform Settings** > **SNMP** > **Hosts** Supported platforms: Firepower Threat Defense
Specify SHA256 for SNMPv3 users' authorization algorithm	6.6	You can now select SHA256 for SNMPv3 users' authorization algorithm. New/Modified screen: **Devices** > **Platform Settings** > **SNMP** > **Users** Supported platforms: Firepower Threat Defense

Feature	Version	Details
DES encryption and the MD5 authentication algorithm for SNMPv3 users on Threat Defense have been deprecated	6.5	We recommend that you not use the MD5 authentication algorithm or DES encryption for SNMPv3 users on Firepower 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 previous to 6.5, 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 screen: **Devices** > **Platform Settings** > **SNMP** > **Users** Supported platforms: Firepower Threat Defense
DES encryption and the MD5 authentication algorithm for SNMPv3 users on Threat Defense will soon be deprecated	6.4	We recommend that you not use the MD5 authentication algorithm or DES encryption for SNMPv3 users on Firepower Threat Defense devices, as these will be deprecated in a future Firepower version. New/Modified screen: **Devices** > **Platform Settings** > **SNMP** > **Users** Supported platforms: Firepower Threat Defense
Allow user traffic to pass when TCP syslog server is down	6.3	We recommend that you allow connections through the FTD 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	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	You can now configure external authentication for SSH access to the Firepower Threat Defense using LDAP or RADIUS. New/Modified screen: **Devices** > **Platform Settings** > **External Authentication** Supported platforms: Firepower Threat Defense
Support for UC/APPL compliance mode	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 screen: **Devices** > **Platform Settings** > **UC/APPL Compliance** Supported platforms: Any device

Feature	Version	Details
SSL settings for remote access VPN	6.2.1	The Firepower 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 screen: **Devices** > **Platform Settings** > **SSL** Supported platforms: Firepower Threat Defense
External Authentication for SSH and HTML removed	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 screen: **Devices** > **Platform Settings** > **External Authentication** Supported platforms: Firepower Threat Defense
Firepower Threat Defense support	6.0.1	This feature was introduced. New/Modified screen: **Devices** > **Platform Settings** Supported platforms: Firepower Threat Defense