Cisco Firepower Threat Defense Hardening Guide, Version 7.0

First Published: 2022-04-30

Cisco Firepower Threat Defense Hardening Guide, Version 7.0

Firepower protects your network assets and traffic from cyber threats, but you should also configure Firepower itself so that it is *hardened*—further reducing its vulnerability to cyber attack. This guide addresses hardening your Firepower deployment, with a focus on Firepower Threat Defense (FTD). For hardening information on other components of your Firepower deployment see the following documents:

- *Cisco Firepower Management Center Hardening Guide, Version 7.0*
- *Cisco Firepower 4100/9300 FXOS Hardening Guide*

This guide refers to two different means of configuring an FTD device, but is not intended as a detailed manual for either of the interfaces involved.

- Some FTD configuration settings can be established through the FMC web interface; cross-references for that product refer to the *Firepower Management Center Configuration Guide, Version 7.0* .
- Some FTD configuration settings can be established using the FTD Command Line Interface (CLI). Full information about all CLI commands referenced in this document is available in the *Cisco Firepower Threat Defense Command Reference* .

All feature descriptions within this document refer to Firepower Version 7.0. Not all configuration settings discussed in this manual are available in all Firepower versions. For detailed information about configuring your Firepower deployment, see the Firepower documentation for your version.

Security Certifications Compliance

Your organization might be required to use only equipment and software that comply with security standards established by the U.S. Department of Defense or other governmental certification organizations. Once certified by an appropriate certifying authority, and when configured in accordance with certification-specific guidance documents, Firepower is designed to comply with the following certification standards:

- Common Criteria (CC): a global standard established by the international Common Criteria Recognition Arrangement, defining requirements for security products.
- Department of Defense Information Network Approved Products List (DoDIN APL): a list of products meeting security requirements established by the U.S. Defense Information Systems Agency (DISA).

Note The U.S. Government has changed the name of the Unified Capabilities Approved Products List (UCAPL) to the DODIN APL. References to UCAPL in Firepower documentation and the Firepower Management Center web interface can be interpreted as references to DoDIN APL.

- Federal Information Processing Standards (FIPS) 140: a requirements specification for encryption modules.

Certification guidance documents are available separately once product certifications have completed; publication of this hardening guide does not guarantee completion of any of these product certifications.

The Firepower configuration settings described in this document do not guarantee strict compliance with all current requirements of the certifying entity. For more information on hardening procedures required, refer to the guidelines for this product provided by the certifying entity.

This document provides guidance for increasing the security of your FTD, but some FTD features do not support certification compliance even using the configuration settings described herein. For more information see "Security Certifications Compliance Recommendations" in the *Firepower Management Center Configuration Guide, Version 7.0*. We have endeavored to ensure that this hardening guide and the *Firepower Management Center Configuration Guide, Version 7.0* do not conflict with certification-specific guidance. Should you encounter contradictions between Cisco documentation and certification guidance, use the certification guidance or consult with the system owner.

Monitor Cisco Security Advisories and Responses

The Cisco Product Security Incident Response Team (PSIRT) posts PSIRT Advisories for security-related issues in Cisco products. For less severe issues, Cisco also posts Cisco Security Responses. Security advisories and responses are available at the Cisco Security Advisories and Alerts page. More information about these communication vehicles is available in the Cisco Security Vulnerability Policy.

To maintain a secure network, stay aware of Cisco security advisories and responses. These provide the information you need to evaluate the threats that vulnerabilities pose to your network. Refer to Risk Triage for Security Vulnerability Announcements for assistance with this evaluation process.

Keep the System Up to Date

Cisco periodically releases Firepower software updates to address issues and make improvements. Keeping your system software up to date is essential to maintaining a hardened system. To ensure your system software is properly updated, use the information in the "System Updates" chapter of the *Firepower Management Center Configuration Guide, Version 7.0*, and the *Firepower Management Center Upgrade Guide*.

Cisco also periodically issues updates for the databases Firepower uses to protect your network and assets. To provide optimum protection on FTD devices managed by an FMC, keep the geolocation, intrusion rules, and vulnerabilities databases on the managing FMC up to date. Before you update any component of your Firepower deployment you *must* read the Cisco Firepower Release Notes that accompany the update. These provide critical and release-specific information, including compatibility, prerequisites, new capabilities, behavior changes, and warnings. Some updates may be large and take some time to complete; you should perform updates during periods of low network use to reduce the impact on system performance.

Geolocation Database

Geolocation Database (GeoDB) is a database of geographical data (such as country and city coordinates) and connection-related data (such as Internet service provider, domain name, connection type) associated with routable IP addresses. When Firepower detects GeoDB information that matches a detected IP address, you can view the geolocation information associated with that IP address. To view any geolocation details other than country or continent, you must install the GeoDB on your system.

To update the GeoDB from the FMC web interface, use **System** > **Updates** > **Geolocation Updates**, and choose one of the following methods:

- Update the GeoDB on an FMC with no internet access.
- Update the GeoDB on an FMC with internet access.
- Schedule recurring automatic updates of the GeoDB on an FMC with internet access.

For more information, see "Update the Geolocation Database" in the *Firepower Management Center Configuration Guide, Version 7.0*.

Intrusion Rules

As new vulnerabilities become known, the Cisco Talos Security Intelligence and Research Group (Talos) releases intrusion rule updates (also known as Snort Rules Updates, or SRUs) that you can import onto your FMC, and then implement by deploying the changed configuration to your managed devices. These updates affect intrusion rules, preprocessor rules, and the policies that use the rules.

The FMC web interface provides three approaches to updating the intrusion rules, all under **System** > **Updates** > **Rule Updates**:

- Update intrusion rules on an FMC with no internet access.
- Update intrusion rules on an FMC with internet access.
- Schedule recurring automatic updates of intrusion rules on an FMC with internet access.

For more information, see "Update Intrusion Rules" in the *Firepower Management Center Configuration Guide, Version 7.0*.

You can also import local intrusion rules using **System** > **Updates** > **Rule Updates**. You can create local intrusion rules using the instructions in the Snort users manual (available at http://www.snort.org). Before importing them to your FMC, consult "Best Practices for Importing Local Intrusion Rules" in the *Firepower Management Center Configuration Guide, Version 7.0* and make certain your process for importing local intrusion rules complies with your security policies.

Vulnerabilities Database

Vulnerabilities Database (VDB) is a database of known vulnerabilities to which hosts may be susceptible, as well as fingerprints for operating systems, clients, and applications. The system uses the VDB to help determine whether a particular host increases your risk of compromise.

The FMC web interface offers two approaches to updating the VDB:

- Manually update the VDB (**System** > **Updates** > **Product Updates**).
- Schedule VDB updates (**System** > **Tools** > **Scheduling**).

For more information, see "Update the Vulnerability Database" in the *Firepower Management Center Configuration Guide, Version 7.0*.

Security Intelligence Lists and Feeds

Security Intelligence lists and feeds are collections of IP addresses, domain names, and URLs that you can use to quickly filter traffic that matches an entry on a list or feed.

There are system-provided feeds, and predefined lists. You can also use custom feeds and lists. To view these lists and feeds, choose **Objects > Object Management > Security Intelligence**. As part of system-provided feeds, Cisco provides the following feeds as Security Intelligence objects:

- Security Intelligence feeds are updated regularly with the latest threat intelligence from Talos:
  - Cisco-DNS-and-URL-Intelligence-Feed (under DNS Lists and Feeds)
  - Cisco-Intelligence-Feed (for IP addresses, under Network Lists and Feeds)

  You cannot delete the system-provided feeds, but you can change the frequency of (or disable) their updates. The FMC can now update Cisco-Intelligence-Feed data for every 5 or 15 minutes.
- Cisco-TID-Feed (under Network Lists and Feeds)

  You must enable and configure Threat Intelligence Director to use this feed, which is a collection of TID observables data.

For more information, see "Security Intelligence Lists and Feeds" in the *Firepower Management Center Configuration Guide, Version 7.0*.

Enable CC or UCAPL Mode

To apply multiple hardening configuration changes with a single setting, choose CC or UCAPL mode for the FTD. Apply this setting thorugh the FMC web interface in the FTD platform settings policy, found under **Devices** > **Platform Settings**. The change does not take effect on the FTD until you deploy the new configuration; see “Enable Security Certifications Compliance” in the *Firepower Management Center Configuration Guide, Version 7.0* for full details.

Choosing one of these configuration options puts into effect the changes listed under “Security Certification Compliance Characteristics” in the *Firepower Management Center Configuration Guide, Version 7.0*. Be aware that all appliances in your Firepower deployment should operate in the same security certifications compliance mode.

Caution After you enable this setting, you cannot disable it. Consult “Security Certifications Compliance” in the *Firepower Management Center Configuration Guide, Version 7.0* for full information before enabling CC or UCAPL mode. If you need to reverse this setting, contact Cisco TAC for assistance.

Note Enabling security certifications compliance does not guarantee strict compliance with all requirements of the security mode selected. Additional settings recommended to harden your deployment above and beyond those provided by CC or UCAPL modes are described in this document. For full information on hardening procedures required for complete compliance, refer to the guidelines for this product provided by the certifying entity.

Gain Traffic Visibility with NetFlow

Cisco's IOS NetFlow enables you to monitor traffic flows in your network in real time. The FTD device can coordinate with some NetFlow features, such as viewing and resetting runtime counters. (See the **show flow-export counters** and **clear flow-export counters** CLI commands.)

Through the FMC web interface you can disable FTD syslog messages that are redundant with those captured by NetFlow. To do this, create an FTD platform settings policy under **Devices** > **Platform Settings**, and choose **Syslog** from the menu. On the **Syslog Settings** tab check the **NetFlow Equivalent Syslogs** check box (Use the **show logging flow-export-syslogs** CLI command to determine which syslog messages are redundant.)

You can take advantage of these abilities if you configure network devices with NetFlow. Regardless of whether flow information is exported to a remote collector, you can use NetFlow reactively if needed. See "Netflow Data in the Firepower System" in the *Firepower Management Center Configuration Guide, Version 7.0* for more information.

Secure the Local Network Infrastructure

Your Firepower deployment may interact with other network resources for a number of purposes. Hardening these other services can protect your Firepower system as well as all your network assets. To identify everything that needs to be addressed, try diagramming the network and its components, assets, firewall configuration, port configurations, data flows, and bridging points.

Establish and adhere to an operational security process for your network that takes security issues into account.

Secure the Network Time Protocol Server

Synchronizing the system time on the FMC and its managed devices is essential to successful operation of Firepower. We strongly recommend using a secure and trusted Network Time Protocol (NTP) server to synchronize system time on the FMC and the devices it manages.

Configure NTP time synchronization for FTD devices from the FMC web interface by creating an FTD platform settings policy under **Devices** > **Platform Settings**, and choosing the **Time Synchronization** tab within the policy page. For more information, see "Configure NTP Time Synchronization for Threat Defense" in the *Firepower Management Center Configuration Guide, Version 7.0*.

We recommend that you secure the communication with the NTP servers using MD5, SHA-1, or AES-128 CMAC symmetric key authentication.

Caution Unintended consequences may occur when time is not synchronized between the FMC and managed devices. To ensure proper synchronization, configure the FMC and all the devices it manages to use the same NTP server.

Secure the Domain Name System (DNS)

Computers communicating with each other in a networked environment depend on the DNS protocol to provide mapping between IP addresses and host names. Configuring an FTD device to connect with a local Domain Name System to support communication over its management interface is a part of the initial configuration process, described in the Quick Start Guide for your model.

Certain FTD functions that use the data or diagnostic interfaces also use DNS—examples include NTP, access control policies, VPN services provided by the FTD, ping, or traceroute. To configure DNS for the data or diagnostic interfaces, create an FTD platform settings policy under **Devices** > **Platform Settings**, and choose

DNS from the table of contents. For more information, see “Configure DNS” under ”Platform Settings for Firepower Threat Defense” in the *Firepower Management Center Configuration Guide, Version 7.0*.

DNS can be susceptible to specific types of attacks tailored to take advantage of weak points in a DNS server that is not configured with security in mind. Be sure your local DNS server is configured in keeping with industry-recommended best practices for security; Cisco offers guidelines in this document: http://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html.

Secure SNMP Polling and Traps

You can configure an FTD to support SNMP polling and traps as described in “Configure SNMP for Threat Defense” in the *Firepower Management Center Configuration Guide, Version 7.0*. If you choose to use SNMP polling, you should be aware that the SNMP Management Information Base (MIB) contains system details that could be used to attack your deployment, such as contact, administrative, location, and service information; IP addressing and routing information; and transmission protocol usage statistics. Choose configuration options to protect your system from SNMP-based threats.

To configure SNMP features for an FTD device, create an FTD platform settings policy under **Devices** > **Platform Settings**, and choose **SNMP** from the table of contents. For complete instructions, see “Configure SNMP for Threat Defense” in the *Firepower Management Center Configuration Guide, Version 7.0*.

Use the following options to harden SNMP access to the FTD device:

- When creating SNMP users, choose SNMPv3, which supports:
  - Authentication algorithms such as SHA, SHA224, SHA256, and SHA384.
  - Encryption with AES256, AES192, and AES128.
  - Read-only users.
- Create SNMPv3 users with the following options:
  - Choose **Priv** for the **Security Level**.
  - Choose **Encrypted** for the **Encryption Password Type**.

See “Add SNMPv3 Users” in the *Firepower Management Center Configuration Guide, Version 7.0* for full instructions.

Important Although you can establish a secure connection to an SNMP server from Firepower, the authentication module is not FIPS compliant.

Secure Network Address Translation (NAT)

Typically networked computers use Network Address Translation (NAT) for reassigning source or destination IP addresses in network traffic. To protect your Firepower deployment as well as your overall network infrastructure from NAT-based exploits, configure the NAT service in your network in adherence with industry best practices as well as recommendations from your NAT provider.

For information about configuring your Firepower deployment to operate in a NAT environment, see “NAT Environments” in the *Firepower Management Center Configuration Guide, Version 7.0*. Use this information at two stages when establishing your deployment:

- When performing the initial setup for your FMC as described in the Cisco Firepower Management Center Getting Started Guide for your hardware model.
- When registering a managed device to the FMC as described in "Add Devices to the Firepower Management Center" in the *Firepower Management Center Configuration Guide, Version 7.0*.

Secure the FMC and Other Appliances in Your Deployment

Your Firepower deployment includes the FMC and security devices managed by the FMC, each providing different means of access. Managed devices exchange information with the FMC and their security is important to the security of your overall deployment. Analyze the appliances in your deployment and apply hardening configurations as appropriate, such as securing user access and closing unneeded communication ports.

Harden Network Protocol Settings

The FTD device can interact with other network devices using a number of protocols; choose configuration settings for network communications to protect the FTD device as well as the data it sends and receives.

- By default the FTD device allows up to 24 fragments per IP packet, and up to 200 fragments awaiting reassembly. You might need to allow fragments on your network if you have an application that routinely fragments packets, such as NFS over UDP. However, fragmented packets are often used in Denial of Service (DoS) attacks, so we recommend that you do not allow fragments.
  - To configure the fragments settings for an FTD device, create an FTD platform settings policy under **Devices** > **Platform Settings**, and choose **Fragment** from the table of contents.
  - To disallow fragments in the network traffic handled by an FTD device, set the **Chain (Fragment)** option to 1.

  For complete instructions, see "Configure Fragment Handling" in the *Firepower Management Center Configuration Guide, Version 7.0*.
- For FTD devices managed by a Firepower Management Center, HTTPS connections with the FTD can be used only to download packet capture files for troubleshooting.

  Configure FTD devices to allow HTTPS access only for IP addresses that should be allowed to download packet captures. In the FMC web interface create an FTD platform settings policy under **Devices** > **Platform Settings**, and choose **HTTP** from the table of contents. See "Configure HTTP" in the *Firepower Management Center Configuration Guide, Version 7.0* for full instructions.
- By default the FTD can receive ICMP packets on any interface using either IPv4 or IPv6 with two exceptions:
  - The FTD does not respond to ICMP echo requests directed to a broadcast address.
  - The FTD responds only to ICMP traffic sent to the interface that traffic comes in on; you cannot send ICMP traffic through an FTD interface to a far interface.

  To protect an FTD device from ICMP-based attack, you can use ICMP rules to limit ICMP access to selected hosts, networks, or ICMP types. In the FMC web interface, create an FTD platform settings policy under **Devices** > **Platform Settings**, and choose **ICMP** from the table of contents. For details, see "Configure ICMP Access Rules" in the *Firepower Management Center Configuration Guide, Version 7.0*.

- The FTD can be configured to provide DHCP and DDNS services (see “DHCP and DDNS Services for Threat Defense” in the *Firepower Management Center Configuration Guide, Version 7.0*). By their nature these protocols are vulnerable to attack. If you choose to configure your FTD device for DHCP or DDNS it is important to apply industry best practices for security, provide physical protection for your network assets, and harden user access to the FTD device.

Secure VPN Services

You can configure the FTD to provide two kinds of Virtual Private Network (VPN) services:

- Remote Access Virtual Private Network (RA VPN): To secure message transmissions to and from remote clients over RA VPN connections, the FTD can use Transport Layer Security (TLS) or IPsec_IKEv2. Before you deploy an RA VPN configuration to the FTD, the FMC ensures that you meet the criteria described in "AnyConnect Licenses" in the *Firepower Management Center Configuration Guide, Version 7.0*.

  Remote Access VPN on FTD supports AD, LDAP, and RADIUS AAA servers for authentication.

  From 7.0, RA VPN supports local authentication and multi-certificate authentication.

  - Local Authentication: You can use this authentication method as the primary or secondary authentication method, or as a fallback in case the configured remote server can’t be reached. We recommend that you use a strong password for the local authentication. For more information, see "Associating a Local Realm with a Remote Access VPN Policy" in *Firepower Management Center Configuration Guide, Version 7.0*.
  - Multi-certificate Authentication: We recommend that you validate the machine or device certificate to ensure that the device is a corporate-issued device and authenticate the user identity certificate to allow VPN access. Use AnyConnect client for VPN access during SSL or IKEv2 EAP phase. For more information, see "Configuring Multiple Certificate Authentication" in *Firepower Management Center Configuration Guide, Version 7.0*.

- Site-to-site Virtual Private Network – To secure message transmissions to and from remote networks over site-to-site VPN connections, the FTD can use IPSEC_IKEv1 or IPSEC_IKEv2. Depending on your device license, you may be able to apply strong encryption to site-to-site VPN transmissions. Site-to-site VPN with strong encryption requires special licensing; see "Licensing for Export-Controlled Functionality" in the *Firepower Management Center Configuration Guide, Version 7.0*.

  There are two types of site-to-site VPNs: Policy-based (Crypto Map) and Route-based (Virtual Tunnel Interface (VTI)). We recommend that you use the route-based VTI VPN for enhanced security. For more information, see "Site-to-Site VPNs for Firepower Threat Defense" in the *Firepower Management Center Configuration Guide, Version 7.0*.

  When you configure the FTD VPN IKE and IPsec options (**Devices > VPN > Site To Site > Add**, and click **IKE** or **IPsec** tabs), we recommend that you:

  - Choose IKEv2.
  - Use a strong key for the pre-shared key manual key.
  - Use the default IKEv2 policy. For example, AES-GCM-NULL-SHA-LATEST.
  - Check the **Enable Security Association (SA) Strength Enforcement** check box.

    This option ensures that the encryption algorithm used by the child IPsec SA isn’t stronger than the parent IKE SA.

- Check the **Enable Perfect Forward Secrecy** check box.

  This option generates and uses a unique session key for each encrypted exchange. The unique session key protects the exchange from subsequent decryption. If you select this option, select the Diffie-Hellman key derivation algorithm to use when generating the PFS session key from the **Modulus Group** drop-down list.

For more information about the above FTD VPN IKE options, see "Configuring Firepower Threat Defense Site-to-site VPNs" in the *Firepower Management Center Configuration Guide, Version 7.0*.

To configure these services, see “Firepower Threat Defense VPN” in the *Firepower Management Center Configuration Guide, Version 7.0*. Firepower supports a wide range of encryption and hash algorithms, and Diffie-Hellman groups from which to choose. Choosing strong encryption can worsen system performance, so you must find the balance between security and performance that provides sufficient protection without compromising efficiency. For a discussion of the options available and the factors to consider, see “How Secure Should a VPN Connection Be?” in the *Firepower Management Center Configuration Guide, Version 7.0*.

Harden FTD User Access

The FTD supports two types of users:

- Internal users—The device checks a local database for user authentication.
- External users—If the user is not present in the local database, the system queries an external LDAP or RADIUS authentication server.

You might consider establishing user access through an external authentication mechanism such as LDAP or RADIUS, to integrate user management with existing infrastructure in your network environment, or leverage capabilities such as two-factor authentication. Establishing external authentication requires creating an external authentication object within the FMC web interface; external authentication objects can be shared to authenticate external users for the FMC as well as the FTD.

Be aware that using external authentication requires that you configure a Domain Name Server for your deployment. Be sure to follow hardening recommendations for your DNS. (See Secure the Domain Name System (DNS))

This discussion of user management refers to features available in Firepower Version 7.0; not all user account configuration features addressed in this section apply to all Firepower versions. For information specific to your system, see the Firepower documentation for your version.

Firepower Threat Defense devices managed by an FMC provide a single means of user access: a command line interface which can be accessed using an SSH, serial, or keyboard and monitor connection for physical devices. With certain configuration settings in place these users can also access the Linux shell.

Restrict Config Privileges

By default FTD devices provide a single **admin** user with full administrator rights to all FTD CLI commands. This user can create additional accounts and grant them one of two levels of access privilege with the **configure user access** CLI command:

- Basic: the user can use FTD CLI commands that do not affect system configuration
- Config: the user can use all FTD CLI commands, including those that provides significant system configuration abilities.

Consider carefully when assigning Config access rights to an account, and when choosing to which users you grant access to an account with Config access rights.

Restrict Linux Shell Access

The FTD managed by the FMC supports only CLI access through its management interface, using an SSH, serial, or keyboard and monitor connection. This is available to the **admin** account, internal users, and can be made available to external users.

Users with Config level access can use the CLI **expert** command to access the Linux shell.

Caution On all devices, accounts with CLI Config level access or Linux shell access can obtain sudoers privileges in the Linux shell, which can present a security risk. To increase system security, we recommend:

- When giving users access to externally-authenticated accounts on FTD devices keep in mind that all externally authenticated accounts on FTD devices have CLI Config level access.
- Do not add new accounts directly in the Linux shell; on FTD devices create new accounts using only the **configure user add** CLI command.
- Use the FTD CLI command **configure ssh-access-list** to limit the IP addresses from which an FTD device will accept SSH connections on its management interface.

Administrators can also configure the FTD to block all access to the Linux shell using the **system lockdown-sensor** CLI command. Once the system lockdown has completed, any user who logs in to the FTD will have access only to the FTD CLI commands. This can be a significant hardening action, but use it with careful consideration, because it cannot be reversed without a hotfix from Cisco TAC.

Harden Internal User Accounts

When configuring individual internal users, users with Config access can use the **configure user** FTD CLI commands to harden the system against attacks through web interface login mechanisms. The following settings are available:

- Restrict the maximum number of failed logins before a user is locked out and must be reactivated by an administrator (**configure user maxfailedlogins**).
- Enforce a minimum password length (**configure user minpasswdlen**).
- Set the number of days passwords are valid (**configure user aging**).
- Require strong passwords (**configure user strengthcheck**).
- Assign user access privileges appropriate only to the type of access the user requires (**configure user access**).
- Force the user to reset the account password on the next login (**configure user forcereset**).

If your Firepower deployment uses multitenancy, consider the domain to which an FTD device belongs when granting users access to that device.

For more information, see “Domain Management” in the *Firepower Management Center Configuration Guide, Version 7.0*.

Harden External User Accounts

If you choose to use an external server for FTD user authentication, bear in mind that external users always have Config privileges; other user roles are not supported. Configure external authentication for FTD users from the FMC web interface by creating an FTD platform settings policy under **Devices > Platform Settings**, and choosing **External Authentication** from the table of contents. Configuring external user accounts requires establishing a connection with an LDAP or RADIUS server though an external authentication object. For more information, see "Configure External Authentication for SSH" in the *Firepower Management Center Configuration Guide, Version 7.0*.

Important You can set up secure connections with LDAP or RADIUS servers from Firepower, but the authentication module is not FIPS compliant.

- Be aware that all FTD external users have Config access, and unless you block access to the Linux shell with the **system lockdown-sensor** command, these users can gain access to the Linux shell. Linux shell users can gain root privileges, which presents a security risk.
- If you use LDAP for external authentication, under **Advanced Options**, configure TLS or SSL encryption.

Establish Session Timeouts

Limiting the duration of connections to an FTD reduces the opportunity for unauthorized users to exploit unattended sessions.

To set session timeouts on an FTD device, create an FTD platform settings policy under **Devices** > **Platform Settings**, and choose **Timeouts** from the table of contents. See "Configure Global Timeouts" in the *Firepower Management Center Configuration Guide, Version 7.0* for full instructions.

FTD REST API Considerations

The Firepower Threat Defense REST API provides a lightweight interface for third-party applications to view and manage appliance configuration using a REST client and standard HTTP methods. The API is described in the *Cisco Firepower Threat Defense REST API Guide*.

Important Although you can establish secure connections between the FTD and a REST API client using TLS, the authentication module is not FIPS compliant.

Protect Backups

To protect system data and its availability, perform regular backups of your FTD device. The backup function appears under **System** > **Tools** > **Backup/Restore** in the FMC web interface and is described in "Backup Devices Remotely" in the *Firepower Management Center Configuration Guide, Version 7.0*. To restore a saved FTD configuration, use the FTD CLI **restore** command.

The FMC provides the ability to automatically store backups on a remote device. Using this feature is not recommended for a hardened system because the connection between the FMC and the remote storage device cannot be secured.

Secure Data Export

The FTD CLI provides the ability to download certain files from the FTD to a local computer. This capability is provided so you can collect information to provide to Cisco TAC when troubleshooting your system, and should not be used casually. Take precautions to protect any files you download from the FTD; choose the most secure options available when downloading, secure the local computer where you store the data, and use the most secure protocols available when transmitting files to TAC. In particular, be aware of the possible risks when using the following commands:

- **show asp inspect-dp snort queue-exhaustion** [**snapshot** *snapshot_id*] [**export** *location*]

  The **export** option supports TFTP only.

- **file copy** *host_name user_id path filename_1* [*filename_2 ... filename_n*]

  This command transfers files to remote host using unsecured FTP.

- **copy [/noverify] /noconfirm** {**/pcap capture:**/[*buffer_name*] | *src_url* | **running-config** | **startup-config**} *dest_url*

  The following options for *src_url* and *dest_url* provide methods of securing the data copied:

  - Internal flash memory
  - System memory
  - Optional external flash drive
  - HTTPS secured with password
  - SCP secured with password, specifying target interface on SCP server
  - FTP secured with password
  - TFTP secured with password, specifying target interface on TFTP server

  We recommend against using the following *src_url* and *dest_url* options in a hardened system:

  - SMB UNIX server local file system
  - Cluster trace file system. (Systems with security certifications compliance enabled do not support clusters.)

- **cpu profile dump** *dest_url*

  The following options for *dest_url* provide methods of securing the data dump:

  - Internal flash memory
  - Optional external flash drive
  - HTTPS secured with password
  - SMB UNIX server local file system
  - SCP secured with password, specifying target interface on SCP server
  - FTP secured with password
  - TFTP secured with password, specifying target interface on TFTP server

We recommend against using cluster file systems for *src_url* and *dest_url* options in a hardened system.

- **file secure-copy** *host_name user_id path filename_1* [*filename_2 ... filename_n*]

  Copies file(s) to a remote host using SCP.

Secure Syslog

The FTD can send syslog messages to an external syslog server; choose secure options when configuring syslog functionality:

1. Create an FTD platform settings policy under **Devices** > **Platform Settings**, and choose **Syslog** from the table of contents. When adding a syslog server under the **Syslog Servers** tab, be sure to choose the TCP protocol and check the **Enable secure syslog** check box. These options apply to syslog messages generated by the FTD if you do not override them elsewhere in your device configuration.

   Note By default, when secure syslog is enabled, if a syslog server using TCP is down, the FTD will not forv traffic. To override this behavior, check the **Allow user traffic to pass when TCP syslog server is do** checkbox.

2. Configure logging in your access control policies to inherit the logging settings from the platform settings policy. (Under **Policies** > **Access Control** <each policy> **> Logging** check the **Use the syslog settings configured in the FTD Platform Settings policy deployed on the device** checkbox.)

With these two configuration settings in place the FTD syslog behaves as follows:

- The syslog settings in the platform settings policy apply to syslog messages related to device and system health, and network configuration.
- The syslog settings in the platform settings apply to syslogs for connection and security intelligence events *unless* you override the setting for the access control policy in any of the places listed in "Configuration Locations for Syslogs for Configuration and Security Intelligence Events (All Devices)" in the *Firepower Management Center Configuration Guide, Version 7.0*. These overrides do not provide a secure syslog option, so we recommend against using them in a secure environment.
- The syslog settings in the platform settings policy apply to syslogs for intrusion events *unless* you override the setting for the access control policy in any of the places listed in "Configuration Locations for Syslogs for Intrusion Events (FTD 6.3 Devices)" in the *Firepower Management Center Configuration Guide, Version 7.0*. These overrides do not provide a secure syslog option, so we recommend against using them in a secure environment.

Customize the Login Banner

You can configure the FTD device to convey essential information to users when they log in to the CLI. From a security perspective, the login banner should discourage unauthorized access; consider text such as this example:

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

To configure the login banner for an FTD device, create an FTD platform settings policy under **Devices** > **Platform Settings**, and choose **Banner** from the table of contents. See "Configure Banners" in the *Firepower Management Center Configuration Guide, Version 7.0* for full instructions.

Secure Connections to Servers Supporting Network User Authoritative Logins, Awareness, and Control

Firepower identity policies use identity sources to authenticate network users and collect user data for user awareness and control. Establishing user identity sources requires a connection between the FMC or a managed device and one of the following types of servers:

- Microsoft Active Directory
- Linux Open LDAP
- RADIUS

Important Although you can set up a secure connection to LDAP, Microsoft AD, or RADIUS servers from Firepower, the authentication module is not FIPS compliant.

Note If you choose to use LDAP or Microsoft AD for external authentication, review the information in Harden External User Accounts, on page 11.

Note Firepower uses each of these servers to support a different combination of the possible user identity features. For full details, see "About User Identity Sources" in the *Firepower Management Center Configuration Guide, Version 7.0*.

Securing Connections with Active Directory and LDAP Servers

Firepower objects called *realms* describe connection settings associated with a domain on an Active Directory or LDAP server. For full information on configuring realms see "Create and Manage Realms" in the *Firepower Management Center Configuration Guide, Version 7.0*.

When you create a realm (**System** > **Integration** > **Realms** in the FMC web interface) keep the following in mind to secure the connections with AD or LDAP servers:

For realms associated with Active Directory servers:

- Choose strong passwords for the **AD Join Password** and **Directory Password**.
- When adding a directory to an Active Directory realm:
  - Select **STARTTLS** or **LDAPS** for the **Encryption** mode (do not choose **None**).
  - Specify an **SSL Certificate** to use for authentication to the Active Directory domain controller. We recommend using a certificate generated by globally known and trusted certificate authority.

For realms associated with LDAP servers:

- Choose strong passwords for the **Directory Password**.
- When adding a directory to an LDAP realm:
  - Select **STARTTLS** or **LDAPS** for the **Encryption** mode (do not choose **None**).
  - Specify an **SSL Certificate** to use for authentication to the LDAP server. We recommend using a certificate generated by globally known and trusted certificate authority.

Securing Connections with RADIUS Servers

To configure a connection with a RADIUS server, create a RADIUS Server Group object (**Objects** > **Object Management** > **RADIUS Server Group** in the FMC web interface) and add a RADIUS server to the group. To secure the connection with the RADIUS server, choose the following options in the **New RADIUS Server** dialog:

- Supply a **Key** and **Confirm Key** to encrypt data between the managed device and the RADIUS server.
- Specify an interface for the connection that can support secure data transmission.

Note Firepower connects with a RADIUS server for user identity only if a managed FTD device in the deployment is configured to provide Remote Access VPN, which will be used as the user identity source. For information on configuring and securing Remote Access VPN, see Harden Network Protocol Settings.

Secure Certificate Enrollment

You can configure certificate enrollment for FTD over a secure channel. The device uses Enrollment over Secure Transport (EST) to obtain an identity certificate from the CA. EST uses TLS for secure message transport.

To configure EST, choose **Objects > Object Management**, then from the navigation pane choose **PKI > Cert Enrollment**. Click **Add Cert Enrollment** and click the **CA Information** tab. From the **Enrollment Type** drop-down list, choose EST.

If you don’t want FTD to validate the EST server certificate, we recommend that you don’t check the **Ignore EST Server Certificate Validations** check box. By default, FTD validates the EST server certificate. EST enrollment type supports only RSA and ECDSA keys, and doesn’t support EdDSA keys. For more information, see "Certificate Enrollment Object EST Options" in *Firepower Management Center Configuration Guide, Version 7.0*.

On FMC and FTD Versions 7.0 and higher, you can’t enroll certificates with RSA key sizes smaller than 2048 bits and keys using SHA-1. To override these restrictions on FMC 7.0 managing FTD running versions lesser than 7.0, the **Enable Weak-Crypto** option is available (**Devices > Certificates**). By default, the weak-crypto option is disabled. We don’t recommend you to enable weak-crypto keys as these keys aren’t as secure as the ones with higher key sizes. For FMC and FTD versions 7.0 and higher, you can enable weak-crypto to allow validation of peer certificates and so on. However, this configuration doesn’t apply to the certificate enrollment.

Harden Supporting Components

The FTD software depends on complex underlying firmware and operating system software. These underlying software components carry their own security risks that must be addressed:

- Establish an operational security process for your network that takes security issues into account.
- For FTD models 2100, 4100, and 9300 devices, secure the Firepower eXtensible Operating System the FTD runs on; see the *Cisco Firepower 4100/9300 FXOS Hardening Guide*.