

Troubleshooting the System

The following topics describe ways to diagnose problems you may encounter with the Firepower System:

- First Steps for Troubleshooting, on page 1
- System Messages, on page 1
- View Basic System Information, on page 4
- Managing System Messages, on page 4
- Memory Usage Thresholds for Health Monitor Alerts, on page 8
- Disk Usage and Drain of Events Health Monitor Alerts, on page 9
- Health Monitor Reports for Troubleshooting, on page 12
- Advanced Troubleshooting for the Firepower Threat Defense Device, on page 14
- Feature-Specific Troubleshooting, on page 20

First Steps for Troubleshooting

- Before you make changes to try to fix a problem, generate a troubleshooting file to capture the original problem. See Health Monitor Reports for Troubleshooting, on page 12 and its subsections.

  You may need this troubleshooting file if you need to contact Cisco TAC for support.

- Start your investigation by looking at error and warning messages in the Message Center. See System Messages, on page 1

- Look for applicable Tech Notes and other troubleshooting resources under the "Troubleshoot and Alerts" heading on the product documentation page for your product. See Top-Level Documentation Listing Pages for FMC Deployments.

System Messages

When you need to track down problems occurring in the Firepower System, the Message Center is the place to start your investigation. This feature allows you to view the messages that the Firepower System continually generates about system activities and status.

To open the Message Center, click on the System Status icon, located to the immediate right of the Deploy button in the main menu. This icon can take one of the following forms, depending on the system status:

- — Indicates one or more errors and any number of warnings are present on the system.

- — Indicates one or more warnings and no errors are present on the system.
- — Indicates no warnings or errors are present on the system.

If a number is displayed with the icon, it indicates the total current number of error or warning messages.

To close the Message Center, click anywhere outside of it within the Firepower System web interface.

In addition to the Message Center, the web interface displays pop-up notifications in immediate response to your activities and ongoing system activities. Some pop-up notifications automatically disappear after five seconds, while others are "sticky," meaning they display until you explicitly dismiss them by clicking **Dismiss** ( ). Click the **Dismiss** link at the top of the notifications list to dismiss all notifications at once.

Tip Hovering your cursor over a non-sticky pop-up notification causes it to be sticky.

The system determines which messages it displays to users in pop-up notifications and the Message Center based on their licenses, domains, and access roles.

Message Types

The Message Center displays messages reporting system activities and status organized into three different tabs:

Deployments

This tab displays current status related to configuration deployment for each appliance in your system, grouped by domain. The Firepower System reports the following deployment status values on this tab. You can get additional detail about the deployment jobs by clicking **Show History**.

- Running (**Spinning**) — The configuration is in the process of deploying.
- **Success** — The configuration has successfully been deployed.
- **Warning** ( ) — Warning deployment statuses contribute to the message count displayed with the **Warning System Status icon**.
- **Failure** — The configuration has failed to deploy; see Out-of-Date Policies. Failed deployments contribute to the message count displayed with the **Error System Status icon**.

Health

This tab displays current health status information for each appliance in your system, grouped by domain. Health status is generated by health modules as described in About Health Monitoring. The Firepower System reports the following health status values on this tab:

- **Warning** ( ) — Indicates that warning limits have been exceeded for a health module on an appliance and the problem has not been corrected. The Health Monitoring page indicates these conditions with a **Yellow Triangle** ( ). Warning statuses contribute to the message count displayed with the **Warning System Status icon**.
- **Critical** ( ) — Indicates that critical limits have been exceeded for a health module on an appliance and the problem has not been corrected. The Health Monitoring page indicates these conditions

with a **Critical** () icon. Critical statuses contribute to the message count displayed with the **Error System Status icon**.

- **Error** () — Indicates that a health monitoring module has failed on an appliance and has not been successfully re-run since the failure occurred. The Health Monitoring page indicates these conditions with a **Error icon**. Error statuses contribute to the message count displayed with the **Error System Status icon**.

You can click on links in the Health tab to view related detailed information on the Health Monitoring page. If there are no current health status conditions, the Health tab displays no messages.

Tasks

In the Firepower System, you can perform certain tasks (such as configuration backups or update installation) that can require some time to complete. This tab displays the status of these long-running tasks, and can include tasks initiated by you or, if you have appropriate access, other users of the system. The tab presents messages in reverse chronological order based on the most recent update time for each message. Some task status messages include links to more detailed information about the task in question. The Firepower System reports the following task status values on this tab:

- **Waiting**() — Indicates a task that is waiting to run until another in-progress task is complete. This message type displays an updating progress bar.
- **Running** — Indicates a task that is in-progress. This message type displays an updating progress bar.
- **Retrying** — Indicates a task that is automatically retrying. Note that not all tasks are permitted to try again. This message type displays an updating progress bar.
- **Success** — Indicates a task that has completed successfully.
- **Failure** — Indicates a task that did not complete successfully. Failed tasks contribute to the message count displayed with the **Error System Status icon**.
- **Stopped or Suspended** — Indicates a task that was interrupted due to a system update. Stopped tasks cannot be resumed. After normal operations are restored, start the task again.
- Skipped — A process in progress prevented the task from starting. Try again to start the task.

New messages appear in this tab as new tasks are started. As tasks complete (status success, failure, or stopped), this tab continues to display messages with final status indicated until you remove them. Cisco recommends you remove messages to reduce clutter in the Tasks tab as well as the message database.

Message Management

From the Message Center you can:

- Configure pop-up notification behavior (choosing whether to display them).
- Display additional task status messages from the system database (if any are available that have not been removed).
- Remove individual task status messages. (This affects all users who can view the removed messages.)
- Remove task status messages in bulk. (This affects all users who can view the removed messages.)

Tip Cisco recommends that you periodically remove accumulated task status messages from the Task tab to reduce clutter in the display as well the database. When the number of messages in the database approaches 100,000, the system automatically deletes task status messages that you have removed.

View Basic System Information

The About page displays information about your appliance, including the model, serial number, and version information for various components of the Firepower System. It also includes Cisco copyright information.

Procedure

Step 1 Click **Help** in the toolbar at the top of the page.

Step 2 Choose **About**.

View Appliance Information

Procedure

Choose **System** > **Configuration**.

Managing System Messages

Procedure

Step 1 Click System Status to display the Message Center.

Step 2 You have the following choices:

- Click **Deployments** to view messages related to configuration deployments. See Viewing Deployment Messages, on page 5. You must be an Admin user or have the **Deploy Configuration to Devices** permission to view these messages.
- Click **Health** to view messages related to the health of your Firepower Management Center and the devices registered to it. See Viewing Health Messages, on page 6. You must be an Admin user or have the **Health** permission to view these messages.
- Click **Tasks** to view or manage messages related to long-running tasks. See Viewing Task Messages, on page 6 or Managing Task Messages, on page 7. Everyone can see their own tasks. To see the tasks of other users, you must be an Admin user or have the **View Other Users' Tasks** permission.

- Click **Cog** ( ) in the upper right corner of the Message Center to configure pop-up notification behavior. See Configuring Notification Behavior, on page 7.

Viewing Deployment Messages

You must be an Admin user or have the **Deploy Configuration to Devices** permission to view these messages.

Procedure

Step 1 Click System Status to display the Message Center.

Step 2 Click **Deployments**.

Step 3 You have the following choices:

- Click **total** to view all current deployment statuses.
- Click a status value to view only messages with that deployment status.
- Hover your cursor over the time elapsed indicator for a message (for example, **1m 5s**) to view the elapsed time, and start and stop times for the deployment.

Step 4 Click **show deployment history** to view more detailed information about the deployment jobs.

The Deployment History table lists the deployment jobs in the left column in reverse chronological order.

a) Select a deployment job.

The table in the right column shows each device that was included in the job, and the deployment status per device.

b) To view responses from the device, and commands sent to the device during deployment, click download in the **Transcript** column for the device.

The transcript includes the following sections:

- **Snort Apply**—If there are any failures or responses from Snort-related policies, messages appear in this section. Normally, the section is empty.
- **CLI Apply**—This section covers features that are configured using commands sent to the Lina process.
- **Infrastructure Messages**—This section shows the status of different deployment modules.

In the **CLI Apply** section, the deployment transcript includes commands sent to the device, and any responses returned from the device. These response can be informative messages or error messages. For failed deployments, look for messages that indicate errors with the commands. Examining these errors can be particularly helpful if you are using FlexConfig policies to configure customized features. These errors can help you correct the script in the FlexConfig object that is trying to configure the commands.

Note There is no distinction made in the transcript between commands sent for managed features and those generated from FlexConfig policies.

For example, the following sequence shows that the FMC sent commands to configure GigabitEthernet0/0 with the logical name outside. The device responded that it automatically set the security level to 0. Firepower Threat Defense does not use the security level for anything.

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

Related Topics

Deploy Configuration Changes

Viewing Health Messages

You must be an Admin user or have the **Health** permission to view these messages.

Procedure

Step 1 Click System Status to display the Message Center.

Step 2 Click **Health**.

Step 3 You have the following choices:

- Click **total** to view all current health statuses.
- Click on a status value to view only messages with that status.
- Hover your cursor over the relative time indicator for a message (for example, **3 day(s) ago**) to view the time of the most recent update for that message.
- To view detailed health status information for a particular message, click the message.
- To view complete health status on the Health Monitoring page, click **Health Monitor**.

Related Topics

About Health Monitoring

Viewing Task Messages

Everyone can see their own tasks. To see the tasks of other users, you must be an Admin user or have the **View Other Users' Tasks** permission.

Procedure

Step 1 Click System Status to display the Message Center.

Step 2 Click **Tasks**.

Step 3 You have the following choices:

- Click **total** to view all current task statuses.
- Click a status value to view only messages for tasks with the that status.

Note Messages for stopped tasks appear only in the total list of task status messages. You cannot filter on stopped tasks.

- Hover your cursor over the relative time indicator for a message (e.g., **3 day(s) ago**) to view the time of the most recent update for that message.
- Click any link within a message to view more information about the task.
- If more task status messages are available for display, click **Fetch more messages** at the bottom of the message list to retrieve them.

Managing Task Messages

Everyone can see their own tasks. To see the tasks of other users, you must be an Admin user or have the **View Other Users' Tasks** permission.

Procedure

Step 1 Click System Status to display the Message Center.

Step 2 Click Tasks.

Step 3 You have the following choices:

- If more task status messages are available for display, click on **Fetch more messages** at the bottom of the message list to retrieve them.
- To remove a single message for a completed task (status stopped, success, or failure), click on **Remove** (✕) next to the message.
- To remove all messages for all tasks that have completed (status stopped, success, or failure), filter the messages on **total** and click on **Remove all completed tasks**.
- To remove all messages for all tasks that have completed successfully, filter the messages on **success**, and click on **Remove all successful tasks**.
- To remove all messages for all tasks that have failed, filter the messages on **failure**, and click on **Remove all failed tasks**.

Configuring Notification Behavior



Note This setting affects all pop-up notifications and persists between login sessions.

Procedure

Step 1 Click System Status to display the Message Center.

Step 2 Click **Cog** ( ) in the upper right corner of the Message Center.

Step 3 To enable or disable pop-up notification display, click the **Show notifications** slider.

Step 4 Click **Cog** ( ) again to hide the slider.

Step 5 Click System Status again to close the Message Center.

Memory Usage Thresholds for Health Monitor Alerts

The Memory Usage health module compares memory usage on an appliance to the limits configured for the module and alerts when usage exceeds the levels. The module monitors data from managed devices and from the FMC itself.

Two configurable thresholds for memory usage, Critical and Warning, can be set as a percentage of memory used. When these thresholds are exceeded, a health alarm is generated with the severity level specified. However, the health alarm system does not calculate these thresholds in an exact manner.

With high memory devices, certain processes are expected to use a larger percentage of total system memory than in a low memory footprint device. The design is to use as much of the physical memory as possible while leaving a small value of memory free for ancillary processes.

Compare two devices, one with 32 GB of memory and one with 4 GB of memory. In the device with 32 GB of memory, 5% of memory (1.6GB) is a much larger value of memory to leave for ancillary processes than in the device with 4 GB of memory (5% of 4GB = 200MB).

To account for the higher percentage use of system memory by certain processes, the FMC calculates the total memory to include both total physical memory and total swap memory. Thus the enforced memory threshold for the user-configured threshold input can result in a Health Event where the “Value” column of the event does not match the value that was entered to determine the exceeded threshold.

The following table shows examples of user-input thresholds and the enforced thresholds, depending on the installed system memory.

Note The values in this table are examples. You can use this information to extrapolate thresholds for devices that do not match the installed RAM shown here, or you can contact Cisco TAC for more precise threshold calculations.

Table 1: Memory Usage Thresholds Based On Installed RAM

User-input Threshold Value	Enforced Threshold Per Installed Memory (RAM)			
	4 GB	6 GB	32 GB	48 GB
10%	10%	34%	72%	81%

User-input Threshold Value	Enforced Threshold Per Installed Memory (RAM)			
	4 GB	6 GB	32 GB	48 GB
20%	20%	41%	75%	83%
30%	30%	48%	78%	85%
40%	40%	56%	81%	88%
50%	50%	63%	84%	90%
60%	60%	70%	88%	92%
70%	70%	78%	91%	94%
80%	80%	85%	94%	96%
90%	90%	93%	97%	98%
100%	100%	100%	100%	100%

Disk Usage and Drain of Events Health Monitor Alerts

The Disk Usage health module compares disk usage on a managed device's hard drive and malware storage pack to the limits configured for the module and alerts when usage exceeds the percentages configured for the module. This module also alerts when the system excessively deletes files in monitored disk usage categories, or when disk usage excluding those categories reaches excessive levels, based on module thresholds.

This topic describes the symptoms and troubleshooting guidelines for two health alerts generated by the Disk Usage health module:

- Frequent Drain of Events
- Drain of Unprocessed Events

The disk manager process manages the disk usage of a device. Each type of file monitored by the disk manager is assigned a silo. Based on the amount of disk space available on the system the disk manager computes a High Water Mark (HWM) and a Low Water Mark (LWM) for each silo.

To display detailed disk usage information for each part of the system, including silos, LWMs, and HWMs, use the **show disk-manager** command.

Examples

Following is an example of the disk manager information.

```
> show disk-manager
Silo                                Used        Minimum     Maximum
Temporary Files                     0 KB        499.197 MB  1.950 GB
Action Queue Results                0 KB        499.197 MB  1.950 GB
User Identity Events                0 KB        499.197 MB  1.950 GB
UI Caches                           4 KB        1.462 GB    2.925 GB
Backups                             0 KB        3.900 GB    9.750 GB
```

```
Updates                                 0 KB        5.850 GB    14.625 GB
Other Detection Engine                  0 KB        2.925 GB    5.850 GB
Performance Statistics                  33 KB       998.395 MB  11.700 GB
Other Events                            0 KB        1.950 GB    3.900 GB
IP Reputation & URL Filtering           0 KB        2.437 GB    4.875 GB
Archives & Cores & File Logs            0 KB        3.900 GB    19.500 GB
Unified Low Priority Events             1.329 MB    4.875 GB    24.375 GB
RNA Events                              0 KB        3.900 GB    15.600 GB
File Capture                            0 KB        9.750 GB    19.500 GB
Unified High Priority Events            0 KB        14.625 GB   34.125 GB
IPS Events                              0 KB        11.700 GB   29.250 GB
```

Health Alert Format

When the Health Monitor process on the FMC runs (once every 5 minutes or when a manual run is triggered) the Disk Usage module looks into the diskmanager.log file and, if the correct conditions are met, the respective health alert is triggered.

The structures of these health alerts are as follows:

- Frequent drain of <*SILO NAME*>
- Drain of unprocessed events from <*SILO NAME*>

For example,

- Frequent drain of Low Priority Events
- Drain of unprocessed events from Low Priority Events

It's possible for any silo to generate a *Frequent drain of <SILO NAME>* health alert. However, the most commonly seen are the alerts related to events. Among the event silos, the *Low Priority Events* are often seen because these type of events are generated by the device more frequently.

A *Frequent drain of <SILO NAME>* event has a **Warning** severity level when seen in relation to an event-related silo, because events will be queued to be sent to the FMC. For a non-event related silo, such as the *Backups* silo, the alert has a **Critical** severity level because this information is lost.



Important Only event silos generate a *Drain of unprocessed events from <SILO NAME>* health alert. This alert always has **Critical** severity level.

Additional symptoms besides the alerts can include:

- Slowness on the FMC user interface
- Loss of events

Common Troubleshoot Scenarios

A *Frequent drain of <SILO NAME>* event is caused by too much input into the silo for its size. In this case, the disk manager drains (purges) that file at least twice in the last 5-minute interval. In an event type silo, this is typically caused by excessive logging of that event type.

In the case of a *Drain of unprocessed events of <SILO NAME>* health alert, this can also be caused by a bottleneck in the event processing path.

There are three potential bottlenecks with respect to these Disk Usage alerts:

- Excessive logging — The EventHandler process on FTD is oversubscribed (it reads slower than what Snort writes).
- Sftunnel bottleneck — The Eventing interface is unstable or oversubscribed.
- SFDataCorrelator bottleneck — The data transmission channel between the FMC and the managed device is oversubscribed.

Excessive Logging

One of the most common causes for the health alerts of this type is excessive input. The difference between the Low Water Mark (LWM) and High Water Mark (HWM) gathered from the **show disk-manager** command shows how much space there is available to take on that silo to go from LWM (freshly drained) to the HWM value. If there are frequent drain of events (with or without unprocessed events) the first thing to review is the logging configuration.

- Check for double logging — Double logging scenarios can be identified if you look at the correlator *perfstats* on the FMC:

  ```
  admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
  ```

- Check logging settings for the ACP — Review the logging settings of the Access Control Policy (ACP). If logging both "Beginning" and "End" of connection, log only the end as it will include everything included when the beginning is logged as well as reduce the amount of events.

  Ensure that you follow the best practices described in Best Practices for Connection Logging.

Communications Bottleneck – Sftunnel

Sftunnel is responsible for encrypted communications between the FMC and the managed device. Events are sent over the tunnel to the FMC. Connectivity issues and/or instability in the communication channel (sftunnel) between the managed device and the FMC can be due to:

- Sftunnel is down or is unstable (flaps).

  Ensure that the FMC and the managed device have reachability between their management interfaces on TCP port 8305.

  The sftunnel process should be stable and should not restart unexpectedly. Verify this by checking the **/var/log/message** file and search for messages that contain the ***sftunneld*** string.

- Sftunnel is oversubscribed.

  Review trend data from the Heath Monitor and look for signs of oversubscription of the FMC's management interface, which can be a spike in management traffic or a constant oversubscription.

  Use as a secondary management interface for Firepower-eventing. To use this interface, you must configure its IP address and other parameters at the FTD CLI using the **configure network management-interface** command.

Communications Bottleneck – SFDataCorrelator

The SFDataCorrelator manages data transmission between the FMC and the managed device; on the FMC, it analyzes binary files created by the system to generate events, connection data, and network maps. The first step is to review the **diskmanager.log** file for important information to be gathered, such as:

- The frequency of the drain.
- The number of files with Unprocessed Events drained.
- The occurrence of the drain with Unprocessed Events.

Each time the disk manager process runs it generates an entry for each of the different silos on its own log file, which is located under **[/ngfw]/var/log/diskmanager.log**. Information gathered from the diskmanager.log (in CSV format) can be used to help narrow the search for a cause.

Additional troubleshooting steps:

- The command **stats_unified.pl** can help you to determine if the managed device does have some data which needs to be sent to FMC. This condition can happen when the managed device and the FMC experience a connectivity issue. The managed device stores the log data onto a hard drive.

  ```
  admin@FMC:~$ sudo stats_unified.pl
  ```

- The **manage_proc.pl** command can reconfigure the correlator on the FMC side.

  ```
  root@FMC:~# manage_procs.pl
  ```

Before You Contact Cisco Technical Assistance Center (TAC)

It is highly recommended to collect these items before you contact Cisco TAC:

- Screenshots of the health alerts seen.
- Troubleshoot file generated from the FMC.
- Troubleshoot file generated from the affected managed device.

  Date and Time when the problem was first seen.

- Information about any recent changes done to the policies (if applicable).

  The output of the stats_unified.pl command as described in the Communications Bottleneck — SFDataCorrelator, on page 11.

Health Monitor Reports for Troubleshooting

In some cases, if you have a problem with your appliance, Support may ask you to supply troubleshooting files to help them diagnose the problem. The system can produce troubleshooting files with information targeted to specific functional areas, as well as advanced troubleshooting files you retrieve in cooperation with Support. You can select any of the options listed in the table below to customize the contents of a troubleshooting file for a specific function.

Note that some options overlap in terms of the data they report, but the troubleshooting files will not contain redundant copies, regardless of what options you select.

Table 2: Selectable Troubleshoot Options

This option...	Reports...
Snort Performance and Configuration	data and configuration settings related to Snort on the appliance

This option...	Reports...
Hardware Performance and Logs	data and logs related to the performance of the appliance hardware
System Configuration, Policy, and Logs	configuration settings, data, and logs related to the current system configuration of the appliance
Detection Configuration, Policy, and Logs	configuration settings, data, and logs related to detection on the appliance
Interface and Network Related Data	configuration settings, data, and logs related to inline sets and network configuration of the appliance
Discovery, Awareness, VDB Data, and Logs	configuration settings, data, and logs related to the current discovery and awareness configuration on the appliance
Upgrade Data and Logs	data and logs related to prior upgrades of the appliance
All Database Data	all database-related data that is included in a troubleshoot report
All Log Data	all logs collected by the appliance database
Network Map Information	current network topology data

Producing Troubleshooting Files for Specific System Functions

You can generate and download customized troubleshooting files that you can send to Support.

In a multidomain deployment, you can generate and download troubleshooting files for devices in descendant domains.

Caution Generating troubleshooting files for lower-memory devices can trigger Automatic Application Bypass (AAB) when AAB is enabled, At a minimum, triggering AAB restarts the Snort process, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See Snort® Restart Traffic Behavior for more information. In some such cases, triggering AAB can render the device temporarily inoperable. If inoperability persists, contact Cisco Technical Assistance Center (TAC), who can propose a solution appropriate to your deployment. Susceptible devices include Firepower 7010, 7020, and 7030; ASA 5506-X, 5508-X, 5516-X, 5512-X , 5515-X, and 5525-X; NGIPSv.

Before you begin

You must be an Admin, Maintenance, Security Analyst, or Security Analyst (Read Only) user to perform this task.

Procedure

Step 1 Perform the steps in Viewing Appliance Health Monitors.

Step 2 Click **Generate Troubleshooting Files.**

Step 3 Choose All Data to generate all possible troubleshooting data, or check individual boxes as described in Viewing Task Messages, on page 6.

Step 4 Click **OK.**

Step 5 View task messages in the Message Center; see Viewing Task Messages, on page 6.

Step 6 Find the task that corresponds to the troubleshooting files you generated.

Step 7 After the appliance generated the troubleshooting files and the task status changes to `Completed`, click **Click to retrieve generated files**.

Step 8 Follow your browser's prompts to download the file. (The troubleshooting files are downloaded in a single `.tar.gz` file.)

Step 9 Follow the directions from Support to send the troubleshooting files to Cisco.

Downloading Advanced Troubleshooting Files

In a multidomain deployment, you can generate and download troubleshooting files for devices in descendant domains. You can download files from the Firepower Management Center only from the Global domain.

Before you begin

You must be an Admin, Maintenance, Security Analyst, or Security Analyst (Read Only) user to perform this task.

Procedure

Step 1 View the health monitor for the appliance; see Viewing Appliance Health Monitors.

Step 2 Click **Advanced Troubleshooting.**

Step 3 In **File Download**, enter the file name supplied by Support.

Step 4 Click **Download.**

Step 5 Follow your browser's prompts to download the file.

Note For managed devices, the system renames the file by prepending the device name to the file name.

Step 6 Follow the directions from Support to send the troubleshooting files to Cisco.

Advanced Troubleshooting for the Firepower Threat Defense Device

You can use Packet Tracer and Packet Capture features for performing an in-depth troubleshooting analysis on a Firepower Threat Defense device. Packet-tracer allows a firewall administrator to inject a virtual packet into the security appliance and track the flow from ingress to egress. Along the way, the packet is evaluated against flow and route lookups, ACLs, protocol inspection, NAT, and intrusion detection. The power of the utility comes from the ability to simulate real-world traffic by specifying source and destination addresses

with protocol and port information. Packet capture is available with the trace option, which provides you with a verdict as to whether the packet is dropped or successful.

For more information about the troubleshooting files, see Downloading Advanced Troubleshooting Files, on page 14.

Using the Firepower Threat Defense CLI from the Web Interface

You can execute selected Firepower Threat Defense command line interface (CLI) commands from the Firepower Management Center web interface. These commands are **ping**, **traceroute**, and **show** (except for **show history** and **show banner**).

In a multidomain deployment, you can enter Firepower Threat Defense CLI commands through the Firepower Management Center web interface for managed devices in descendant domains.

Note In deployments using Firepower Management Center high availability, this feature is available only in the active Firepower Management Center.

For more information on the Firepower Threat Defense CLI, see the *Command Reference for Firepower Threat Defense*.

Before you begin

You must be an Admin, Maintenance, or Security Analyst user to use the CLI.

Procedure

Step 1 View the health monitor for the appliance; see Viewing Appliance Health Monitors.

Step 2 Click **Advanced Troubleshooting.**

Step 3 Click **Threat Defense CLI**.

Step 4 From the **Command** drop-down list, select a command.

Step 5 Optionally, enter command parameters in the **Parameters** text box.

Step 6 Click **Execute** to view the command output.

Packet Tracer Overview

Using the packet tracer, you can test your policy configuration by modeling a packet based on source and destination addressing, and protocol characteristics. The trace does a policy lookup to test access rules, NAT, routing, access policies and rate limiting policies, to check if the packet would be permitted or denied. The packet flow is simulated based on interfaces, source address, destination address, ports and protocols. By testing packets this way, you can see the results of your policies and test whether the types of traffic you want to allow or deny are handled as desired. Besides verifying your configuration, you can use the tracer to debug unexpected behavior, such as packets being denied when they should be allowed. To simulate the packet fully, packet tracer traces the data path; slow-path and fast-path modules. Processing is transacted based on per-session

and per-packet basis. Tracing packets and capture with trace log the tracing data on per packet basis when the Next-Generation Firewall (NGFW) processes packets per-session or per-packet.

Use the Packet Tracer

You can use packet tracer on Firepower Threat Defense devices. You must be an Admin or Maintenance user to use this tool.

Procedure

Step 1 On the Firepower Management Center, choose **Devices** > **Device Management**.

Step 2 Select a device.

Step 3 Click troubleshooting.
The **Health Monitor** page appears.

Step 4 Click **Advanced Troubleshooting**.

Step 5 Click **Packet Tracer**.

Step 6 Select the **Packet type** for the trace, and specify the protocol characteristics:

- **ICMP**—Enter the ICMP type, ICMP code (0-255), and optionally, the ICMP identifier.
- **TCP**/**UDP**/**SCTP**—Enter the source and destination port numbers.
- **IP**—Enter the protocol number, 0-255.

Step 7 Select the ingress **Interface** for the packet trace.

Step 8 Select the **Source** type for the packet trace, and enter the source IP address.

Source and destination types include IPv4, IPv6, and fully-qualified domain names (FQDN). You can specify IPv4 or IPv6 addresses and FQDN, if you use Cisco TrustSec.

Step 9 Select the **Source Port** for the packet trace.

Step 10 Select the **Destination** type for the packet trace, and enter the destination IP address.

Step 11 Select the **Destination Port** for the packet trace.

Step 12 Optionally, if you want to trace a packet where the Security Group Tag (SGT) value is embedded in the Layer 2 CMD header (TrustSec), enter a valid **SGT number**.

Step 13 If you want packet tracer to enter a parent interface, which is later redirected to a sub-interface, enter a **VLAN ID**.

This value is optional for non-sub-interfaces only, since all the interface types can be configured on a sub-interface.

Step 14 Specify a **Destination MAC Address** for the packet trace.

If the Firepower Threat Defense device is running in transparent firewall mode, and the ingress interface is VTEP, **Destination MAC Address** is required if you enter a value in **VLAN ID**. Whereas if the interface is a bridge group member, **Destination MAC Address** is optional if you enter a **VLAN ID** value, but required if you do not enter a **VLAN ID** value.

If the Firepower Threat Defense is running in routed firewall mode, **VLAN ID** and **Destination MAC Address** are optional if the input interface is a bridge group member.

Step 15 Select the **Output Format** for the packet logs.

Step 16 Click **Start**.

Packet Capture Overview

The packet capture feature with trace option allows real packets that are captured on the ingress interface to be traced through the system. The trace information is displayed at a later stage. These packets are not dropped on the egress interface, as they are real data-path traffic. Packet capture for Firepower Threat Defense devices supports troubleshooting and analysis of data packets.

Once the packet is acquired, Snort detects the tracing flag that is enabled in the packet. Snort writes tracer elements, through which the packet traverses. Snort verdict as a result of capturing packets can be one of .the following:

Table 3: Snort Verdicts

Verdict	Description
Pass	Allow analyzed packet.
Block	Packet not forwarded.
Replace	Packet modified.
White list	Flow passed without inspection.
Blacklist	Flow was blocked.
Ignore	Flow was blocked; occurs only for sessions with flows blocked on passive interfaces.
Retry	Flow is stalled, waiting on a enamelware or URL category/reputation query. In the event of a timeout, processing continues with an unknown result: in the case of enamelware, the file is allowed; in the case of URL category/reputation, AC rule lookup continues with an uncategorized and unknown reputation.

Based on the Snort verdict, the packets are dropped or allowed. For example, the packet is dropped if the Snort verdict is **Blacklist**, and the subsequent packets in the session are dropped before reaching Snort. When the Snort verdict is **Block** or **Blacklist**, the **Drop Reason** can be one of the following:

Table 4: Drop Reasons

Blocked or Flow Blocked by...	Cause
Snort	Snort is unable to process the packet, erg., snort can’t decode packet since it is corrupted or has invalid format.

Blocked or Flow Blocked by...	Cause
the App Id preprocessed	App Id module/preprocessed does not block packet by itself; but this may indicate that App Id detection causes other module (erg., firewall) to match a blocking rule.
the SSL preprocessed	There is a block/reset rule in SSL policy to match the traffic.
the firewall	There is a block/reset rule in firewall policy to match the traffic.
the captive portal preprocessed	There is a block/reset rule using the identity policy to match the traffic.
the safe search preprocessed	There is a block/reset rule using the safe-search feature in firewall policy to match the traffic.
the SI preprocessed	There is a block/reset rule a in Security Intelligence tab of AC Policy to block the traffic, erg., DNS or URL SI rule.
the filterer preprocessed	There is a block/reset rule in filterer tab of AC policy to match the traffic.
the stream preprocessed	There is an intrusion rule blocking/reset stream connection, erg., blocking when TCP normalization error.
the session preprocessed	This session was already blocked earlier by some other module, so session preprocessed is blocking further packets of the same session.
the fragmentation preprocessed	Blocking because earlier fragment of the data is blocked.
the snort response preprocessed	There is a react snort rule, erg., sending a response page on a particular HTTP traffic.
the snort response preprocessed	There is a snort rule to send custom response on packets matching conditions.
the reputation preprocessed	Packet matches a reputation rule, erg., blocking a given IP address.
the x-Link2State preprocessed	Blocking due to buffer overflow vulnerability detected in SMTP.
back orifice preprocessed	Blocking due to detection of back orifice data.
the SMB preprocessed	There is a snort rule to block SMB traffic.
the file process preprocessed	There is file policy that blocks a file, erg., enamelware blocking.

Blocked or Flow Blocked by...	Cause
the IPS preprocessed	There is a snort rule using IPS, erg., rate filtering.

The **file-size** option is used when you need to capture packets with the size limit more than 32 MB.

Use the Capture Trace

Packet capture data includes information from Snort and preprocessors about verdicts and actions the system takes while processing a packet. Multiple packet captures are possible at a time. You can configure the system to modify, delete, clear, and save captures.



Note Capturing packet data requires packet copy. This operation may cause delays while processing packets and may also degrade the packet throughput. Cisco recommends that you use packet filters to capture specific traffic data.

The saved traffic data can be downloaded in *pcap* or *ASCII* file formats.

Before you begin

You can use packet capture on Firepower Threat Defense devices. You must be an Admin or Maintenance user to use this tool.

Procedure

Step 1 On the Firepower Management Center, choose **Devices** > **Device Management**.

Step 2 Select a device.

Step 3 Click troubleshooting.
The **Health Monitor** page appears.

Step 4 Click **Advanced Troubleshooting**.

Step 5 Select **Capture w/Trace**.

Step 6 Click **Add Capture**.

Step 7 Enter the **Name** for capturing the trace.

Step 8 Select the **Interface** for the capturing the trace.

Step 9 Specify **Match Criteria** details:

a) Select the **Protocol**.
b) Enter the IP address for the **Source Host**.
c) Enter the IP address for the **Destination Host**.
d) (Optional) Check **SGT number** check box, and enter a Security Group Tag (SGT).

Step 10 Specify **Buffer** details:

a) (Optional) Enter a maximum **Packet Size**.
b) (Optional) Enter a minimum **Buffer Size**.
c) Select either **Continuous Capture** if you want the traffic captured without interruption, or **Stop when full** if you want the capture to stop when the maximum buffer size is reached.
d) Select **Trace** if you want to capture the details for each packet.

e) (Optional) Check **Trace Count** check box. Default value is 50. You can enter values in the range of 1-1000.

Step 11 Click **Save**.

Feature-Specific Troubleshooting

See the following table for feature-specific troubleshooting tips and techniques.

Table 5: Feature-Specific Troubleshooting Topics

Feature	Relevant Troubleshooting Information
Application control	Troubleshoot Application Control Rules
LDAP external authentication	Troubleshooting LDAP Authentication Connections
Licensing	Troubleshoot FTD Licensing
FMC high availability	Troubleshooting Firepower Management Center High Availability
7000 and 8000 Series device high-availability state sharing	Device High Availability State Sharing Statistics for Troubleshooting
User rule conditions	Troubleshoot User Control
User identity sources	Troubleshoot the User Agent Identity Source Troubleshoot the ISE/ISE-PIC or Cisco TrustSec Issues Troubleshoot the TS Agent Identity Source Troubleshoot the Captive Portal Identity Source Troubleshoot the Remote Access VPN Identity Source Troubleshooting LDAP Authentication Connections
URL filtering	Troubleshoot URL Filtering
Realms and user data downloads	Troubleshoot Realms and User Downloads
Network discovery	Troubleshooting Your Network Discovery Strategy
Custom Security Group Tag (SGT) rule conditions	Troubleshooting Custom SGT Conditions
SSL rules	Troubleshoot TLS/SSL Rules
Cisco Threat Intelligence Director (TID)	Troubleshoot Threat Intelligence Director
Firepower Threat Defense syslog	About Configuring Syslog
Intrusion performance statistics	Intrusion Performance Statistic Logging Configuration

Feature	Relevant Troubleshooting Information
7000 and 8000 Series NGIPSv ASA with FirePOWER Services	generate-troubleshoot (Command in the Command Line Interface (CLI))