

Troubleshooting

The following topics describe ways to diagnose problems you may encounter:

- Guidelines and best practices for troubleshooting, on page 1
- System messages, on page 2
- View basic system information, on page 4
- View appliance information, on page 5
- Manage system messages, on page 5
- Memory usage thresholds for health monitor alerts, on page 9
- Fault monitoring, on page 11
- Disk usage and drain of events health monitor alerts, on page 14
- Clear disk space, on page 17
- Health monitor reports for troubleshooting, on page 18
- Troubleshooting syslogs in the Secure Firewall Management Center, on page 20
- Enhanced troubleshooting experience using Cisco RADKit integration, on page 22
- General troubleshooting, on page 26
- Connection-based troubleshooting, on page 26
- Advanced troubleshooting for the Secure Firewall Threat Defense device, on page 27
- Feature-specific troubleshooting, on page 38

Guidelines and best practices for troubleshooting

Follow these best practices to troubleshoot system issues effectively and prepare for potential support escalation:

- 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 18 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 2

- Look for applicable Tech Notes and other troubleshooting resources under the "Troubleshoot and Alerts" heading on the product documentation page for your product.

- During the troubleshooting process, as several commands are executed simultaneously, the CPU usage becomes high. We recommend that you perform troubleshooting during periods of lower network traffic and fewer users.

- The time taken to troubleshoot the system depends on the configuration settings and the number of devices configured. This duration can range from nine to sixty minutes.

System messages

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

Message center access and display

To open the Message Center, click the System Status icon, next to the **Deploy** button on the home page. This icon changes based on the system status:

- **Error** ( ): Indicates one or more errors and any number of warnings are present on the system.
- **Warning** ( ): Indicates one or more warnings and no errors are present on the system.
- **Success** ( ): 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 web interface.

The web interface also displays pop-up notifications in response to your actions 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.

The Message Center organizes system status messages into these tabs:

- **Deployments**: Displays current status related to configuration deployment for each appliance in your system, grouped by domain.
- **Upgrades**: Displays the current status related to software upgrade tasks for the managed devices.
- **Health**: Displays current health status information for each appliance in your system, grouped by domain.
- **Tasks**: Displays the status of long-running tasks such as configuration backups, update installation, etc,.

Deployment status

The system reports these deployment statuses. 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. Failed deployments contribute to the message count displayed with the **Error System Status icon**.

Upgrade status

The system reports these upgrade status values on the Upgrade tab:

- **In progress**: Indicates that the upgrade task is in progress.
- **Completed**: Indicates that the software upgrade task is completed successfully.
- **Failed**: Indicates that the software upgrade task has failed to complete.

Health status

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 Health monitoring in Firewall Management Center. The 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 an **Error icon**. Error statuses contribute to the message count displayed with the **Error System Status icon**.

You can click the 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.

Task status

Certain tasks (such as configuration backups or update installation) 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 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. We recommend you remove messages to reduce clutter in the Tasks tab as well as the message database.

Message management

From the Message Center you can perform these tasks:

- Choose to display pop-up notifications.
- Display more task status messages from the system database (if any are available that have not been removed).
- Download a report of all the task manager notifications.
- 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 both the display and 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 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 **Administration** > **Configuration**.

Manage system messages

Use the Message Center to monitor and manage different types of system notifications including configuration deployments, device upgrades, system health alerts, and long-running tasks.

Procedure

Step 1 Click **Notifications** to display the Message Center.

Step 2 Choose from the available notification types:

- Click **Deployments** to view messages related to configuration deployments. See View deployment messages, on page 6. You must be an Admin user or have the **Deploy Configuration to Devices** permission to view these messages.
- Click **Upgrades** to view messages related to device upgrade tasks. See Viewing Upgrade Messages. See Viewing Upgrade Messages. You must be an Admin user or have **Updates** permission to view these messages.

  New, suggested upgrade version is displayed. You can choose to set reminder or view more information using the **Remind Me** or **Details** options respectively.

- Click **Health** to view messages related to the health of your Firewall Management Center and the devices registered to it. See View health messages, on page 7. You must be an Admin user or have the **Health** permission to view these messages.

  You can navigate to the Health Monitor page by clicking the **Health monitor** link.

- Click **Tasks** to view or manage messages related to long-running tasks. See View task messages, on page 8 or Manage task messages, on page 9. 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. You can remove the completed tasks from the notification by clicking the **Remove completed tasks** link.

- Click the **Download Report** icon to generate a report of all the notifications in the task manager. Choose **Download CSV** or **Download PDF** to download the report.
- Click **Show Notifications** slider to enable or disable pop-up notification display.

View deployment messages

View deployment messages to monitor the status of configuration deployments and access detailed deployment history for troubleshooting.

If you are an Admin user or have the **Deploy Configuration to Devices** permission, you can view deployment messages and history.

Complete these steps to view deployment messages and deployment history:

Procedure

Step 1 Click **Notifications** 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, this 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 lists commands sent to the device as well as any responses returned from the device. These responses can be informative messages or error messages. If a deployment fails, review the error messages to understand which commands were problematic. If you

use FlexConfig policies to configure features, these messages can help you identify and correct issues in your FlexConfig scripts.

Note The transcript does not distinguish between commands sent for managed features and those generated from FlexConfig policies.

For example, this sequence shows that the Firewall Management Center sent commands to configure GigabitEthernet0/0 with the logical name outside. The device responded that it automatically set the security level to 0. The Firewall 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.
```

You can view deployment messages, monitor deployment statuses, and access detailed deployment history, including device transcripts to troubleshoot deployment issues.

View upgrade messages

View and monitor upgrade messages to track the status of current upgrade tasks and access detailed information about upgrade processes.

Only Admin users or users with the **Updates** permission can view these messages.

Procedure

Step 1 Click **Notifications** to display the Message Center.

Step 2 Click **Upgrades**.

Step 3 You can do the following:

- Click **total** to view all current upgrade tasks.
- Click on a status value to see messages with only that status.
- Click **Device Management** for more details on the upgrade task.

View health messages

Monitor system status, identify issues, and access detailed health information for troubleshooting and maintenance.

You must be an Admin user or have the **Health** permission to view health messages. Using the Message Center provides a streamlined way to monitor the system's health and filter messages by severity.

Complete these steps to view health messages in the Message Center:

Procedure

Step 1 Click **Notifications** to display the Message Center.

Step 2 Click **Health**.

Step 3 You have the following choices:

- Click **total** to view all current health statuses. You also see the severity levels: warning, critical, and error.
- 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**.

You can now view, filter, and access detailed health status messages for monitoring and troubleshooting your system.

View task messages

View task status messages to monitor the progress and completion status of various system tasks.

You can view your tasks. But, 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 **Notifications** to display the Message Center.

Step 2 Click **Tasks**.

Step 3 You have these choices:

- Click **total** to view all current task statuses. To view tasks based on a specific status—such as waiting, running, retrying, success, or failure—click its corresponding label.
- Click a status value to view only messages for tasks with 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.

Manage task messages

You can view your tasks. But, 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 **Notifications** to display the Message Center.

Step 2 Click **Tasks**.

Step 3 Select one of the available management options:

- If more task status messages are available for display, click **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 **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 **Remove all completed tasks**.
- To remove all messages for all tasks that have completed successfully, filter the messages on **success**, and click **Remove all successful tasks**.
- To remove all messages for all tasks that have failed, filter the messages on **failure**, and click **Remove all failed tasks**.

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 Firewall Management Center 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 Firewall Management Center 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.

Beginning with version 7.4.1, the memory usage health module calculates memory usage by taking into account the free memory available, swap memory available, and buffer cache. To avoid premature memory usage health alerts, it is recommended not to exceed the warning and critical alarm thresholds of 88% and 90%, respectively.

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%
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%

Caution If the Firewall Management Center reaches a critical system memory condition, the system might terminate the processes that use high memory or reboot the Firewall Management Center if memory usage remains high.

Fault monitoring

The Firewall Threat Defense fault manager monitors the device for faults such as block depletion and memory buffer depletion. It also recovers the device when a fault occurs. You can configure fault-monitor using the FlexConfig commands to monitor the device and recover it from faults. To learn how to create and apply the FlexConfig policies on the devices, see FlexConfig Policies chapter in *Cisco Secure Firewall Management Center Device Configuration Guide*.

Block depletion monitoring in cluster devices

When block depletion is detected on a node within a cluster, the affected node is transitioned to a disabled state and removed from the cluster. With block depletion monitoring enabled, the system continuously checks for block recovery. Once recovery is detected, the fault-monitoring service notifies the cluster that the fault condition has been resolved. The previously disabled node then attempts to rejoin the cluster.



Note When block depletion is detected on a control node, it leaves the cluster, force crashes, and then reloads; one of the data node becomes the control node. After reloading, the node rejoins the cluster as a data node. If a data node is detected with block depletion, it leaves the cluster, force crashes and reloads to rejoin the cluster as a data node.

Block depletion monitoring in HA units

In an HA, when block depletion is observed on the device, the active device is moved to failed state, allowing the standby device to take over. This switchover reduce downtime and packet drops. The failed peer sends logs, and `show tech` command is used to diagnose and debug the cause for the block depletion.

Block depletion troubleshooting log

When block depletion is detected, a compressed troubleshooting file is created in the `disk0:/FaultMonitor/` directory. The filename follows the format *bdep-ts_YYYYMMDD_HHMMSS_TIMEZONE.log*. Older files are purged automatically, retaining only the latest 10 compressed files.

How to configure block depletion monitoring

To configure block depletion monitoring, create a FlexConfig policy, apply it to the target devices (control nodes in case of clusters), and deploy. Create FlexConfig policy objects for these commands:

To do this	Use this command
Disable block-depletion monitoring	`fault-monitor` `  no block-depletion`
Enable block-depletion monitoring	`fault-monitor` `  block-depletion`
Change recovery action to none[1]	`fault-monitor` `  block-depletion recovery-action none`

To do this	Use this command

Modify monitoring interval	`fault-monitor block-depletion monitor-interval <duration>`
	Default value is 60 seconds. You can enter a value between 30 and 300.
	Example
	`fault-monitor block-depletion monitor-interval 60`

[1]To configure the recovery option on the device, define the FlexConfig object to reload or not. The default recovery action is **reload**, because when the device detects a block pool depletion, device reload is the only way to recovery. Avoiding device reload using the **none** option must be used with caution and with guidance from the Cisco TAC team. Typically, **none** is used if there are any false positive block detection or the TAC team needs to collect additional data before device goes for auto reload.

To clear the configuration, use the following Firewall Threat Defense CLI command:

```
clear configure fault-monitor block-depletion
```

Memory buffer monitoring

Provides monitoring for pre-allocated memory buffer pools on DPDK-based platform devices to identify and report critical faults, collect troubleshooting diagnostics, and reload the device when MBUF depletion occurs.

Memory buffer monitor on DPDK-based platform devices

On Data Plane Development Kit (DPDK)-based platform devices such as Secure Firewall 200 and 1200 series (excluding Virtual platforms (ARM64_VIRTUAL), SMP (x86), SSP (x86)), packet processing depends on pre-allocated memory buffer (MBUF) pools. If MBUFs are exhausted due to leaks, traffic bursts, or resource non-availability, the incoming packets are dropped without notifications. Therefore, it is necessary to monitor and report MBUFs actively.

You can enable MBUF monitoring under fault-monitor to report a critical fault, collect troubleshooting diagnostics, and optionally reload the device when MBUF depletion is identified. The monitoring timeline and threshold limits are:

Activity	Interval/Frequency
Periodic polling for MBUF depletion detection.	2 seconds
Monitoring window to execute availability check, baseline capture, and sustained depletion confirmation.	(default) 60 seconds, range 30–300
Delay timer after system reboot. This setting enables removal of false positives during initialization after a system reboot.	15 minutes
Cooldown timer for restarting monitoring after a fault is processed.	10 minutes

Activity	Interval/Frequency
Reload cooldown timer to prevent repeated reload loops.	60 minutes

MBUF depletion monitoring in HA units

In a high-availability setup, by default the MBUF is not monitored. However, if the configuration is modified on the active unit, the same is replicated on the standby unit. Thus, when MBUF depletion is detected on the device, the system moves the active device to a failed state to allow the standby device to take over. This switchover reduces downtime and packet loss. The failed peer sends logs for diagnostics. Use the `show block` command to diagnose and debug the cause of block depletion.

MBUF depletion troubleshooting log

When block depletion is detected, a compressed troubleshooting file is created in the `disk0:/FaultMonitor/` directory. The filename follows the format *bdep-ts_YYYYMMDD_HHMMSS_TIMEZONE.log*. Older files are purged automatically, retaining only the latest 10 compressed files.

How to configure MBUF depletion monitoring

To configure MBUF depletion monitoring, create FlexConfig policy, apply to the target devices (control nodes in case of clusters), and deploy. Create FlexConfig policy objects for these commands:

To do this	Use this command
Disable mbuf-depletion monitoring	`fault-monitor` `  no mbuf-depletion`
Enable mbuf-depletion monitoring	`fault-monitor` `  mbuf-depletion`
Change recovery action to none[1]	`fault-monitor` `  mbuf-depletion recovery-action none`

Modify monitoring interval	`fault-monitor`
	`  mbuf-depletion monitor-interval <duration>`
	Default value is 60 seconds. You can enter a value between 30 and 300.
	Example
	`fault-monitor`
	`  mbuf-depletion monitor-interval 60`

[1]To configure the recovery option on the device, define the FlexConfig object to enable or disable reload. The default recovery action is **reload**, because when the device detects a MBUF pool depletion, device reload is the only way to recovery. Avoiding device reload using the **none** option must be used with caution and with guidance from the Cisco TAC team. Typically, **none** is used if there are any false positive MBUF detections or if the TAC team needs to collect additional data before device goes for auto reload.

To clear the configuration, use the following Firewall Threat Defense CLI command:

```
clear configure fault-monitor mbuf-depletion
```

Disk usage and drain of events health monitor alerts

This topic describes the symptoms and troubleshooting guidelines for the Drain of Unprocessed Events health alerts generated by the Disk Usage health module.

Disk usage overview

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.

The disk manager process manages the disk usage of a device. Each type of file monitored by the disk manager is assigned with 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

The 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 Firewall Management Center 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 health alert is triggered.

The structure of the health alert is—Drain of unprocessed events from *SILO NAME* .

For example, Drain of unprocessed events from Low Priority Events.

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

Additional symptoms besides the alerts can include:

- Slowness on the Firewall Management Center user interface
- Loss of events

Common troubleshoot scenarios

A *Drain of unprocessed events of SILO NAME* health alert is 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 Firewall Threat Defense 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 Firewall Management Center 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 drain of unprocessed events, review the logging configuration.

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

  ```
  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 the logging setting includes both "Beginning" and "End" of connection, modify the setting to log only the end to reduce the number 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 Firewall Management Center and the managed device. Events are sent over the tunnel to the Firewall Management Center. Connectivity issues and/or instability in the communication channel (sftunnel) between the managed device and the Firewall Management Center can be due to:

- Sftunnel is down or is unstable (flaps).

  Ensure that the Firewall Management Center 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 Firewall Management Center's management interface, which can be a spike in management traffic or a constant oversubscription.

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

Communications Bottleneck – SFDataCorrelator

The SFDataCorrelator manages data transmission between the Firewall Management Center and the managed device; on the Firewall Management Center, 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 must be sent to Firewall Management Center. This condition can happen when the managed device and the Firewall Management Center experience a connectivity issue. The managed device stores the log data on to a hard drive.

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

- The **manage_proc.pl** command can reconfigure the correlator on the Firewall Management Center side.

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

Before you contact Cisco TAC

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

- Screenshots of the health alert seen.
- Troubleshoot file generated from the Firewall Management Center.
- 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 Communications Bottleneck — SFDataCorrelator, on page 16.

Disk usage for device configuration history files

The Disk Usage health module monitors the size of the device configuration history files on the Firewall Management Center and sends a health alert if the size exceeds the allowed limit. The maximum disk size allowed for storing the device configuration history files is 20 GB. In a Firewall Management Center high-availability deployment, this health alert appears on the standby Firewall Management Center only when high-availability synchronization is paused.

The size of device configuration history files exceeding the allowed limit can cause upgrade readiness failure while upgrading the Firewall Management Center. In a Firewall Management Center high-availability deployment, exceeding the device configuration history file size limit can reduce high-availability synchronization speed.

To resolve the device configuration history files size health alert, choose **Deploy** > **Deployment History** ( ) and click **Deployment Setting**. In the **Deployment Setting** page, reduce the **Number of Versions to Retain**. Reducing the number of versions removes the oldest configuration versions to match the version size you have selected. The **Estimated Configuration Version Size** provides the approximate size for the configuration history files on the Firewall Management Center, based on the number of versions you choose to retain. Change the number of versions using the estimated value to decrease the size of configuration versions below the allowed limit.

For more information, refer to Set the Number of Configuration Versions in *Cisco Secure Firewall Management Center Device Configuration Guide*.

Clear disk space

Low disk space can reduce the performance of the managed Firewall Threat Defense devices. It can also prevent device upgrades and increase the risk of accidentally deleting important files when trying to recover space.

You can free up disk space by removing the following temporary files from your Firewall Threat Defense device:

- **Backup files**: These are the Firewall Threat Defense device backup files. Device backups include only the configuration data. For more information, refer to Backing Up Management Centers or Managed Devices.
- **Content updates**: This includes SRU, VDB, and GeoDB update files. For more information, refer to About System Updates.
- **Troubleshooting files**: These are log files generated for troubleshooting purposes. For more information, refer to Health Monitor Reports for Troubleshooting.

When you clear the disk space, the system retains the latest file and deletes all older files.

Caution Clearing disk space will permanently delete the selected files.

Procedure

Step 1 If Unified Firewall Management is enabled in your organization, choose **Troubleshooting** > **FTD health** > **Monitor**. For classic experience, perform the next step.

Step 2 Choose **Troubleshooting** > **Health** > **Monitor**.

Step 3 In the left navigation pane, click the device for which you want to clear disk space.

Step 4 In the **Disk Usage** widget, click **Clear disk space**.

Step 5 Choose the type of temporary files that you want to remove by checking the corresponding check box.

Step 6 Click **Clear disk space**.

Step 7 Click **Clear** to continue.

Check the message center for the progress of the disk cleanup task. When the task is complete, the **Disk Usage** widget will display the updated storage data.

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 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
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

This option...	Reports...
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

Generate troubleshooting files for specific system functions

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

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 View the device health monitor.

Step 2 Choose **Troubleshooting** > **Health** > **Monitor**.

Step 3 Click the device in the left panel, then **View System & Troubleshoot Details**, and then click **Generate Troubleshooting Files**.

Note

- Troubleshooting files generated from the Firewall Management Center web interface are stored on the Firewall Management Center. Only the latest troubleshooting file for each appliance is stored.
- Troubleshooting files generated from the CLI are stored locally and are not overwritten.
- If you initiate the troubleshooting log generation while one is already in the queue, the new request is dropped.

Step 4 Choose **All Data** to generate all possible troubleshooting data, or check individual boxes as described in View task messages, on page 8.

Step 5 Click **Generate**. Find the task that corresponds to the troubleshooting files you generated in the Message Center; see View task messages, on page 8.

Step 6 After the appliance generated the troubleshooting files and the task status changes to `Completed`, click **Click to retrieve generated files**.

Step 7 Follow your browser's prompts to download the file. (The troubleshooting files are downloaded in a single `.tar.gz` file.)

Step 8 Follow the directions from Support to send the troubleshooting files to Cisco.

Download advanced troubleshooting files

Download troubleshooting files and share them with Cisco support for advanced troubleshooting assistance when requested.

Before you begin

You must have **Admin**, **Maintenance**, **Security Analyst**, or **Security Analyst (Read Only)** user roles to perform this task.

Procedure

Step 1 View the health monitor for the appliance; refer to , View the device health monitor.

Step 2 Choose **Troubleshooting** > **Health** > **Monitor**.

Step 3 Click a device in the left pane for which you dowload the troubleshooting files.

Step 4 Click **View System & Troubleshoot Details**, and then click **Advanced Troubleshooting.**

Step 5 In **File** field, enter the name of the file to download. Cisco support provides this file name.

Step 6 Click **Download**.

Step 7 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 8 Follow the directions from Cisco support to send the troubleshooting files to Cisco.

Troubleshooting syslogs in the Secure Firewall Management Center

You can enable the Firewall Threat Defense devices to log troubleshooting syslogs and send them to the Firewall Management Center. Logging data can help you identify and isolate network or device configuration issues. When you enable logging, the Firewall Threat Defense devices send syslogs to the Firewall Management Center for analysis and storage.

Logging configuration and management

You can manage the logging and the message severity by editing the **Logging to Secure Firewall Management Center** option in the Firewall Threat Defense platform settings policy for targeted devices. See *Configure Syslog Logging for Threat Defense Devices* in the *Cisco Secure Firewall Management Center Device Configuration Guide* for details on enabling logging, configuring syslog servers, and viewing system logs.

All troubleshooting logs

Configure Firewall Threat Defense devices to log all diagnostic syslogs to the management center and view them as **Troubleshoot Events** alongside other events in the **Unified Events** table (from **Analysis**, choose

Unified Events). Use the Unified Events table to see the troubleshooting logs in real-time and correlate them with the recent device configuration changes while performing the troubleshooting. You can filter and analyze the logs with other event types on the same table to gain insights and troubleshoot your Firewall Threat Defense devices.

See Work with unified events for more information about viewing the **Troubleshoot Events**.

You can opt to send all troubleshooting syslogs with severity levels Critical, Alerts, or Emergencies to the Firewall Management Center.

VPN troubleshooting logs

Configure the Firewall Threat Defense devices to send only the VPN troubleshooting syslogs to the Firewall Management Center for analysis. The VPN syslogs appear with a default severity level Errors or a higher severity (unless changed). We recommend that you set the logging level of the VPN logs as Errors. Setting the VPN logging level to 4 or a lower severity (Warnings, Notifications, Informational, or Debugging) could overload the Firewall Management Center.



Note When you configure a device with site-to-site or remote access VPN, it automatically enables sending VPN syslogs to the Firewall Management Center by default.

View troubleshooting syslogs

The Firewall Threat Defense device captures event information to help you to gather additional information about the device configuration issues or the source of your VPN problems. By default the rows are sorted by the **Time** column.

Before you begin

- Enable logging by configuring the **Logging to Secure Firewall Management Center** option in the Firewall Threat Defense platform settings. For more information, see *Enable Logging and Configure Basic Settings* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.
- You must be an Admin user in a leaf domain to perform this task.

Procedure

Step 1 Choose **Troubleshooting** > **+ Show more** > **Advanced** > **Troubleshooting Logs**.

Step 2 Select from these options:

- **Search**: To filter current message information, click **Edit Search**.
- **View**: To view VPN details associated with the selected message in the view, click **View**.
- **View All**: To view VPN details for all messages in the view, click **View All**.
- **Delete**: To delete selected messages from the database, click **Delete** or click **Delete All** to delete all the messages.

What to do next

If you choose to send all troubleshooting syslogs to the management center, from **Analysis**, choose **Unified Events** to view the logged **Troubleshoot Events** in real-time and alongside other secure firewall event types.

Enhanced troubleshooting experience using Cisco RADKit integration

The Cisco Remote Automation Development Kit (RADKit) is a network-wide orchestrator designed to provide Cisco support engineers with secure access to network devices for diagnosing and troubleshooting system issues. You can install RADKit on a remote server and integrate its services with Firewall Management Centers and their managed Firewall Threat Defense devices such that the data required for diagnosing issues are available automatically.

RADKit integration capabilities



Note RADKit supports only the instances of a cluster device, not the chassis itself.

Integrating RADKit with the Firewall Management Center enables you to:

- Access the Firewall Management Center and Firewall Threat Defense device remotely.
- Assign an engineer with controlled access to the Firewall Management Center and Firewall Threat Defense devices for diagnosing configuration discrepancies and hardware issues.
- Leverage automation capabilities to collect diagnostic data and analyze problems.
- Navigate to the previous sessions, view, and download all the operations logs as an archive file.

Guidelines and limitations for RADKit integration

Follow these guidelines when configuring RADKit integration to ensure proper functionality:

- If the Firewall Management Center is restored with a backup file of another Firewall Management Center, the devices mapped to the current authorizations are cleared. You must edit the authorization and repeat device selection in the **Authorization** page.
- If you are using HTTP proxy, configure the proxy in the Firewall Management Center before enabling the RADKit service for a sucessful enrolment of the service. In case of incorrect proxy configuration at the time of RADKit enablement, disable the RADKit service, after configuring the correct proxy, re-enable for sucessful enrolment of the service.

Enroll RADKit service

You can enroll the RADKit service with SSO, which establishes connectivity with the RADKit client.

Before you begin

- Not all users have access to the Firewall Management Center's RADKit page. Only Administrator users and users whose roles are assigned with RADKit access permissions can use the RADKit feature.
- If you intend to use HTTP proxy, configure the proxy in the management center before enabling the RADKit service for sucessful enrolment of the service.

Procedure

Step 1 Choose **Troubleshooting** > **Tools** > **Remote Diagnostics**.

Step 2 To enroll the service in the RADKit cloud, click the **Enable the RADKit service** toggle button, and then click **Enroll with SSO**.

Step 3 Enter your email address (with domain name), and click **Submit**.

Note You cannot enroll multiple times within a short period using the same email ID. Each time that you enroll, a new certificate is generated for the email ID account. Creating multiple certificates for the same user account is not efficient. Hence, RADKit Cloud restricts the number of issued certificates per user to 12 new Service IDs for a six-month duration.

Step 4 Complete the SSO process.

Step 5 In the **Cisco RADKit Access** page, click **Accept**.

After enrollment, the page displays the success message and the token ID.

Step 6 (Optional) To disable the service, click the **Disable the RADKit service** toggle button.

Caution When you disable the service, all the associated data and existing authorizations will be lost.

Manage RADKit service authorization

Before you begin

Enroll to RADKit service. For information about the procedure to enroll, see Enroll RADKit service, on page 22.

You can manage authorizations by enabling the TAC engineers to access the devices remotely for troubleshooting. You can also grant access to remote users to either access all the devices' inventory or only of selected devices for a specific duration.

Note The authorizations can be added and viewed only from the Global domain.

Procedure

Step 1 Choose **Troubleshooting** > **Tools** > **Remote Diagnostics**.

The **Remote Diagnostics** page lists the current authorizations. Ensure that you have enrolled to the RADKit service.

Step 2 To create a new authorization, click **Create New Authorization**.

Step 3 Under **Setup Authorization** , enter the support engineer's email address. The Email address must not exceed 40 characters.



Note
- The support engineer's email address is unique to an authorization record. Hence, you cannot modify this value after creating authorization.
- You cannot create an authorization account for the same email address.

Step 4 Click **Next**.

Step 5 Under **Device Selection**, specify the devices and the Firewall Management Center that the support engineer can access. Select the relevant option, and then click **Next**:

- **Grant access to all devices**: Click this radio button, and then check the **I agree to provide access to all devices** check box to agree for granting access to all devices and the Firewall Management Center.
- **Grant access to specific devices**: Click this radio button, and then from the **Select Devices** drop-down list, choose the device IP addresses and the Firewall Management Center that the support engineer can access. Ensure to check the **I agree to provide access to the selected devices** check box.



Note Only devices running Version 7.7 and later are supported and are available for selection.

Step 6 Under **Schedule the Access**, specify the timeline during which the support engineer can access the devices:

- **Now**: Click this radio button, and then under **Duration** fields, specify the time duration for granting access. To set the duration preset, click the **Time presets** links, namely, 1 hour, 6 hours, 12 hours, 1 day, or 1 week.
- **Grant access until revoke**: Click this radio button to grant perpetual access to the devices.



Note To revoke access, in the **Current Authorizations** grid, click the respective revoke icon under the **Actions** column.

Step 7 Under **Summary**, preview the selections you have made for the authorization account. To modify the choices made, click the Edit icon and make the corresponding changes.

Note The support engineer's email address is unique to an authorization record. Hence, you cannot modify the email address.

Step 8 Click **Create**.

In the subsequent window, a confirmation message for the new authorization with the user email address and the RADKit service id used in the RADKit client is displayed.

Step 9 (Optional) To create another authorization, click **Create Another Authorization**.

Step 10 To exit, click **Close**.

What to do next

The **Remote Diagnostics** window displays a list of current authorizations. You can perform the following actions:

- Edit the settings.
- Revoke the authorization.
- Enable sudo access for the devices and Firewall Management Center.

Enable sudo access for devices

When you provide sudo device access, regular users can have administrative rights to the devices. Irrespective of the user role, when you enable sudo access for a device, all the users of the device can enjoy this privilege.

Before you begin

Ensure that you have added the required devices in the Firewall Management Center.

Procedure

Step 1 Choose **Troubleshooting** > **Tools** > **Remote Diagnostics**.

Step 2 To enable sudo access to devices, click the **Device Sudo Access** tab.

The devices deployed in the Firewall Management Center and the Firewall Management Center are listed.

Step 3 To enable sudo access for a device, click the respective toggle button under **Sudo Status**.

Step 4 For bulk action, check the check boxes adjacent to the devices, and click **Enable**.

Step 5 To disable sudo access, click the respective toggle button under **Sudo Status**.

Download session logs

The **Previous Sessions** tab displays a list of log files for the operations performed by the RADKit client in the Firewall Threat Defense devices and the Firewall Management Center. These session logs can be downloaded as an archive. The RADKit sessions' logs are added to the Firewall Management Center log rotate mechanism and fall under the default log rotate mechanism as that of other Firewall Management Center log files.

Procedure

Step 1 Choose **Troubleshooting** > **Tools** > **Remote Diagnostics** and click the **Previous Sessions** tab.

Step 2 Search for a specific session log by entering the search string in the **Past Session Logs** search bar.

Step 3 Download the logs as an archive using **Download All Logs**.

Note You can download the logs from the **Current Authorization** page too.

General troubleshooting

An internal power failure (hardware failure, power surge, and so on) or an external power failure (unplugged cord) can result in an ungraceful shutdown or reboot of the system. This can result in data corruption.

Connection-based troubleshooting

Connection-based troubleshooting or debugging provides uniform debugging across modules to collect appropriate logs for a specific connection. It also supports level-based debugging up to seven levels and enables uniform log collection mechanism across modules. Connection-based debugging supports the following:

- A common connection-based debugging subsystem to troubleshoot issues in Firewall Threat Defense
- Uniform format for debug messages across modules
- Persistent debug messages across reboots
- End-to-end debugging across modules based on an existing connection
- Debugging ongoing connections

For more information about the troubleshooting connections, see Troubleshoot a connection, on page 26.

Troubleshoot a connection

This task enables you to identify and analyze connection issues by capturing and examining packet debug information for specific traffic flows.

Procedure

Step 1 Configure a filter to identify a connection using the **debug packet-condition** command.

Example:

```
Debug packet-condition match tcp 192.168.100.177 255.255.255.255 192.168.102.177
255.255.255.255
```

Step 2 Enable debugs for the interested modules and the corresponding levels. Enter the **debug packet** command.

Example:

```
Debug packet acl 5
```

Step 3 Start debugging the packets using the following command:

```
debug packet-start
```

Step 4 Fetch the debug messages from database to analyze the debug messages using the following command:

```
show packet-debugs
```

Step 5 Stop debugging the packets using the following command:

```
debug packet-stop
```

Advanced troubleshooting for the Secure Firewall Threat Defense device

You can use Packet Tracer and Packet Capture features to perform an in-depth troubleshooting analysis on a Secure Firewall Threat Defense device. A packet tracer allows a firewall administrator to inject a virtual packet into a 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. This utility is effective because it can 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 Download advanced troubleshooting files, on page 20.

Packet capture

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 Firewall Threat Defense devices supports troubleshooting and analysis of data packets.

Snort verdict processing

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.
AllowFlow	Flow passed without inspection.
BlockFlow	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 **BlockFlow**, and the subsequent packets in the session are dropped before reaching Snort. When the Snort verdict is **Block** or **BlockFlow**, the **Drop Reason** can be one of these:

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.
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.

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

The packet capture feature allows you to capture and download packets that are stored in the system memory. However, the buffer size is limited to 32 MB due to memory constraint. Systems capable of handling very high volume of packet captures exceed the maximum buffer size quickly and thereby the necessity of increasing the packet capture limit is required. It is achieved by using the secondary memory (by creating a file to write the capture data). The maximum supported file size is 10 GB.

When the **file-size** is configured, the captured data gets stored to the file and the file name is assigned based on the capture name **recapture**.

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

For information, see the *Cisco Secure Firewall Threat Defense Command Reference*.

Use a packet capture trace

Packet capture is a utility that provides a live snapshot of network traffic passing the specified interface of a device based on a defined criteria. This process continues to capture the packets as long as it has not paused, or the allocated memory has not exhausted.

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 Packet capture does not support ICMP for IPv6.

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

Before you begin

To use the packet capture tool on Secure Firewall Threat Defense devices, you can be an Admin, Maintenance, Security Analyst, or of any user with Packet Capture permission, including a read-only user.

While the read-only users—Security Analyst (Read Only) and custom read-only roles with the applicable feature permission—can add, start, pause, view, and export (save) packet captures, they cannot perform the edit, delete, and clear capture operations.

Procedure

Step 1 In the Firewall Management Center, choose **Troubleshooting** > **Tools** > **Packet Capture**.

Step 2 Select a device.

Step 3 Click **Add Capture**.

Step 4 Enter the **Name** for capturing the trace.

Step 5 Select the **Interface** for the capturing the trace.

Step 6 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) Check **SGT number** check box, and enter a Security Group Tag (SGT).

Step 7 Specify **Buffer** details:

a) Enter a maximum **Packet Size**.
b) 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.

Note If **Continues Capture** is enabled, and when the allocated memory is full, the oldest captured packets in the memory is overwritten by the new captured packets.

d) Check the check box of **Trace**, if you want to capture the details for each packet.
e) Enter the value in **Trace Count** field. Default value is 128 . You can enter values in the range of 1-1000.

Step 8 Click **Save**.

The packet capture screen displays the packet capture details and its status. To have the packet capture page auto refreshed, check the **Enable Auto Refresh** check box and enter the auto refresh interval in seconds.

You can do the following on the packet capture:

- **Edit** ( ) to modify the capture criteria. This option is not applicable for read-only users.
- **Delete** ( ) to delete the packet capture and the captured packets. This option is not applicable for read-only users.
- **Clear** ( ) to erase all the captured packets from a Packet Capture. To erase the captured packets from all of the existing packet captures, click **Clear All Packets**. This option is not applicable for read-only users.
- **Pause** ( ) to temporarily halt capturing packets.
- **Save** ( ) to save a copy of captured packets on a local machine in ASCII or PCAP format. Choose the required format option, and click **Save**. The saved packet capture is downloaded to your local machine.
- To view the details of the packets being captured, click the required capture row.

Packet tracer tool overview

A packet tracer tool is a network analysis utility. It simulates packet flows by modeling source and destination addresses and protocol characteristics. The tool validates network policies by performing lookups against access rules, NAT, routing, and rate-limiting policies. It also captures and logs detailed tracing information for each packet to assist with policy troubleshooting and debugging.

Packet tracer tool simulation and PCAP replay

Use the packet tracer tool to simulate the complete data path of a packet, including slow-path and fast-path modules. This simulation helps verify whether your configured policies allow or deny intended traffic. This tool helps you confirm your policy effectiveness and troubleshoot when your packets are blocked.

You can use packet capture (PCAP) files to replay complete traffic flows. Make sure your PCAP file contains a single Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) flow with up to 100 packets. On replay, the tool initializes client and server entities and synchronizes packet transmission, logging trace results for each packet in the flow.

For NAT-configured devices, the replayed packets reflect translated addresses, so that the addresses are processed without being dropped. IPv4 to IPv6 and IPv6 to IPv4 NAT are not supported in PCAP replay. To capture identity and TLS decryption trace information, configure Snort 3 as the detection engine on the device.

For more realistic simulation, the tool can imitate packet timing based on PCAP timestamps, using the **honor-timestamp** keyword in the `packet-tracer` command.

Note The timestamp accuracy decreases if the device takes longer to process each packet than the inter-packet time interval recorded in the capture.

Packet tracer data generated by the device can be stored in a PCAP file using the **export-pcapng** keyword in the `show packet tracer` command. The resulting pcapng file can be viewed with external tools like Wireshark.

Run a packet trace

Follow these steps to run a packet trace on Firewall Threat Defense.

Before you begin

- You must have the Administrator, Maintenance User, or Security Analyst role, or a custom role with packet tracer permission.

  Read-only users cannot upload PCAP files to the packet tracer. They can perform protocol-based packet tracing or use PCAP files uploaded by another user.

- Uploaded PCAP files can contain up to 100 packets from one Ethernet connection or one VLAN-encapsulated TCP or UDP connection. The maximum file size is 1 MB. Only .pcap and .pcapng files are supported.

Procedure

Step 1 In Firewall Management Center, choose **Troubleshooting** > **Tools** > **Packet Tracer**.

Step 2 Select the device where you want to run the trace.

Step 3 Select the ingress interface for the packet trace.

You cannot select a VTI as the ingress interface.

Step 4 To use a PCAP file, select **Upload or edit a PCAP File**.

You can upload a new file or select an existing file.

After you select a file, you can edit its filename, source and destination IP addresses and ports, and VLAN ID. For a transparent firewall, you can also edit the destination MAC address. To change the protocol, source type, or destination type, upload a new file.

Skip the next step and continue with optional trace settings.

Step 5 To configure the packet trace manually, select **Use Protocol** and complete these steps:

a) Select a packet type from **Protocol** and specify its parameters:

- **ICMP**: Source and destination addresses, type, code (0 to 255), and an optional ID (1 to 65535).

- **TCP**, **UDP**, or **SCTP**: Source and destination addresses and required ports (0 to 65535).
- **GRE**: GRE EtherType, outer-header source and destination addresses, and the inner-packet protocol and addresses.
- **IPIP**: Outer-header source and destination addresses and the inner-packet protocol and addresses.
- **ESP**: Source and destination addresses and the source Security Parameter Index (SPI) value (0 to 4294967295).
- **RAWIP**: Source and destination addresses and ID/Next Header (0 to 255).

Source and destination addresses can be IPv4 or IPv6. If you use Cisco TrustSec, you can also enter an FQDN. Available destination types depend on the selected source type.

b) (Optional) To trace a packet where the Security Group Tag (SGT) value is embedded in the Layer 2 CMD header (TrustSec), enter a valid **Inline Tag**.

c) To trace traffic that enters a parent interface and is redirected to a subinterface, enter a **VLAN ID**.

This value is optional only for interfaces that are not subinterfaces because all interface types can be configured on a subinterface.

d) Enter a **Destination MAC Address** according to these requirements:

- Transparent firewall mode, VTEP ingress interface: Destination MAC address is required when you enter a VLAN ID.
- Transparent firewall mode, bridge group member ingress interface: Destination MAC address is optional when you enter a VLAN ID and required when you do not.
- Routed firewall mode, bridge group member ingress interface: Destination MAC address and VLAN ID are optional.

Step 6 (Optional) Select any of these options:

- **Bypass security checks for the simulated packet** to ignore security checks. This option allows the packet to be traced even if the system would otherwise drop it.
- **Treat the simulated packet as an IPsec/SSL VPN-decrypted packet** to treat the packet as decrypted VPN traffic.
- **Allow the simulated packet to transmit from the device** to send the packet through the device's egress interface.

Step 7 Select **Trace**.

If you have unsaved PCAP file changes, the system prompts you to save them before the trace begins.

Trace Result displays results for each processing phase. Select a packet to view its trace results, which show the elapsed time for each phase and the total packet-processing time from the ingress interface to the egress interface.

Trace History stores details for up to 100 packet traces. You can run saved traces again, search for or delete them, clear the trace history, or stop saving traces.

The audit log records PCAP file saves, PCAP file uploads, and packet traces. To view these records, choose **Events & Logs** > **Analysis** > **Audit Logs**.

CPU profiler overview

The CPU profiler gathers data on CPU usage by individual modules or inspectors of Snort 3, while packets are being processed within a specific timeframe. It provides information on the amount of CPU time that each module consumes in relation to the total CPU usage of the Snort 3 process. Using the CPU profiler does not require reloading the configuration or restarting Snort 3, thus minimizing downtime. The profiling result displays the processing time taken by all the modules during the last profiling session. CPU profiling results are saved in JSON format in the threat defense device and synchronized in the management center.



Caution CPU profiling might cause system performance degrade of approximately 3 percent.



Note Standby Threat Defense devices cannot be profiled using the Management Center UI; profiling is only possible through the device's CLI. Note that if you start the profiling process from the CLI, you can stop it only from the CLI, and not from the UI.

Use the CPU profiler

Use the CPU profiler to identify which Snort 3 modules or inspectors are consuming the most processing time and contributing to performance issues.

Before you begin

You must have Version 7.6 or later devices with Snort 3 to use CPU Profiling.

Procedure

Step 1 From the management center, choose **Troubleshooting** > **+ Show more** > **Intrusion & discovery** > **Snort 3 Profiling**.

Step 2 Click the **CPU Profiling** tab.

Step 3 From the **Select device for CPU Profiling** drop-down list, choose a device for CPU profiling.



Note You can run multiple profiling sessions simultaneously on different devices.

Step 4 To start a CPU profiling session, click **Start**. (The session automatically stops after 120 minutes.)

You can stop the profiling session at any time by clicking **Stop**. However, canceling it before the scheduled 120 minutes might not give precise results.

Note While the CPU profiling session is in progress, a task is created. Click **Notifications** (message center), and then click the **Tasks** tab to view the details.

The latest profiling result is automatically displayed in the **CPU Profiling Results** section. The table contains statistics for the processing time taken by all the Snort 3 modules or inspectors during the last profiling session. You can view the CPU profiler output in tabular format:

- **Module**: Name of the module or inspector.
- **% Total of CPU Time**: Percentage of time taken by the module relative to the overall time taken by Snort 3 for processing traffic. If this value is considerably higher than that of other modules, it means the module is contributing more to the unsatisfactory performance of Snort 3.
- **Time (µs)**: Total time (in microseconds) taken by each module.
- **Avg/Check**: Average time taken by the module each time the module was invoked.
- **% Caller**: Time taken by the submodule (if configured) relative to the main module. This value is used for debugging purposes.

Step 5 (Optional) Click **Download Snapshot** to download the profiling result. The downloaded file is in CSV format and contains all the fields from the profiling results page.

Step 6 (Optional) Click the **Filter by % of Snort time** toggle button to filter out modules whose execution consumed more than *n*% of the profiling time.

Step 7 (Optional) Use the **Search** field to search through the fields in the **CPU Profiling Results** table.

Note Except for **Module**, you can click any of the other column headers to sort the data.

Step 8 (Optional) Click the **Profiling History** section (collapsible panel on the left) to expand it and view a set of cards representing the previous profiling sessions for a chosen device. When you click a card from history, the details are displayed in the **CPU Profiling Results** section.

The CPU profiling session provides detailed statistics about the processing time of each Snort 3 module, helping you identify performance bottlenecks.

Note If you initiate a deployment while CPU profiling is running, the profiling session is automatically terminated to accommodate the deployment, except for deployments resulting from changes to the access control policy rules and security intelligence. You must run the CPU profiling for the device again.

Rule profiler overview

The Snort 3 rule profiler gathers data on the time spent processing a set of Snort 3 intrusion rules, highlights potential issues, and shows the rules with unsatisfactory performance. Within the Snort 3 engine, the rule

profiler inspects traffic using the Snort 3 intrusion detection mechanism. The rule profiler displays the top 100 IPS rules that required the maximum time to check. Triggering the rule profiler does not require Snort 3 reload or restart. The rule profiling results are saved in JSON format in the threat defense device and synchronized in the management center.

Note Standby Threat Defense devices cannot be profiled using the Management Center UI; profiling is only possible through the device's CLI. Note that if you start the profiling process from the CLI, you can stop it only from the CLI, and not from the UI.

Use the rule profiler

The Rule Profiler helps you identify IPS rules that consume excessive processing time, allowing you to optimize performance by analyzing rule execution statistics and identifying poorly performing rules that may need adjustment or replacement.

Before you begin

You must have version 7.6 or later devices with Snort 3 to use Rule Profiling.

Procedure

Step 1 From the management center, choose **Troubleshooting** > **+ Show more** > **Intrusion & discovery** > **Snort 3 Profiling**.

Step 2 Click the **Rule Profiling** tab.

Step 3 From the **Select device for Rule Profiling** drop-down list, choose a device for rule profiling.

Note You can run multiple profiling sessions simultaneously on different devices.

Step 4 To start a rule profiling session, click **Start**.

The session automatically stops after 120 minutes. You can stop the profiling session at any time by clicking **Stop**. However, canceling it before the scheduled 120 minutes might not give precise results.

Note While the rule profiling session is in progress, a task is created. Click **Notifications** > **Tasks** to view the details.

The latest profiling result is automatically displayed in the **Rule Profiling Results** section. The table contains statistics for the rules that took the most time to process (sorted in descending order) by the total time (in microseconds [µs]). You can view the IPS rule profiler output in tabular format:

- **% of Snort Time**: Time spent for processing the rule, relative to the total time of the Snort 3 operation.
- **Rev**: Revision number of the rule.
- **Checks**: Number of times the IPS rule was executed.

- **Matches**: Number of times the IPS rule fully matched in the traffic.
- **Alerts**: Number of times the IPS rule triggered an IPS alert.
- **Time**: Time (in microseconds) spent by Snort in checking the IPS rule.
- **Avg/Check**: Average time spent by Snort on a single check of the rule.
- **Avg/Match**: Average time spent by Snort on a single check, which resulted in a match.
- **Avg/Non-Match**: Average time spent by Snort on a single check, which did not result in a match.
- **Timeouts**: Number of times the rule exceeded the Rule Handling - Threshold configured in the Latency-Based Performance Settings of the access control policy.
- **Suspends**: Number of times the rule was suspended due to consecutive threshold violations.

Step 5 Click **Download Snapshot** to download the profiling result.

The downloaded file is in CSV format and contains all the fields from the profiling results page.

Step 6 Click the **Filter by % of Snort time** toggle button to filter out rules whose execution took more than *n*% of the profiling time.

In general, a rule is considered as performing unsatisfactorily if it consumes 0.2% or more of Snort's overall processing time.

Step 7 Use the **Search** field to search through the fields in the **Rule Profiling Results** table.

Step 8 Click the **Rule Profiling History** section (collapsible panel on the left) to expand it and view a set of cards representing the previous profiling sessions for a chosen device.

When you click a card from the history, the details are displayed in the **Rule Profiling Results** section.



Note If you initiate a deployment while rule profiling is running, the profiling session is automatically terminated to accommodate the deployment, except for deployments resulting from changes to the access control policy rules and security intelligence. You must run the rule profiling for the device again.

Use the Firewall Threat Defense diagnostic CLI from the web interface

Use the diagnostic CLI to execute selected commands for quick troubleshooting of your device from the web interface without requiring direct SSH access to the device.

You can execute the selected Firewall Threat Defense diagnostic CLI commands from the Firewall Management Center. The commands **ping** (except **ping system**), **traceroute**, and select **show** commands run in the diagnostic CLI rather than the regular CLI.

When you run the **show** commands, if the message `Unable to execute the command properly. Please see logs for more details` is displayed, it means that the command is not valid in the diagnostic CLI. For example, **show access-list** works, but this message will be displayed if you enter **show access-control-policy**. To use non-diagnostic commands, use SSH to log in to a device outside management center.

For more information on the Firewall Threat Defense CLI, see the *Cisco Secure Firewall Threat Defense Command Reference*.

Before you begin

- You must be an Admin, Maintenance, or Security Analyst to use the diagnostic CLI.
- The purpose of diagnostic CLI is to enable the quick use of a few commands that are useful in troubleshooting a device. For access to the full range of commands, open an SSH session directly with the device.
- In deployments using Firewall Management Center high availability,diagnostic CLI is available only in the active Firewall Management Center.

Procedure

Step 1 Choose **Troubleshooting** > **Tools** > **Threat Defense CLI**.

You can also access the CLI tool through the health monitor for the device (**Troubleshooting** > **Health** > **Monitor**). From there, you can select the device, click the **View System and Troubleshoot Details** link, click **Advanced Troubleshooting**, then click **Threat Defense CLI** on that page.

Step 2 From the **Device** drop-down list, choose the device on which to execute the diagnostic command.

Step 3 From the **Command** drop-down list, choose the command that you want to execute.

Step 4 Enter the command parameters in the **Parameters** field.

See the *Cisco Secure Firewall Threat Defense Command Reference* for the valid parameters.

For example, to execute **show access-list** command, choose **show** from the **Command** drop-down list, then enter **access-list** in the **Parameters** field.

Note Do not type the full command in the **Parameters** field. Type only the relevant keywords.

Step 5 Click **Execute** to view the command output.

If the message `Unable to execute the command properly. Please see logs for more details.` is displayed, examine the parameters closely. There might be syntax errors.

This message can also mean that the command you are trying to execute is not a valid command within the context of the diagnostic CLI (which you have accessed from the device using the **system support diagnostic-CLI** command). Log in to the device using SSH to use these commands.

Feature-specific troubleshooting

This reference provides a comprehensive list of troubleshooting resources organized by feature. Each entry includes links to detailed troubleshooting information, best practices, and configuration guidance for specific system features and components.

Table 5: Feature-specific troubleshooting topics

Feature	Relevant Troubleshooting Information
Application control	*Best Practices for Application Control* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
LDAP external authentication	Troubleshoot LDAP authentication connections
Licensing	Troubleshoot Smart Licensing Troubleshoot Specific License Reservation
Firewall Management Center high availability	Troubleshoot Firewall Management Center high availability
User rule conditions	*Troubleshoot User Control* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
User identity sources	For troubleshooting information on ISE/ISE-PIC, TS Agent Identity Source, Captive Portal Identity Source, and Remote Access VPN Identity Source, see the corresponding sections in the *Cisco Secure Firewall Management Center Device Configuration Guide* Troubleshoot LDAP authentication connections
URL filtering	*Troubleshoot URL Filtering* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Realms and user data downloads	*Troubleshoot Realms and User Downloads* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Network discovery	*Troubleshooting Your Network Discovery Strategy* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Custom Security Group Tag (SGT) rule conditions	*Custom SGT Rule Conditions* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
SSL rules	Chapter on SSL rules in the *Cisco Secure Firewall Device Manager Configuration Guide*
Cisco Threat Intelligence Director (TID)	*Troubleshoot Secure Firewall Threat Intelligence Director* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Secure Firewall Threat Defense syslog	*About Configuring Syslog* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Connection-based Troubleshooting	Connection-based troubleshooting, on page 26