Collect Data for Root Cause Analysis of Software Traceback/Crash in Secure Firewall

Contents

Introduction

This document describes the steps to collect data in case of a software traceback.

Prerequisites

Requirements

Basic product knowledge.

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

The information in this document is based on these software and hardware versions:

- Secure Firewall 1200, 3100, 4200
- Firepower 1000, 4100, 9300
- Cisco Secure eXtensible Operating System (FXOS) 2.16(0.136)
- Cisco Secure Firewall Threat Defense (FTD) 7.6.1.291
- Cisco Secure Firewall Management Center (FMC) 7.6.1.291
- Adaptive Security Appliance (ASA) 9.22.2.9

Background

FTD or ASA software can traceback and usually reload due to different reasons such as:

- Software defects including the defects in the operating system and third party components.
- Hardware exceptions, such as low-level memory or CPU errors.
- In some cases, due to lack of system resources, such as memory.
- Manually triggered by the user for diagnostic purposes under TAC supervision:

```
<#root>

>

system support diagnostic-cli


Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower>

enable


Password:
firepower#

crashinfo force ?


page-faultc  Crash by causing a page fault exception
process     Crash the specified process
watchdog    Crash by causing a watchdog timeout
```

In the case of a traceback also known as the **crash**, depending on the process, usually a **crashinfo**, **core** or **minidump files** files are generated:

- **crashinfo** contains minimum diagnostic data from the process memory.
- **core file** is a complete dump of the process memory at the time of the traceback.
- **minidump** file is specific to Snort3 and contains diagnostic data from the process memory.

In the Secure Firewall software, the process that had a traceback can be in any of the these components:

- Firepower 1000, 2100, 4100, 9300, Secure Firewall 1200, 3100, 4200 chassis.
- Firepower 4100, 9300 security modules.

Apart from core and crashinfo files, the root cause analysis (RCA) of a traceback requires additional information, such as troubleshoot and show-tech files, syslog messages and so on.

Core and crashfinfo file analysis are handled by TAC and Cisco as part of a service request (case).

Data Collection

Proceed with these steps to collect the necessary data for the RCA of the traceback. Due to the risk of data loss caused by file rotations, please provide the requested data as soon as possible.

1. Clarify these items:

1a. Exact hardware.

1b. Software version.

1c. Secure firewall software type (ASA or FTD).

1d. Deployment mode (native or multi-instance mode).

Refer to Verify Firepower Software Versions and Verify Firepower, Instance, Availability, Scalability Configuration for detailed verification steps.

2. Clarify if there were any recent environmental changes, such as:

2a. Addition of traffic.

2b. Major configuration changes including commands.

Ensure to include the timestamps and the time zone as precisely as possible.

3. If the traceback occurred after configuration changes using specific commands, collect terminal session outputs. If command authorization is configured on the ASA, collect command authorization reports from the remote server, such as the Identity Services Engine (ISE).

4. In the next steps ensure to verify the crashinfo, core or minidump files with the most recent timestamps and take a note of the full path to each file. The full paths are needed for the collection of the files as shown in the **How to Collect Crashinfo, Coredump and Minidump Files from Secure Firewall?** section.

ASA

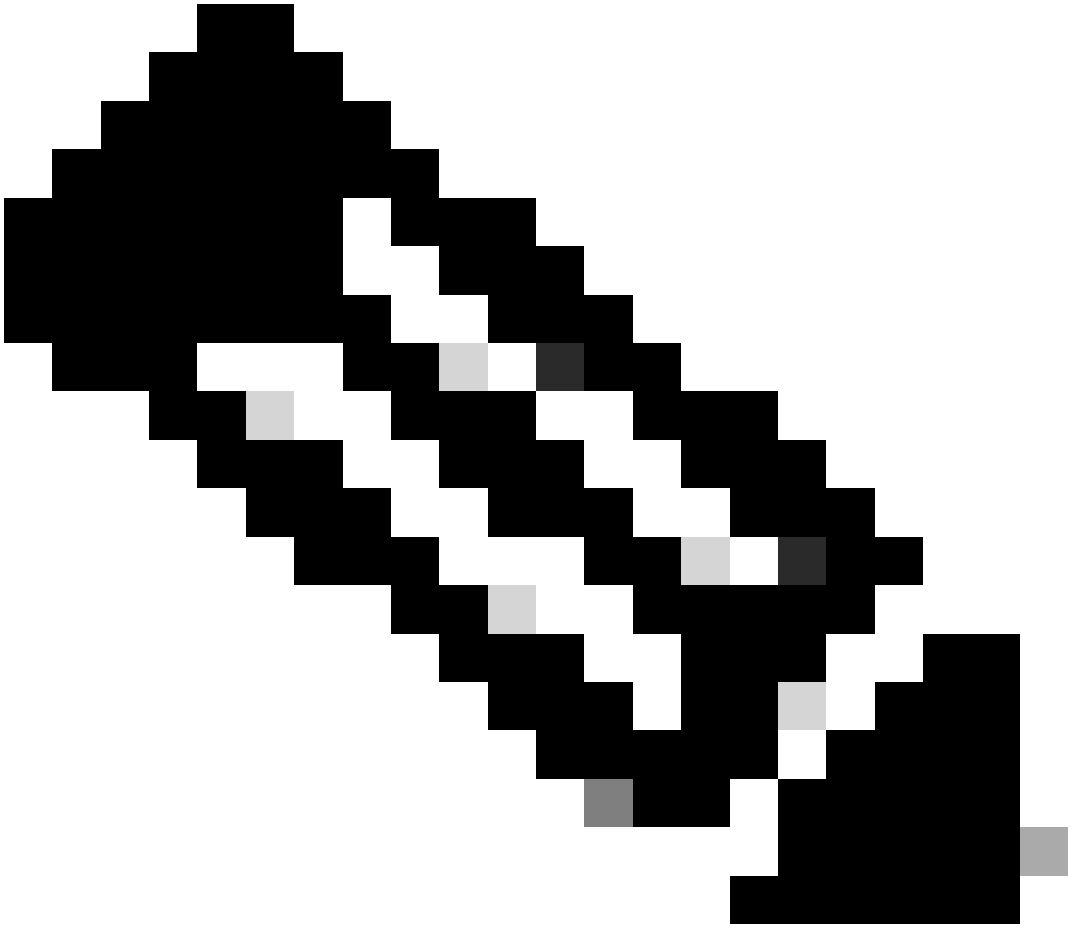
4.1. Verify the presence of an crashinfo file. To view the latest crashinfo, run the **show crashinfo** command. The crashinfo files can be found in the output of the **dir** command.

```
<#root>

asa#

dir


Directory of disk0:/
…
1610891723  -rw-  413363       20:51:22 Aug 13 2025

crashinfo_lina.14664.20250813.205102
```

4.2. Verify the presence of ASA core files using the **dir coredumpfsys** command:

```
<#root>

asa#

dir coredumpfsys


Directory of disk0:/coredumpfsys/
24577  -rw-  419619286    12:43:07 Aug 04 2025
```

```
core.lina.11.10335.1754311379.gz

11      drwx  16384        00:15:57 Jan 01 2010  lost+found
```



Note: On virtual ASA the coredump feature by default is disabled:

<#root>

```
ciscoasa#
show coredump


filesystem 'disk0:' has no coredump filesystem
```

To enable the coredump feature, refer to the **coredump enable** section in the Cisco Secure Firewall

---

ASA Series Command Reference, A-H Commands.

FTD

4.1. Verify the presence of an FTD crashinfo file. To view the latest crashinfo, run the **show crashinfo** command. The crashinfo files can be found in the output of the **dir** command.

```
<#root>

ftd#

dir


Directory of disk0:/
…
1610891723  -rw-  413363       20:51:22 Aug 13 2025

crashinfo_lina.14664.20250813.205102
```

On FTD, the crashinfo files can be found in the expert mode **/mnt/disk0/** directory:

```
<#root>

>

expert


admin@firepower:~$

ls -l /mnt/disk0/


total 496472
..
-rw-r--r-- 1 root root    460812 Aug 13 10:31

crashinfo_lina.13050.20250813.103059
```

In FTD troubleshoot file, the crashinfo files are in **dir-archives/var-log/mnt-disk0/:**

```
<#root>

$

ls -l


/dir-archives/mnt-disk0


total 9456
-rw-r--r-- 1 root root  453024 Aug  8 23:51
```

crashinfo_lina.13949.20250808.235100

4.2. Verify the presence of FTD core files. On FTD, the core files are accessible in the **expert** mode **/ngfw/var/data/cores/** and **/ngfw/var/common/** directories:

<#root>

admin@ftd:~$

ls -l /ngfw/var/data/cores/

total 1255512
-rw-r--r-- 1 root root 602208441 Jul 24 09:28

core.lina.11.14993.1753342057.gz

-rw-r--r-- 1 root root 682148808 Jul 24 09:38

core.lina.11.80997.1753342659.gz

In FTD troubleshoot file the core file names are in the file **command-outputs/for\ CORE\ in\ \`ls\ *:**

<#root>

command-outputs $

cat for\ CORE\ in\ \`ls\ *

/var/data/cores/core.lina.11.38967.1732272744.gz: gzip compressed data, was "core.lina.11.38967.1732272

FTD Snort3-specific coredump

This section is applicable only to FTD running the Snort3 engine.

4.1. Verify the presence of Snort3 engine crashinfo files **snort3-crashinfo.*** are in the expert mode **/ngfw/var/log/crashinfo/** directory.

<#root>

admin@ftd$

ls -l /ngfw/var/log/crashinfo

total 8
-rw-r--r-- 1 root root 1104 Aug 22 19:10

snort3-crashinfo.1755889806.134825

```
-rw-r--r-- 1 root root 1104 Aug 22 19:15
snort3-crashinfo.1755890128.201213
```

In FTD troubleshoot file, the same files are in **dir-archives/var-log/crashinfo/.**

4.2. Verify the presence of Snort3 minidump files **minidump_*** in /**ngfw/var/data/cores/:**

```
<#root>
admin@firepower:~$
ls -l /ngfw/var/data/cores/

total 936580
-rw------- 1 root root    977760 Aug 22 19:10
minidump_1755889805_firepower_snort3_17455.dmp
```

In FTD troubleshoot file the minidump files are in **file-contents/ngfw/var/data/cores/:**

```
<#root>
$
ls -l file-contents/ngfw/var/data/cores/

total 1904
-rw------- 1 root root 977760 Aug 22 19:10
minidump_1755889805_firepower_snort3_17455.dmp
```

Firepower 4100 and 9300 security modules

This section is applicable only to Firepower 4100 and 9300 modules.

4.1. Verify the presence of crashinfo and core files:

```
<#root>
firepower #
connect module 1 console

Firepower-module1>
support filelist
```

```
============================
Directory: /
Downloads_Directory
CSP_Downloaded_Files
Archive_Files
```

Crashinfo_and_Core_Files

```
Boot_Files
ApplicationLogs
Transient_Core_Files

Type a sub-dir name to list its contents, or [x] to Exit:
```

Crashinfo_and_Core_Files

```
----------sub-dirs----------
lost+found
-----------files------------
2025-08-04 14:43:07 | 419619286  | core.lina.11.10335.1754311379.gz
2025-08-13 12:45:11 | 419798152  | core.lina.11.10466.1755081904.gz
2025-08-14 13:35:02 | 419449591  | core.lina.11.46717.1755171295.gz
2025-08-18 12:48:26 | 419624883  | core.lina.6.10412.1755514099.gz
([b] to go back)
…
```

FXOS

4.1. On Firepower 1000, 2100 and Secure Firewall 1200, 3100, 4200 chassis, Verify the presence of core files using the **dir workspace:/cores** and **dir workspace:/cores_fxos** commands in the **local-mgmt** shell.

If the ASA application is installed, then connect to the FXOS shell using the **connect fxos admin** command:

<#root>

```
firepower-1120#
```

connect local-mgmt

```
Warning: network service is not available when entering 'connect local-mgmt'

firepower-1120(local-mgmt)#
```

dir workspace:/cores

```
1 119710270 Jul 25 11:41:12 2025
```

core.lina.6.19811.1753443666.gz

```
2     16384 Jul 22 21:13:57 2025 lost+found/
3      4096 Jul 22 21:16:07 2025 sysdebug/

Usage for workspace://
159926181888 bytes total
```

```
5545205760 bytes used
154380976128 bytes free

firepower-1120(local-mgmt)#
```

dir workspace:/cores_fxos

```
1 9037 Jul 25 10:52:17 2025 kp_init.log
```

The core files are also mentioned in /**opt/cisco/platform/logs/prune_cores.log** files in the chassis troubleshoot file:

<#root>

$

less opt/cisco/platform/logs/prune_cores.log

```
Fri Jul 25 11:41:31 UTC 2025 -  Avoiding compress/move for for ./core.lina.6.19811.1753443666: UptimeIn
Fri Jul 25 11:42:32 UTC 2025 -  Number of pre-compressed core file : 0
Fri Jul 25 11:42:32 UTC 2025 -
```

Uncompressed file ./core.lina.6.19811.1753443666: uptimeInSec: 3141; SafeIntval:45; Timestamp Diff: 80;

4.2. On Firepower 4100 and 9300 chassis, verify the presence of core files by using the **dir workspace:/cores** commands in the **local-mgmt** shell:

<#root>

```
firewall(local-mgmt)#
```

dir workspace:/cores

```
Usage for workspace://
4160421888 bytes total
461549568 bytes used
3484127232 bytes free
```

The core file names can be found inside the chassis troubleshoot file, in the outputs of the **show cores** command in file ***_BC1_all/FPRM_A_TechSupport/sw_techsupportinfo,** where * is the part of the troubleshoot file name, for example, **20250311123356_ FW**_BC1_all.tar.

5. Verify if the crashinfo, coredump and minidump files are relevant to the incident.

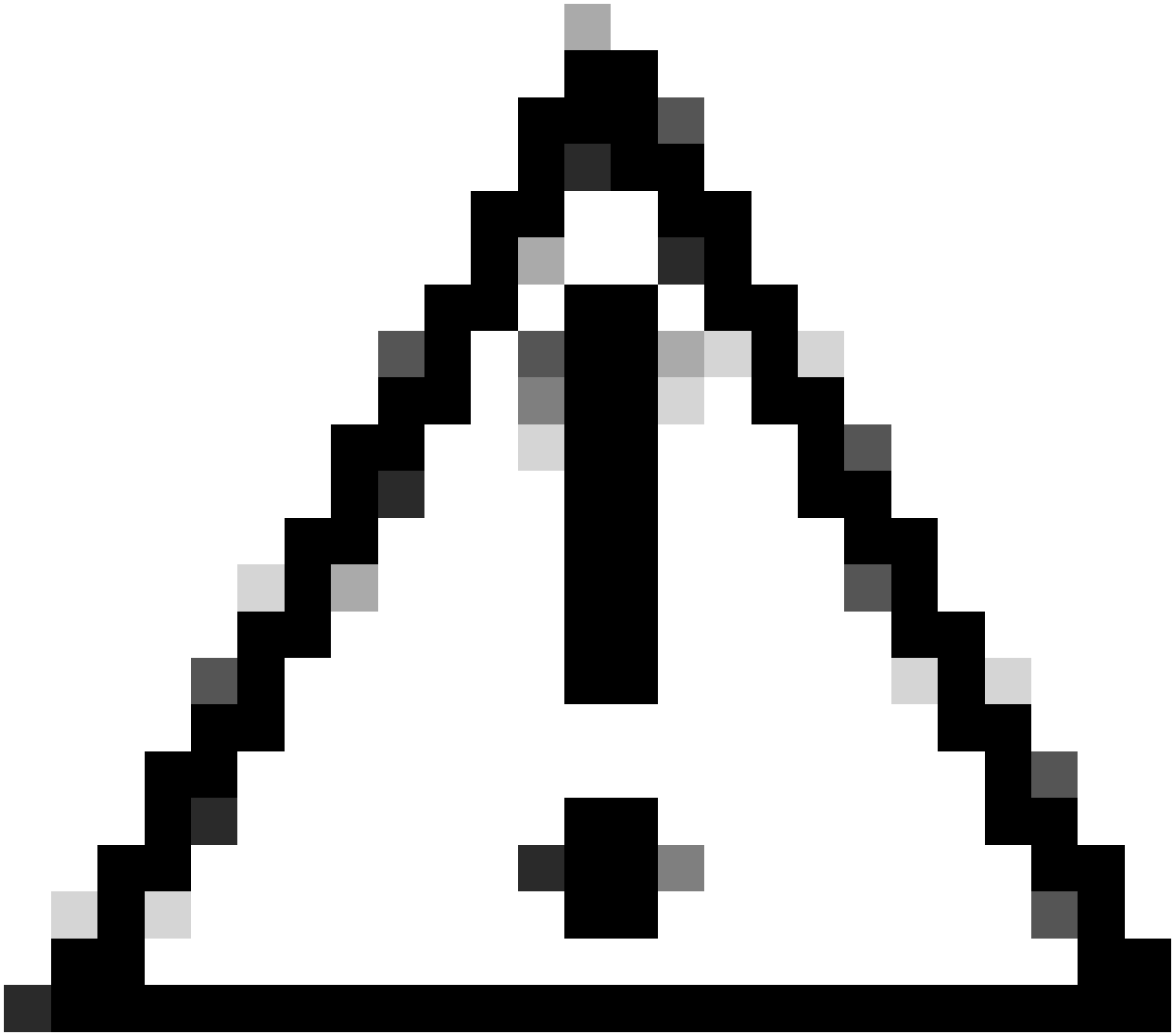
- Compare the file timestamps to the timestamp of the incident, or..
- Convert the epoch timestamp from the filename to date using the Linux **date** command.

For core and minidump files the epoch timestamps can be converted to date time using the **date** on any Linux host:

<#root>

```
admin@ftd:~$
ls -l /ngfw/var/data/cores/

total 1255512
-rw-r--r-- 1 root root 602208441 Jul 24 09:28 core.lina.11.14993
.1753342057.
gz
linux $
date -d @1753342057

Thu Jul 24 07:27:37 UTC 2025
```

6. Refer to the **How to Collect Crashinfo, Coredump and Minidump Files from Secure Firewall?** section to download the crashinfo, minidump and core files from steps 4-5.



Caution: Do not rename core, crashinfo or minidump files.

7. Proceed with steps in Troubleshoot Firepower File Generation Procedures to collect show-tech and troubleshoot files:

7a. ASA show-tech file.

7b. FTD troubleshoot file.

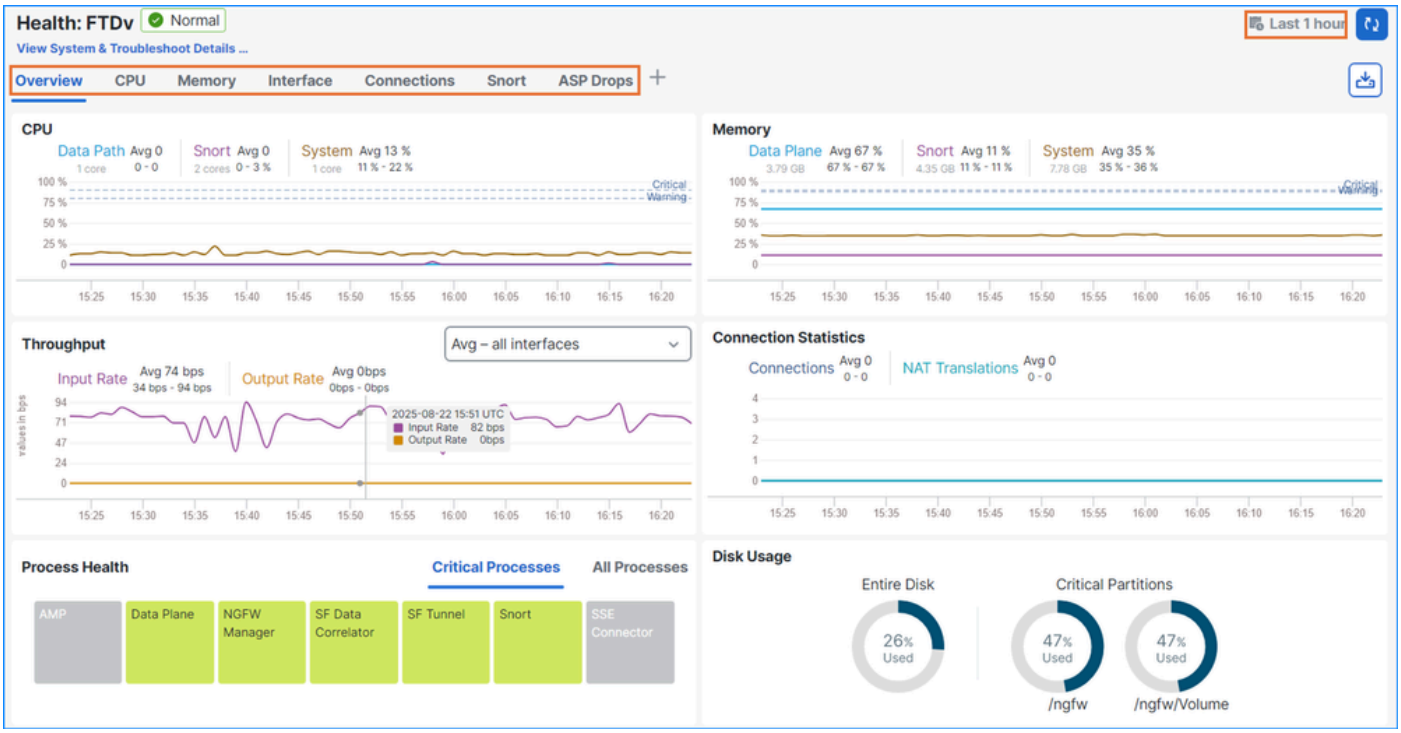
7c. Firepower 4100 and 9300 security module show-tech file.

7d. Firepower 4100 and 9300 chassis show-tech file.

7e. Firepower 1000, 2100 and Secure Firewall 1200, 3100, 4200 chassis show-tech file. Chassis troubleshoot files for Secure Firewall 3100, 4200 in container mode can be downloaded via the FMC > **Devices** > **[chassis]** > **3 dots** > **Troubleshoot Files** option.

8. In the case of FTD, collect screenshots of the health monitoring tabs on FMC covering at least **30** minutes before the traceback. Ensure to include the screenshots of **all** highlighted tabs. In case of recurring traceback, collect screenshots covering a few incidents.

Additionally, in the case of high availability and clustering, collect screenshots for all affected units:



9. Collect **raw** (unparsed) Lina engine syslog messages from syslog servers covering at least **30** minutes before the traceback. Raw format is essential for internal processing by TAC and engineering tools.

In case of recurring traceback, collect the raw messages covering a few incidents. Additionally, in the case of high availability and clustering, collect raw syslogs from all affected units.

Verification on the ASA/FTD CLI:

<#root>

```
ftd#
```

```
show run logging
```

```
logging enable
logging trap informational
logging host inside
```

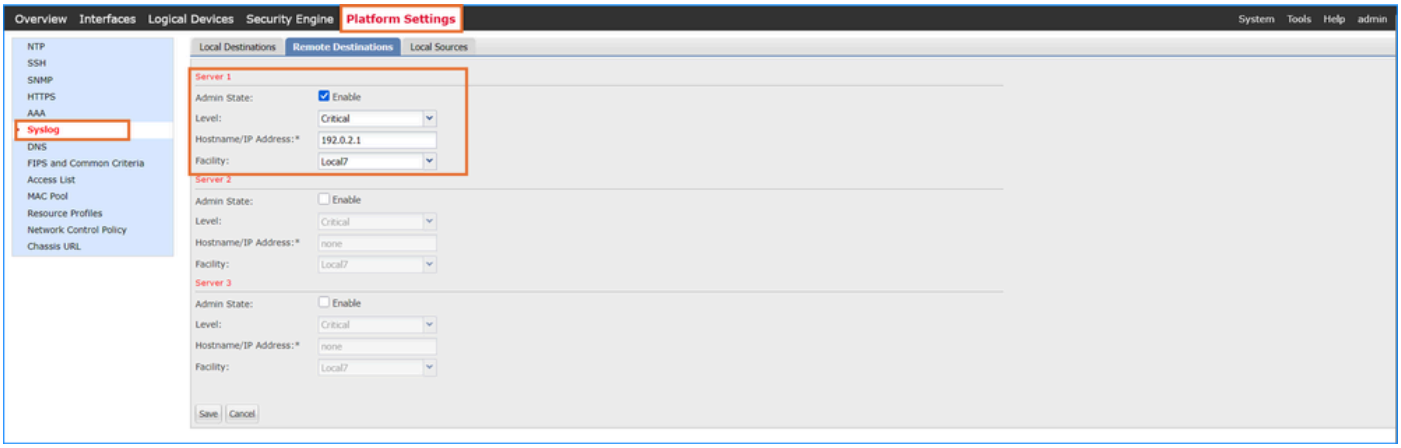
```
192.0.2.1
```

```
<-- syslog server address
```

10. In the case of Firepower 4100 and 9300, collect **raw** (unparsed) FXOS messages from syslog servers at least 10 minutes before the traceback. Raw format is essential for internal processing by TAC and engineering tools.

Additionally, in the case of high availability and clustering, collect raw syslogs from all affected chassis.

Verification on the Firepower Chassis Manager (FCM) User Interface (UI):



Verification on the FXOS CLI:

<#root>

```
firepower #
```

```
scope monitoring
```

```
firepower /monitoring #
```

```
show syslog
```

```
console
    state: Disabled
    level: Critical

monitor
    state: Disabled
    level: Critical

file
    state: Enabled
```

```
    level: Critical
    name:  messages
    size:  4194304

remote destinations
    Name     Hostname             State    Level         Facility
    -------- -------------------- -------- ------------- --------


Server 1 192.0.2.1            Enabled  Critical      Local7

<-- syslog server address
    Server 2 none                 Disabled Critical      Local7
    Server 3 none                 Disabled Critical      Local7

sources
    faults: Enabled
    audits: Disabled
    events: Disabled
```

11. Collect ASA or FTD CPU, memory, interface data including traps from the configured SNMP servers. Ensure to include data covering at least **30** minutes before the traceback.

In case of recurring traceback, collect the raw messages covering a few incidents. Additionally, in the case of high availability and clustering, collect raw messages from all affected chassis.

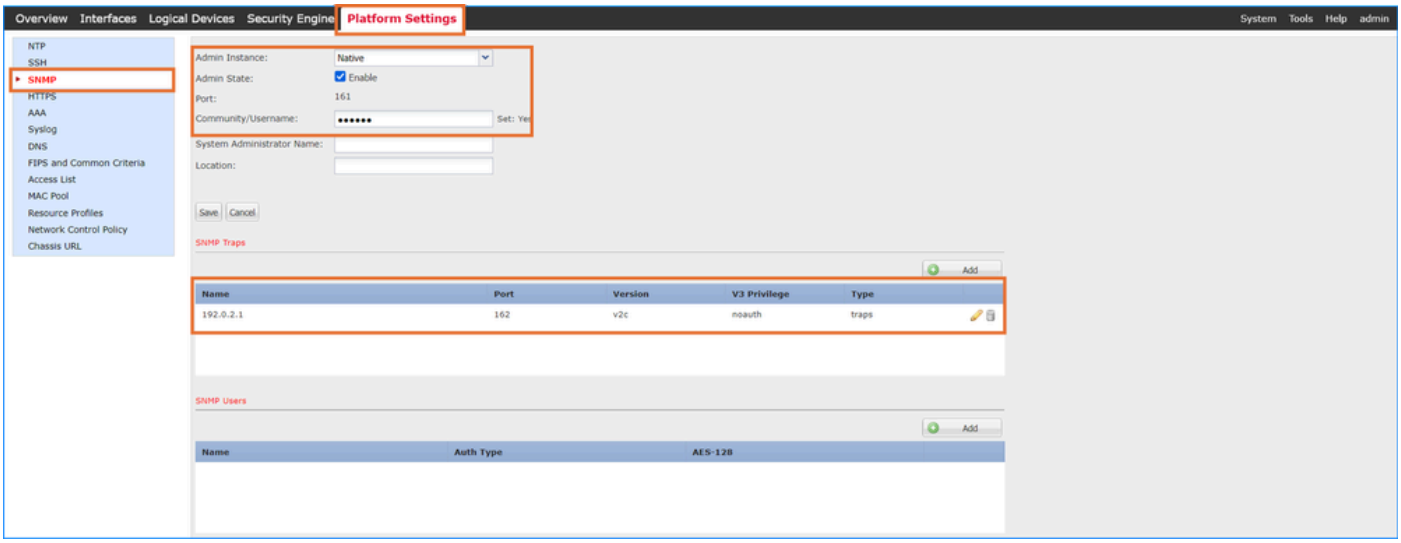
Verification on the ASA/FTD CLI:

```
<#root>

ftd#

show run snmp-server


snmp-server host inside 192.0.2.1 community ***** version 2c

<-- SNMP server addresses

snmp-server host inside 192.0.2.2 community ***** version 2c


no snmp-server location
no snmp-server contact
```

12. In the case of Firepower 4100 and 9300, collect CPU, memory, interface data including traps from the configured SNMP servers. Ensure to include data covering at least **30** minutes before the traceback.

In case of recurring traceback, collect the raw messages covering a few incidents. Additionally, in the case of high availability and clustering, collect raw messages from all affected chassis.

Verification on the FCM UI:



Verification on the FXOS CLI:

<#root>

```
firepower #
```

scope monitoring

```
firepower /monitoring #
```

show configuration

…

enable snmp

enter snmp-trap 192.0.2.1

```
<-- SNMP server address
 !        set community
          set notificationtype traps
          set port 162
          set v3privilege noauth
          set version v2c
```

13. Collect traffic profile from the Netflow collectors. Ensure to include data covering at least **30** minutes before the traceback.

In case of recurring traceback, collect data covering a few incidents. Additionally, in the case of high availability and clustering, collect data from all affected chassis.

Verification on the ASA/FTD CLI:

<#root>

```
ftd#
```

show run flow-export

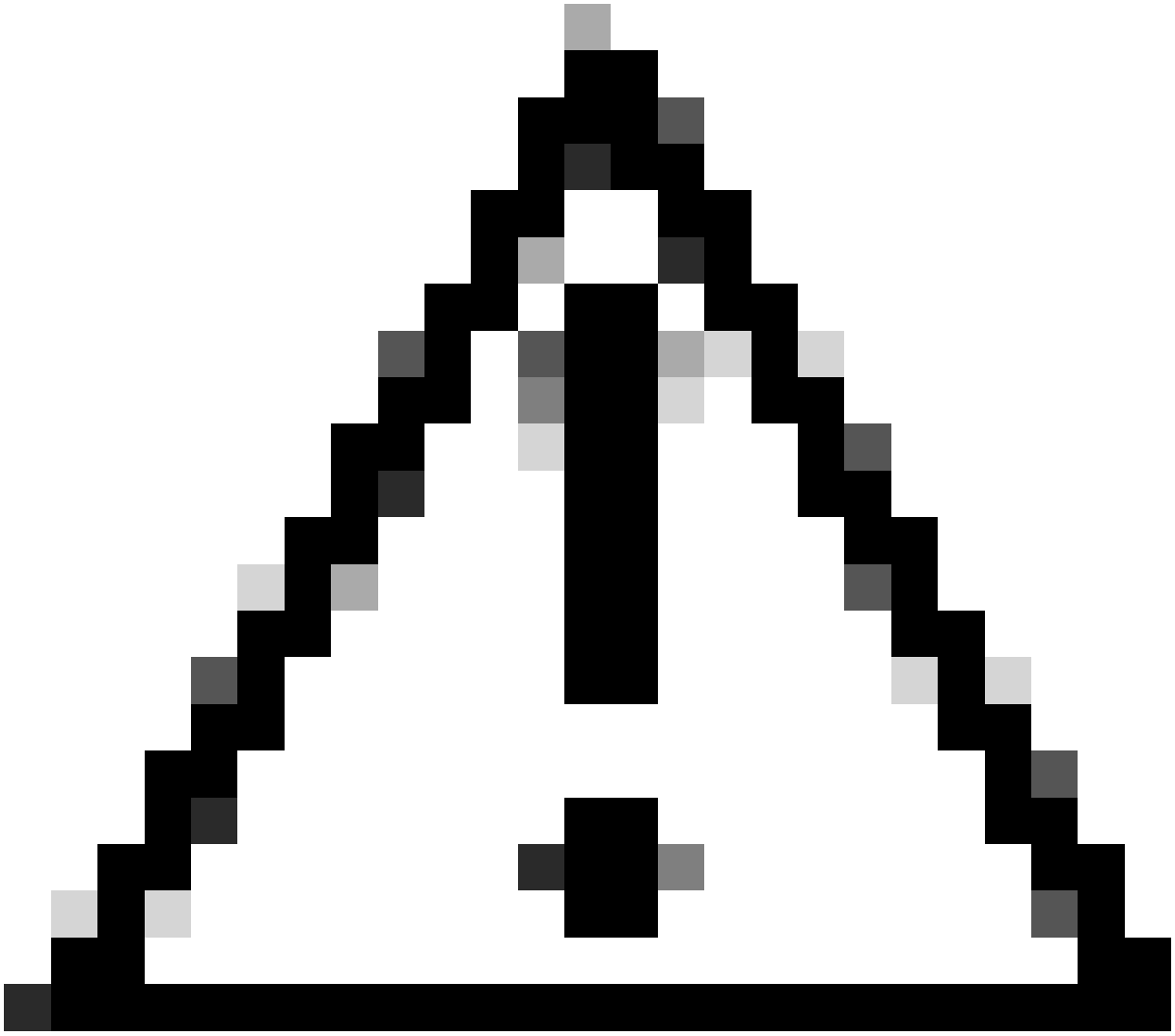
```
flow-export destination inside 192.0.2.1 1255

<-- Netflow collector address

flow-export delay flow-create 1



ftd#

show run policy-map global_policy


!
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect sip
  inspect netbios
  inspect tftp
  inspect icmp
  inspect icmp error
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP


class netflow



  flow-export event-type all destination 192.0.2.1

<-- Netflow collector address
  class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
```

14. In the case of recurring traceback, collect the output of the console sessions.

15. Open a TAC case and provide all the data.

How to Collect Crashinfo, Coredump and Minidump Files from Secure Firewall?

Proceed with these steps crashinfo, coredump and minidump Files from Secure Firewall:



Caution: Warning: Do not rename core, crashinfo or minidump files.

ASA

Upload files from the ASA CLI to the remote server:

<#root>

ASA#

copy flash:/crashinfo_lina.14664.20250813.205102 ?

```
  cluster:        Copy to cluster: file system
  disk0:          Copy to disk0: file system
  flash:          Copy to flash: file system
  ftp:            Copy to ftp: file system
  running-config  Update (merge with) current system configuration
  scp:            Copy to scp: file system
  smb:            Copy to smb: file system
```

```
  startup-config  Copy to startup configuration
  system:         Copy to system: file system
  tftp:           Copy to tftp: file system
```

FTD

Option 1 – Collect files using the Lina CLI

1. If the remote server is reachable from the Lina engine, copy files to **/mnt/disk0** and upload files from the Lina CLI:

```
<#root>

>

expert


admin@firepower:~$

ls -l /ngfw/var/data/cores/


total 928152
-rw-r--r-- 1 root root 500163689 Aug 13 10:30

core.lina.11.13050.1755081050.gz


-rw-r--r-- 1 root root 449295230 Aug 13 20:51 core.lina.11.14664.1755118254.gz
drwx------ 2 root root     16384 Aug 10 20:59 lost+found
drwxr-xr-x 3 root root      4096 Aug 10 21:01 sysdebug

admin@firepower:~$

sudo cp /ngfw/var/data/cores/core.lina.11.13050.1755081050.gz /mnt/disk0/

admin@firepower:~$

 exit



>

system support diagnostic-cli


Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower>

enable


Password:
firepower#

dir


Directory of disk0:/
```

```
…
1610612928  -rw-  500163689    17:00:13 Aug 22 2025
```

core.lina.11.13050.1755081050.gz

```
firepower#
```

copy disk0:/core.lina.11.13050.1755081050.gz ?

```
  cache:    Copy to cache: file system
  cluster:  Copy to cluster: file system
  disk0:    Copy to disk0: file system
  disk1:    Copy to disk1: file system
  flash:    Copy to flash: file system
  ftp:      Copy to ftp: file system
  scp:      Copy to scp: file system
  smb:      Copy to smb: file system
  system:   Copy to system: file system
  tftp:     Copy to tftp: file system
```

2. When the files from the remote server are downloaded, ensure to delete the copied files from **/mnt/disk0/** on FTD**:**

<#root>

```
admin@firepower:~$
```

cd /mnt/disk0/

```
admin@firepower:/mnt/disk0/:$
```

sudo rm core.lina.11.13050.1755081050.gz

Option 2 – Collect files using the expert mode CLI

Using Linux TFTP, SFTP, or SCTP clients upload the files from the expert mode to the remote server:

<#root>

```
>
```

expert

```
admin@firepower:~$
```

cd /ngfw/var/data/cores/

```
admin@firepower:/ngfw/var/data/cores$
```

sudo sctp core.lina.11.13050.1755081050.gz admin@192.0.2.1:/

```
admin@firepower:/ngfw/var/data/cores$
sudo tftp -l core.lina.11.13050.1755081050.gz -r core.lina.11.13050.1755081050.gz -p 192.0.2.1
```

Option 3 – Collect files using the FXOS local-mgmt CLI

On native mode FTD running on Firepower 1000, 2100 and Secure Firewall 1200, 3100, 4200 chassis, the core and minidump files can be collected from the FXOS local-mgmt CLI:

```
<#root>
firepower#
connect local-mgmt

firepower(local-mgmt)#
dir workspace:/cores

1 500163689 Aug 13 10:30:59 2025
core.lina.11.13050.1755081050.gz

firepower(local-mgmt)#
copy workspace:/core.lina.11.13050.1755081050.gz

?

  ftp:        Dest File URI
  http:       Dest File URI
  https:      Dest File URI
  scp:        Dest File URI
  sftp:       Dest File URI
  tftp:       Dest File URI
  usbdrive:   Dest File URI
  volatile:   Dest File URI
  workspace:  Dest File URI
```

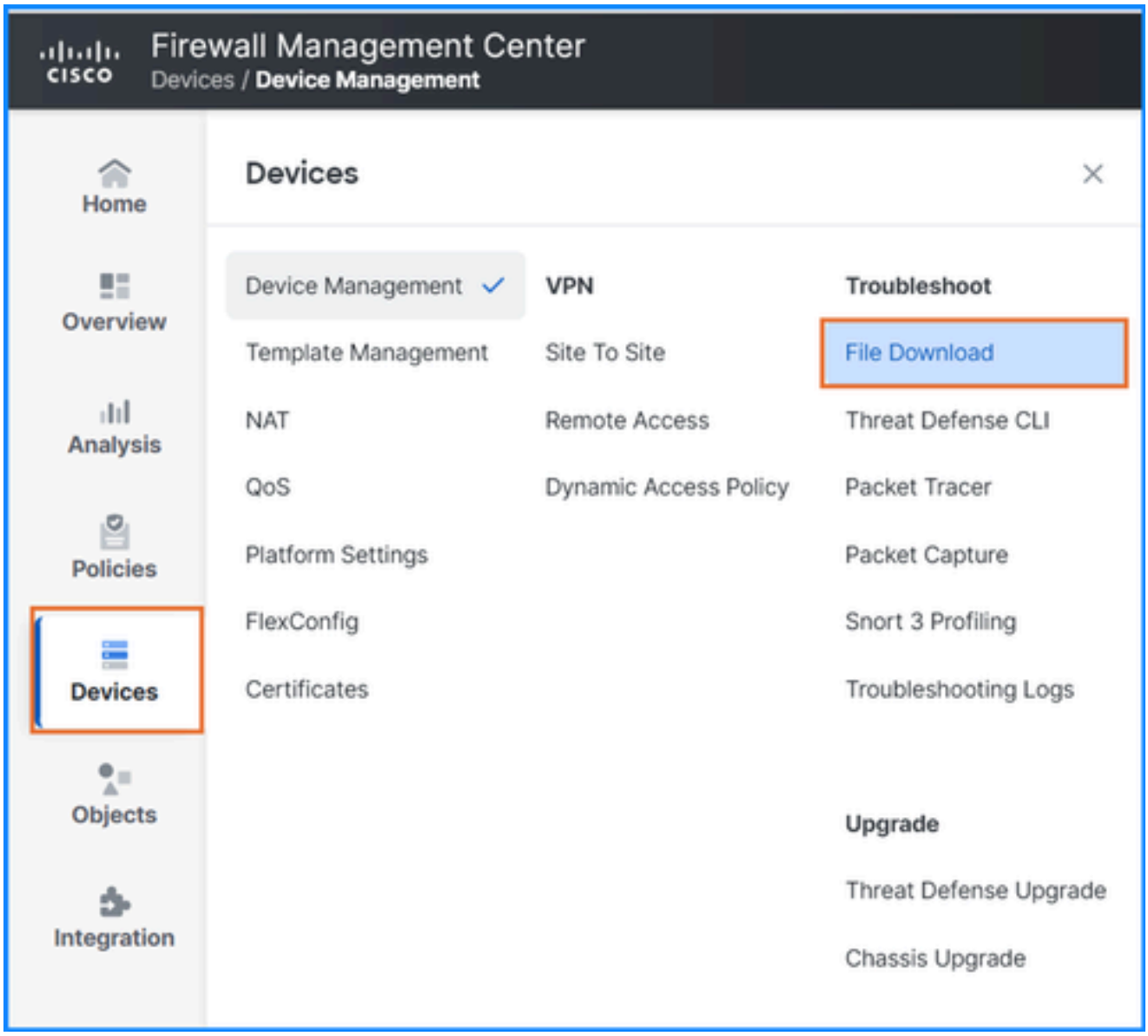
Option 4 – Collect files using the FMC UI

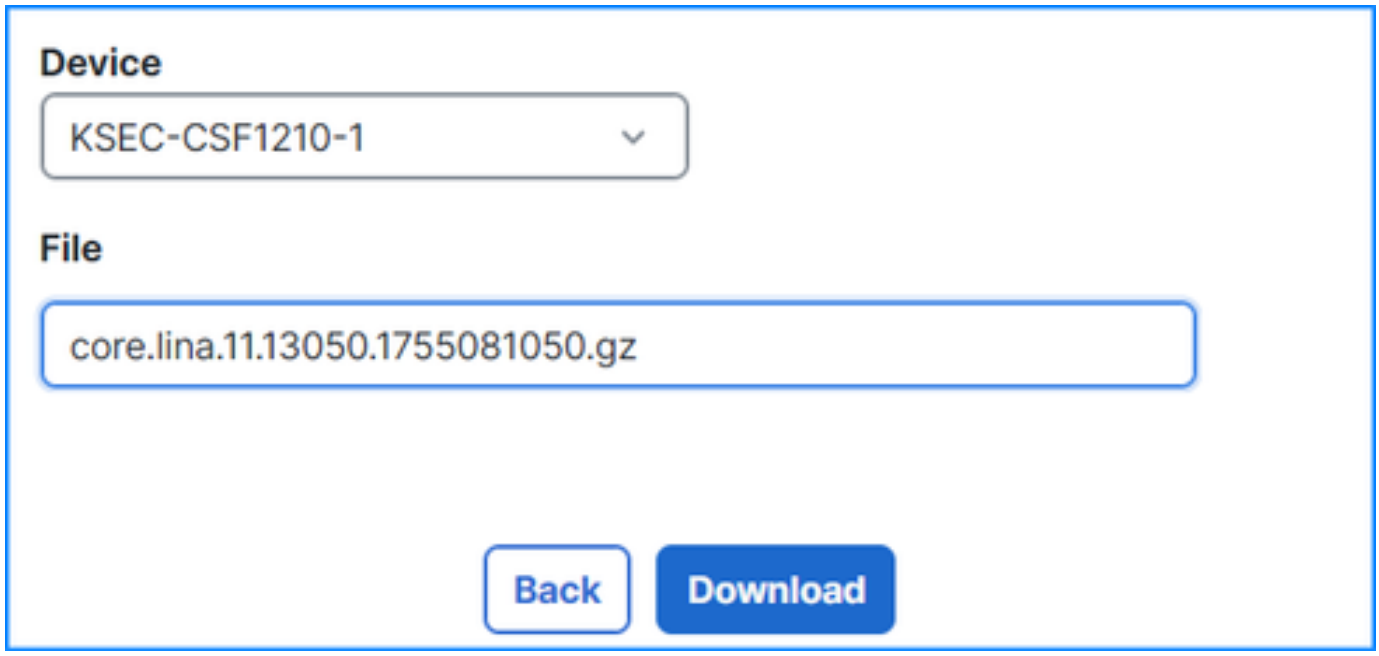
Copy files to **/ngfw/var/common:**

```
<#root>
>
expert

admin@firepower:~$
```

```
ls -l /ngfw/var/data/cores/


total 928152
-rw-r--r-- 1 root root 500163689 Aug 13 10:30

core.lina.11.13050.1755081050.gz


-rw-r--r-- 1 root root 449295230 Aug 13 20:51 core.lina.11.14664.1755118254.gz
drwx------ 2 root root     16384 Aug 10 20:59 lost+found
drwxr-xr-x 3 root root      4096 Aug 10 21:01 sysdebug

admin@firepower:~$

sudo cp /ngfw/var/data/cores/core.lina.11.13050.1755081050.gz /ngfw/var/common/

admin@firepower:~$

ls -l /ngfw/var/common/

total 928152
1610612928  -rw-  500163689    17:00:13 Aug 22 2025

core.lina.11.13050.1755081050.gz
```

2. Download the file from FMC UI using the **Devices** > **File Download** option:





3. When the files from the remote server are downloaded, ensure to delete the copied files from **/ngfw/var/common/** on FTD**:**

```
<#root>

admin@firepower:~$

cd


/ngfw/var/common/


admin@firepower:/mnt/disk0/:$

 sudo rm core.lina.11.13050.1755081050.gz
```

Firepower 4100 and 9300 Security Modules

1. Connect to the module and collect the core and crashinfo files as part of the module show-tech file:

```
<#root>

firepower #

connect module 1 console


Firepower-module1>

support diagnostic



======= Diagnostic =======
1. Create default diagnostic archive
2. Manually create diagnostic archive
3. Exit

Please enter your choice:

2


=== Manual Diagnostic ===
1. Add files to package
2. View files in package
3. Complete package
4. Exit.

Please enter your choice:

1


=== Add files to package | Manual Diagnostic ===
1. Platform Logs
2. Config Platform Logs
3. Crash Info files & Core dumps
4. Applications Logs
5. ASA Logs
b. Back to main menu
```

Please enter your choice:

3

----------sub-dirs----------
lost+found
-----------files------------
2025-08-04 12:43:07 | 419619286 |

core.lina.11.13050.1755081050.gz

([b] to go back or [m] for the menu or [s] to select files to add)
Type a sub-dir name to see its contents:

s

Type the partial name of the file to add ([*] for all, [<] to cancel)
>

core.lina.11.13050.1755081050.gz

core.lina.11.13050.1755081050.gz
Are you sure you want to add these files? (y/n)

y

=== Package Contents ===
[Added] core.lina.11.13050.1755081050.gz
========================
----------sub-dirs----------
lost+found
-----------files------------
2025-08-04 12:43:07 | 419619286 | core.lina.11.13050.1755081050.gz

([b] to go back or [m] for the menu or [s] to select files to add)
Type a sub-dir name to see its contents:

b

=== Manual Diagnostic ===
1. Add files to package
2. View files in package
3. Complete package
4. Exit.

Please enter your choice:

2

=== Package Contents ===
core.lina.11.13050.1755081050.gz
========================

=== Manual Diagnostic ===
1. Add files to package
2. View files in package
3. Complete package

```
4. Exit.

Please enter your choice:
```

3

```
Creating Manual archive
Added file: core.lina.11.13050.1755081050.gz
```

Created archive file Firepower-Module1_08_04_2025_13_17_50.tar

```
Firepower-module1>
```

support fileupload

```
Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status

Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status

Please enter your choice [x] to Exit:
```

1

```
-----------files------------
2025-08-04 13:17:50.723396 | 419624960  |
```

Firepower-Module1_08_04_2025_13_17_50.tar

```
([s] to select files or [x] to Exit):
```

s

```
Type the partial name of the file to add, [<] to cancel
>
```

Firepower-Module1_08_04_2025_13_17_50.tar

```
Firepower-Module1_08_04_2025_13_17_50.tar
Are you sure you want to add these files? (y/n)
```

y

```
=== Package Contents ===
[Added] Firepower-Module1_08_04_2025_13_17_50.tar
========================
```

```
Type the partial name of the file to add, [<] to cancel
>
```

<

```
Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status
Please enter your choice [x] to Exit:
```

2

```
1 : Firepower-Module1_08_04_2025_13_17_50.tar

Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status

Please enter your choice [x] to Exit:
```

3

Transfer of Firepower-Module1_08_04_2025_13_17_50.tar started.

```
Firepower-module1>
Firepower-module1>
Firepower-module1> ß
```

Shift + ~

```
telnet> quit
Connection closed.

firepower /ssa #
```

connect local-mgmt

```
firepower(local-mgmt)#
```

dir workspace:/bladelog/blade-1/

```
1 152828400 Aug 04 13:26:35 2025
```

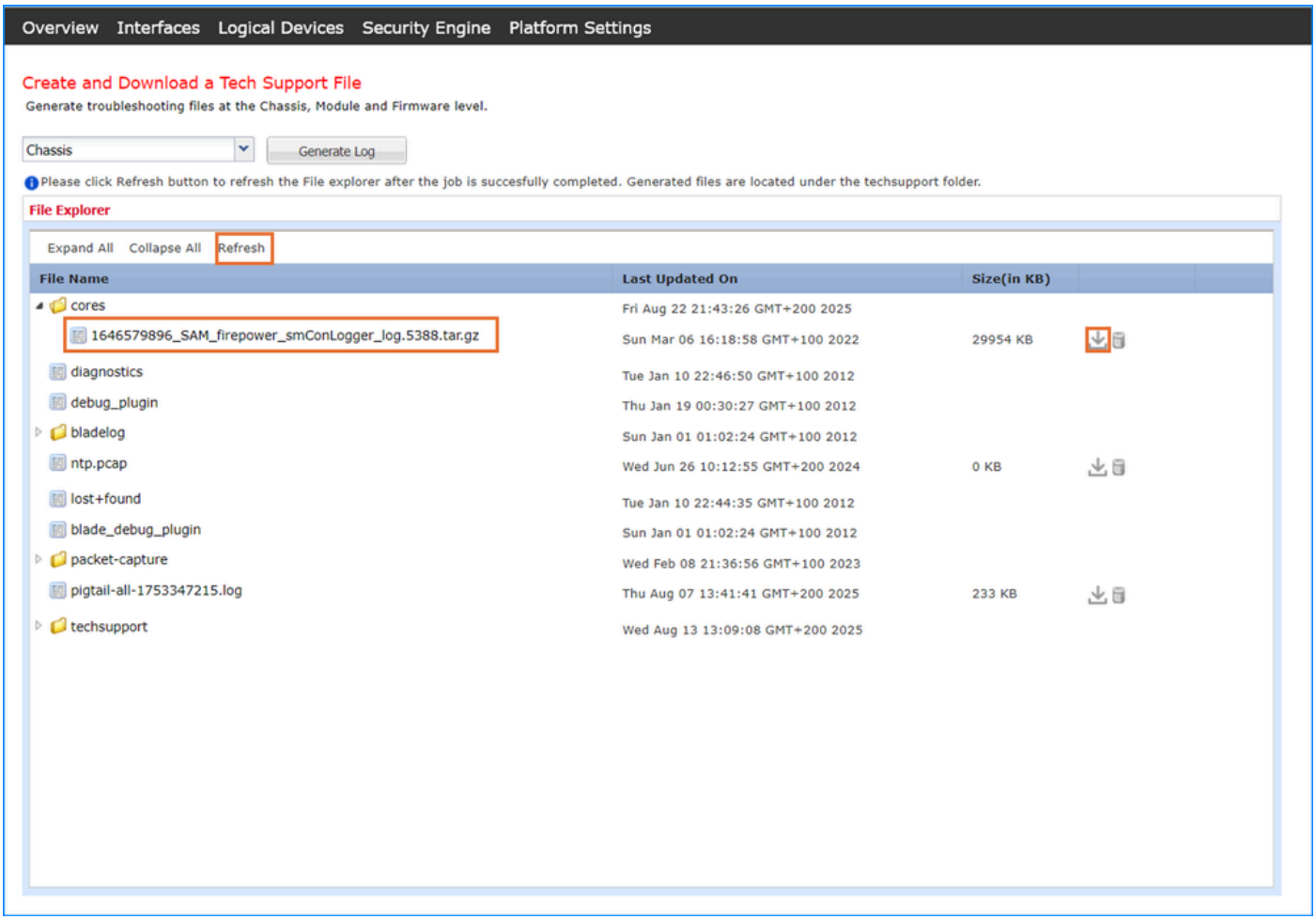
Firepower-Module1_08_04_2025_13_17_50.tar

Firepower 4100 and 9300 Chassis

1. Collect core files using the FXOS local-mgmt CLI:

```
<#root>

firepower#

connect local-mgmt


firepower(local-mgmt)#

dir workspace:/cores


1 30673335 Mar 06 16:18:58 2022

1646579896_SAM_firepower-1_smConLogger_log.5388.tar.gz


firepower(local-mgmt)#

copy workspace:/cores/1646579896_SAM_firepower-1_smConLogger_log.5388.tar.gz ?


  ftp:        Dest File URI
  http:       Dest File URI
  https:      Dest File URI
  scp:        Dest File URI
  sftp:       Dest File URI
  tftp:       Dest File URI
  usbdrive:   Dest File URI
  volatile:   Dest File URI
  workspace:  Dest File URI
```

2. Alternatively, collect files from the FCM UI via **Tools** > **Troubleshooting Logs.** Click **Refresh** to update the file directory view and the download icon next to the core file:



References

- Verify Firepower Software Versions
- Verify Firepower, Instance, Availability, Scalability Configuration
- Troubleshoot Firepower File Generation Procedures
- ASA Command Reference