보안 방화벽에서 소프트웨어 추적/충돌의 근본 원인 분석을 위한 데이터 수집

목차

소개

이 문서에서는 소프트웨어 역추적 시 데이터를 수집하는 단계를 설명합니다.

사전 요구 사항

요구 사항

기본 제품 지식

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

배경

FTD 또는 ASA 소프트웨어는 다음과 같은 서로 다른 이유로 역추적되며 일반적으로 다시 로드됩니다.

- 운영 체제 및 타사 구성 요소의 결함을 포함한 소프트웨어 결함.
- 하위 수준 메모리 또는 CPU 오류와 같은 하드웨어 예외
- 메모리와 같은 시스템 리소스가 부족한 경우도 있습니다.
- TAC 감독하에 진단 목적을 위해 사용자가 수동으로 트리거한 작업:

```
<#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
```

추격이라고도 하는 추적의 경우 프로세스에 따라 대개 crashinfo, core 또는 minidump 파일이 생성됩니다.

- crashinfo에는 프로세스 메모리의 최소 진단 데이터가 포함되어 있습니다.
- core 파일은 역추적 시 프로세스 메모리의 전체 덤프입니다.
- minidump 파일은 Snort3에 해당하며 프로세스 메모리의 진단 데이터를 포함합니다.

Secure Firewall 소프트웨어에서 추적이 수행된 프로세스는 다음 구성 요소 중 하나에 포함될 수 있습니다.

- Firepower 1000, 2100, 4100, 9300, Secure Firewall 1200, 3100, 4200 섀시
- Firepower 4100, 9300 보안 모듈.

코어 및 crashinfo 파일 외에도, 역추적의 RCA(근본 원인 분석)에는 문제 해결 및 show-tech 파일, syslog 메시지 등과 같은 추가 정보가 필요합니다.

코어 및 crashinfo 파일 분석은 TAC와 Cisco에서 서비스 요청의 일부로 처리합니다(사례).

데이터 수집

역추적의 RCA에 필요한 데이터를 수집하려면 다음 단계를 진행합니다. 파일 회전으로 인한 데이터 손실 위험 때문에, 요청한 데이터를 빠른 시일 내에 제공해 주시기 바랍니다.

1. 다음 항목을 명확히 하십시오.

1a. 정확한 하드웨어.

10억 소프트웨어 버전.

1c. 보안 방화벽 소프트웨어 유형(ASA 또는 FTD).

1d. 구축 모드(기본 또는 다중 인스턴스 모드).

자세한 확인 단계는 Firepower 소프트웨어 버전 확인 및 Firepower, 인스턴스, 가용성, 확장성 구성 확인을 참조하십시오.

2. 다음과 같은 최근의 환경 변화 여부를 명확히 할 것

2a. 트래픽 추가.

20억 명령을 비롯한 주요 구성 변경 사항

타임스탬프와 시간대를 최대한 정확하게 포함해야 합니다.

3. 특정 명령을 사용하여 컨피그레이션을 변경한 후 역추적이 발생한 경우 터미널 세션 출력을 수집합니다. ASA에서 명령 권한 부여가 구성된 경우 ISE(Identity Services Engine)와 같은 원격 서버에서 명령 권한 부여 보고서를 수집합니다.

4. 다음 단계에서는 최신 타임스탬프가 있는 crashinfo, core 또는 minidump 파일을 확인하고 각 파일의 전체 경로를 확인합니다. 전체 경로는 How to Collect Crashinfo, Coredump and Minidump Files from Secure Firewall(보안 방화벽에서 Crashinfo, Coredump 및 Minidump 파일을 수집하는 방법)에 나와 있는 파일 수집에 필요합니다. 섹션을 참조하십시오.

ASA

4.1. crashinfo 파일이 있는지 확인합니다. 최신 crashinfo를 보려면 show crashinfo 명령을 실행합니다. crashinfo 파일은 dir 명령 출력에서 찾을 수 있습니다.

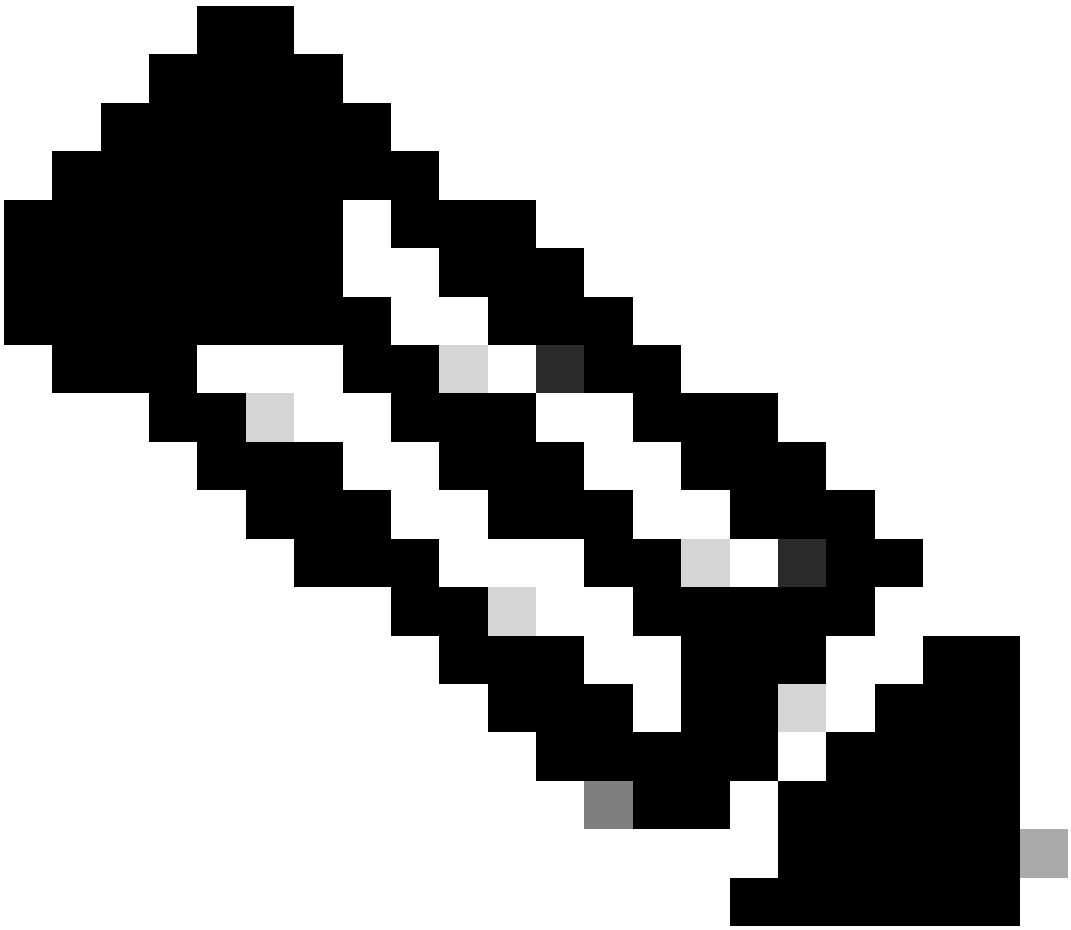
<#root>

```
asa#
dir

Directory of disk0:/
…
1610891723  -rw-  413363       20:51:22 Aug 13 2025
crashinfo_lina.14664.20250813.205102
```

4.2. dir coredumpfsys 명령을 사용하여 ASA 코어 파일이 있는지 확인합니다.

<#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
```



참고: 가상 ASA에서는 기본적으로 코어덤프 기능이 비활성화되어 있습니다.

<#root>

ciscoasa#

show coredump

filesystem 'disk0:' has no coredump filesystem

코어덤프 기능을 활성화하려면 Cisco Secure Firewall ASA Series Command Reference, A-H Commands의 코어덤프 활성화 섹션을 참조하십시오.

FTD

4.1. FTD crashinfo 파일이 있는지 확인합니다. 최신 crashinfo를 보려면 show crashinfo 명령을 실행합니다. crashinfo 파일은 dir 명령 출력에서 찾을 수 있습니다.

<#root>

ftd#

dir

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

crashinfo_lina.14664.20250813.205102

FTD에서 crashinfo 파일은 expert mode/mnt/disk0/ 디렉터리에서 찾을 수 있습니다.

<#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

FTD 문제 해결 파일에서 crashinfo 파일은 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. FTD 코어 파일이 있는지 확인합니다. FTD에서 코어 파일은 expert 모드 /ngfw/var/data/cores/and/ngfw/var/common/directories에서 액세스할 수 있습니다.

<#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

FTD 트러블슈팅 파일에서 코어 파일 이름은 \ \`ls*의 파일 명령 출력/for\ CORE에 있습니다.

<#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 전용 코어덤프

이 섹션은 Snort3 엔진을 실행하는 FTD에만 적용됩니다.

4.1. Snort3 엔진 crashinfo 파일 snort3-crashinfo.*가 expert 모드/ngfw/var/log/crashinfo/ 디렉터리에 있는지 확인합니다.

<#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

FTD 문제 해결 파일에서 동일한 파일이 dir-archives/var-log/crashinfo/에 있습니다.

4.2. /ngfw/var/data/cores/에서 Snort3 minidump 파일 minidump_*가 있는지 확인합니다.

<#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

FTD 문제 해결 파일에서 미니덤프 파일은 file-contents/ngfw/var/data/cores/에 있습니다.

<#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 및 9300 보안 모듈

이 섹션은 Firepower 4100 및 9300 모듈에만 적용됩니다.

4.1. crashinfo 및 core 파일이 있는지 확인합니다.

<#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. Firepower 1000, 2100 및 Secure Firewall 1200, 3100, 4200 섀시에서 local-mgmt 셸의 dir workspace:/cores 및 dir workspace:/cores_fxos 명령을 사용하여 코어 파일이 있는지 확인합니다.

ASA 애플리케이션이 설치된 경우, connect fxos admin 명령을 사용하여 FXOS 셸에 연결합니다.

```
<#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
```

코어 파일은 섀시 문제 해결 파일의 /opt/cisco/platform/logs/prune_cores.log 파일에도 나와 있습니다.

```
<#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. Firepower 4100 및 9300 섀시에서 local-mgmt 셸의 dir workspace:/cores 명령을 사용하여 코어 파일이 있는지 확인합니다.

<#root>

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

dir workspace:/cores

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

코어 파일 이름은 섀시 문제 해결 파일 내에서 찾을 수 있습니다. 파일 *_BC1_all/FPRM_A_TechSupport/sw_techsupportinfo에서 show cores 명령 출력에서 *는 문제 해결 파일 이름의 일부입니다(예: 20250311123356_ FW_BC1_all.tar).

5. 크래시정보, 코어덤프 및 미니덤프 파일이 사고와 관련이 있는지 확인합니다.

- 파일 타임스탬프를 인시던트의 타임스탬프와 비교합니다.
- Linux date 명령을 사용하여 파일 이름의 에포크 타임스탬프를 날짜로 변환합니다.

코어 및 미니덤프 파일의 경우 Linux 호스트의 날짜를 사용하여 에포크 타임스탬프를 날짜 시간으로 변환할 수 있습니다.

<#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
```

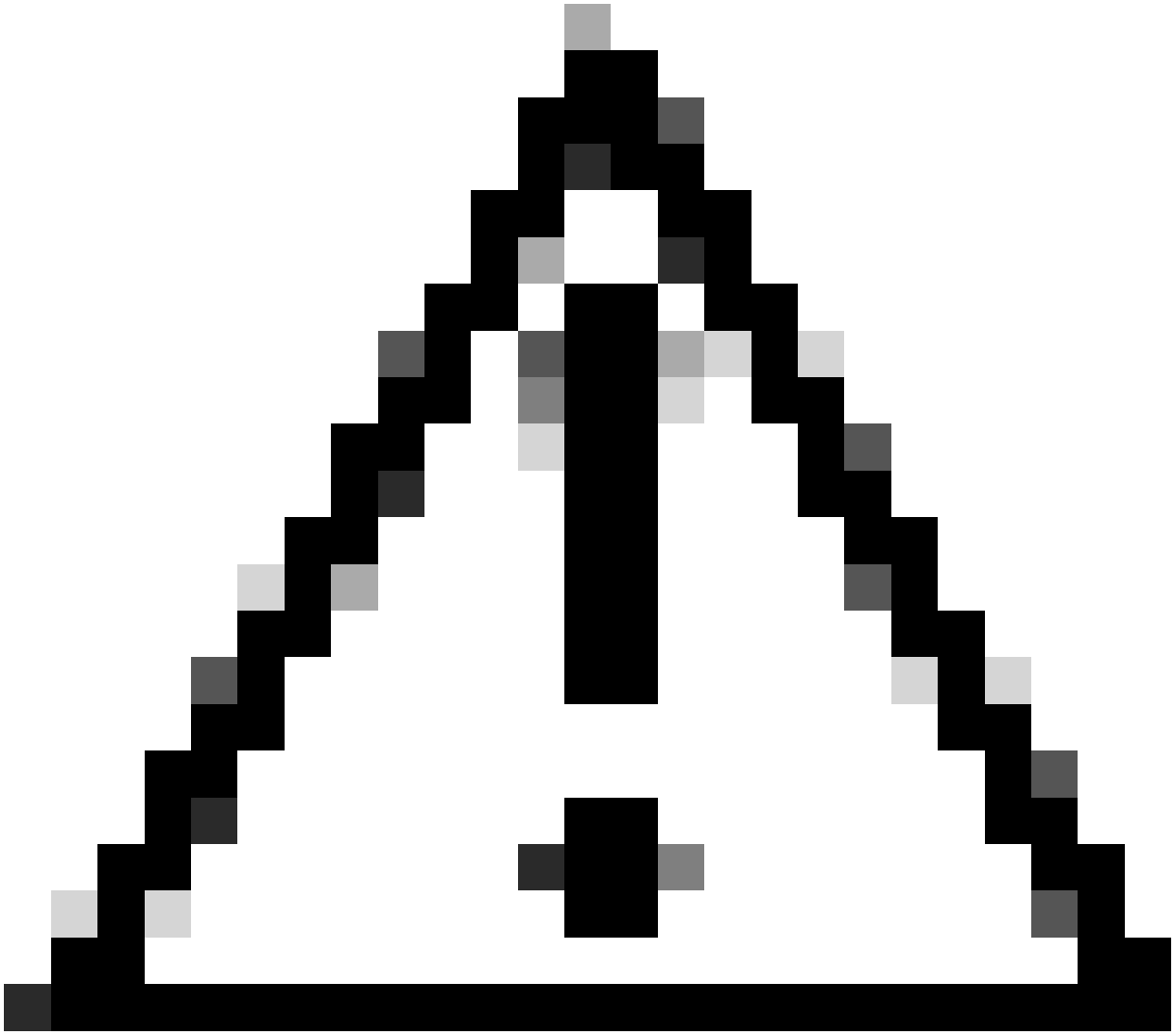
.1753342057.

```
gz

linux $
```

date -d @1753342057

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

6. 단계 4-5에서 crashinfo, minidump 및 core 파일을 다운로드하려면 How to Collect Crashinfo, Coredump and Minidump Files from Secure Firewall? 섹션을 참조하십시오.



주의: core, crashinfo 또는 minidump 파일의 이름을 변경하지 마십시오.

---

7. Firepower 파일 생성 절차 문제 해결의 단계를 진행하여 show-tech 및 troubleshoot 파일을 수집합니다.

7a. ASA show-tech 파일.

70억 FTD 문제 해결 파일.

7시 Firepower 4100 및 9300 보안 모듈 show-tech 파일

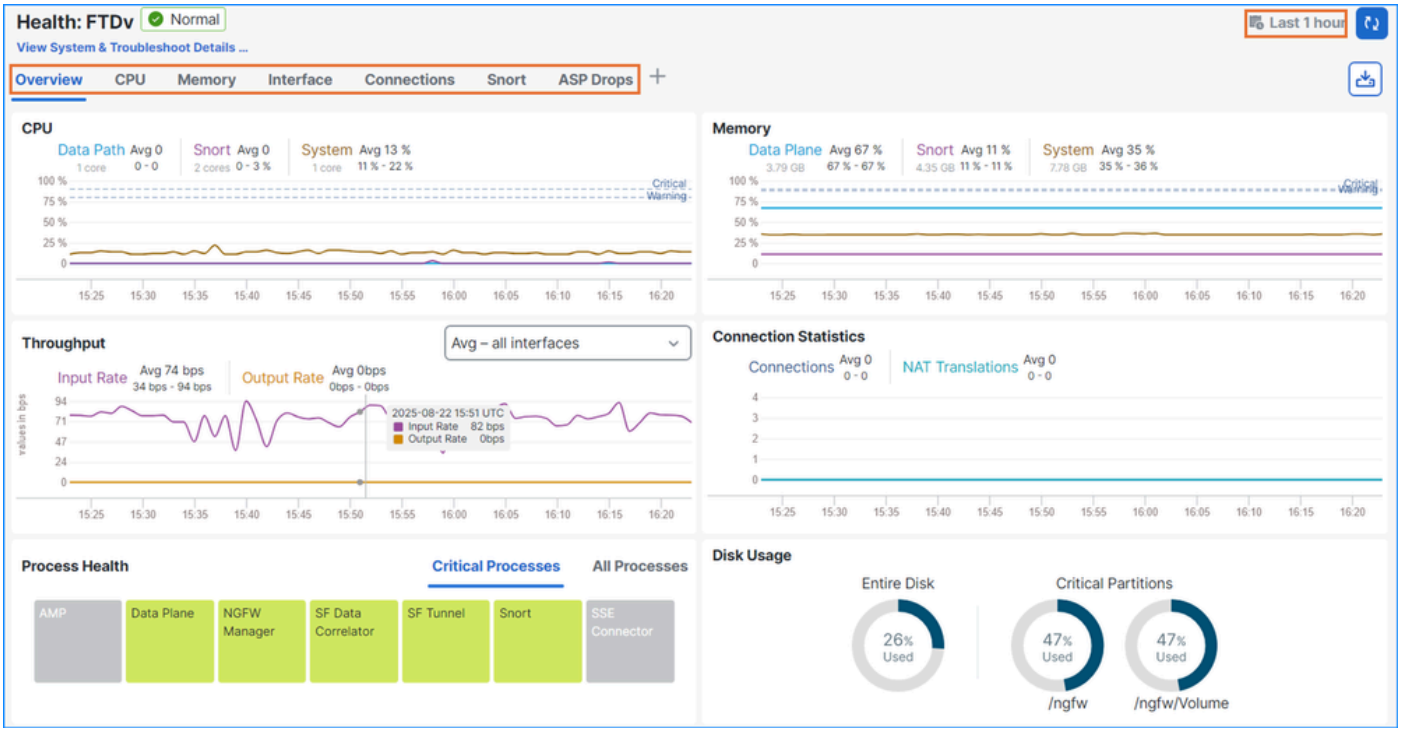
7일 Firepower 4100 및 9300 섀시 show-tech 파일

7e. Firepower 1000, 2100 및 Secure Firewall 1200, 3100, 4200 섀시 show-tech 파일 컨테이너 모드의 Secure Firewall 3100, 4200용 섀시 문제 해결 파일은 FMC > Devices > [chassis] > 3 dots > Troubleshoot Files 옵션을 통해 다운로드할 수 있습니다.

8. FTD의 경우 역추적 전 30분 이상에 FMC의 상태 모니터링 탭에 대한 스크린샷을 수집합니다. 강

조 표시된 모든 탭의 스크린샷을 포함해야 합니다. 역추적 반복의 경우 몇 가지 사고에 대한 스크린샷을 수집하십시오.

또한 고가용성 및 클러스터링의 경우 영향을 받는 모든 유닛에 대한 스크린샷을 수집합니다.



9. 역추적 전에 최소 30분 동안 syslog 서버에서 원시(구문 분석되지 않은) Lina 엔진 syslog 메시지를 수집합니다. 원시 형식은 TAC 및 엔지니어링 툴의 내부 처리에 필수적입니다.

되풀이 역추적의 경우 몇 가지 인시던트를 다루는 원시 메시지를 수집합니다. 또한 고가용성 및 클러스터링의 경우 영향을 받는 모든 유닛에서 원시 syslog를 수집합니다.

ASA/FTD CLI에서 확인:

<#root>

```
ftd#
```

show run logging

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

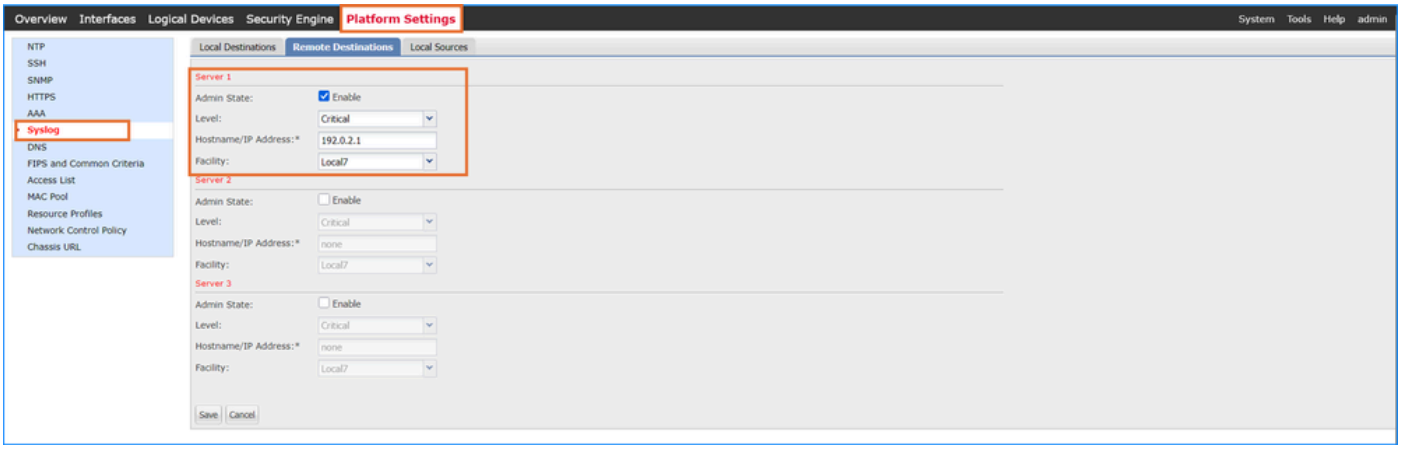
192.0.2.1

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

10. Firepower 4100 및 9300의 경우 역추적 10분 전에 syslog 서버에서 원시(구문 분석되지 않은) FXOS 메시지를 수집합니다. 원시 형식은 TAC 및 엔지니어링 툴의 내부 처리에 필수적입니다.

또한 고가용성 및 클러스터링의 경우 영향을 받는 모든 섀시에서 원시 syslog를 수집합니다.

firepower FCM(Chassis Manager) UI(User Interface) 확인:



FXOS CLI에서 확인:

<#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. 구성된 SNMP 서버에서 트랩을 포함한 ASA 또는 FTD CPU, 메모리, 인터페이스 데이터를 수집합니다. 역추적 전 30분 이상 데이터를 포함해야 합니다.

되풀이 역추적의 경우 몇 가지 인시던트를 포함하는 원시 메시지를 수집합니다. 또한 고가용성 및 클러스터링의 경우 영향을 받는 모든 섀시에서 원시 메시지를 수집합니다.

ASA/FTD CLI에서 확인:

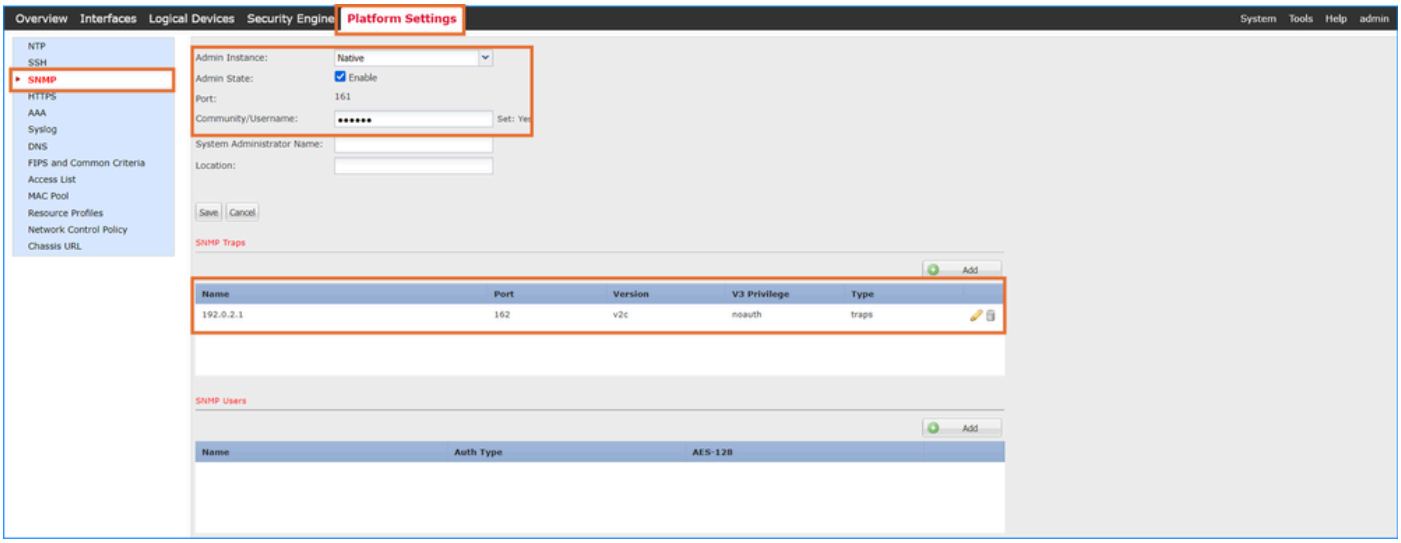
<#root>

```
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. Firepower 4100 및 9300의 경우 구성된 SNMP 서버에서 CPU, 메모리, 트랩을 포함한 인터페이스 데이터를 수집합니다. 역추적 전 30분 이상 데이터를 포함해야 합니다.

되풀이 역추적의 경우 몇 가지 인시던트를 포함하는 원시 메시지를 수집합니다. 또한 고가용성 및 클러스터링의 경우 영향을 받는 모든 섀시에서 원시 메시지를 수집합니다.

FCM UI 확인:



FXOS CLI에서 확인:

<#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. Netflow 컬렉터에서 트래픽 프로필을 수집합니다. 역추적 전 30분 이상 데이터를 포함해야 합니다.

되풀이 역추적의 경우, 몇 가지 인시던트에 대한 데이터를 수집합니다. 또한 고가용성 및 클러스터링의 경우 영향을 받는 모든 섀시에서 데이터를 수집합니다.

ASA/FTD CLI에서 확인:

```
<#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
```

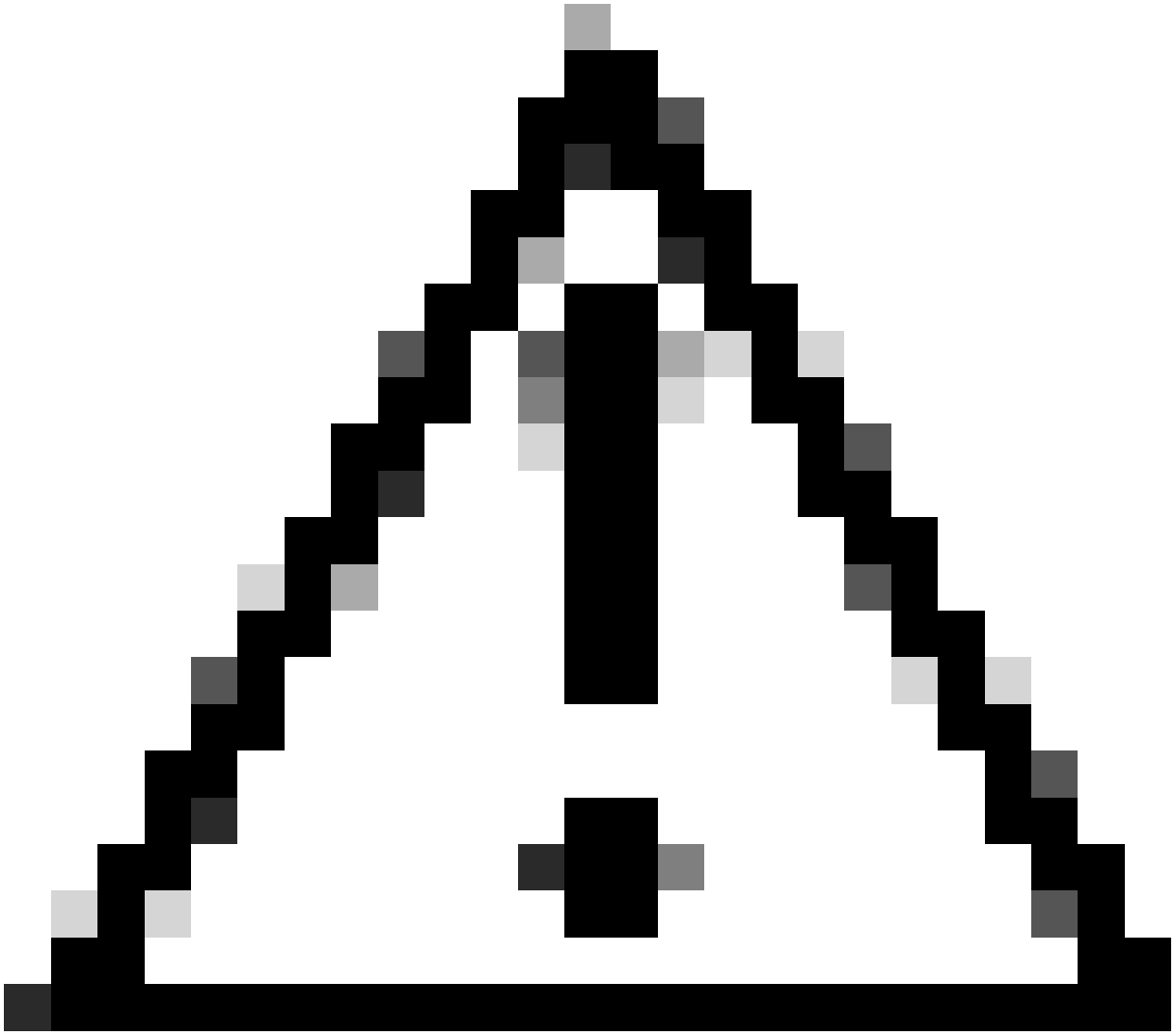
```
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect sip
  inspect netbios
  inspect tftp
  inspect icmp
  inspect icmp error
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP


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. 반복 역추적의 경우 콘솔 세션의 출력을 수집합니다.

15. TAC 케이스를 열고 모든 데이터를 제공합니다.

보안 방화벽에서 Crashinfo, Coredump 및 Minidump 파일을 수집하는 방법?

보안 방화벽에서 crashinfo, coredump 및 minidump 파일을 다음 단계를 진행합니다.



주의: 경고: core, crashinfo 또는 minidump 파일의 이름을 변경하지 마십시오.

ASA

ASA CLI에서 원격 서버로 파일을 업로드합니다.

<#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

옵션 1 - Lina CLI를 사용하여 파일 수집

1. Lina 엔진에서 원격 서버에 연결할 수 있는 경우 파일을 /mnt/disk0에 복사하고 Lina CLI에서 파일을 업로드합니다.

```
<#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. 원격 서버의 파일을 다운로드할 때 FTD의 /mnt/disk0/에서 복사한 파일을 삭제해야 합니다.

<#root>

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

cd /mnt/disk0/

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

sudo rm core.lina.11.13050.1755081050.gz

옵션 2 - 전문가 모드 CLI를 사용하여 파일 수집

Linux TFTP, SFTP 또는 SCTP 클라이언트를 사용하면 expert 모드에서 원격 서버로 파일을 업로드합니다.

<#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
```

옵션 3 - FXOS local-mgmt CLI를 사용하여 파일 수집

firepower 1000, 2100 및 Secure Firewall 1200, 3100, 4200 섀시에서 실행되는 기본 모드 FTD에서는 FXOS 로컬 관리 CLI에서 코어 및 미니덤프 파일을 수집할 수 있습니다.

```
<#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
```

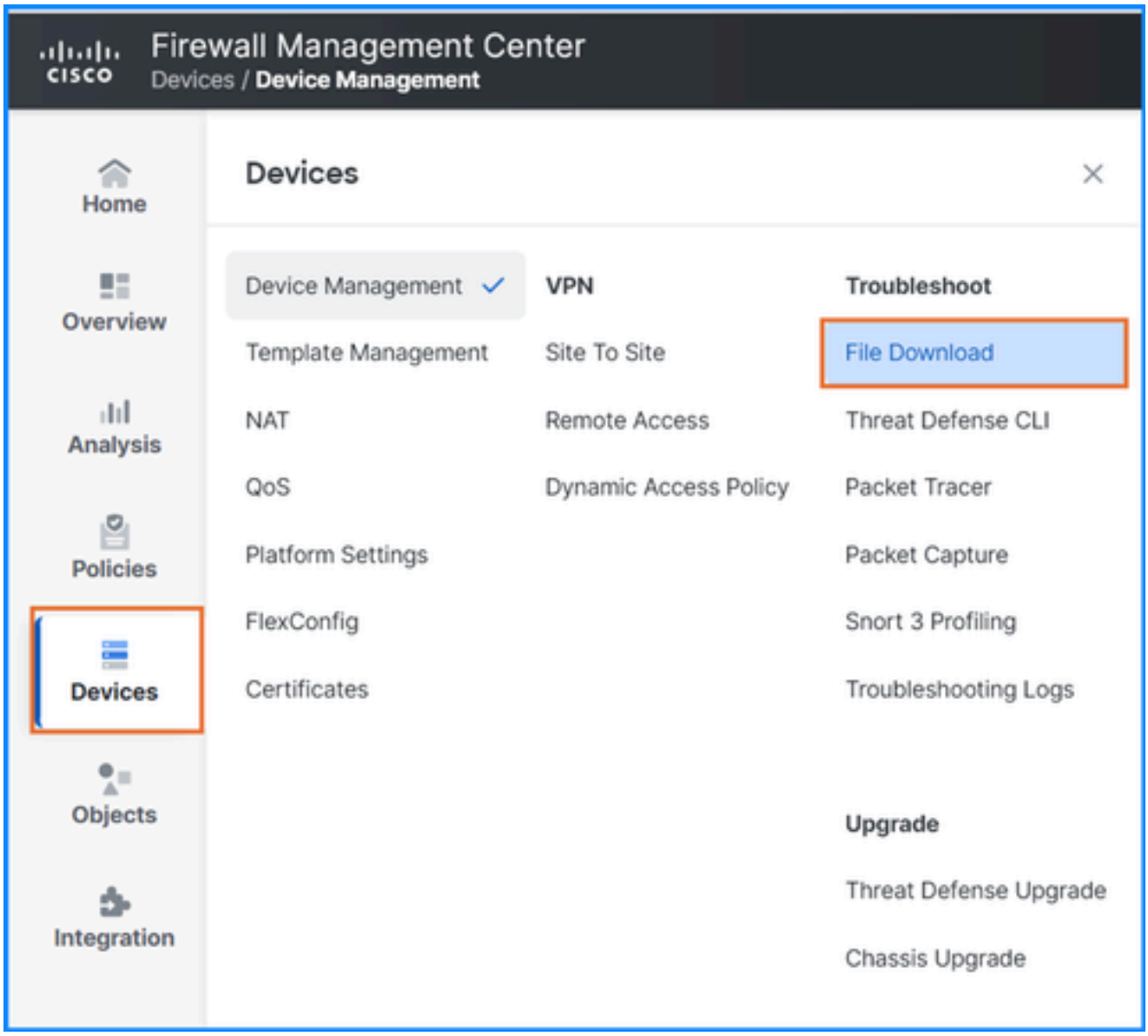
옵션 4 - FMC UI를 사용하여 파일 수집

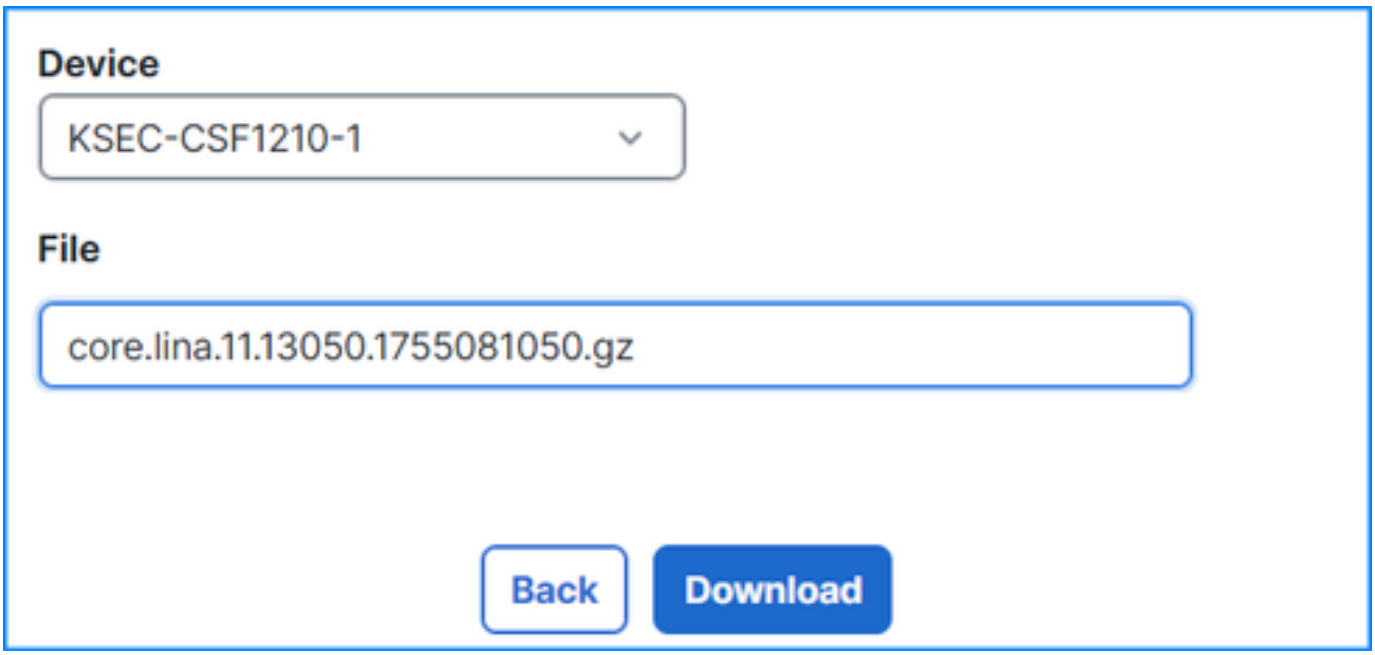
파일을 /ngfw/var/common에 복사합니다.

```
<#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. Devices > File Download 옵션을 사용하여 FMC UI에서 파일을 다운로드합니다.





3. 원격 서버의 파일을 다운로드할 때 FTD의 /ngfw/var/common/에서 복사한 파일을 삭제해야 합니

다.

<#root>

admin@firepower:~$

cd

/ngfw/var/common/

admin@firepower:/mnt/disk0/:$

sudo rm core.lina.11.13050.1755081050.gz

Firepower 4100 및 9300 보안 모듈

1. 모듈에 연결하고 모듈 show-tech 파일의 일부로 core 및 crashinfo 파일을 수집합니다.

<#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

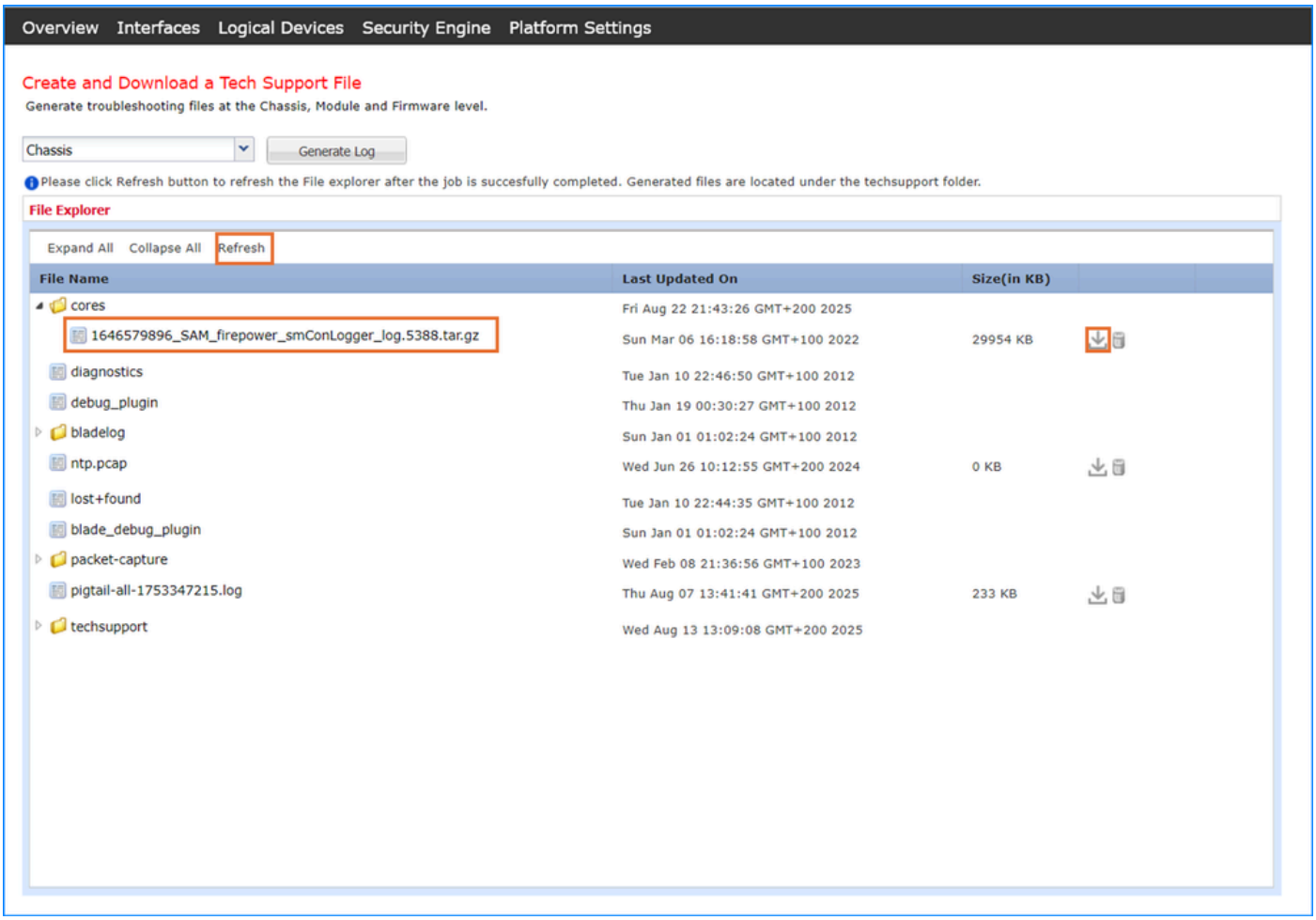
Firepower 4100 및 9300 섀시

1. FXOS local-mgmt CLI를 사용하여 핵심 파일을 수집합니다.

<#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. 또는 Tools > Troubleshooting Logs를 통해 FCM UI에서 파일을 수집합니다. Refresh(새로 고침)를 클릭하여 파일 디렉토리 보기 및 코어 파일 옆의 다운로드 아이콘을 업데이트합니다.



참조

- [firepower 소프트웨어 버전 확인]
- [firepower, 인스턴스, 가용성, 확장성 컨피그레이션 확인]
- [firepower 파일 생성 절차 문제 해결]
- [ASA 명령 참조]

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.