Firepower Threat Defense 디바이스에서 코어 파일 수집

목차

소개

이 문서에서는 FTD 소프트웨어를 지원하는 모든 플랫폼을 통해 FTD 디바이스에 대한 모든 유형의 코어 파일을 수집하는 절차에 대해 설명합니다.FTD의 프로세스에 심각한 문제가 발생하면 프로세스의 실행 중인 메모리의 덤프를 코어 파일로 저장할 수 있습니다.장애의 근본 원인을 확인하기 위해 Cisco 기술 지원에서 코어 파일을 요청할 수 있습니다.

FTD 디바이스에는 두 가지 유형의 핵심 파일, Firepower 코어 및 LINA 코어 파일이 있습니다.

사전 요구 사항

요구 사항

Cisco는 다음 제품에 대해 알고 있는 것이 좋습니다.

- FMC(Firepower Management Center)
- Firepower Device Manager(FDM)
- FTD(Firepower Threat Defense)
- FXOS(Firepower Extensible Operation System)

절차

Firepower 프로세스 코어 파일

FTD가 Firepower 2100, 1000, ASA 어플라이언스 및 ISA 3000 어플라이언스에 있는

경우 Firepower Core 파일의 위치

이 모든 플랫폼에서 모든 Firepower 프로세스와 관련된 코어 파일을 이 절차에 따라 찾을 수 있습니다.

1. SSH 또는 콘솔을 통해 어플라이언스의 CLI에 연결합니다.

2. 전문가 모드로 들어갑니다.

```
> expert
admin@firepower:~$
```

3. 루트 사용자가 됩니다.

```
admin@firepower:~$ sudo su
Password:
root@firepower:/home/admin#
```

4. 다음으로 이동합니다. /ngfw/var/common/ 폴더 - 핵심 파일이 있는 위치입니다.

```
root@firepower:/home/admin# cd /ngfw/var/common/
```

5. 파일의 폴더를 확인합니다.

```
root@firepower:/ngfw/var/common# ls -l | grep -i core
total 21616
-rw-r--r-- 1 root root 22130788 Nov  6  2020 process.core.tar.gz
```

FTD가 Firepower 4100 또는 9300에 있는 경우 Firepower Core 파일의 위치

이 두 플랫폼의 경우 코어 파일은 두 개의 가능한 경로에 배치할 수 있으며, 첫 번째 파일은 이전 섹션과 동일하며, 두 번째 경로는 이 절차에 따라 찾을 수 있습니다.

1. SSH 또는 콘솔을 통해 어플라이언스의 CLI에 연결합니다.

2. 전문가 모드로 들어갑니다.

```
> expert
admin@firepower:~$
```

3. 루트 사용자가 됩니다.

```
admin@firepower:~$ sudo su
Password:
root@firepower:/home/admin#
```

4. 다음으로 이동합니다. /ngfw/var/data/cores/ 폴더 - 핵심 파일이 있는 위치입니다.

```
root@firepower:/home/admin# cd /ngfw/var/data/cores/
```

5. 파일의 폴더를 확인합니다.

```
root@firepower:cores# ls -l | grep -i core
```

```
-rw-r--r-- 1 root root 27873115 Nov 17 15:01
core.snort.59095.1605625274.gz
-rw-r--r-- 1 root root 27856205 Nov 17 15:02
core.snort.59352.1605625368.gz
```

LINA 프로세스 코어 파일

FTD가 Firepower 1000, 2100, 4100 및 9300에 있는 경우 LINA 코어 파일의 위치

1. SSH 또는 콘솔을 통해 어플라이언스의 CLI에 연결합니다.

2. 전문가 모드로 들어갑니다.

```
> expert
admin@firepower:~$
```

3. 루트 사용자가 됩니다.

```
admin@firepower:~$ sudo su
Password:
root@firepower:/home/admin#
```

4. 다음으로 이동합니다. /ngfw/var/data/cores/ 폴더 - 핵심 파일이 있는 위치입니다.

```
root@firepower:/home/admin# cd /ngfw/var/data/cores/
```

5. 핵심 파일의 폴더를 확인합니다.

```
root@firepower:/ngfw/var/data/cores# ls -l | grep -i core
-rw-r--r-- 1 root root 84831856 Nov 17 15:49
core.lina.23228.1605628188.gz
```

FMC를 사용하여 코어 파일을 수집하는 방법

FTD가 설치된 모든 플랫폼에서 이 절차를 수행하여 디바이스에서 코어 파일을 추출해야 합니다.

1. 코어 파일이 있는 모든 플랫폼의 경우 /ngfw/var/data/cores/ 파일을 /ngfw/var/common/.

```
root@firepower:/ngfw/var/data/cores# ls -l | grep -i core
-rw-r--r-- 1 root root 84831856 Nov 17 15:49 core.lina.23228.1605628188.gz
root@firepower:/ngfw/var/data/cores# mv core* /ngfw/var/common/
root@firepower:/ngfw/var/data/cores# cd /ngfw/var/common/
root@firepower:/ngfw/var/common# ls -l | grep -i core
-rw-r--r-- 1 root root 84831856 Nov 17 15:49
core.lina.23228.1605628188.gz
```

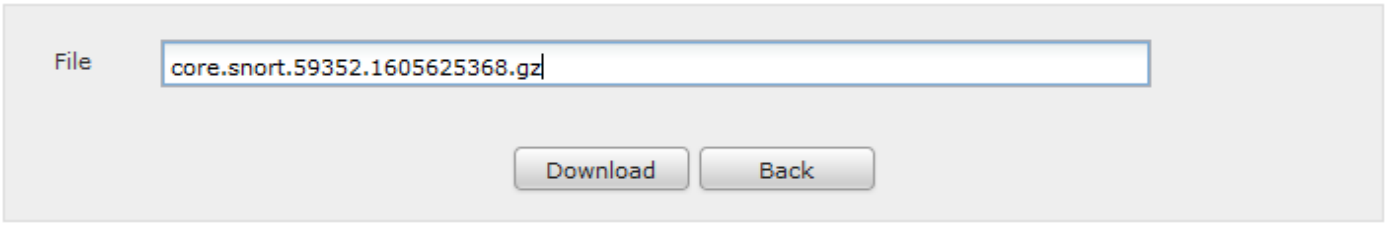
2. HTTPS를 통해 FMC에 액세스하고 System(시스템) > Health(**상태) > Monitor(모니터)로 이동합니다**.

3. 코어 파일이 생성된 FTD를 선택합니다.

4. 고급 문제 해결 옵션을 선택합니다.

5. 파일 다운로드 옵션을 선택합니다.

6. 검색 표시줄에 다운로드할 핵심 파일의 이름을 입력하고 다운로드 옵션을 선택합니다.



7. 다운로드한 파일을 SR에 업로드하여 분석합니다.

FDM을 사용하여 코어 파일을 수집하는 방법

FDM을 사용하는 경우 사용자 인터페이스를 사용하여 특정 파일을 수집할 수 없습니다. 대신 다음 절차를 사용하여 FTD의 문제 해결 파일과 함께 핵심 파일을 수집해야 합니다.

1. 파일이 있는 모든 플랫폼의 경우 /ngfw/var/common/ 및 /ngfw/var/data/cores/ 파일을 /ngfw/var/log/.

```
root@firepower:cores# ls -l | grep -i core
-rw-r--r-- 1 root root 409612433 Nov 17 16:08 core.lina.3137.1605629317.gz
-rw-r--r-- 1 root root  27873115 Nov 17 15:01 core.snort.59095.1605625274.gz
-rw-r--r-- 1 root root  27856205 Nov 17 15:02 core.snort.59352.1605625368.gz
root@firepower:cores# mv core* /ngfw/var/log/
root@firepower:cores# cd /ngfw/var/log
root@firepower:log# ls -l | grep -i core
-rw-r--r-- 1 root root 409612433 Nov 17 16:08 core.lina.3137.1605629317.gz
-rw-r--r-- 1 root root  27873115 Nov 17 15:01 core.snort.59095.1605625274.gz
-rw-r--r-- 1 root root  27856205 Nov 17 15:02 core.snort.59352.1605625368.gz
```

2. FDM을 사용하여 FTD에서 문제 해결 파일을 생성하고 다운로드합니다.

FDM 프로시저를 사용하여 파일 생성 문제 해결

3. 다운로드한 파일을 SR에 업로드하여 분석합니다.