

# Verzameling van kernbestanden van een FirePOWER-beschermingsapparaat

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Procedure](#)

[Firepower verwerkt kernbestanden](#)

[Plaats van Firepower Core Files wanneer de FTD in Firepower 2100, 1000, ASA-apparaat en ISA 3000-apparaat is geïnstalleerd](#)

[Plaats van Firepower Core Files wanneer de FTD in Firepower 4100 of 9300 is](#)

[LINA Proccorebestand](#)

[Plaats van LINA Core Files wanneer de FTD in Firepower 1000, 2100, 4100 en 9300 is](#)

[Hoe de kernbestanden worden verzameld met behulp van het FMC](#)

[Hoe de kernbestanden worden verzameld met FDM](#)

## Inleiding

Dit document beschrijft de procedure om alle typen kernbestanden voor FTD-apparaten te verzamelen via alle platforms die FTD-software ondersteunen. Wanneer een proces op de FTD een kritiek probleem tegenkomt, kan een stortplaats van het actieve geheugen van het proces als kernbestand worden opgeslagen. Om de basisoorzaak van de mislukking te bepalen, kan Cisco Technical Support de kernbestanden vragen.

Voor FTD-apparaten hebben we 2 soorten kernbestanden, FirePOWER-cores en LINA-coresbestanden.

Bijgedragen door Neri Cruz en bewerkt door Yeraldin Sanchez, Cisco TAC-engineers.

## Voorwaarden

### Vereisten

Cisco raadt u aan om kennis te hebben over deze producten:

- FireSIGHT Management Center (FMC)
- Firepower Devices Manager (FDM)
- Firepower Threat Defense (FTD)
- Firepower Extension System (FXOS)

## Procedure

# Firepower verwerkt kernbestanden

## Plaats van Firepower Core Files wanneer de FTD in Firepower 2100, 1000, ASA-apparaat en ISA 3000-apparaat is geïnstalleerd

Voor al deze platforms kunnen de kernbestanden met betrekking tot alle vuurenergieprocessen zich in de volgende procedure bevinden.

1. Sluit de stekker van het apparaat aan op de CLI van het apparaat via de SSH of de console.
2. Voer de informatie in als expert-modus.

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

3. Word een basisgebruiker.

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

4. Navigeren naar de `/ngfw/var/common/` map waarin de kernbestanden zich bevinden.

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

5. Controleer de map op het bestand.

```
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
```

## Plaats van Firepower Core Files wanneer de FTD in Firepower 4100 of 9300 is

Voor deze 2 platforms kunnen de kernbestanden in 2 mogelijke paden worden geplaatst, is de eerste hetzelfde als de vorige sectie, het tweede pad kan worden gevonden met de volgende procedure.

1. Sluit de stekker van het apparaat aan op de CLI van het apparaat via de SSH of de console.
2. Voer de informatie in als expert-modus.

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

3. Word een basisgebruiker.

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

4. Navigeren naar de `/ngfw/var/data/cores/` map waarin de kernbestanden zich bevinden.

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

5. Controleer de map op het bestand.

```
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 Procесscorebestand

### Plaats van LINA Core Files wanneer de FTD in Firepower 1000, 2100, 4100 en 9300 is

1. Sluit de stekker van het apparaat aan op de CLI van het apparaat via de SSH of de console.
2. Voer de informatie in als expert-modus.

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

3. Word een basisgebruiker.

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

4. Navigeren naar de `/ngfw/var/data/cores/` map waarin de kernbestanden zich bevinden.

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

5. Controleer de map op het kernbestand.

```
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
```

## Hoe de kernbestanden worden verzameld met behulp van het FMC

Voor alle platforms, waar de FTD is geïnstalleerd, dient de volgende procedure te worden gevolgd om de kernbestanden van de apparatuur te halen.

1. Voor alle platforms waar de kernbestanden zich bevinden onder `/ngfw/var/data/cores/` De bestanden onder `/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. Toegang tot het VCC via HTTPS en ga onder **Systeem > Health > Monitor**.

3. Selecteer de FTD waar de Core Files zijn gegenereerd.

4. Selecteer optie Geavanceerde probleemoplossing.

## Health Monitor



Appliance

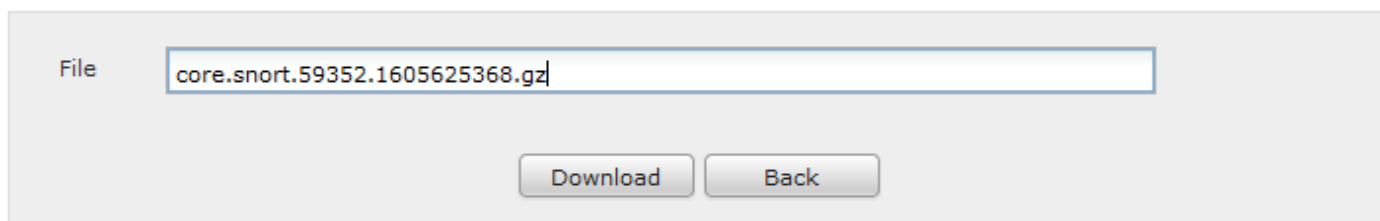
FTD-1K

Generate Troubleshooting Files

Advanced Troubleshooting

5. Selecteer optie Bestand downloaden.

6. Voer in de zoekbalk de naam in van het corebestand dat wordt gedownload en selecteer optie Downloaden.



File

core.snort.59352.1605625368.gz

Download Back

7. Nadat u de bestanden hebt gedownload, kunt u deze uploaden naar de SR voor analyse.

## Hoe de kernbestanden worden verzameld met FDM

Wanneer u FDM gebruikt, is het niet mogelijk om specifieke bestanden te verzamelen met behulp van de gebruikersinterface. In plaats daarvan moeten we de volgende procedure gebruiken om de kernbestanden te verzamelen met de bestanden met probleemoplossing van de FTD.

1. Voor alle platforms waar de bestanden zich bevinden onder `/ngfw/var/common/` en `/ngfw/var/data/cores/` De bestanden onder `/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. Generate en download de probleemoplossing van de FTD met behulp van FDM.

[Bestanden oplossen met behulp van FDM-procedure.](#)

3. Nadat u het bestand hebt gedownload, uploadt u het naar de SR voor analyse.