# Collection of Core Files From a Firepower Threat Defense Device

## Contents

## Introduction

This document describes the procedure to collect all the types of core files for FTD devices through all the platforms that support FTD software. When a process on the FTD encounters a critical problem, a dump of the running memory of the process can be saved as a core file. In order to determine the root cause of the failure, Cisco Technical Support might request the core files.

For FTD devices we have two types of core files, Firepower cores and LINA cores files.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these products:

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

## Procedure

## Firepower Processes Core Files

### Location of Firepower Core Files when the FTD is in Firepower 2100, 1000,

## ASA Appliance, and ISA 3000 Appliance

For all these platforms the core files related to all the firepower processes can be located with this procedure.

1. Connect to the CLI of the appliance via SSH or console.

2. Enter as expert mode.

```
> expert
admin@firepower:~$
```
3. Become a root user.

```
admin@firepower:~$ sudo su
Password:
root@firepower:/home/admin#
```
4. Navigate to the /ngfw/var/common/ folder, where the core files are located.

```
root@firepower:/home/admin# cd /ngfw/var/common/
```
5. Check the folder for the file.

```
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
```

## Location of Firepower Core Files when the FTD is in Firepower 4100 or 9300

For these two platforms, the core files can be located in two possible paths, the first one is the same as the previous section, the second path can be located with this procedure.

1. Connect to the CLI of the appliance via SSH or console.

2. Enter as expert mode.

```
> expert
admin@firepower:~$
```
3. Become a root user.

```
admin@firepower:~$ sudo su
Password:
root@firepower:/home/admin#
```
4. Navigate to the /ngfw/var/data/cores/ folder, where the core files are located.

```
root@firepower:/home/admin# cd /ngfw/var/data/cores/
```
5. Check the folder for the file.

```
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 Process Core File

### Location of LINA Core Files when the FTD is in Firepower 1000, 2100, 4100, and 9300

1. Connect to the CLI of the appliance via SSH or console.

2. Enter as expert mode.

```
> expert
admin@firepower:~$
```
3. Become a root user.

```
admin@firepower:~$ sudo su
Password:
root@firepower:/home/admin#
```
4. Navigate to the /ngfw/var/data/cores/ folder, where the core files are located.

```
root@firepower:/home/admin# cd /ngfw/var/data/cores/
```
5. Check the folder for the core file.

```
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
```

# How to Collect the Core Files using the FMC

For all the platforms, where the FTD is installed, this procedure should be followed to extract the core files from the devices.

1. For all the platforms where the Core Files are located under /ngfw/var/data/cores/ will need to move the files under /ngfw/var/common/.
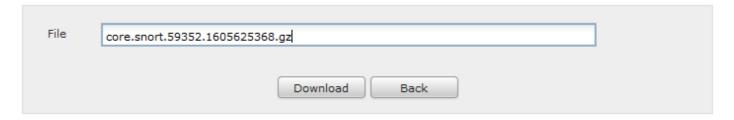
```
root@firepower:/ngfw/var/data/cores# ls -l | grep -i core
-rw-r--r-- 1 root root 84831856 Nov 17 15:49 core.lina.23228.1605628188.gz
root@firepower:/ngfw/var/data/cores# mv core* /ngfw/var/common/
root@firepower:/ngfw/var/data/cores# cd /ngfw/var/common/
root@firepower:/ngfw/var/common# ls -l | grep -i core
-rw-r--r-- 1 root root 84831856 Nov 17 15:49
core.lina.23228.1605628188.gz
```
2. Access to the FMC via HTTPS and go under **System > Health > Monitor**.

3. Select the FTD where the Core Files were generated.

4. Select option Advanced Troubleshooting.

5. Select option File Download.

6. On the search bar, put the name of the Core File that will be downloaded and select option Download.



7. Once downloaded, upload the file(s) to the SR for analysis.

# How to Collect the Core Files using FDM

When using FDM, it is not possible to collect specific files using the User Interface, instead, we need to use the following procedure to collect the Core Files with the troubleshooting files of the FTD.

1. For all the platforms where the files are located under /ngfw/var/common/ and /ngfw/var/data/cores/ will need to move the files under /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 and download the troubleshooting files from the FTD using FDM.

Troubleshooting file generation using FDM procedure.

3. Once downloaded, upload the file to the SR for analysis.