Coleta de arquivos principais de um dispositivo Firepower Threat Defense

Contents

Introduction

Este documento descreve o procedimento para coletar todos os tipos de arquivos principais para dispositivos FTD através de todas as plataformas que suportam o software FTD. Quando um processo no FTD encontra um problema crítico, um dump da memória em execução do processo pode ser salvo como um arquivo central. Para determinar a causa raiz da falha, o Suporte Técnico da Cisco pode solicitar os arquivos principais.

Para dispositivos FTD, temos dois tipos de arquivos principais, núcleos Firepower e arquivos de núcleos LINA.

Prerequisites

Requirements

A Cisco recomenda que você conheça estes produtos:

- Firepower Management Center (FMC)
- Firepower Device Manager (FDM)
- Firepower Threat Defense (FTD)
- Sistema de Operação Extensível Firepower (FXOS)

Procedimento

Arquivos principais dos processos do Firepower

Localização dos arquivos principais do Firepower quando o FTD está no Firepower 2100, 1000, no ASA Appliance e no ISA 3000 Appliance

Para todas essas plataformas, os arquivos principais relacionados a todos os processos de firepower podem ser localizados com este procedimento.

1. Conecte-se à CLI do dispositivo via SSH ou console.

2. Entre no modo de especialista.

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

3. Torne-se um usuário raiz.

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

4. Navegue até o /ngfw/var/common/ , onde os arquivos principais estão localizados.

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

5. Verifique a pasta do arquivo.

```
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
```

Localização dos arquivos principais do Firepower quando o FTD está no Firepower 4100 ou 9300

Para essas duas plataformas, os arquivos principais podem ser localizados em dois caminhos possíveis, o primeiro é o mesmo da seção anterior, e o segundo caminho pode ser localizado com esse procedimento.

1. Conecte-se à CLI do dispositivo via SSH ou console.

2. Entre no modo de especialista.

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

3. Torne-se um usuário raiz.

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

4. Navegue até o /ngfw/var/data/cores/ , onde os arquivos principais estão localizados.

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

5. Verifique a pasta do arquivo.

```
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
```

Arquivo principal do processo LINA

Localização dos arquivos principais do LINA quando o FTD está no Firepower 1000, 2100, 4100 e 9300

1. Conecte-se à CLI do dispositivo via SSH ou console.

2. Entre no modo de especialista.

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

3. Torne-se um usuário raiz.

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

4. Navegue até o /ngfw/var/data/cores/ , onde os arquivos principais estão localizados.

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

5. Verifique se o arquivo principal está na pasta.

```
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
```

Como coletar os arquivos principais usando o FMC

Para todas as plataformas onde o FTD está instalado, este procedimento deve ser seguido para extrair os arquivos principais dos dispositivos.

1. Para todas as plataformas nas quais os arquivos principais estão localizados /ngfw/var/data/cores/ precisará mover os arquivos /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
```

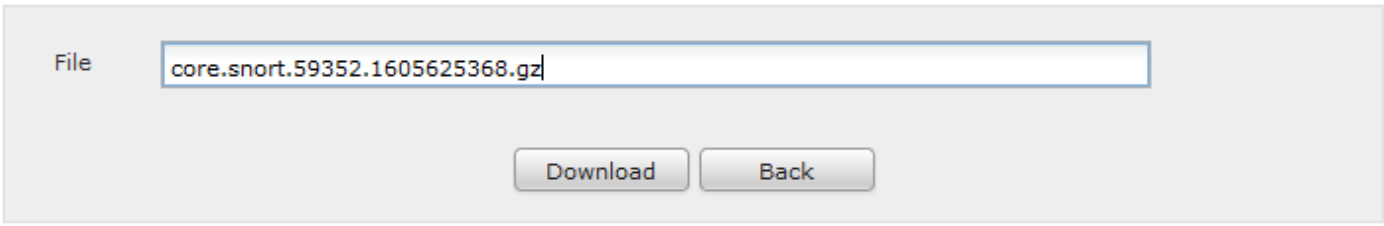
2. Acesso ao FMC via HTTPS e vá em **System > Health > Monitor**.

3. Selecione o FTD onde os arquivos principais foram gerados.

4. Selecione a opção Advanced Troubleshooting (Solução de problemas avançada).

5. Selecione a opção Download de arquivo.

6. Na barra de pesquisa, coloque o nome do Arquivo principal que será baixado e selecione a opção Download.



7. Após o download, carregue os arquivos no SR para análise.

Como coletar os arquivos principais usando o FDM

Ao usar o FDM, não é possível coletar arquivos específicos usando a Interface do usuário; em vez disso, precisamos usar o procedimento a seguir para coletar os arquivos principais com os arquivos de solução de problemas do FTD.

1. Para todas as plataformas nas quais os arquivos estão localizados /ngfw/var/common/ e /ngfw/var/data/cores/ precisará mover os arquivos /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. Gere e faça o download dos arquivos de solução de problemas do FTD usando o FDM.

Solucionando problemas de geração de arquivos usando o procedimento FDM.

3. Após o download, carregue o arquivo no SR para análise.