Decodifique a terminologia de firewall segura (para pessoas novas no Firepower)

Contents

Introdução

Este documento descreve diferentes jargões populares do Cisco Firewall. Este documento também aborda uma forma de passar de um modo CLI para outro.

Pré-requisitos

Requisitos

Não há requisitos anteriores para aprender este tópico.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Firewall Management Center (FMC)
- Defesa contra ameaças (FTD) do Cisco Firepower
- Gerenciamento de dispositivos Cisco Firepower (FDM)
- Firepower eXtensible Operating System (FXOS)
- Firepower Chassis Manager (FCM)
- Dispositivo de segurança adaptável (ASA)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Terminologias Técnicas Mais Usadas

FTD: Defesa contra ameaças do Firepower

O FTD é um firewall de próxima geração que oferece mais do que os firewalls tradicionais. Ele inclui serviços como IPS (Sistema de prevenção de intrusão), AMP (Proteção avançada contra malware), filtragem de URL, inteligência de segurança e assim por diante. O FTD é muito semelhante ao ASA (Adaptive Security Appliance), mas com funcionalidade adicional. O FTD é executado em 2 mecanismos, LINA e SNORT.

LINA: arquitetura de rede integrada baseada em Linux

Nos referimos ao ASA como Lina em dispositivos FTD. LINA não é nada além de simplesmente um código ASA que o FTD executa. Lina tem seu foco principal na segurança da camada de rede. Ele incorpora alguns recursos de firewall da camada 7 através de seus recursos de inspeção e controle de aplicativos.

SNORT

O mecanismo Snort é um sistema de detecção e prevenção de intrusão na rede. Os principais recursos do Snort incluem a inspeção de pacotes para identificar anomalias, detecção baseada em regras, alertas em tempo real, registro e análise e integração com outras ferramentas de segurança. O Snort tem a capacidade de executar a inspeção L7 (tráfego da camada de aplicação), não apenas com base no cabeçalho de um pacote, mas também no conteúdo dos pacotes.

Você tem a flexibilidade de criar suas próprias regras personalizadas para definir padrões ou assinaturas específicos na camada de aplicação, o que melhora os recursos de detecção. Ele faz uma inspeção profunda de pacotes avaliando o payload dos pacotes. Você pode até mesmo executar a descriptografia dos pacotes criptografados aqui.

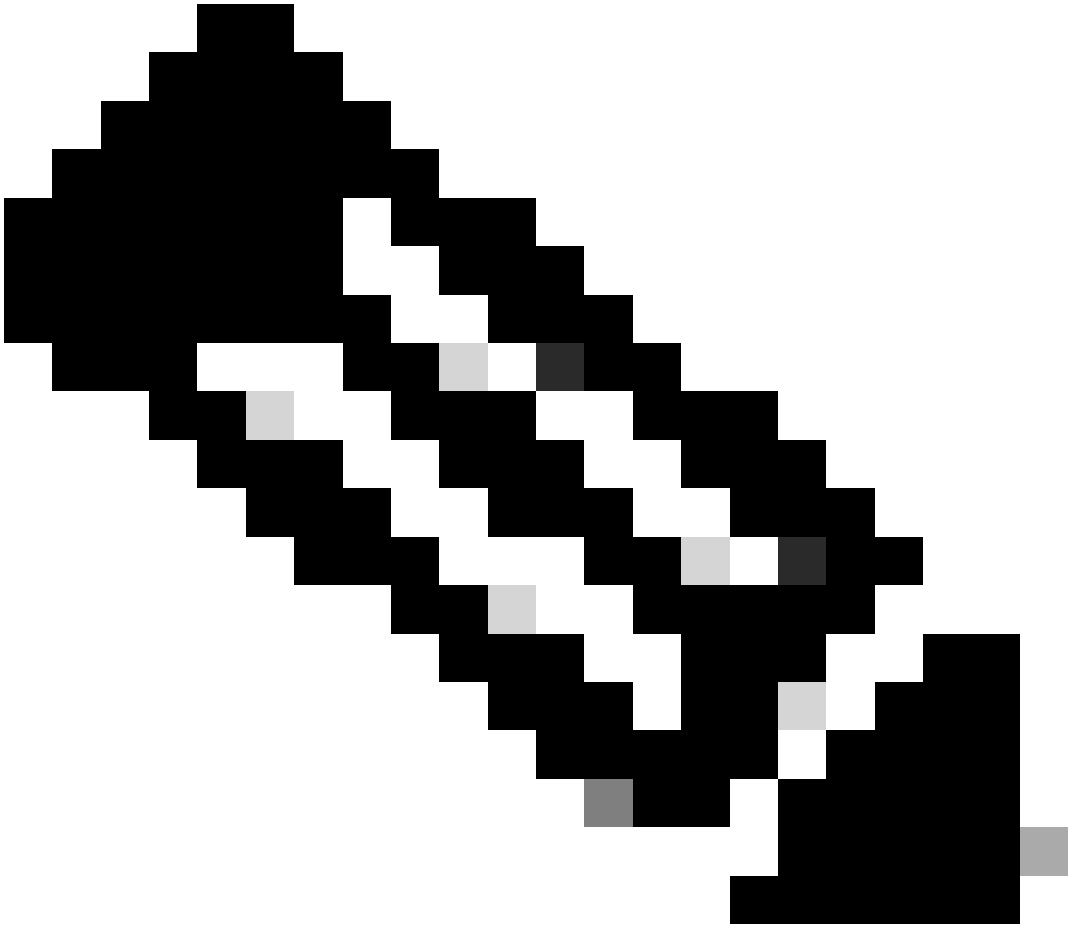
FXOS: sistema operacional extensível Firepower

É um sistema operacional no qual o dispositivo FTD é executado. Dependendo das plataformas, o FXOS é usado para configurar recursos, monitorar o status do chassi e acessar recursos avançados de solução de problemas.

O FXOS no Firepower 4100/9300 e no Firepower 2100 com o software Adaptive Secure Appliance no modo de plataforma permite alterações de configuração, enquanto em outras plataformas, com exceção de recursos específicos, ele é somente leitura.

FCM: Firepower Chassis Manager

O FCM é uma GUI usada para gerenciar o chassi. Ele está disponível apenas para 9300, 4100 e 2100 executando ASA no modo de plataforma.

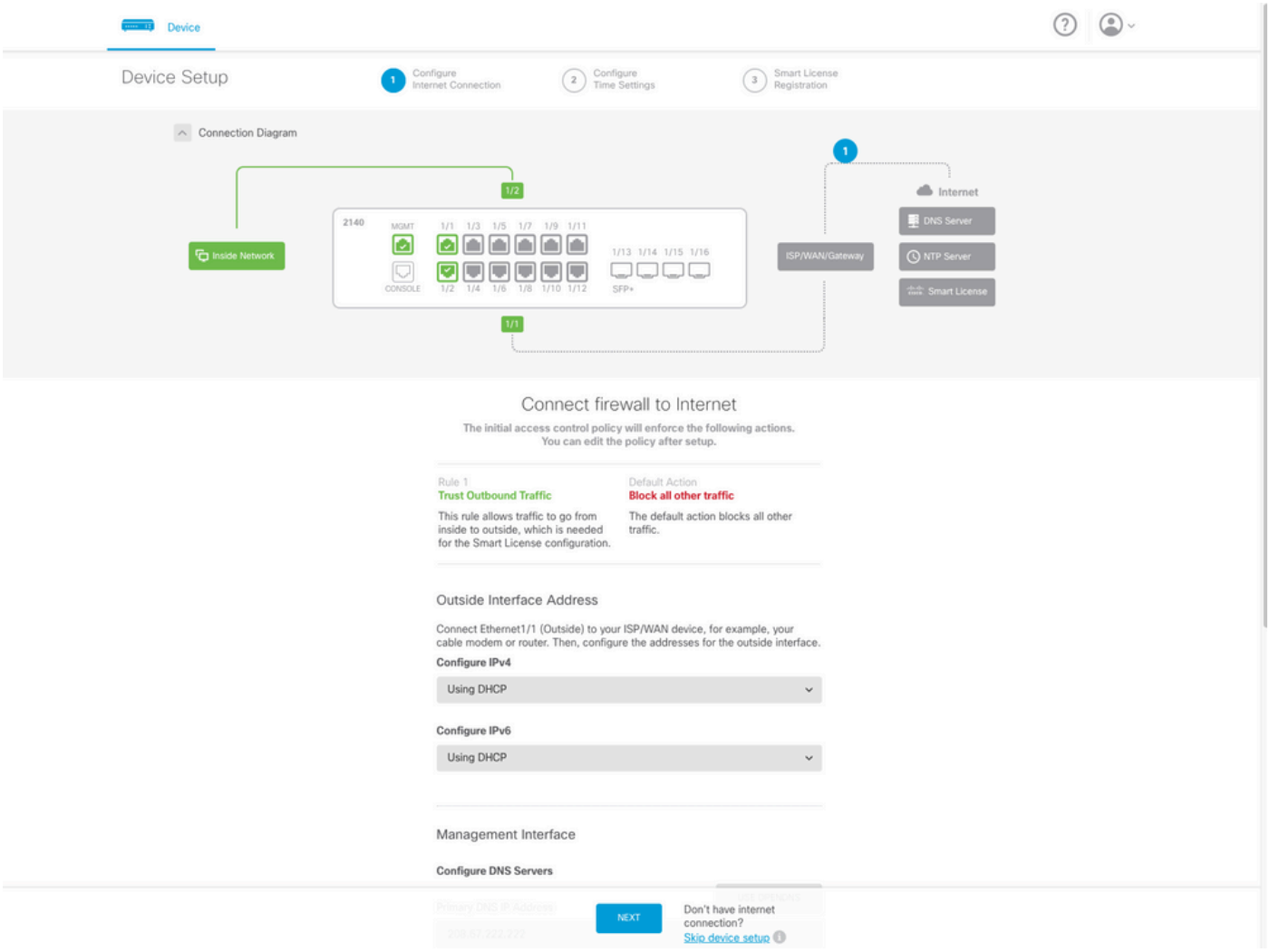


> Observação: você pode fazer uma analogia de um notebook. FXOS é o sistema operacional (SO Windows em laptop), executado no chassi (laptop). Podemos instalar o FTD (instância do aplicativo) nele, que é executado em Lina e Snort (componentes).

Diferentemente do ASA, você não pode gerenciar o FTD via CLI. Você precisa de um gerenciamento separado baseado em GUI. Existem dois tipos de serviços: FDM e FMC.

FDM: Gerenciamento de dispositivos do Firepower

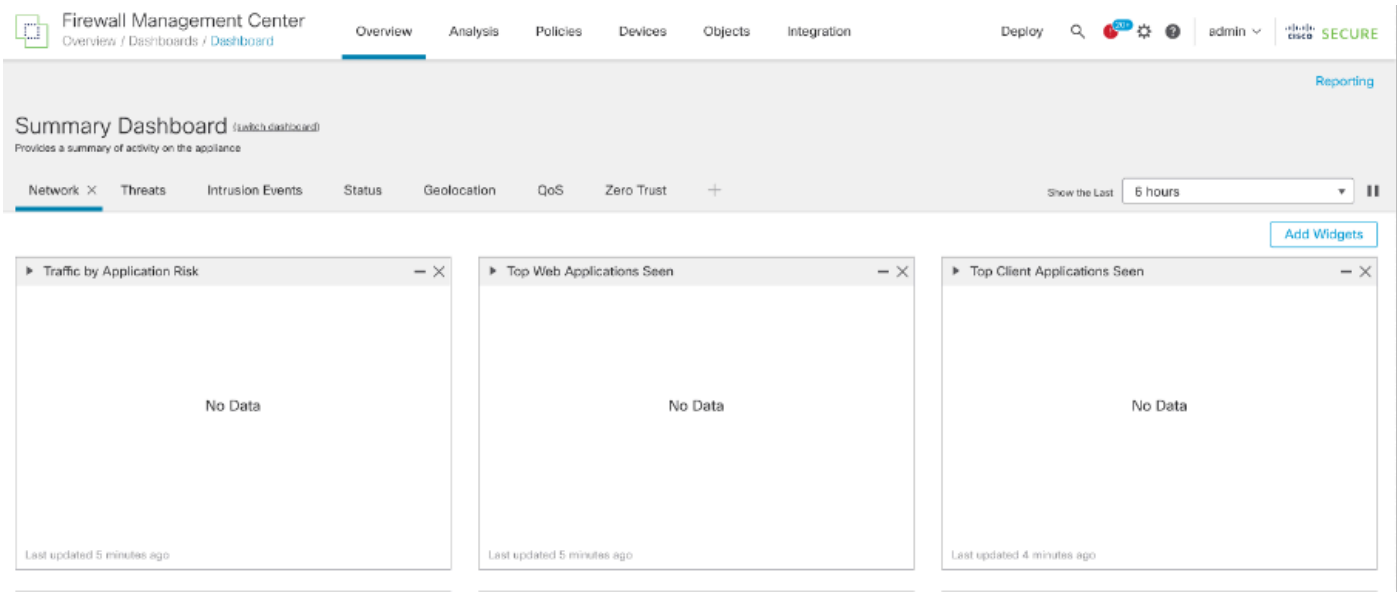
- O FDM é uma ferramenta de gerenciamento integrada. Ele fornece uma interface baseada na Web para configurar, gerenciar e monitorar políticas de segurança e configurações do sistema.
- Uma grande vantagem de usar o FDM é que você não tem uma licença extra para isso.
- Você só pode gerenciar 1 FTD com 1 FDM.



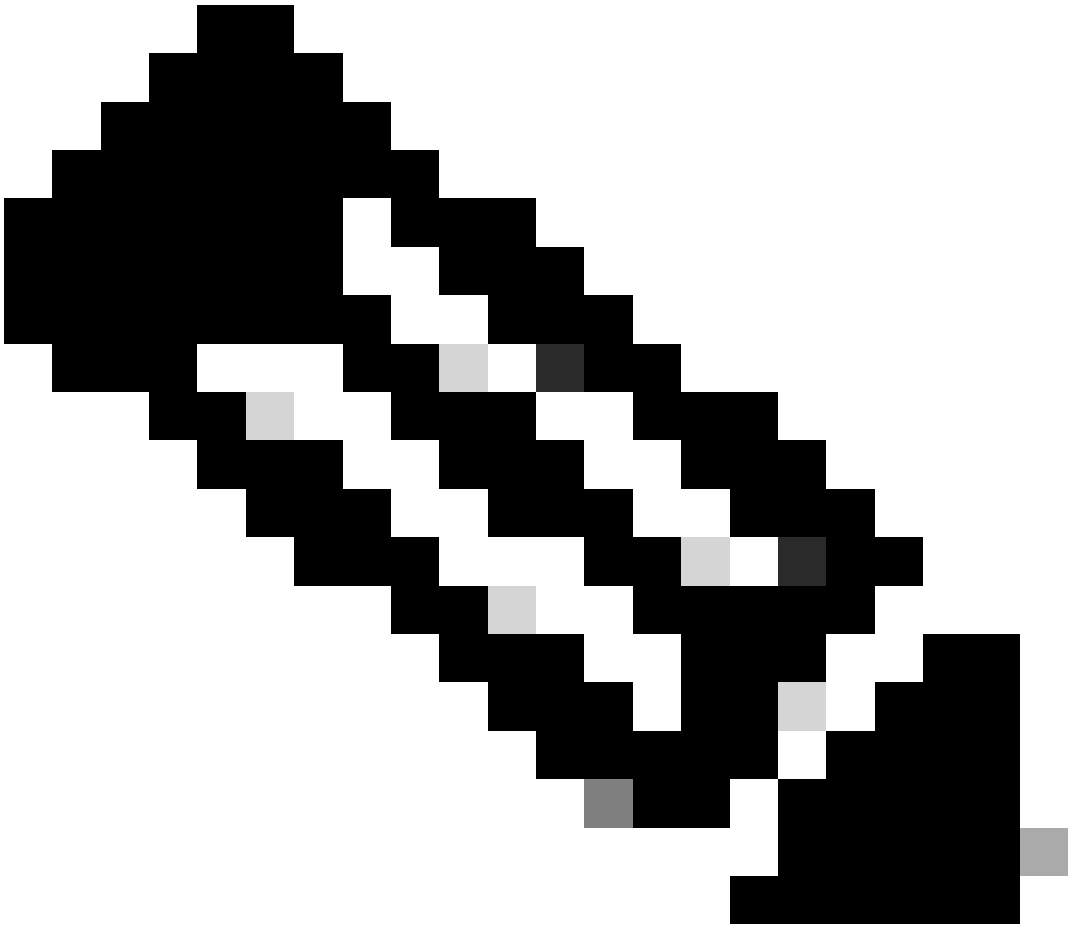
FDM

FMC: Firepower Management Center

- O FMC é uma solução de gerenciamento centralizado para dispositivos Cisco FTD, dispositivos Cisco ASA com Firepower Services. Ele também fornece uma GUI que você pode usar para configurar, gerenciar e monitorar dispositivos FTD.
- Você pode usar um dispositivo FMC de hardware ou um dispositivo FMC virtual.
- Isso requer uma licença separada para funcionar.
- Um ponto positivo do FMC é que você pode gerenciar vários dispositivos FTD com um dispositivo FMC.



CVP



Observação: Não é possível usar o FDM e o FMC para gerenciar um dispositivo FTD. Quando o gerenciamento FDM On-Box estiver habilitado, não será possível usar um FMC

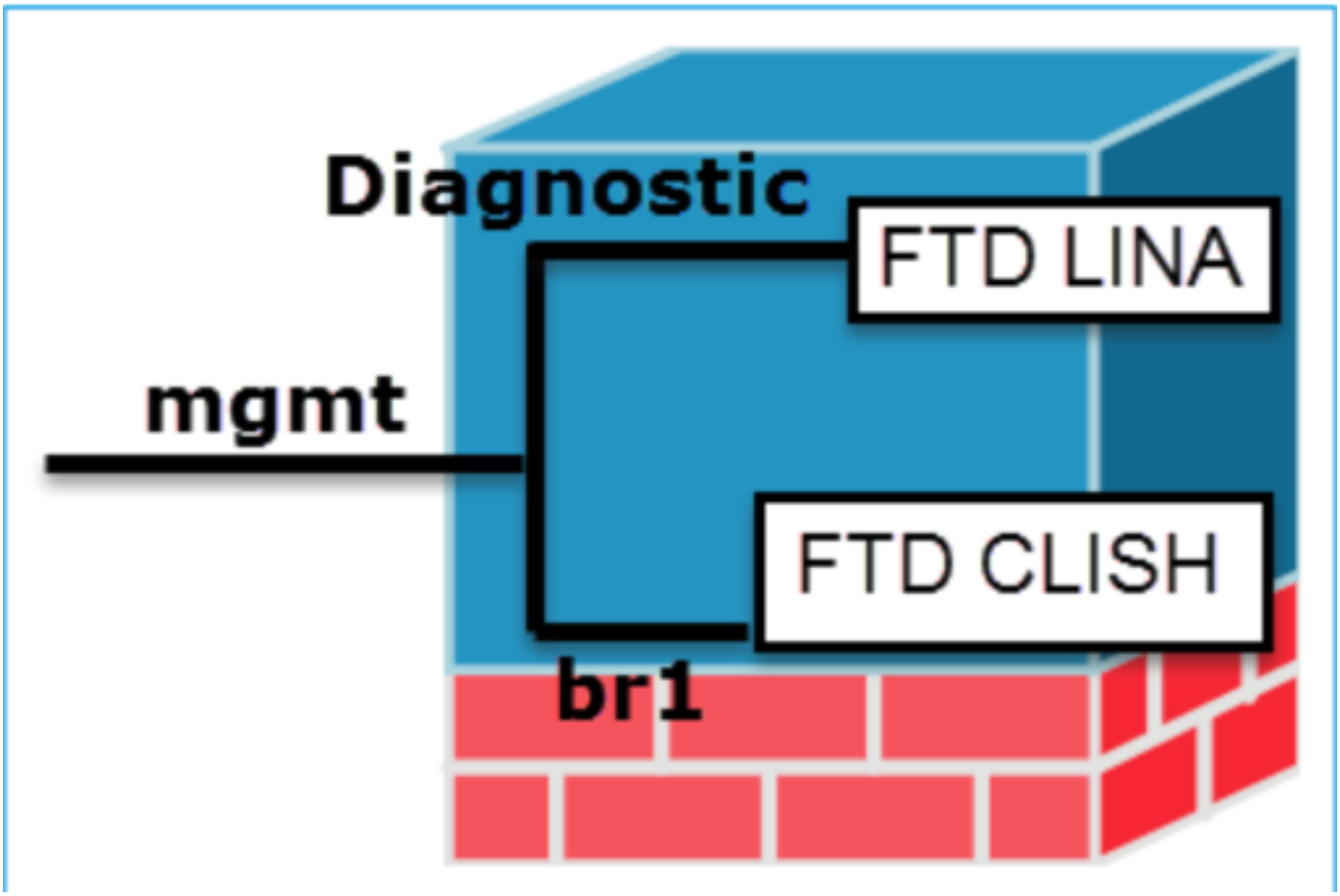
para gerenciar o FTD, a menos que você desabilite o gerenciamento local e reconfigure o gerenciamento para usar um FMC. Por outro lado, registre o FTD em um FMC para desativar o serviço de gerenciamento do FDM On-Box no FTD.

CLISH: Shell de Interface de Linha de Comando

CLISH é uma interface de linha de comando usada em dispositivos Cisco Firepower Threat Defense (FTD). Você pode executar comandos no FTD usando este modo CLISH.

GERENCIAMENTO DE DIAGNÓSTICO

Temos 2 interfaces de gerenciamento no dispositivo FTD, interface de gerenciamento de diagnóstico e interface de gerenciamento FTD. Se tivermos que acessar o mecanismo LINA, usaremos a interface de gerenciamento de diagnóstico. Se precisarmos acessar o mecanismo SNORT, usaremos a interface de gerenciamento do FTD. Ambas são interfaces diferentes e precisam de endereços IP de interface diferentes.



Interfaces de gerenciamento

Modo de plataforma ASA

1. No modo de plataforma, você deve configurar parâmetros operacionais básicos e configurações de interface de hardware no FXOS, como ativar interfaces, estabelecer

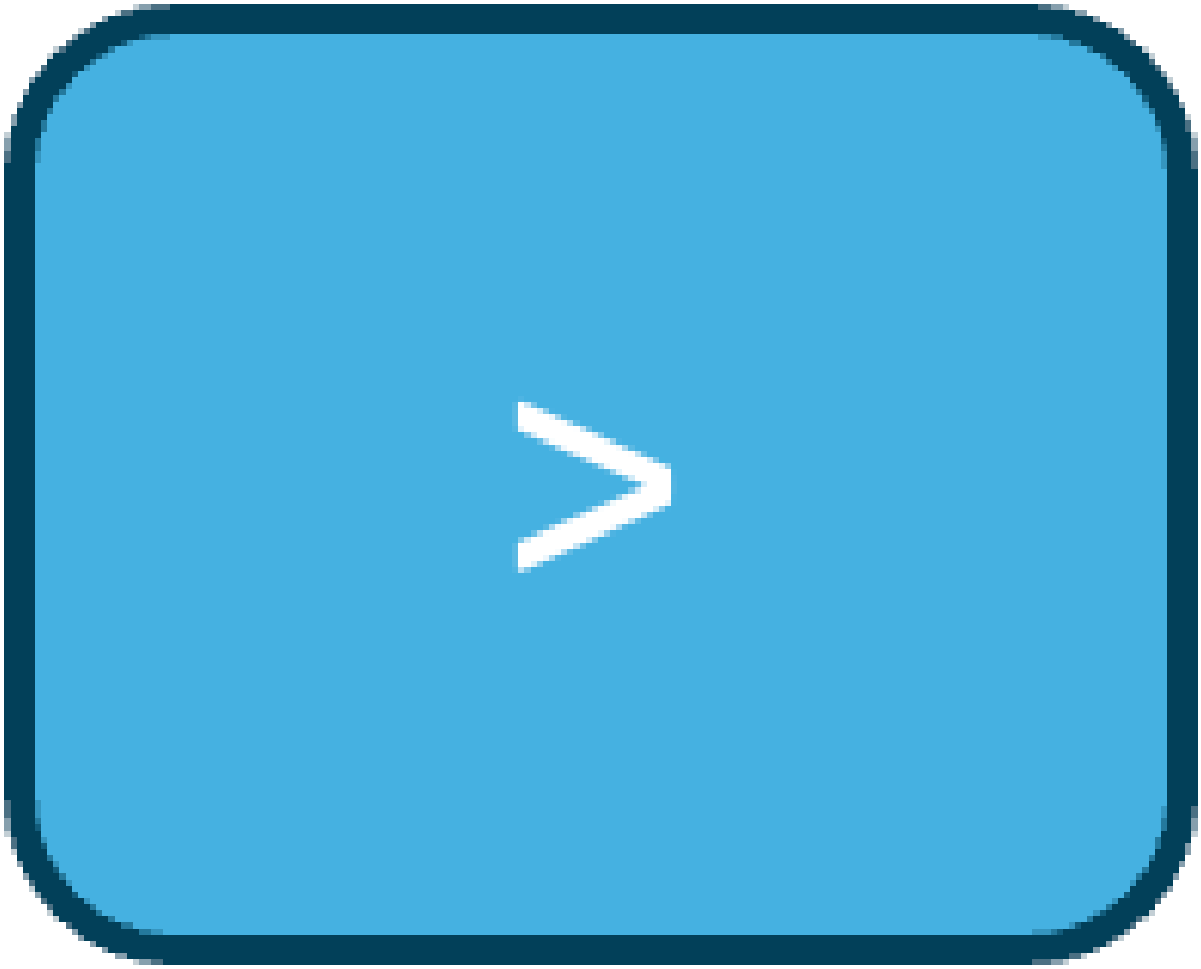
EtherChannels, NTP, gerenciamento de imagens e muito mais.
2. Todas as outras configurações devem ser feitas por meio do ASA CLI/ASDM.
3. Você tem acesso ao FCM neste.

Modo de dispositivo ASA

1. No Firepower 2100, o ASA no modo de dispositivo foi introduzido a partir da versão 9.13 (inclusive).
2. O modo de dispositivo permite que você defina todas as configurações no ASA. Somente comandos avançados de solução de problemas estão disponíveis na CLI FXOS.
3. Não há FCM neste modo.

Prompts Diferentes no FTD

CLISH



CLISH

Modo raiz / Modo avançado

Modo avançado

Modo Lina

Modo Lina

Modo FXOS

Modo FXOS

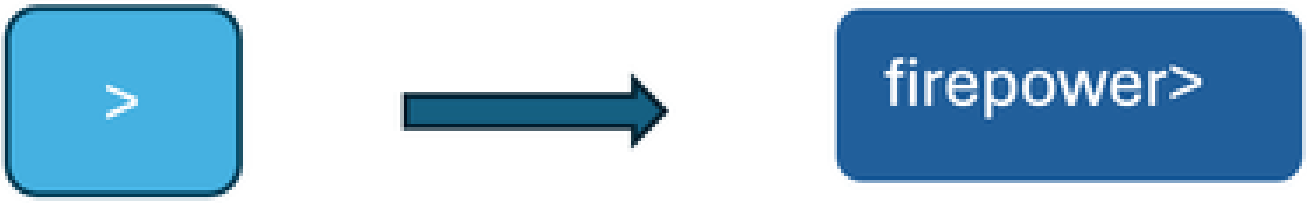
Como Mover-Se Entre Prompts Diferentes

Modo CLISH para modo raiz FTD

Modo Clish para Modo Expert

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

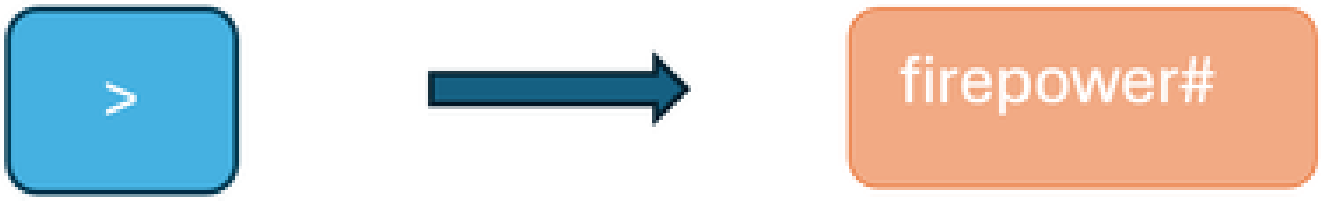
Modo CLISH para modo Lina



Modo Clish para Modo Lina

```
> 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#
```

Modo CLISH para modo FXOS



Modo Clish para modo FXOS

```
> connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.
(------ cropped output -------)
firepower#
```

Modo raiz para modo LINA

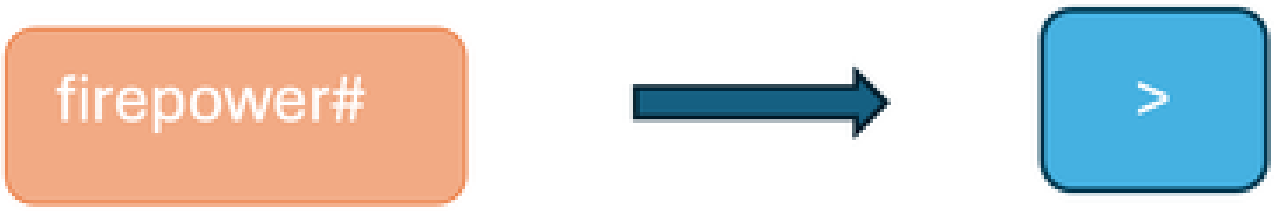
Especialista para o modo Lina

```
root@firepower:/home/admin#
root@firepower:/home/admin#   exit
exit
admin@firepower:~$ exit
logout
>
> 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> en
Password:
firepower#
```

or

```
root@firepower:/home/admin#
root@firepower:/home/admin#   sfconsole
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower#
```

Modo FXOS para CLISH FTD (dispositivo 1000/2100/3100 Series)



Modo FXOS para Clicar

```
firepower# connect ftd
>
To exit the fxos console
> exit
firepower#
```

Modo FXOS para CLISH FTD (dispositivo 4100/9300 Series)

Este exemplo mostra como se conectar à CLI de defesa contra ameaças no módulo 1:

```
firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
CISCO Serial Over LAN:
Close Network Connection to Exit
Firepower-module1> connect ftd
>
```

Saia do console:

Digite ~ e quit para sair do aplicativo Telnet.

```
Example:
>exit
Firepower-module1> ~
telnet> quit
firepower#
```

Documentos relacionados

Para obter mais informações sobre vários comandos que podem ser executados em dispositivos

firepower, consulte Referência de Comandos FXOS , referência de comandos FTD .

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.