

Configurar o acesso de gerenciamento ao FTD (HTTPS e SSH) via FMC

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurar Acesso de Gerenciamento](#)

[Etapa 1. Configurar o IP na interface FTD através da GUI do FMC.](#)

[Etapa 2. Configurar a autenticação externa.](#)

[Etapa 3. Configurar o acesso SSH.](#)

[Etapa 4. Configurar o acesso HTTPS.](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve a configuração do acesso de gerenciamento a um Firepower Threat Defense (FTD) (HTTPS e SSH) através do Firesight Management Center (FMC).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento da tecnologia Firepower
- Conhecimento básico do ASA (Adaptive Security Appliance)
- Conhecimento de acesso de gerenciamento no ASA via HTTPS e SSH (Secure Shell)

Componentes Utilizados

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

- Imagem do Adaptive Security Appliance (ASA) Firepower Threat Defense para ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X), que é executado na versão de

software 6.0.1 e posterior.

- Imagem do ASA Firepower Threat Defense para ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X), que é executado na versão de software 6.0.1 e posterior.
- Firepower Management Center (FMC) versão 6.0.1 e posterior.


The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Com o início do Firepower Threat Defense (FTD), toda a configuração relacionada ao ASA é feita na GUI.

Em dispositivos FTD que executam a versão de software 6.0.1, a CLI de diagnóstico do ASA é acessada quando você entra no **suporte do sistema diagnostic-cli**. No entanto, em dispositivos FTD que executam a versão de software 6.1.0, a CLI é convergida e os comandos ASA inteiros são configurados na CLISH.

```
Cisco Fire Linux OS v6.0.1 (build 37)
Cisco Firepower Threat Defense for VMWare v6.0.1 (build 1213)
```

```
>  CLISH
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
firepower> en
Password:
firepower#  DIAGNOSTIC CLI
```

Para obter acesso de gerenciamento diretamente de uma rede externa, você deve configurar o acesso de gerenciamento via HTTPS ou SSH. Este documento fornece a configuração necessária para obter acesso de gerenciamento sobre SSH ou HTTPS externamente.

Note: Em dispositivos FTD que executam a versão 6.0.1 do software, a CLI não pode ser acessada por um usuário local, uma autenticação externa deve ser configurada para autenticar os usuários. No entanto, em dispositivos FTD que executam o software versão 6.1.0, a CLI é acessada pelo usuário **admin** local, enquanto uma autenticação externa é necessária para todos os outros usuários.

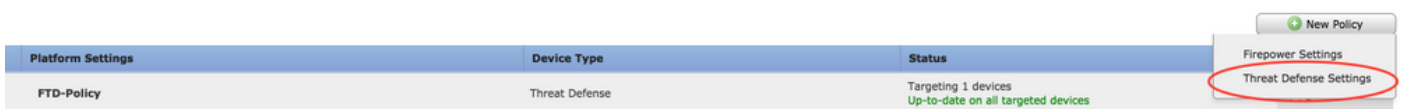
Note: Em dispositivos FTD que executam a versão de software 6.0.1, a CLI de diagnóstico não é diretamente acessível pelo IP configurado para **br1** do FTD. No entanto, em dispositivos FTD que executam a versão de software 6.1.0, a CLI convergente é acessível por qualquer interface configurada para acesso de gerenciamento, no entanto, a interface deve ser configurada com um endereço IP.

Configurar

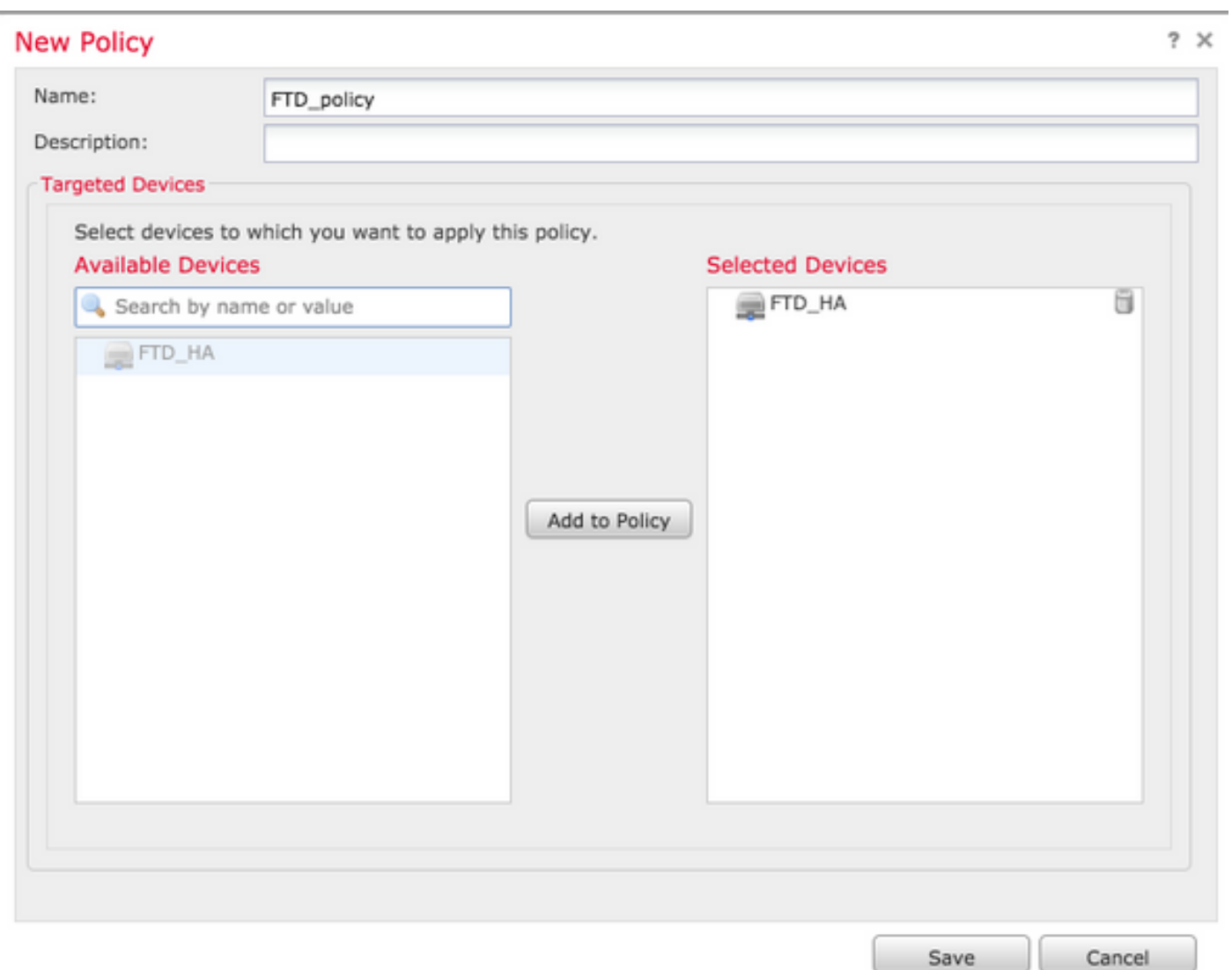
Todas as configurações relacionadas ao Acesso de Gerenciamento são configuradas conforme você navega até a guia **Configurações de Plataforma** em **Dispositivos**, como mostrado na imagem:



Edite a política existente ao clicar no ícone de lápis ou crie uma nova política de FTD ao clicar no botão **Nova política** e selecione o tipo como Configurações de defesa contra ameaças, como mostrado na imagem:



Selecione o dispositivo FTD para aplicar esta política e clique em **Salvar**, como mostrado na imagem:



Configurar Acesso de Gerenciamento

Estas são as quatro principais etapas realizadas para configurar o Acesso de Gerenciamento.

Etapa 1. Configurar o IP na interface FTD através da GUI do FMC.

Configure um IP na interface pela qual o FTD pode ser acessado via SSH ou HTTPS. Edite as interfaces existentes enquanto navega até a guia **Interfaces** do FTD.

Note: Em dispositivos FTD que executam a versão de software 6.0.1, a interface de gerenciamento padrão no FTD é a interface diagnostic0/0. No entanto, em dispositivos FTD que executam a versão de software 6.1.0, todas as interfaces suportam acesso de gerenciamento, exceto a interface de diagnóstico.

Há seis etapas para configurar a interface de diagnóstico.

Etapa 1. Navegue até **Dispositivo > Gerenciamento de Dispositivos**.

Etapa 2. Selecione o dispositivo ou o cluster FTD HA.

Etapa 3. Navegue até a guia **Interfaces**.

Etapa 4. Clique no **ícone do lápis** para configurar/editar a interface para obter acesso de gerenciamento, como mostrado na imagem:



Status	Interface	Logical Name	Type	Interface Objects	MAC Address (Active/Standby)	IP Address	
	GigabitEthernet0/0	transit	Physical			172.16.5.2/30(Static)	
	GigabitEthernet0/1	inside	Physical			172.16.8.1/24(Static)	

Etapa 5. Marque a caixa de seleção **enable** para ativar as interfaces. Navegue até a guia **Ipv4**, escolha o Tipo de IP como **estático** ou **DHCP**. Agora, insira um endereço IP para a interface e clique em **OK**, como mostrado na imagem:

Edit Physical Interface



Mode: ▾

Name: Enabled Management Only

Security Zone: ▾

Description:

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: ▾

IP Address: eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25

OK Cancel

Etapa 6. Clique em **Salvar** e implante a política no FTD.

Observação: a interface de diagnóstico não pode ser usada para acessar a CLI convergida sobre SSH em dispositivos com a versão de software 6.1.0

Etapa 2. Configurar a autenticação externa.

A autenticação externa facilita a integração do FTD a um servidor Active Directory ou RADIUS para autenticação de usuário. Essa é uma etapa necessária porque os usuários configurados localmente não têm acesso direto à CLI de diagnóstico. A CLI de diagnóstico e a GUI são acessadas somente por usuários autenticados via Lightweight Directory Access Protocol (LDAP) ou RADIUS.

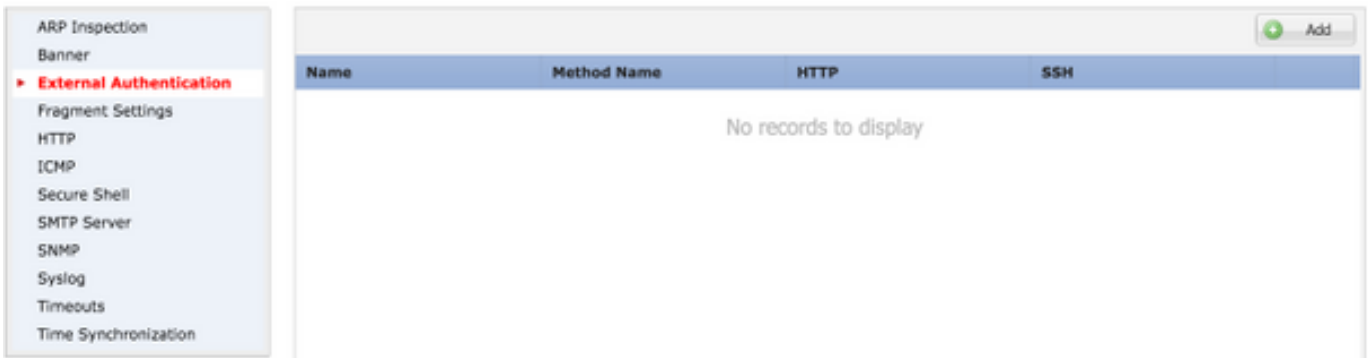
Há 6 etapas para configurar a Autenticação externa.

Etapa 1. Navegue até **Dispositivos > Configurações de plataforma**.

Etapa 2. Edite a política existente ao clicar no ícone do lápis ou crie uma nova política de FTD ao

clique no botão **Nova política** e selecione o tipo como **Configurações do Threat Defense**.

Etapa 3. Navegue até a guia **Autenticação externa**, conforme mostrado na imagem:



Etapa 4. Quando você clica em **Add**, uma caixa de diálogo aparece como mostrado na imagem:

- **Habilitar para HTTP**- Habilite esta opção para fornecer acesso ao FTD sobre HTTPS.
- **Habilitar para SSH**- Habilite esta opção para fornecer acesso ao FTD sobre SSH.
- **Name**- (Nome) Insira o nome da conexão LDAP.
- **Description**- (Descrição) Insira uma descrição opcional para o objeto External Authentication.
- **Endereço IP**- Insira um objeto de rede que armazene o IP do Servidor de autenticação externo. Se não houver nenhum objeto de rede configurado, crie um novo. Clique no ícone (+).
- **Método de autenticação** - Selecione o protocolo RADIUS ou LDAP para autenticação.
- **Ativar SSL** - Ative esta opção para criptografar o tráfego de autenticação.
- **Tipo de servidor** - Selecione o tipo de servidor. Os tipos de servidor conhecidos são MS Active Directory, Sun, OpenLDAP e Novell. Por padrão, a opção está definida para detectar automaticamente o tipo de servidor.
- **Porta** - insira a porta na qual a autenticação ocorre.
- **Timeout**- Insira um valor de timeout para as solicitações de autenticação.
- **DN base**- Insira um DN base para fornecer um escopo no qual o usuário pode estar presente.
- **Escopo LDAP**- Selecione o escopo LDAP a ser procurado. O escopo está dentro do mesmo nível ou para procurar dentro da subárvore.
- **Username**- (Nome de usuário) Insira um nome de usuário para vincular ao diretório LDAP.

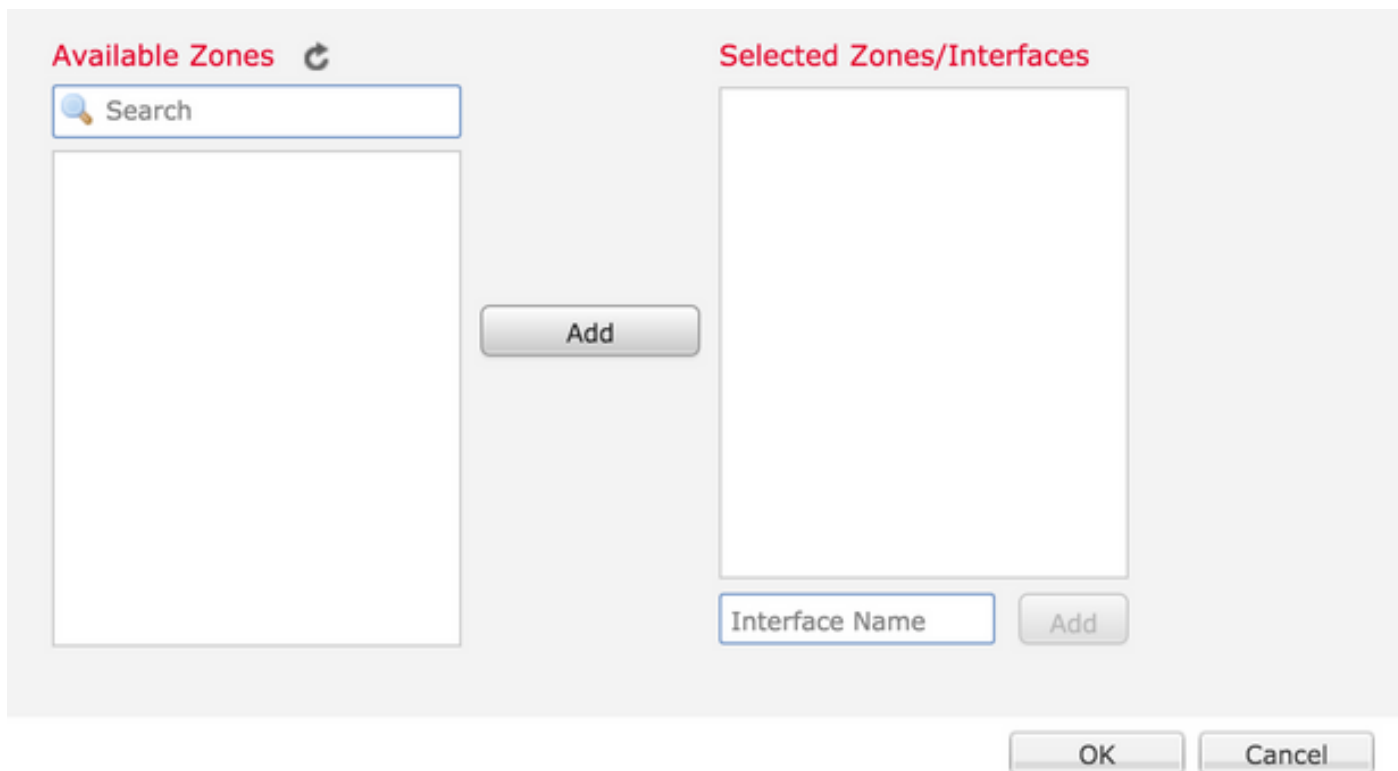
- **Senha de autenticação** - Insira a senha para este usuário.
- **Confirm**- (Confirmar) Insira a senha novamente.
- **Interfaces disponíveis** - Uma lista de interfaces disponíveis no FTD é exibida.
- **Zonas e interfaces selecionadas**- Mostra uma lista de interfaces pelas quais o servidor de autenticação é acessado.

Para a autenticação RADIUS, não há nenhum DN base ou escopo LDAP do tipo de servidor. A porta é a porta RADIUS 1645.

Secret- (Segredo) Insira a chave secreta para o RADIUS.

Add External Authentication ? X

Enable for HTTP	<input type="checkbox"/>	
Enable for SSH	<input type="checkbox"/>	
Name*	<input type="text" value="LDAP"/>	
Description	<input type="text"/>	
IP Address*	<input type="text"/> ▼	+
Authentication Method	<input type="text" value="LDAP"/> ▼	
Enable SSL	<input type="checkbox"/>	
Server Type	<input type="text" value="AUTO-DETECT"/> ▼	
Port	<input type="text" value="389"/>	
Timeout	<input type="text" value="10"/> (0 - 300 Seconds)	
Base DN	<input type="text"/>	<input type="button" value="Fetch DN's"/> ex. dc=cisco,dc=com
Ldap Scope	<input type="text"/> ▼	
Username	<input type="text"/>	ex. cn=jsmith,dc=cisco,dc=com
Authentication Password	<input type="text"/>	
Confirm	<input type="text"/>	



Etapa 5. Após concluir a configuração, clique em **OK**.

Etapa 6. Salve a política e implante-a no dispositivo Firepower Threat Defense.

Observação: a autenticação externa não pode ser usada para acessar a CLI convergida sobre SSH em dispositivos com a versão de software 6.1.0

Etapa 3. Configurar o acesso SSH.

O SSH fornece acesso direto à CLI convergente. Use esta opção para acessar diretamente a CLI e executar comandos debug. Esta seção descreve como configurar o SSH para acessar a CLI do FTD.

Note: Em dispositivos FTD que executam a versão 6.0.1 do software, a configuração SSH nas configurações da plataforma fornece acesso ao CLI de diagnóstico diretamente e não ao CLISH. Você precisa se conectar ao endereço IP configurado em **br1** para acessar o CLISH. No entanto, em dispositivos FTD que executam a versão de software 6.1.0, todas as interfaces navegam para a CLI convergida quando acessadas por SSH

Há 6 etapas para configurar o SSH no ASA

Somente em dispositivos 6.0.1:

Essas etapas são executadas em dispositivos FTD com versões de software inferiores a 6.1.0 e superiores a 6.0.1. Em dispositivos 6.1.0, esses parâmetros são herdados do SO.

Etapa 1. Navegue até **Devices>Platform Settings**.

Etapa 2. Edite a política existente ao clicar no ícone do lápis ou crie uma nova política do Firepower Threat Defense ao clicar no botão **Nova política** e **selecionar o tipo como** Configurações do Threat Defense.

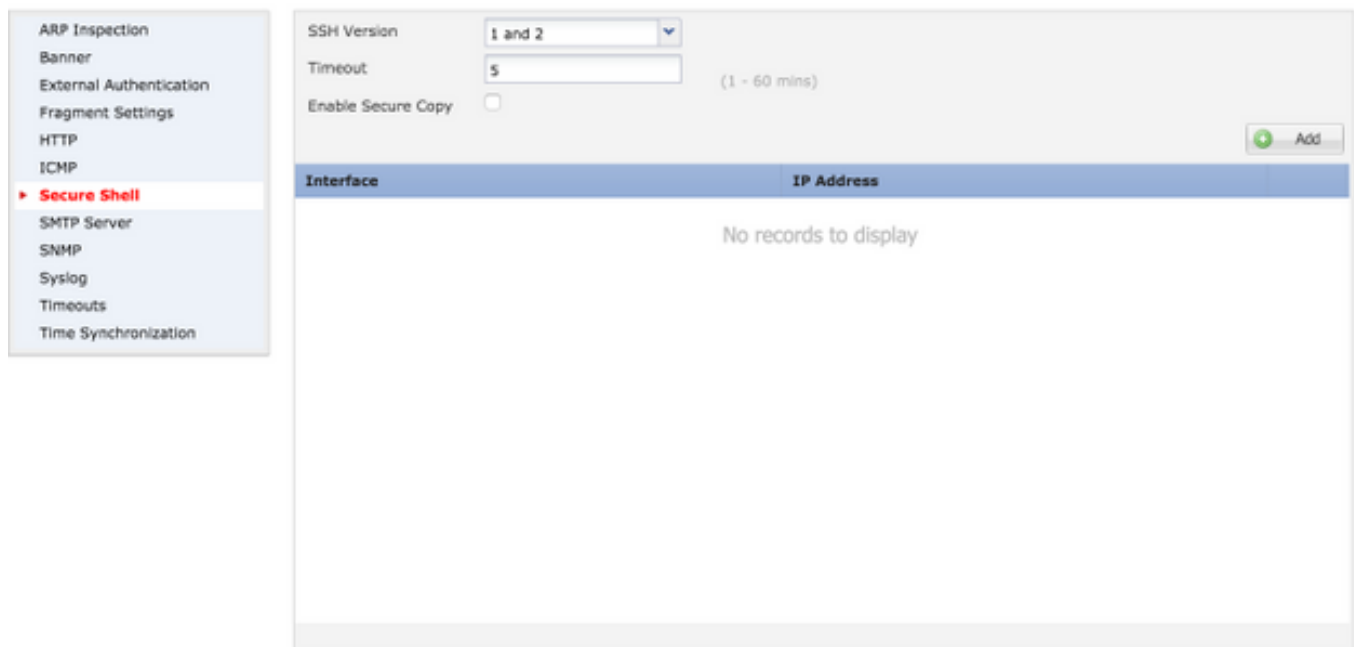
Etapa 3. Navegue até a seção **Secure Shell**. Uma página é exibida, como mostrado na imagem:

Versão do SSH: Selecione a versão do SSH a ser habilitada no ASA. Há três opções:

- **1:** Habilitar somente SSH versão 1
- **2:** Habilitar somente SSH versão 2
- **1 e 2:** Habilite as versões 1 e 2 do SSH

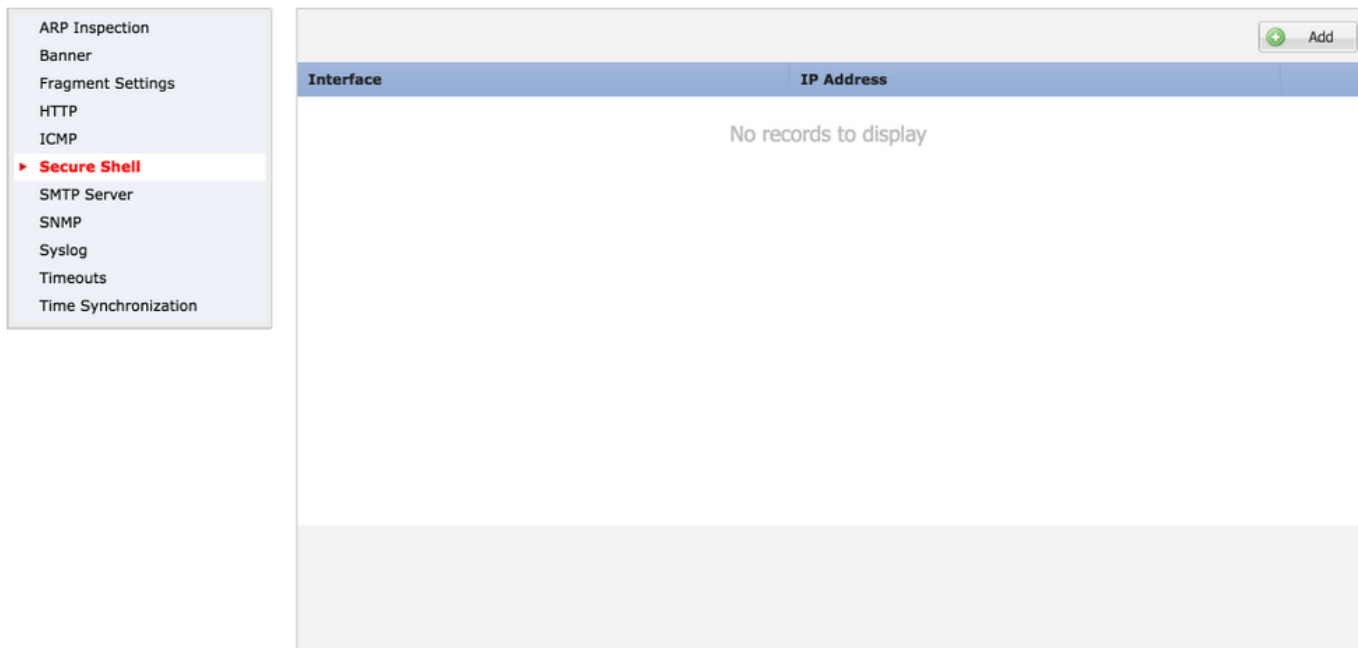
tempo limite: Insira o tempo limite de SSH desejado em minutos.

Ativar cópia segura - Ative esta opção para configurar o dispositivo para permitir conexões SCP (cópia segura) e atuar como um servidor SCP.



Em dispositivos 6.0.1 e 6.1.0:

Essas etapas são configuradas para limitar o acesso de gerenciamento via SSH a interfaces específicas e a endereços IP específicos.



Etapa 1. Clique em **Adicionar** e configure estas opções:

Endereço IP: Selecione um objeto de rede que contenha as sub-redes que têm permissão para acessar a CLI por SSH. Se não houver um objeto de rede, crie-o ao clicar no ícone (+).

Zonas/interfaces selecionadas: Selecione as zonas ou interfaces nas quais o servidor SSH é acessado.

Etapa 2. Clique em **OK**, conforme mostrado na imagem:

Edit Secure Shell Configuration



IP Address*

Available Zones

Selected Zones/Interfaces

outside

A configuração do SSH é visualizada na CLI convergente (CLI de diagnóstico do ASA em dispositivos 6.0.1) com o uso desse comando.

```
> show running-config ssh
ssh 172.16.8.0 255.255.255.0 inside
```

Etapa 3. Após concluir a configuração do SSH, clique em **Save** e implante a política no FTD.

Etapa 4. Configurar o acesso HTTPS.

Para habilitar o acesso HTTPS a uma ou mais interfaces, navegue para a seção **HTTP** nas configurações da plataforma. O acesso HTTPS é especificamente útil para baixar as capturas de pacotes da interface da Web segura de diagnóstico diretamente para a análise.

Há 6 etapas para configurar o acesso HTTPS.

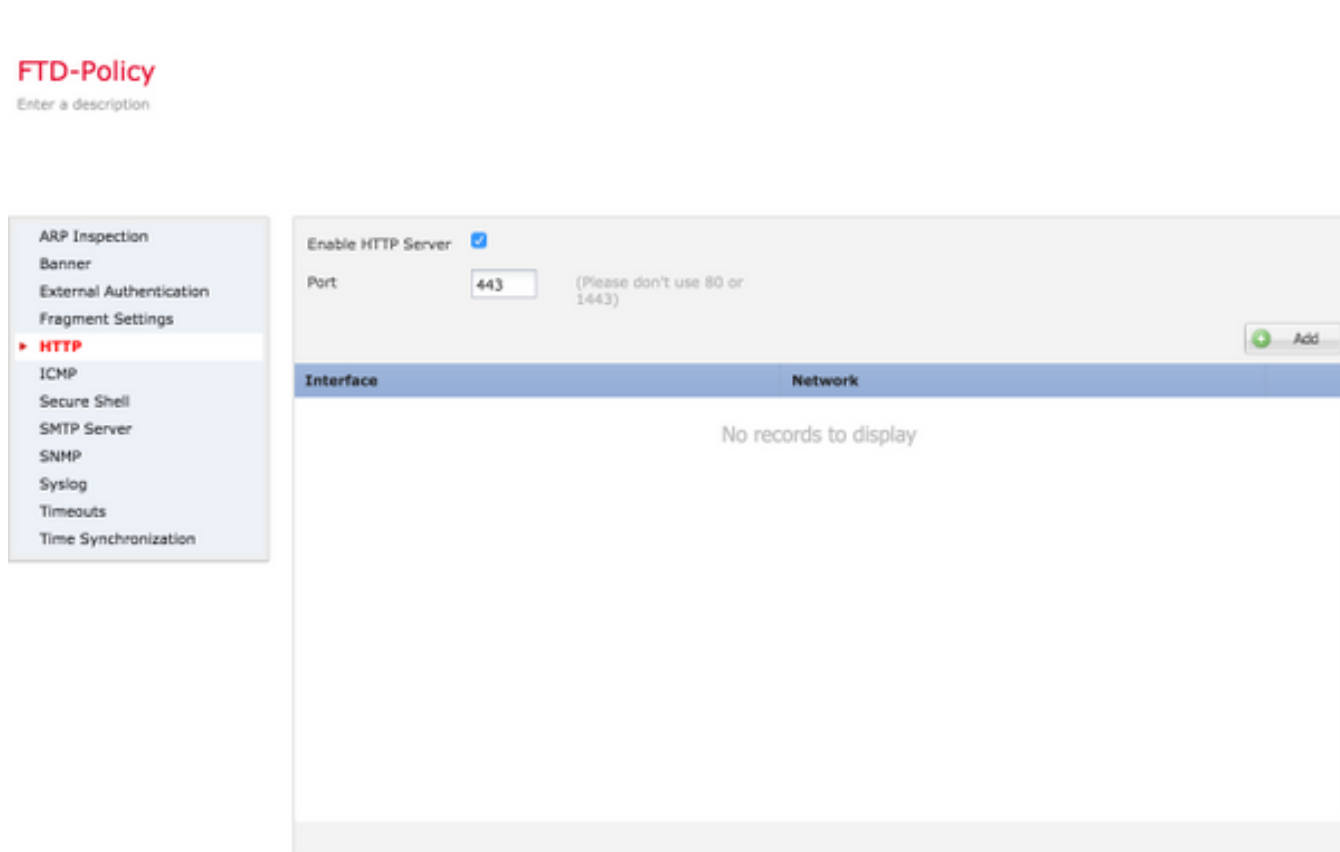
Etapa 1. Navegue até **Devices > Platform Settings**

Etapa 2. Edite a política de configurações da plataforma existente ao clicar no **ícone do lápis** ao lado da política ou crie uma nova política de FTD ao clicar em **Nova política**. Selecione o tipo **Defesa contra ameaças do Firepower**.

Etapa 3. À medida que você navega para a seção **HTTP**, uma página aparece como mostrado na imagem.

Habilitar servidor HTTP: Ative esta opção para fazer para ativar o servidor HTTP no FTD.

Porta: selecione a porta na qual o FTD aceita conexões de gerenciamento.



The screenshot shows the 'FTD-Policy' configuration interface. On the left is a sidebar menu with options: ARP Inspection, Banner, External Authentication, Fragment Settings, **HTTP** (highlighted), ICMP, Secure Shell, SMTP Server, SNMP, Syslog, Timeouts, and Time Synchronization. The main area is titled 'FTD-Policy' with a sub-header 'Enter a description'. It contains the following settings:

- Enable HTTP Server:**
- Port:** (Please don't use 80 or 1443)
- Add:**

Below these settings is a table with two columns: 'Interface' and 'Network'. The table is currently empty, displaying the text 'No records to display'.

Etapa 4. Clique em **Add** e a página aparece como mostrado na imagem:

Endereço IP- Insira as sub-redes que podem ter acesso HTTPS à interface de diagnóstico. Se não houver um objeto de rede, crie um e use a opção **(+)**.

Zonas/interfaces selecionadas- Semelhante ao SSH, a configuração HTTPS precisa ter uma interface configurada na qual seja acessível via HTTPS. Selecione as zonas ou a interface sobre a qual o FTD deve ser acessado via HTTPS.

Edit HTTP Configuration



IP Address* 10.0.0.0_16

Available Zones

Search

Selected Zones/Interfaces

outside

Add

Interface Name Add

OK Cancel

A configuração para HTTPS é visualizada na CLI convergente (CLI de diagnóstico do ASA em dispositivos 6.0.1) e usa esse comando.

```
> show running-config http
http 172.16.8.0 255.255.255.0 inside
```

Etapa 5. Depois de concluir a configuração necessária, selecione **OK**.

Etapa 6. Depois de inserir todas as informações necessárias, clique em **Salvar** e implante a política no dispositivo.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Estas são as etapas básicas para solucionar problemas de acesso de gerenciamento no FTD.

Etapa 1. Certifique-se de que a interface esteja ativada e configurada com um endereço IP.

Etapa 2. Assegure-se de que uma Autenticação externa funcione conforme configurado e que sua acessibilidade da interface apropriada especificada na seção **Autenticação externa** das **Configurações da plataforma**.

Etapa 3. Verifique se o roteamento no FTD é preciso. No software FTD versão 6.0.1, navegue para **system support diagnostic-cli**. Execute os comandos **show route** e **show route management-only** para ver as rotas para o FTD e as interfaces de gerenciamento, respectivamente.

No software FTD versão 6.1.0, execute os comandos diretamente no CLI convergente.

Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)