Configuração do acesso de gerenciamento a FTD (HTTPS e SSH) através de FMC

Índice

Introdução

Este documento descreve a configuração do acesso de gerenciamento a uma defesa da ameaça de FirePOWER (FTD) (HTTPS e SSH) através do centro de gerenciamento de FireSIGHT (FMC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento da tecnologia de FirePOWER
- Conhecimento básico de ASA (ferramenta de segurança adaptável)
- Conhecimento do acesso de gerenciamento no ASA através do HTTPS e do ssh (shell seguro)

Componentes Utilizados

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

- Imagem adaptável da defesa da ameaça de FirePOWER da ferramenta de segurança (ASA)

para o ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X), que é executado na versão de software 6.0.1 e acima
- Imagem da defesa da ameaça ASA FirePOWER para o 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 acima
- Versão 6.0.1 e mais recente do centro de gerenciamento de FirePOWER (FMC)

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Com o início da defesa da ameaça de FirePOWER (FTD), a configuração relacionada inteira ASA é feita no GUI.

Nos dispositivos FTD que executam a versão de software 6.0.1, o ASA CLI diagnóstico é alcançado enquanto você inscreve o **suporte de sistema diagnóstico-CLI**. Contudo, nos dispositivos FTD que executam a versão de software 6.1.0, o CLI é convirgido e os comandos inteiros ASA são configurados no 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
```

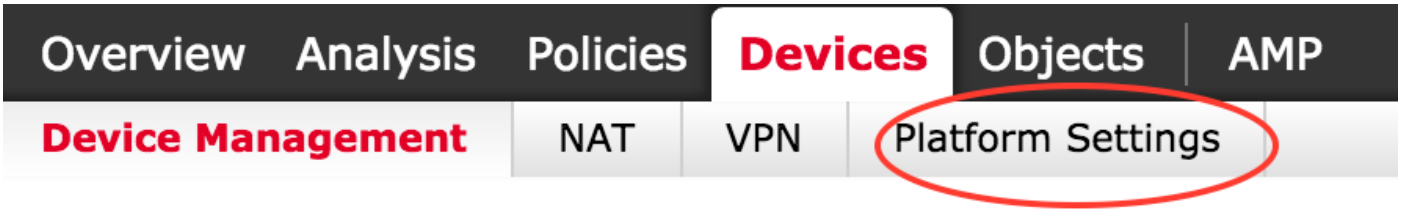
A fim ganhar o acesso de gerenciamento diretamente de uma rede externa, você deve configurar o acesso de gerenciamento através do HTTPS ou do SSH. Este documento fornece a configuração necessária exigida para ganhar externamente o acesso de gerenciamento sobre o SSH ou o HTTPS.

> **Note**: Nos dispositivos FTD que executam a versão de software 6.0.1, o CLI não pode ser alcançado por um usuário local, uma autenticação externa deve ser configurado a fim autenticar os usuários. Contudo, nos dispositivos FTD que executam a versão de software 6.1.0, o CLI está alcançado pelo usuário do admin local quando uma autenticação externa for exigida para todos usuários restantes

> **Note**: Nos dispositivos FTD que executam a versão de software 6.0.1, o CLI diagnóstico não é diretamente acessível sobre o IP que é configurado para **br1 do** FTD. Contudo, nos dispositivos FTD que executam a versão de software 6.1.0, o CLI convirgido é acessível sobre toda a relação configurada para o acesso de gerenciamento, contudo, a relação deve ser configurada com um endereço IP de Um ou Mais Servidores Cisco ICM NT.

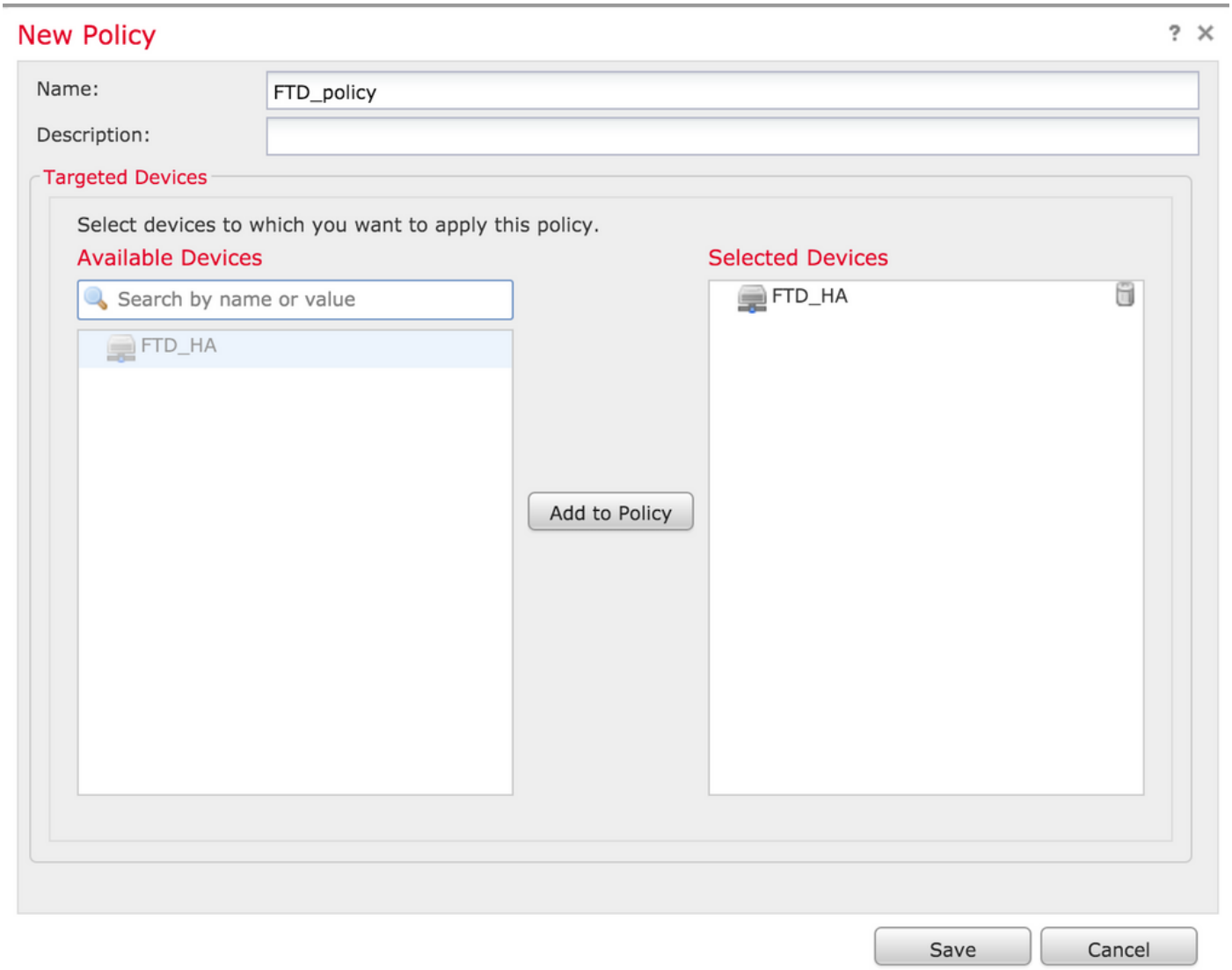
Configurar

Toda a configuração relacionada do acesso de gerenciamento é configurada como você navega à aba dos **ajustes da plataforma nos dispositivos**, segundo as indicações da imagem:



Qualquer um edita a política que existe enquanto você clica sobre o ícone do lápis ou cria uma política nova FTD como você clica o botão **novo da política** e seleciona o tipo como **ajustes da defesa da ameaça**, segundo as indicações da imagem:

Selecione o dispositivo FTD para aplicar esta política e para clicar a **salvaguarda**, segundo as indicações da imagem:



Configurar o acesso de gerenciamento

Estas são as quatro etapas principal tomadas para configurar o acesso de gerenciamento.

Etapa 1. Configurar o IP na relação FTD através de FMC GUI.

Configurar um IP na relação sobre que o FTD é acessível através do SSH ou do HTTPS. Edite as relações que existem enquanto você navega à aba das **relações do** FTD.

> **Note**: Nos dispositivos FTD que executam a versão de software 6.0.1, a interface de gerenciamento padrão no FTD é a relação diagnostic0/0. Contudo, nos dispositivos FTD que executam a versão de software 6.1.0, todas as relações apoiam o acesso de gerenciamento exceto a relação diagnóstica.

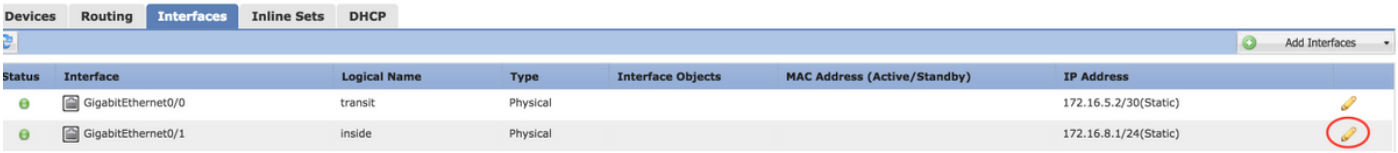
Há seis etapas para configurar a relação diagnóstica.

Etapa 1. Navegue ao **dispositivo > ao Gerenciamento de dispositivos.**

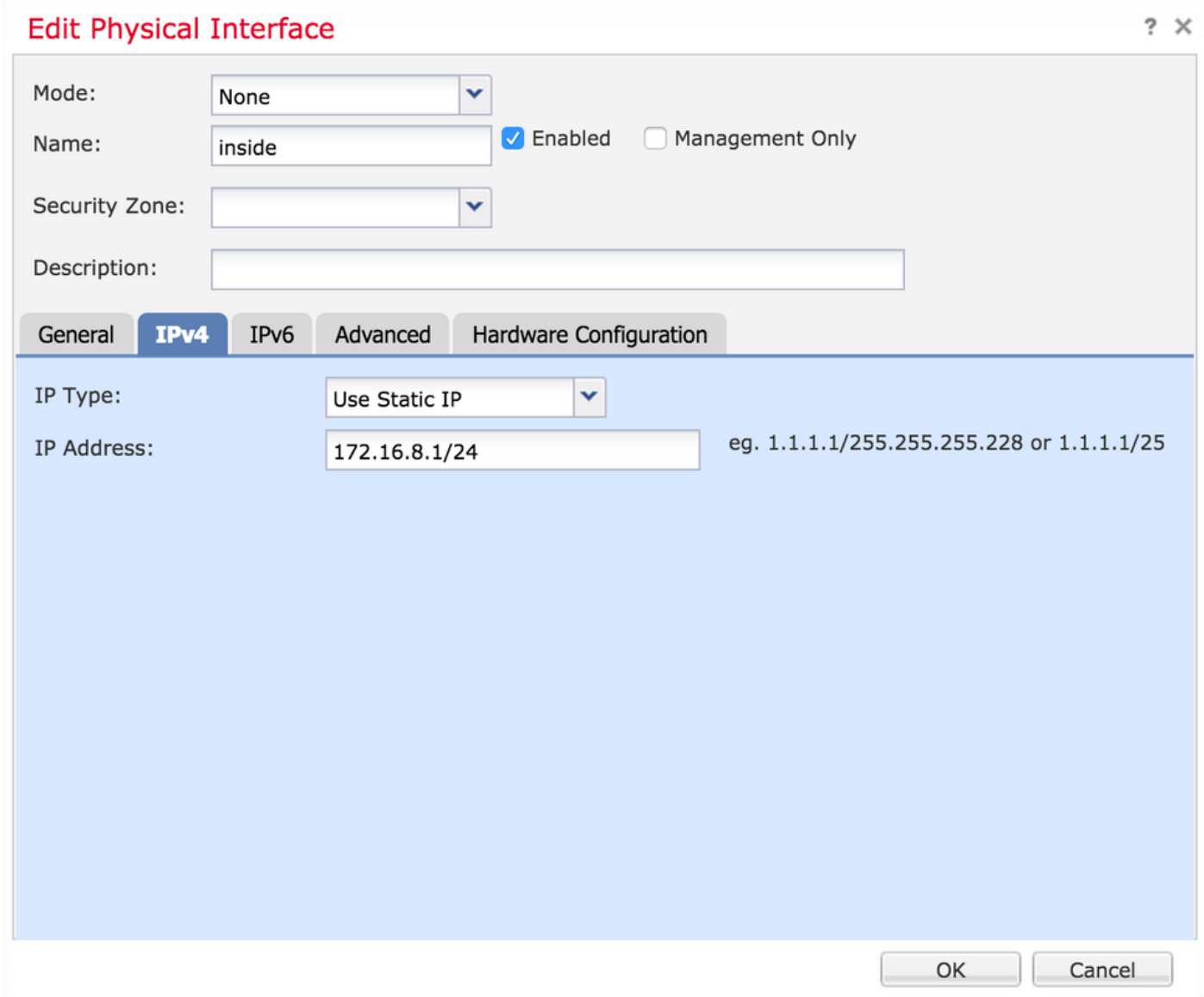
Etapa 2. Selecione o dispositivo ou o conjunto FTD HA.

Etapa 3. Navegue à aba das **relações**.

Etapa 4. Clique o **ícone do lápis** para configurar/edite a relação para ganhar o acesso de gerenciamento, segundo as indicações da imagem:



Etapa 5. Selecione a caixa de seleção da **possibilidade** para permitir as relações. Navegue à aba do **IPv4**, escolha o tipo IP como a **estática ou o DHCP**. Agora incorpore um endereço IP de Um ou Mais Servidores Cisco ICM NT para a relação e clique a **APROVAÇÃO**, segundo as indicações da imagem:



Etapa 6. Clique a **salvaguarda** e distribua então a política ao FTD.

Note: A relação diagnóstica não pode ser usada para alcançar o CLI convirgido sobre o SSH em dispositivos com versão de software 6.1.0

Etapa 2. Configurar a autenticação externa.

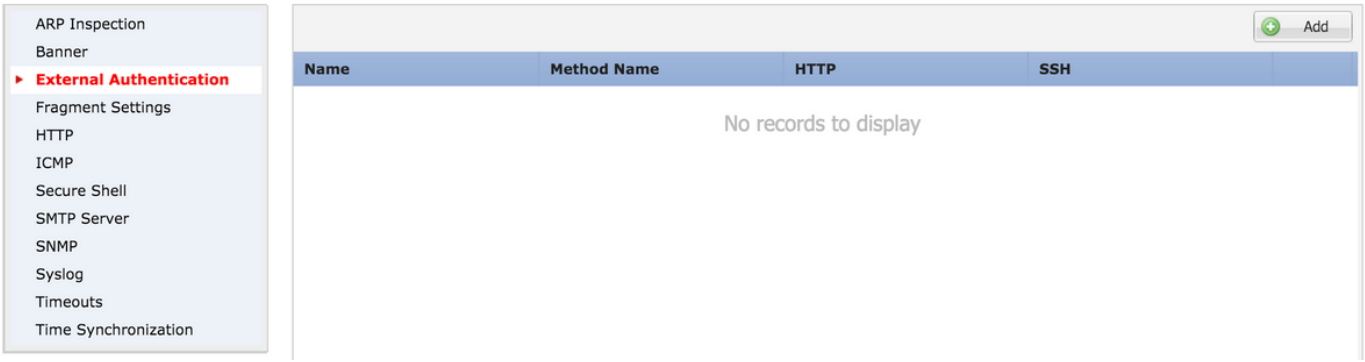
A autenticação externa facilita a integração do FTD a um diretório ativo ou a um servidor Radius para a autenticação de usuário. Esta é uma etapa necessária porque os usuários localmente configurados não têm de acesso direto ao CLI diagnóstico. O CLI diagnóstico e o GUI são alcançados somente pelos usuários que são autenticados através do Lightweight Directory Access Protocol (LDAP) ou do RAIO.

Há as etapas 6 para configurar a autenticação externa.

Etapa 1. Navegue aos **dispositivos > aos ajustes da plataforma.**

Etapa 2. Qualquer um edita a política que existe enquanto você clica sobre o ícone do lápis ou cria uma política nova FTD enquanto você clica o botão **novo da política** e seleciona o tipo como **ajustes da defesa da ameaça.**

Etapa 3. Navegue à aba da **autenticação externa**, segundo as indicações da imagem:



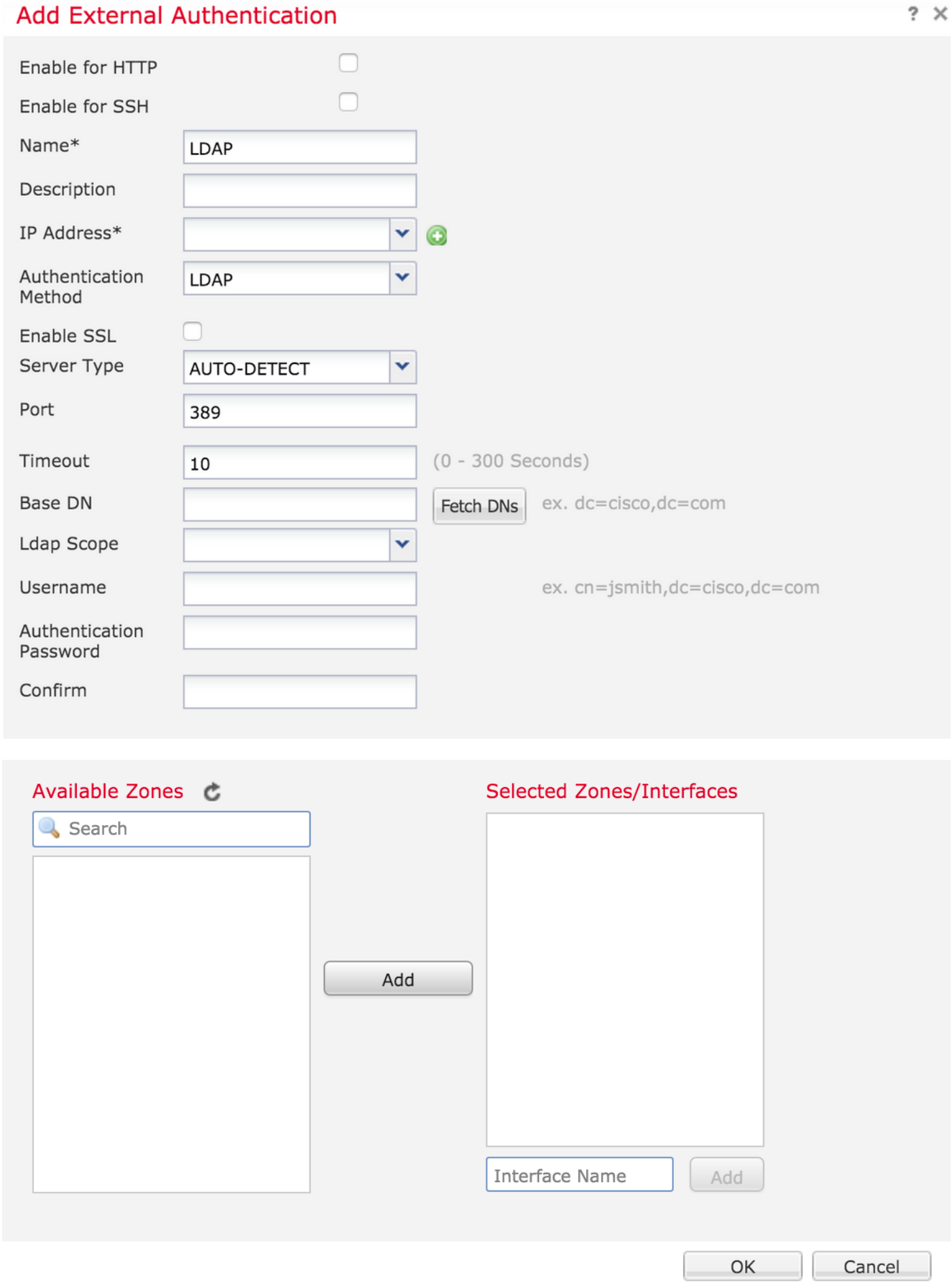
Etapa 4. Porque você clica sobre **Add**, uma caixa de diálogo aparece segundo as indicações da imagem:

- **Permita para o HTTP** permitem esta opção de fornecer o acesso o FTD sobre o HTTPS.
- **Permita para SSH-** permitem esta opção de fornecer o acesso o FTD sobre o SSH.
- **O nome** dá entrada com o nome para a conexão ldap.
- **A descrição** incorpora uma descrição opcional para o objeto da autenticação externa.
- **O endereço IP** incorpora um objeto de rede que armazene o IP do servidor de autenticação externa. Se há nenhum objeto de rede está configurado cria um novo clicando **(+) no** ícone.
- RAIO ou protocolo ldap Método-**seleto da autenticação** para a autenticação.

- **Permita SSL-permitem** esta opção de cifrar o tráfego da autenticação.
- **O tipo de server** seleciona o tipo de servidor. Os tipos de servidor conhecidos são diretório ativo, Sun, OpenLDAP e Novell MS. À revelia, a opção é ajustada auto-para detectar o tipo de servidor.
- **A porta** entra na porta sobre que a autenticação ocorre.
- **O intervalo** incorpora um valor de timeout para os pedidos de autenticação.
- **A base DN** incorpora uma base DN para fornecer um espaço dentro de que o usuário estar presente.
- **O espaço LDAP** seleciona o espaço LDAP para olhar. O espaço está dentro do mesmo nível ou para olhar dentro do subtree.
- **Username** incorpore um username para ligar ao diretório LDAP.
- **Autenticação senha-ENTER a** senha para este usuário.
- **Confirme** reenter a senha.
- **Disponível conecta a** lista A de relações disponíveis no FTD é indicado.
- **As zonas selecionadas e conectam** esta mostram uma lista de relações sobre de que o Authentication Server é alcançado.

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

O segredo incorpora a chave secreta para o RAIO.



Etapa 5. Uma vez que a configuração é feita, clique a **APROVAÇÃO.**

Etapa 6. Salvar a política e distribua-a ao dispositivo da defesa da ameaça de FirePOWER.

Note: A autenticação externa não pode ser usada para alcançar o CLI convirgido sobre o SSH em dispositivos com versão de software 6.1.0

Etapa 3. Configurar o acesso SSH.

O SSH fornece de acesso direto ao CLI convirgido. Use esta opção para alcançar diretamente o CLI e para executar comandos debug. Esta seção descreve como configurar o SSH a fim alcançar o FTD CLI.

Note: Nos dispositivos FTD que executam a versão de software 6.0.1, a configuração SSH em ajustes da plataforma fornece o acesso ao CLI diagnóstico diretamente e não o CLISH. Você precisa de conectar ao endereço IP de Um ou Mais Servidores Cisco ICM NT configurado em **br1** para alcançar o CLISH. Contudo, nos dispositivos FTD que executam a versão de software 6.1.0, todas as relações navegam ao CLI convirgido quando alcançadas sobre o SSH

Há as etapas 6 para configurar o SSH no ASA

Em 6.0.1 dispositivos somente:

Estas etapas são executadas em dispositivos FTD com a versão de software menos de 6.1.0 e maior de 6.0.1. Em 6.1.0 dispositivos estes parâmetros são herdados do OS.

Etapa 1. Navegue aos **ajustes de Devices>Platform.**

Etapa 2. Qualquer um edita a política que existe enquanto você clica sobre o ícone do lápis ou cria uma política em matéria de defesa nova da ameaça de FirePOWER enquanto você clica o botão **novo da política** e seleciona o tipo como **ajustes da defesa da ameaça.**

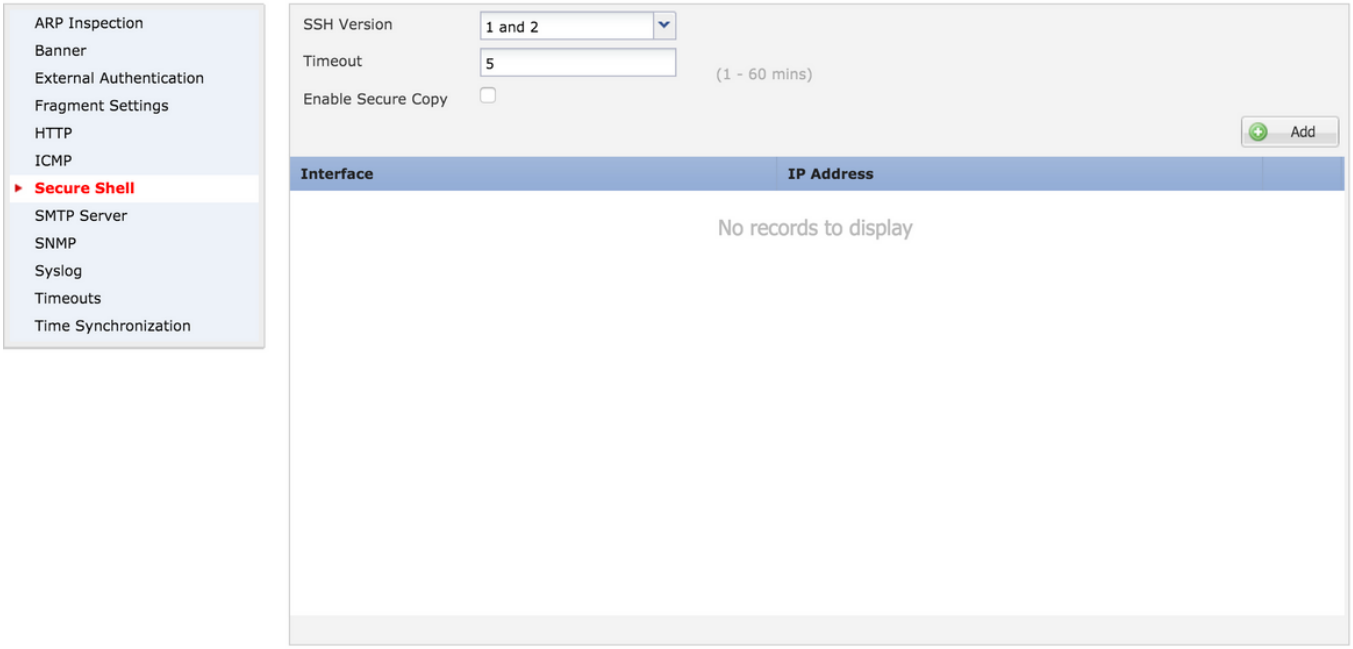
Etapa 3. Navegue à seção do **Secure Shell**. Uma página publica-se, segundo as indicações da imagem:

Versão de SSH: Selecione a versão de SSH para permitir no ASA. Há três opções:

- **1:** Permita somente a versão de SSH 1
- **2:** Permita somente a versão de SSH 2
- **1 e 2:** Permita a versão de SSH 1 e 2

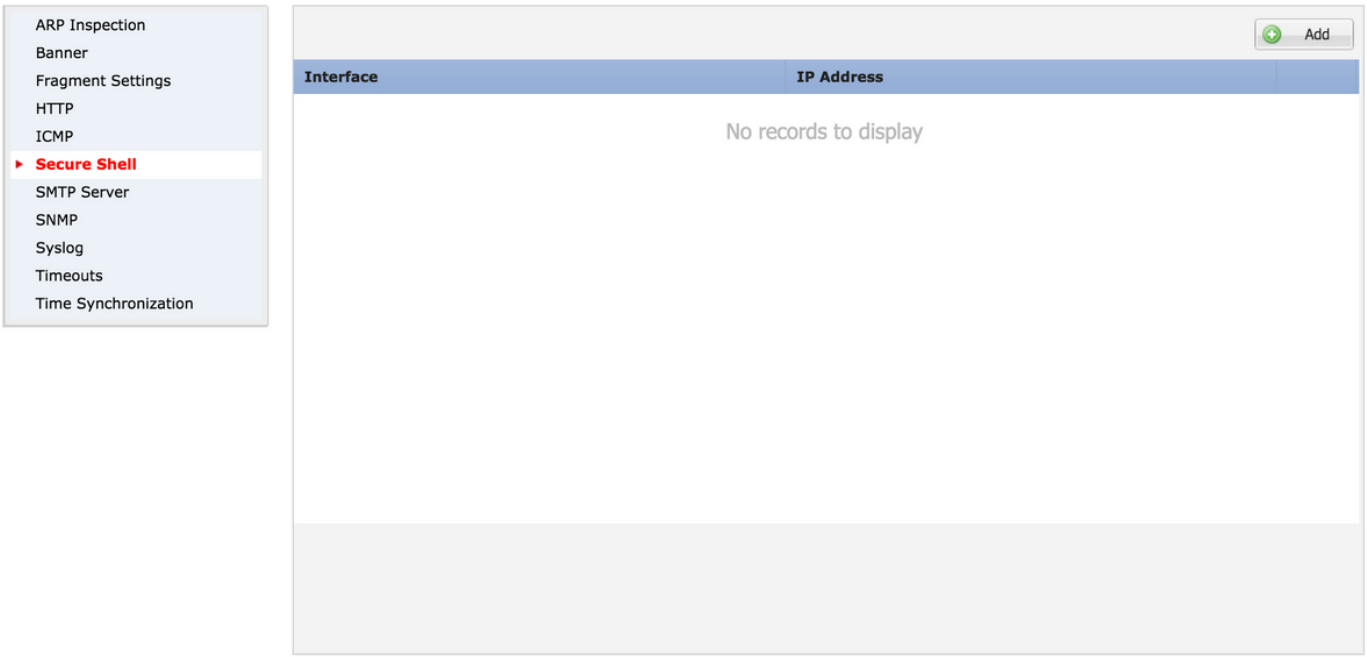
Intervalo: Incorpore o SSH timeout desejado aos minutos.

Permita a cópia segura permitem esta opção de configurar o dispositivo para permitir conexões seguras de Copy(SCP) e para atuar como um server SCP.



Em 6.0.1 e 6.1.0 dispositivos:

Estas etapas são configuradas para limitar o acesso de gerenciamento através do SSH às relações específicas e aos endereços IP de Um ou Mais Servidores Cisco ICM NT específicos.

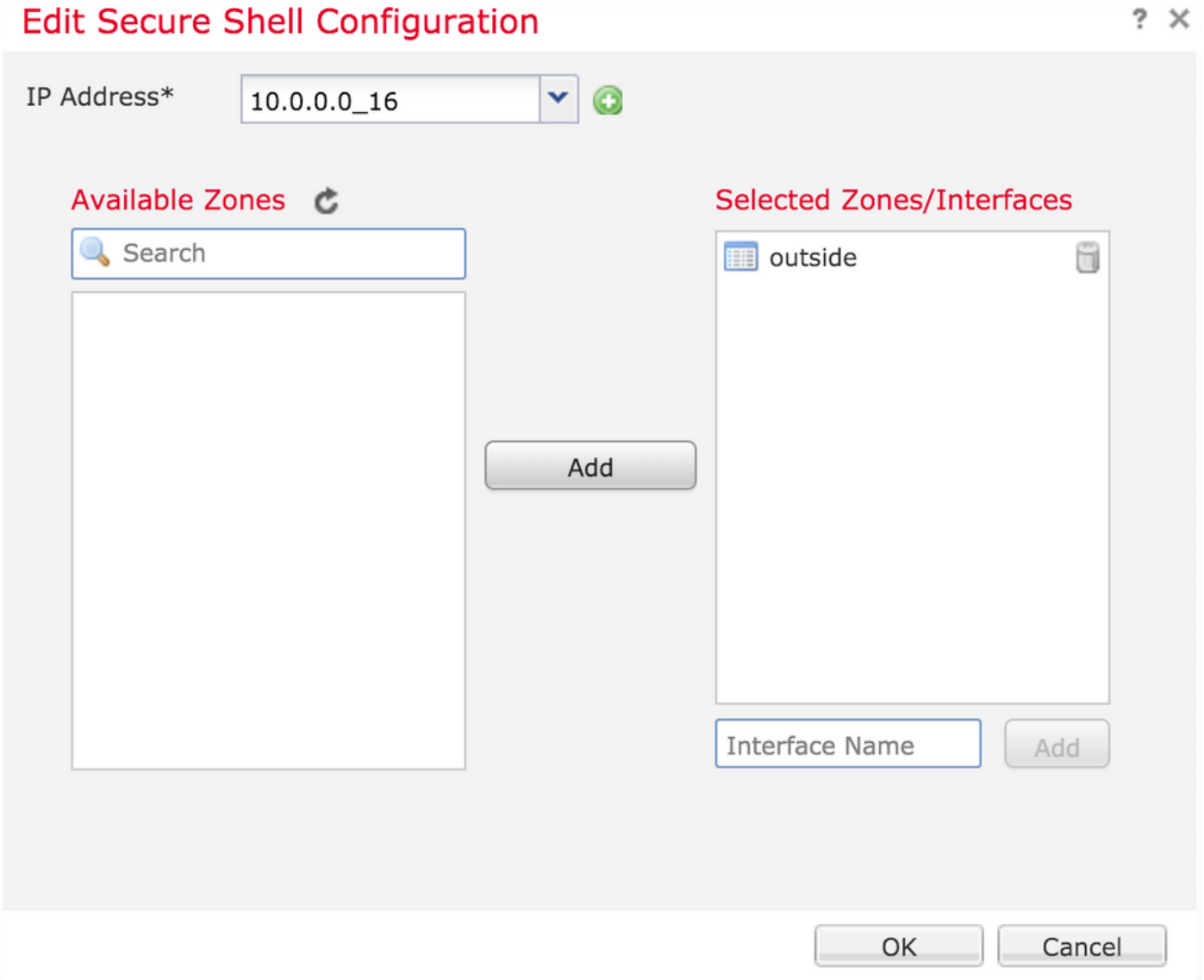


Etapa 1. Clique **adicionam** e configuram estas opções:

Endereço IP de Um ou Mais Servidores Cisco ICM NT: Selecione um objeto de rede que contenha as sub-redes que são permitidas alcançar o CLI sobre o SSH. Se um objeto de rede não está atual, crie um como você clica sobre **(+) o** ícone.

Zonas/relações selecionadas: Selecione as zonas ou as relações sobre de que o servidor de SSH é alcançado.

Etapa 2. **APROVAÇÃO do** clique, segundo as indicações da imagem:



A configuração para o SSH é vista no CLI convirgido (ASA CLI diagnóstico em 6.0.1 dispositivos) que usa este comando.

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

Etapa 3. Uma vez que a configuração SSH é feita, clique a **salvaguarda** e distribua então a política ao FTD.

Etapa 4. Configurar o acesso HTTPS.

A fim permitir o HTTPS alcance a umas ou várias relações, navegam à seção **HTTP em** ajustes da plataforma. O acesso HTTPS é especificamente útil transferir as capturas de pacote de informação da interface da WEB segura diagnóstica diretamente para a análise.

Há as etapas 6 para configurar o acesso HTTPS.

Etapa 1. Navegue aos **dispositivos > aos ajustes da plataforma**

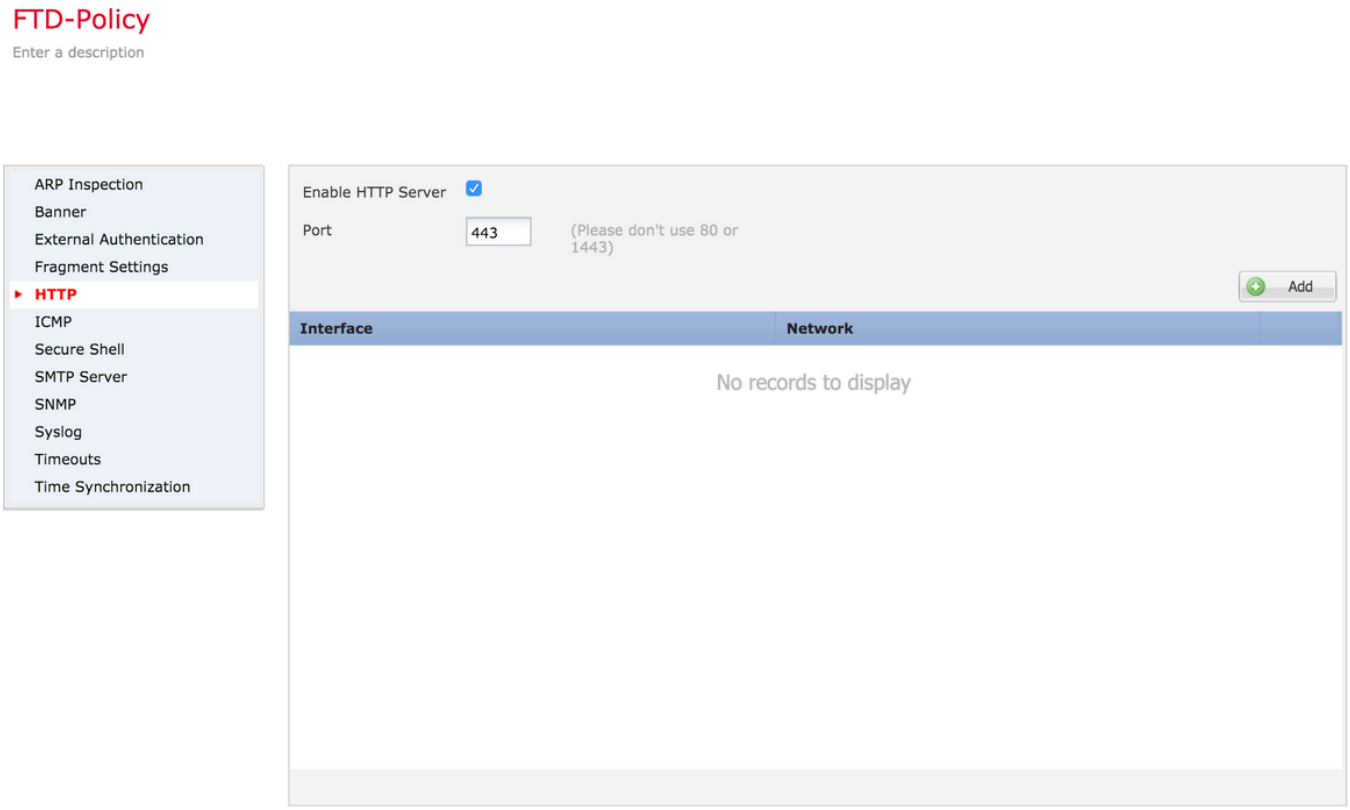
Etapa 2. Qualquer um edita a política dos ajustes da plataforma que existe enquanto você clica o

ícone do lápis ao lado da política ou cria uma política nova FTD enquanto você clica a **política nova**. Selecione o tipo como a **defesa da ameaça de FirePOWER.**

Etapa 3. Enquanto você navega à seção **HTTP**, uma página publica-se segundo as indicações da imagem.

Permita o Server do HTTP: Permita esta opção de fazer para permitir o Server do HTTP no FTD.

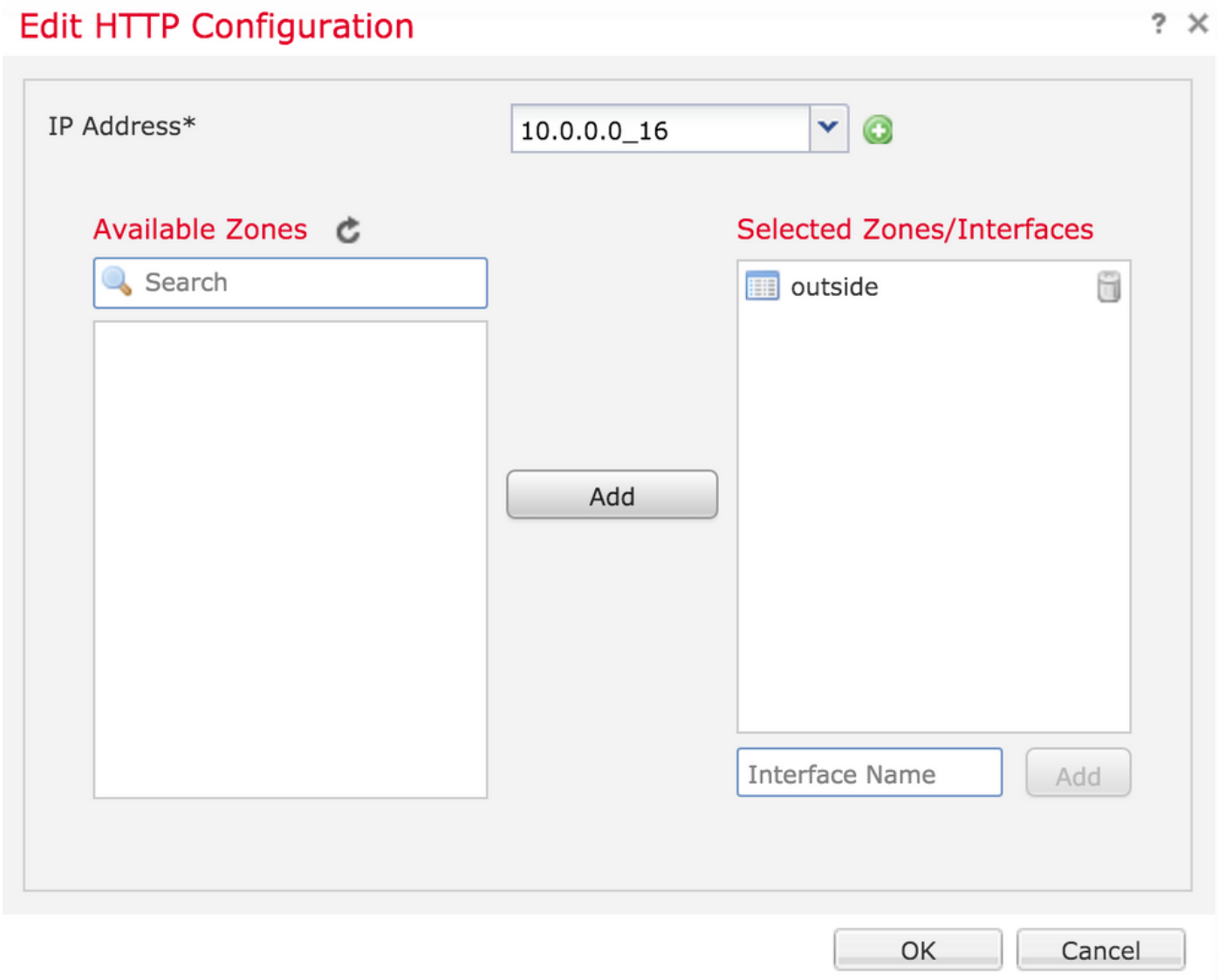
Porta: Selecione a porta em que o FTD aceita conexões de gerenciamento.



A etapa 4.Click **adiciona** e o apage aparece segundo as indicações da imagem:

O endereço IP incorpora as sub-redes que são permitidas ter o acesso HTTPS à relação diagnóstica. Se um objeto de rede não está atual crie um usando **(+) a** opção.

As zonas/relações selecionadas similares ao SSH, configuração HTTPS precisam de ter uma relação configurada sobre qual é acessível através do HTTPS. Selecione as zonas ou a relação sobre que o FTD deve ser alcançado através do HTTPS.



A configuração para o HTTPS é vista no CLI convirgido (ASA CLI diagnóstico em 6.0.1 dispositivos) que usa este comando.

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

Etapa 5. Uma vez que a configuração necessária é **APROVAÇÃO** seleta feita.

Etapa 6. Uma vez que toda a informação requerida foi **salvaguarda** incorporada do clique e distribua então a política ao dispositivo.

Verificar

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

Troubleshooting

Estas são as etapas básicas para pesquisar defeitos a edição do acesso de gerenciamento no

FTD.

Etapa 1. Assegure-se de que a relação esteja permitida e configurada com um endereço IP de Um ou Mais Servidores Cisco ICM NT.

Etapa 2. Assegure-se de que uma autenticação externa trabalhe como configurado e sua alcançabilidade da relação apropriada especificado na seção da **autenticação externa dos ajustes da plataforma**.

Etapa 3. Assegure-se de que o roteamento no FTD esteja exato. Na versão de software 6.0.1 FTD, navegue ao **suporte de sistema diagnóstico-CLI.** Execute os comandos show route e **mostre o Gerenciamento-somente da rota** para ver as rotas para o FTD e as interfaces de gerenciamento respectivamente.

Na versão de software 6.1.0 FTD, execute os comandos diretamente no CLI convirgido.

Informações Relacionadas

- Guia de início rápido da defesa da ameaça de Cisco FirePOWER para o ASA
- Suporte Técnico e Documentação - Cisco Systems