Configurar Acesso de Gerenciamento para SSH e HTTPS no FTD via FDM

Contents

Introdução

Este documento descreve o procedimento para configurar e verificar a lista de acesso de gerenciamento para SSH e HTTPS em FTD gerenciado local ou remotamente.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

- Cisco Secure Firewall Threat Defense executando a versão 7.4.1 gerenciada pelo FDM.

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.

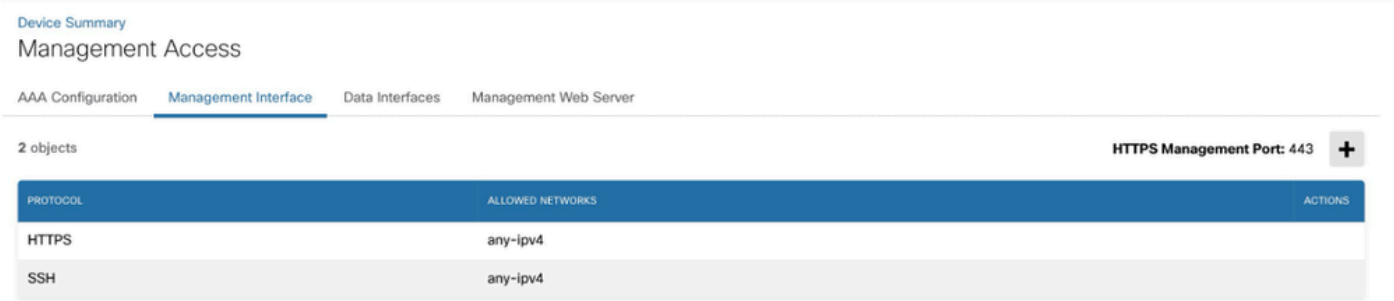
Configurar

O FTD pode ser gerenciado localmente usando o FDM ou o FMC. Neste documento, o foco está no acesso de gerenciamento via FDM e CLI. Usando a CLI, você pode fazer alterações no FDM e no FMC dos cenários.

Caution: Configure as listas de acesso SSH ou HTTPS, uma de cada vez, para evitar o bloqueio da sessão. Primeiro, atualize e implante um protocolo, verifique o acesso e, em seguida, continue com o outro.

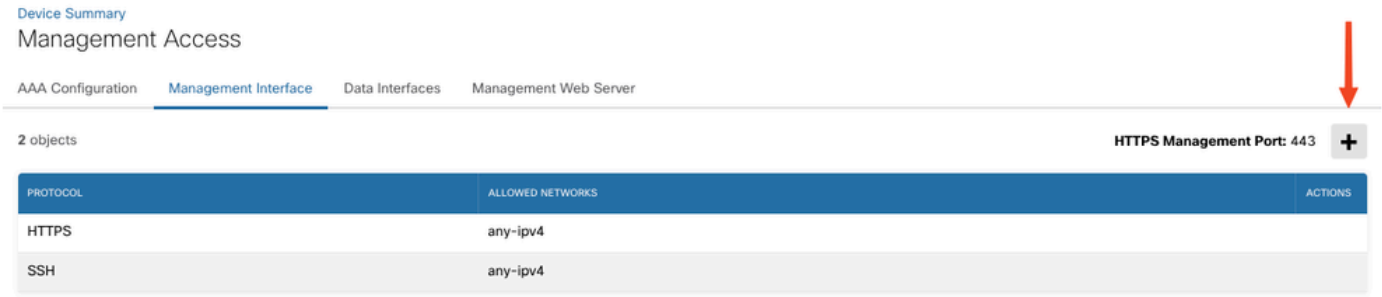
Etapas do FDM:

Passo 1: Faça logon no Firepower Device Manager (FDM) e navegue até Configurações do sistema > Acesso de gerenciamento > Interface de gerenciamento .



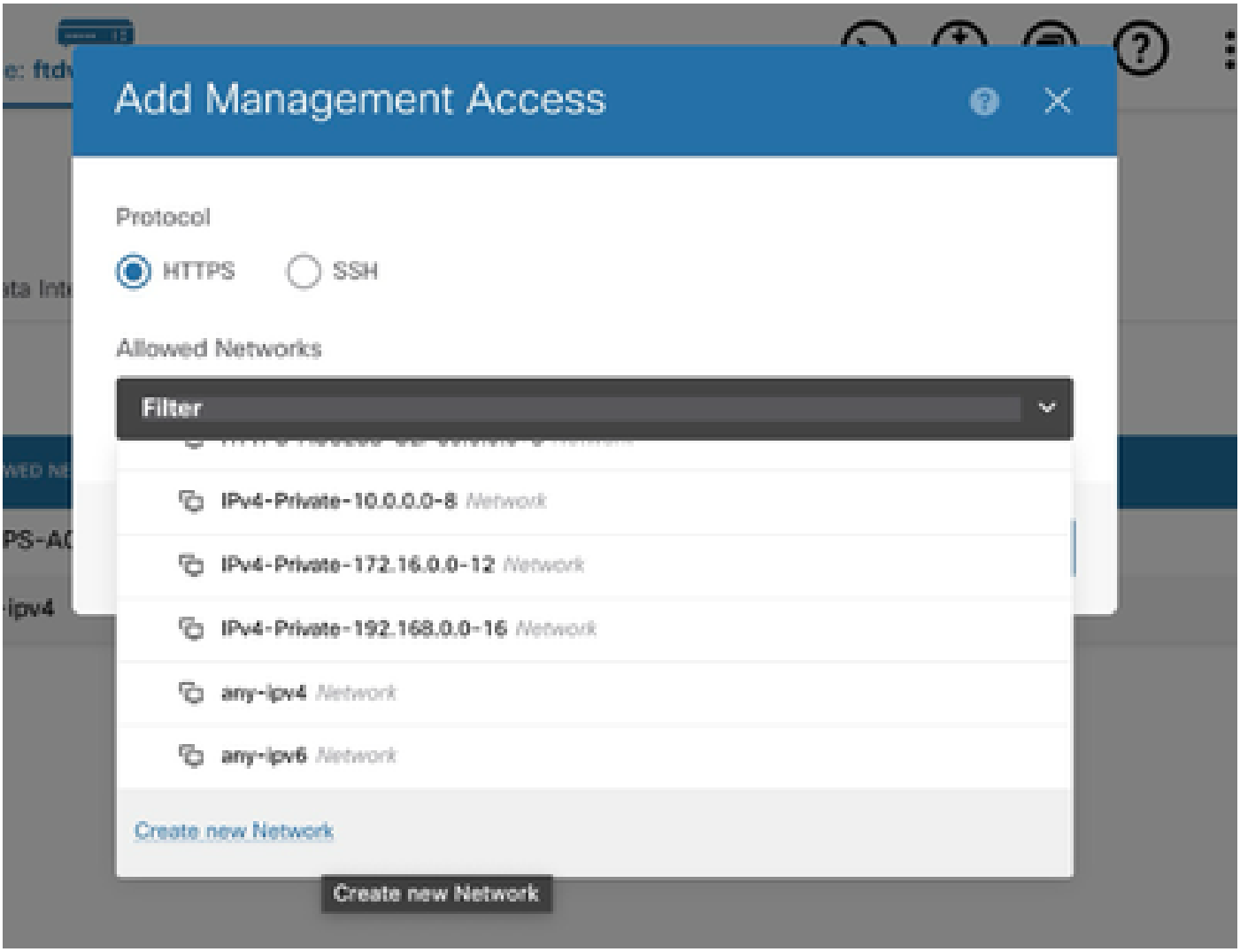
Por padrão, o acesso any-ipv4 é permitido na porta de gerenciamento para SSH e HTTPS

Etapa 2: Clique no ícone + para abrir a janela para adicionar a rede.



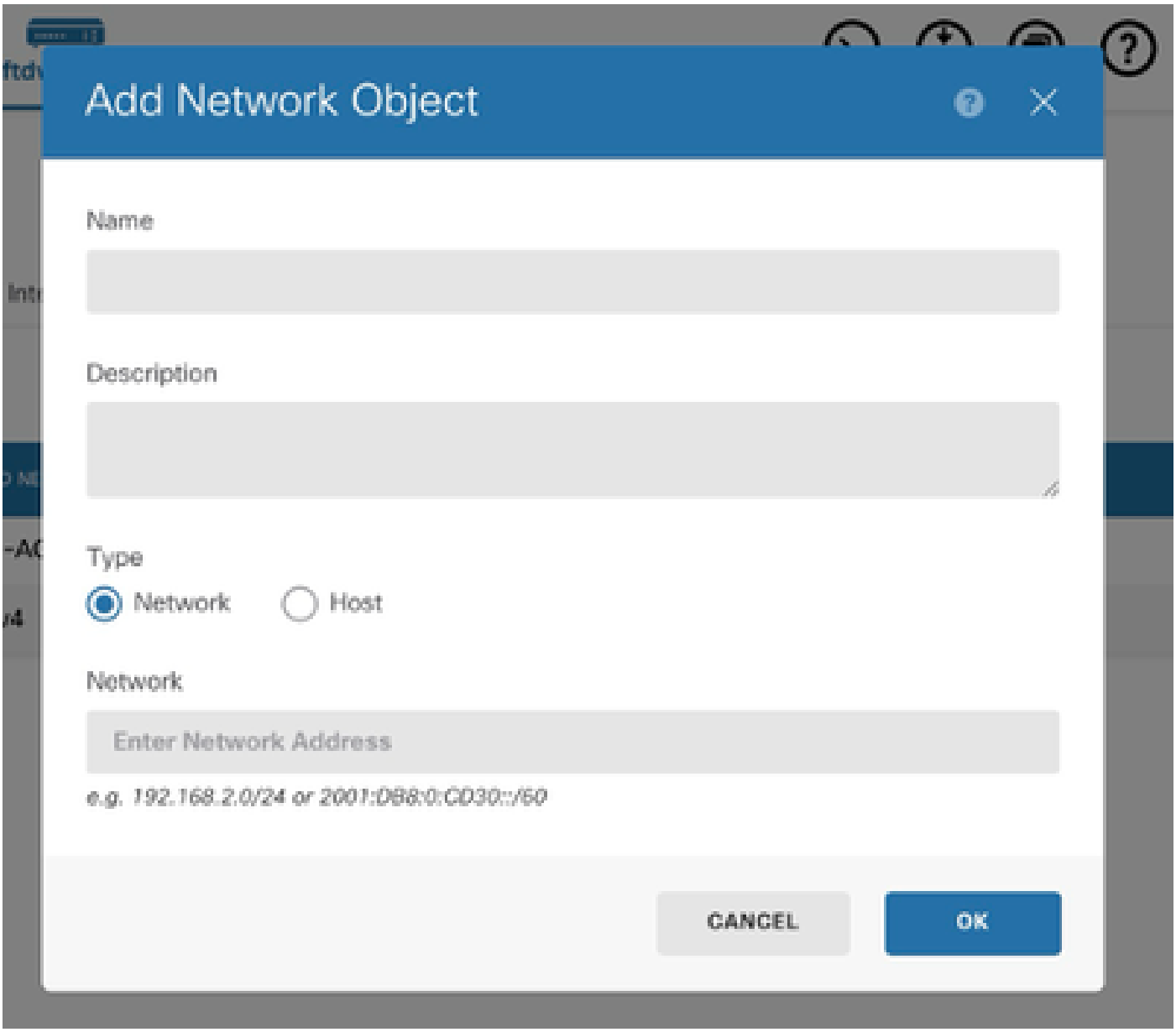
Clique no botão Adicionar no canto superior direito.

Etapa 3: adicione o objeto de rede para ter acesso SSH ou HTTPS. Se precisar criar uma nova rede, selecione a opção Criar nova rede. Você pode adicionar várias entradas para redes ou hosts no acesso de gerenciamento.



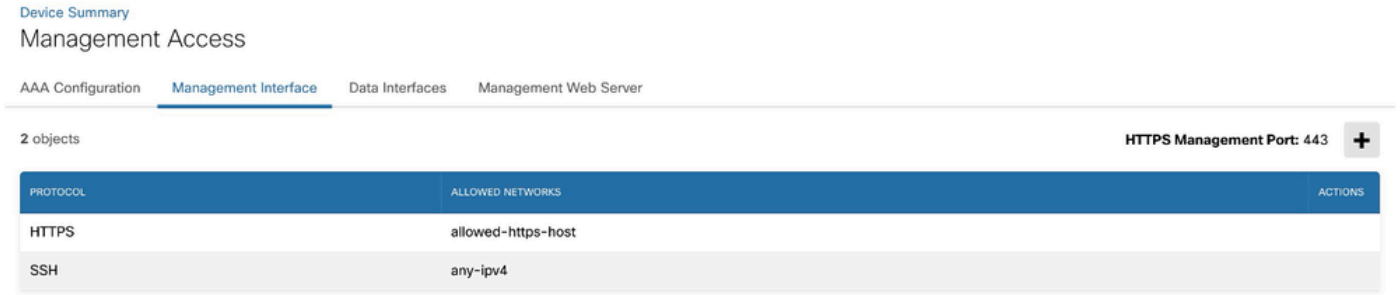
Selecione a rede.

Etapa 4 (opcional): A opção Criar nova rede abre a janela Adicionar objeto de rede.

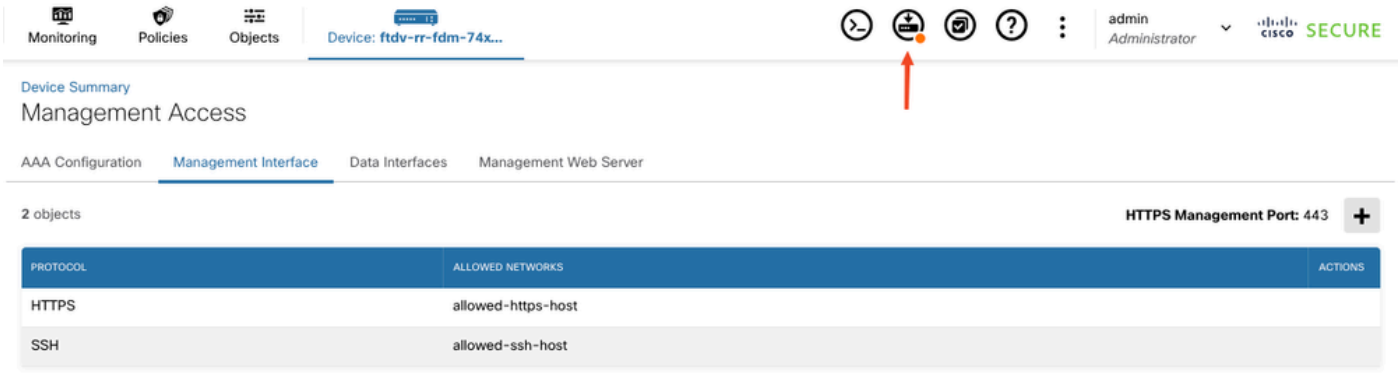


Crie uma rede de hosts conforme sua necessidade.

Etapa 5: verificar as alterações feitas e implantar.

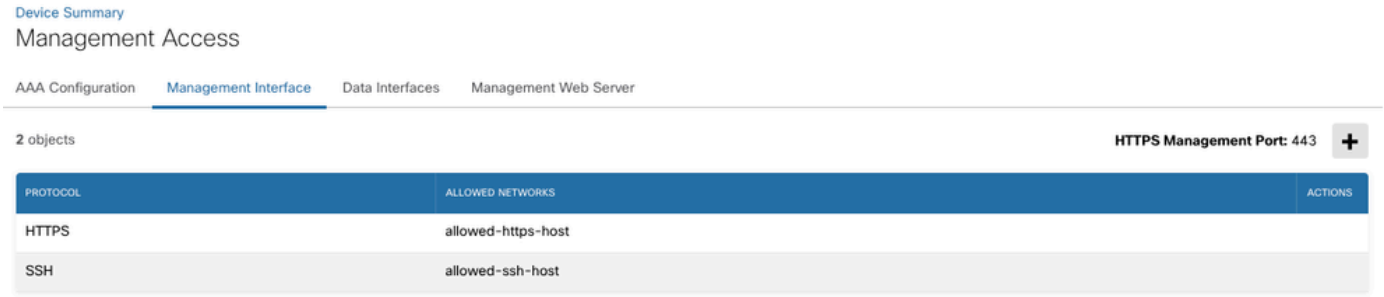


O acesso ao gerenciamento HTTPS foi alterado e qualquer ipv4 foi removido.



Implantar no FDM

Etapa 6 (Opcional): Depois que as alterações feitas anteriormente para HTTPS forem verificadas, repita o mesmo para SSH.



Objeto de rede adicionado para SSH e HTTPS.

Passo 7: Finalmente, implante as alterações e verifique seu acesso ao FTD a partir da rede e do host permitidos.

Etapas da CLISH:

As etapas da CLI podem ser usadas no caso de FDM ou FMC gerenciados.

Para configurar o dispositivo para aceitar conexões HTTPS ou SSH de endereços IP ou rede especificados, use`configure https-access-list`o `configure ssh-access-list` comando theor.

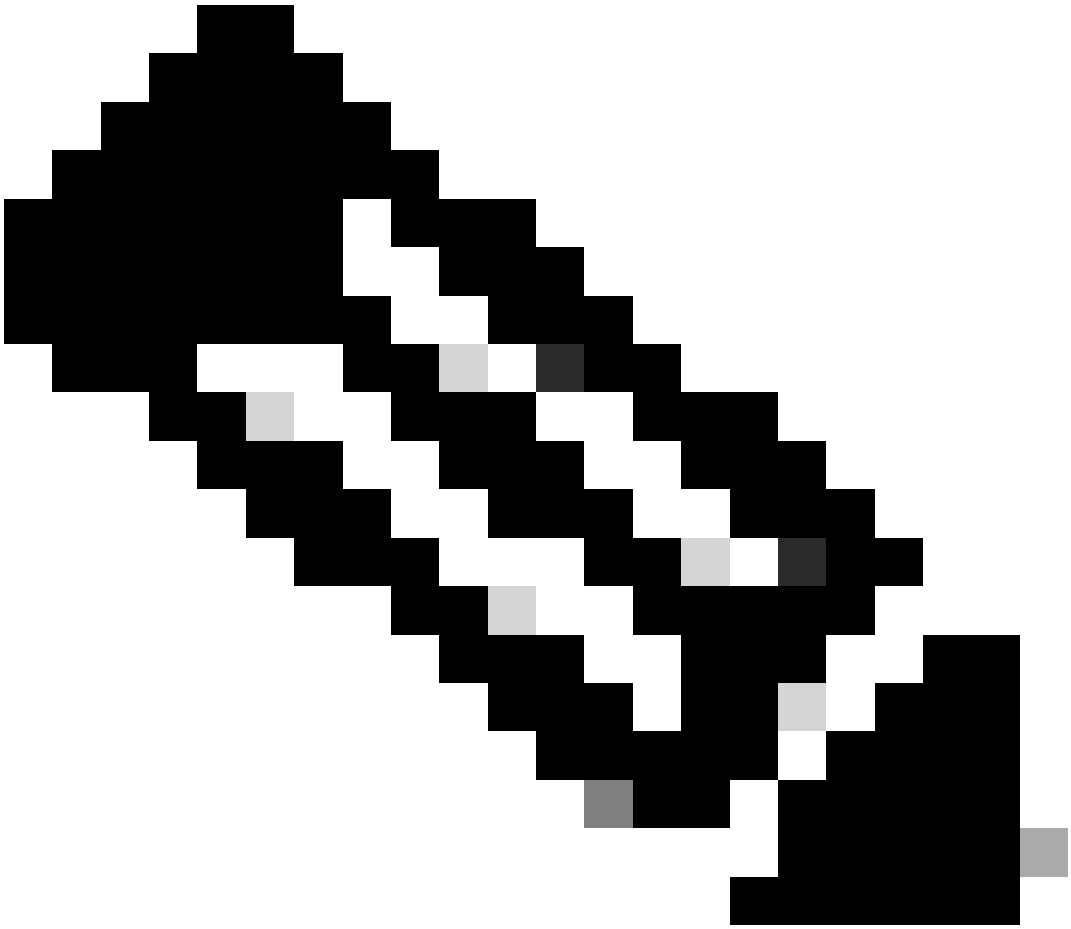
- Você deve incluir todos os hosts ou redes suportados em um único comando. Os endereços especificados nesse comando substituem o conteúdo atual da respectiva lista de acesso.
- Se o dispositivo for uma unidade em um grupo de alta disponibilidade gerenciado localmente, sua alteração substituirá na próxima vez que a unidade ativa implantar atualizações de configuração. Se essa for a unidade ativa, a alteração se propagará para o par durante a implantação.

```
> configure https-access-list x.x.x.x/x,y.y.y.y/y

The https access list was changed successfully.

> show https-access-list
```

```
ACCEPT     tcp  --  x.x.x.x/x            anywhere             state NEW tcp dpt:https
ACCEPT     tcp  --  y.y.y.y/y            anywhere             state NEW tcp dpt:https
```



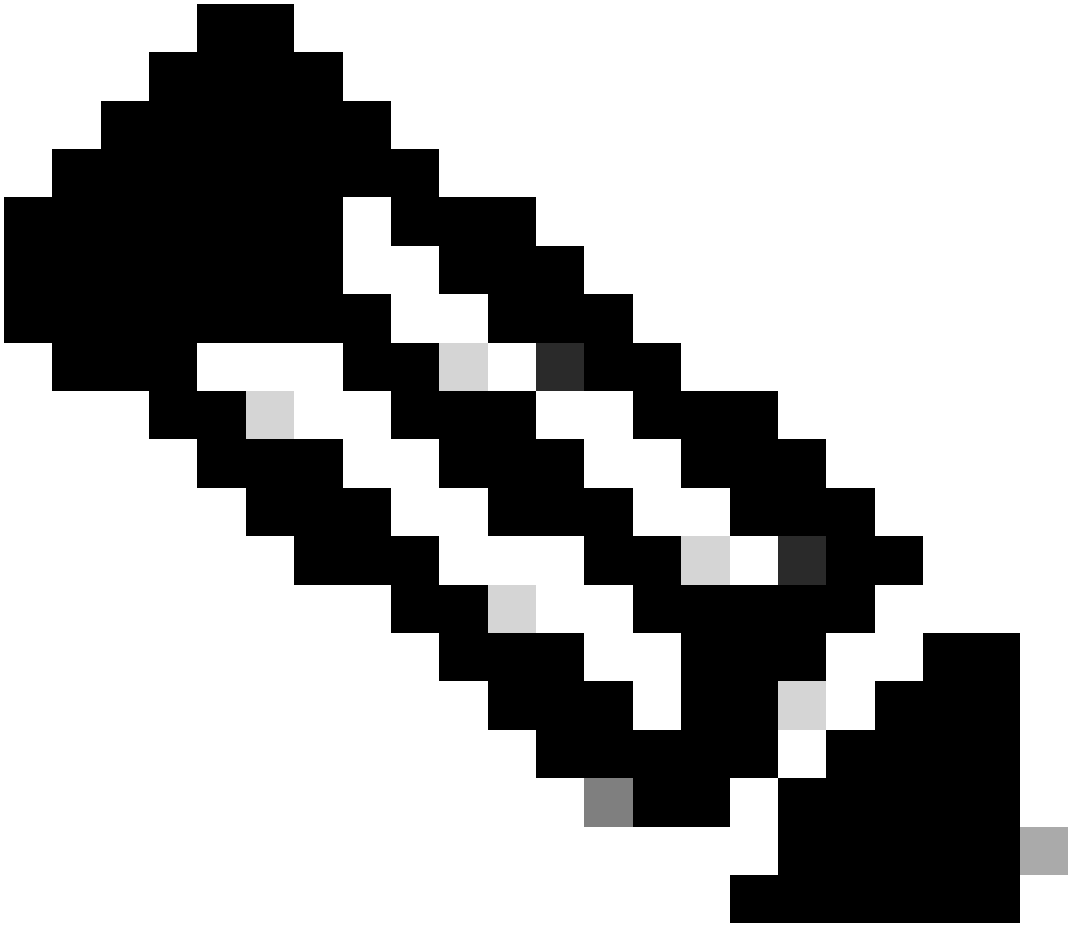
Note: x.x.x.x/x e y.y.y.y/y representa o endereço ipv4 com notação CIDR.

Da mesma forma, para conexões SSH, use o`configure ssh-access-list`comando com um ou vários comandos separados.

```
> configure ssh-access-list x.x.x.x/x

The ssh access list was changed successfully.

> show ssh-access-list
ACCEPT     tcp  --  x.x.x.x/x            anywhere             state NEW tcp dpt:ssh
```



Note: Você pode usar comandos **configure disable-https-access** ouconfigure disable-ssh-accesspara desativar o acesso HTTPS ou SSH, respectivamente. Verifique se você está ciente dessas alterações, pois isso pode bloqueá-lo fora da sessão.

Verificar

Para verificar a partir do CLISH, você pode usar comandos:

```
> show ssh-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:ssh

> show https-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:https
```

Referências

Referência de Comandos do Cisco Secure Firewall Threat Defense

Guia de configuração do Cisco Firepower Threat Defense para o gerenciador de dispositivos Firepower

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.