FDMを介したFTDでのSSHおよびHTTPSの管理アクセスの設定

内容

はじめに

このドキュメントでは、ローカルまたはリモートで管理されるFTDでSSHおよびHTTPSの管理アクセスリストを設定および確認する手順について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

- FDMによって管理されるバージョン7.4.1を実行しているCisco Secure Firewall Threat Defense。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

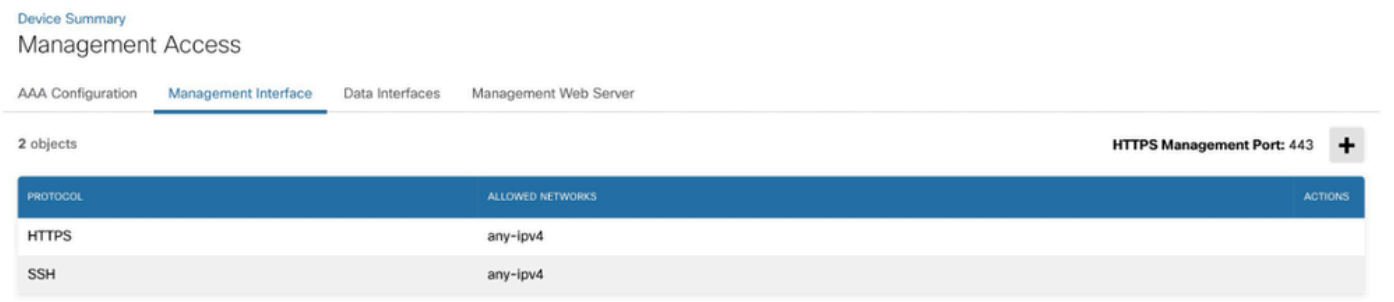
設定

FTDは、FDMを使用してローカルで管理するか、FMCを介して管理できます。このドキュメントでは、FDMおよびCLIを介した管理アクセスに重点を置いています。CLIを使用すると、シナリオFDMとFMCの両方に変更を加えることができます。

注意：セッションロックアウトを回避するために、SSHまたはHTTPSアクセスリストを1つずつ設定します。まず、1つのプロトコルを更新して展開し、アクセスを確認してから、もう1つのプロトコルに進みます。

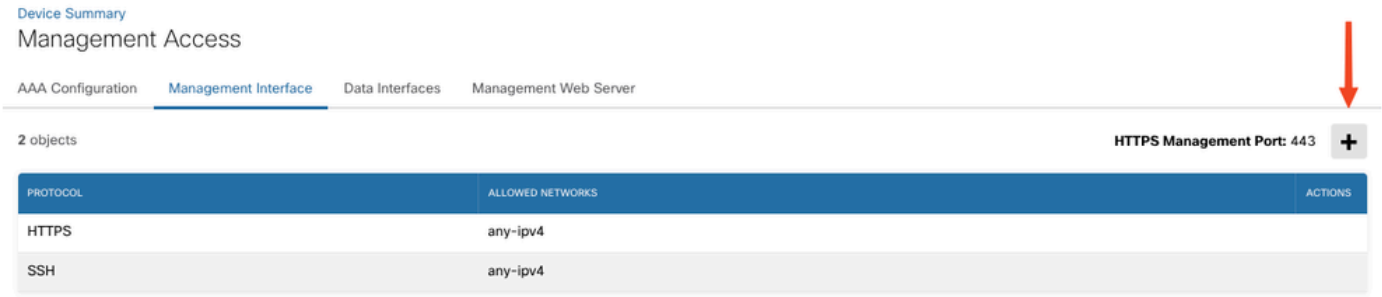
FDM手順：

ステップ1:Firepower Device Manager(FDM)にログインし、System Settings > Management Access > Management Interfaceの順に移動します。



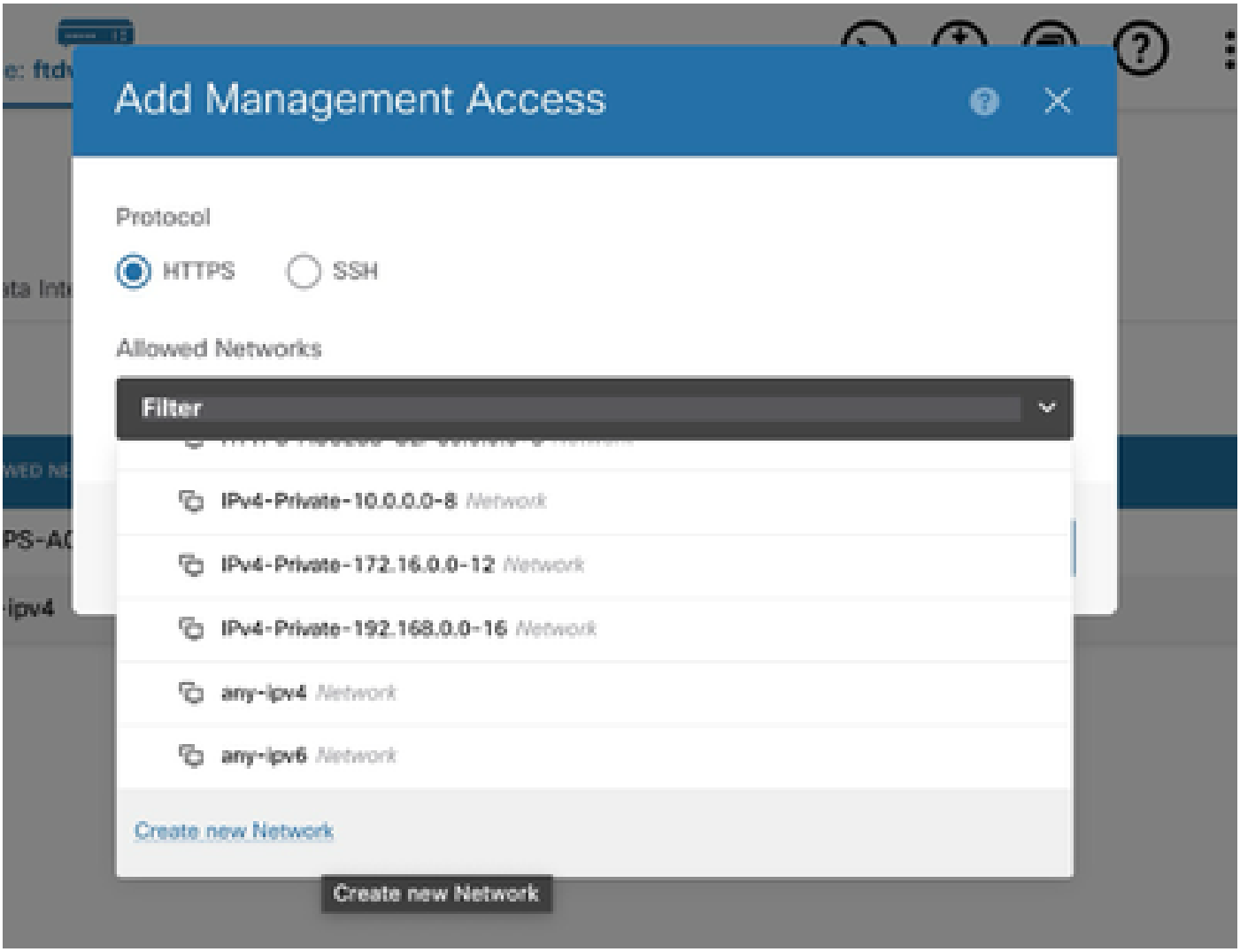
デフォルトでは、SSHおよびHTTPSの管理ポートでany-ipv4アクセスが許可されます

ステップ2:+アイコンをクリックして、ネットワークを追加するためのウィンドウを開きます。



右上のAddボタンをクリックします。

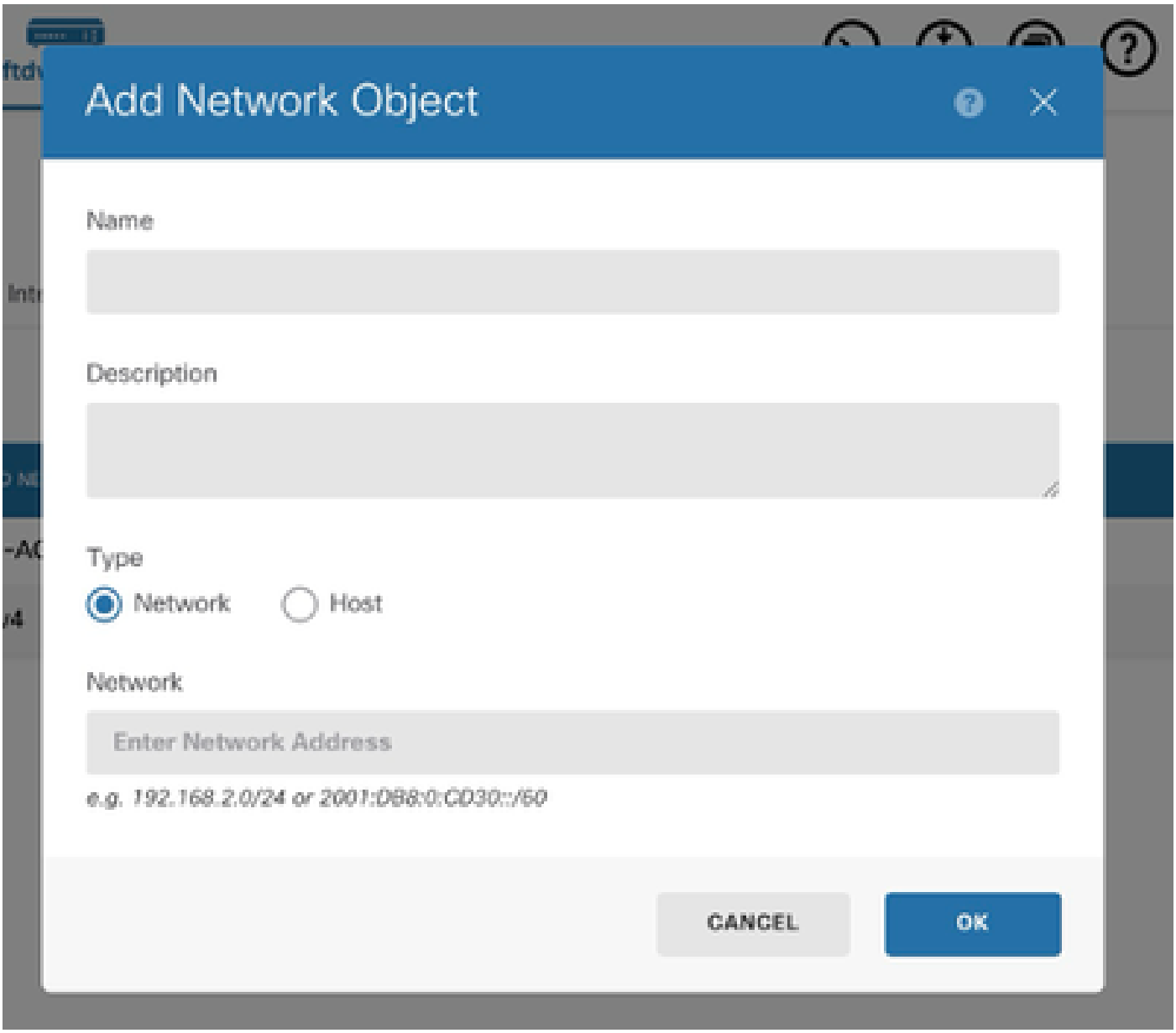
ステップ3:ネットワークオブジェクトを追加して、SSHまたはHTTPSアクセスを許可します。新しいネットワークを作成する必要がある場合は、Create new Networkオプションを選択します。管理アクセスでは、ネットワークまたはホストに対して複数のエントリを追加できます。



ネットワークを選択します。

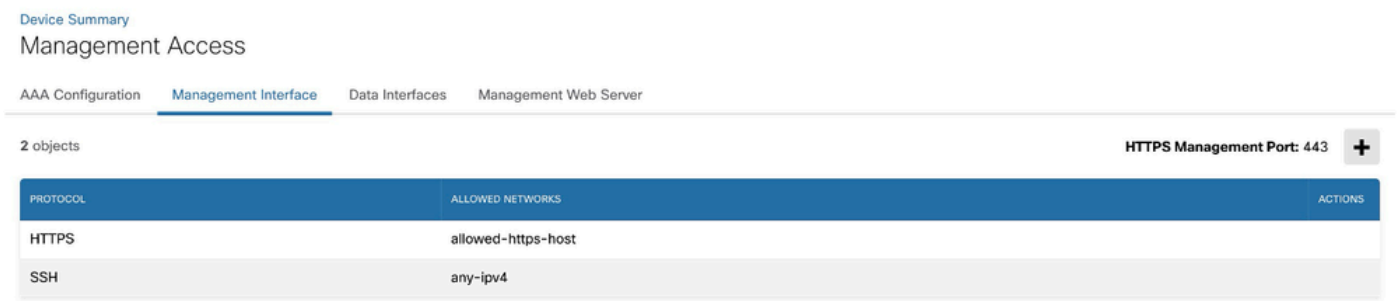
ステップ4（オプション）:Create new Networkオプションを選択すると、Add Network Objectウ

ィンドウが開きます。

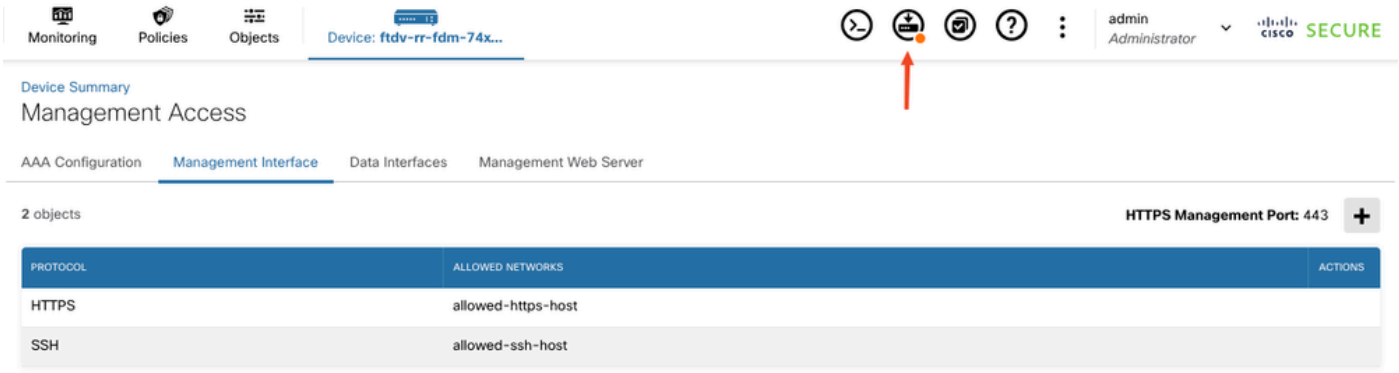


必要に応じて、ホストのネットワークを作成します。

手順5:変更を確認し、導入します。

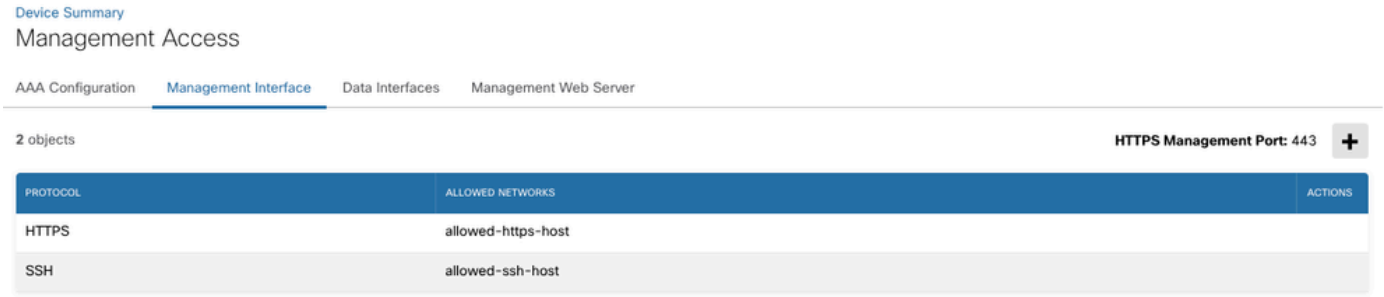


HTTPS管理アクセスが変更され、any-ipv4が削除されました。



FDMでの配置

ステップ6（オプション）:以前に行ったHTTPSの変更を確認したら、SSHについても同じ手順を繰り返します。



SSHおよびHTTPSのネットワークオブジェクトを追加。

ステップ7:最後に変更を導入し、許可されたネットワークとホストからFTDへのアクセスを確認します。

クリックの手順:

CLIステップは、FDMとFMCの両方が管理されている場合に使用できます。

指定したIPアドレスまたはネットワークからのHTTPS接続またはSSH接続を受け入れるようにデバイスを設定するには、configure https-access-listconfigure ssh-access-listtheorcommandを使用します。

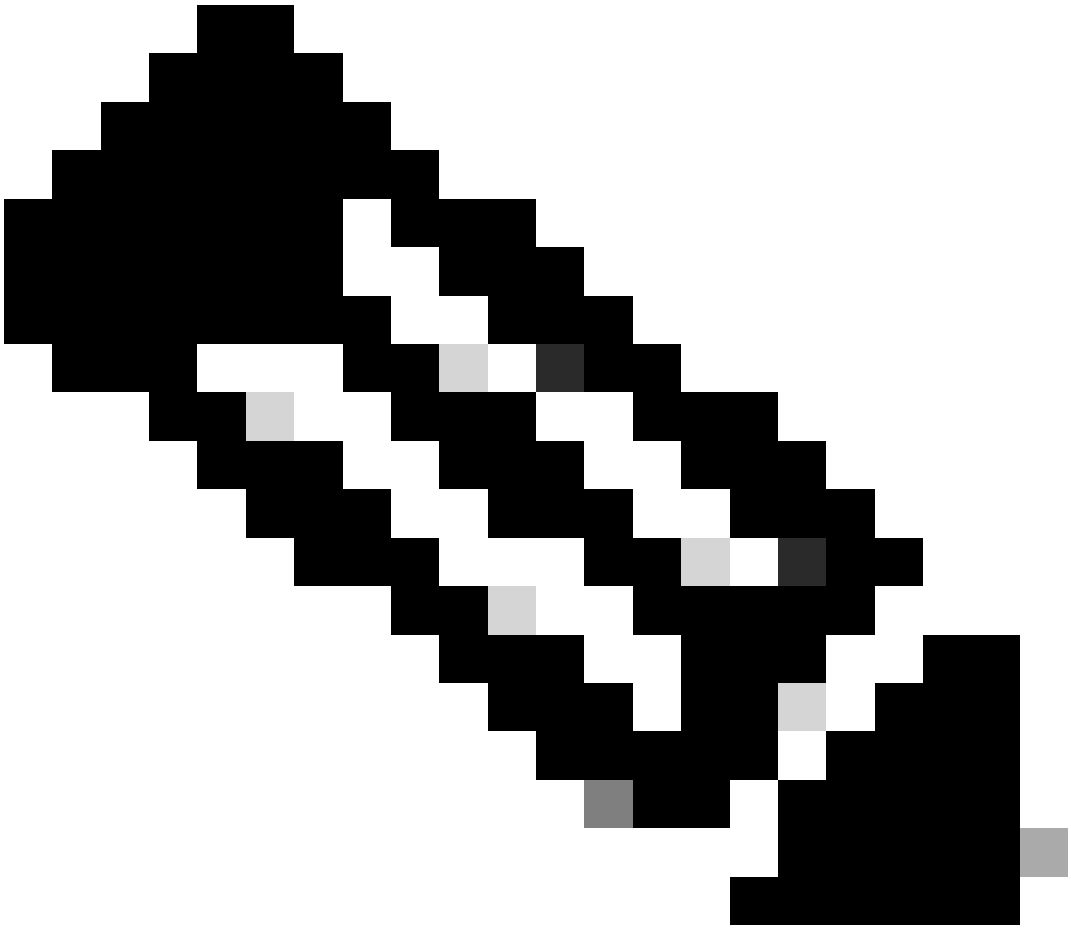
- サポートされているすべてのホストまたはネットワークを1つのコマンドに含める必要があります。このコマンドで指定されたアドレスは、それぞれのアクセスリストの現在の内容を上書きします。
- デバイスがローカルで管理されるハイアベイラビリティグループ内のユニットである場合、アクティブユニットが次回に設定の更新を導入するときに、この変更が上書きされます。これがアクティブユニットの場合、変更は導入時にピアに伝搬されます。

```
> 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
```



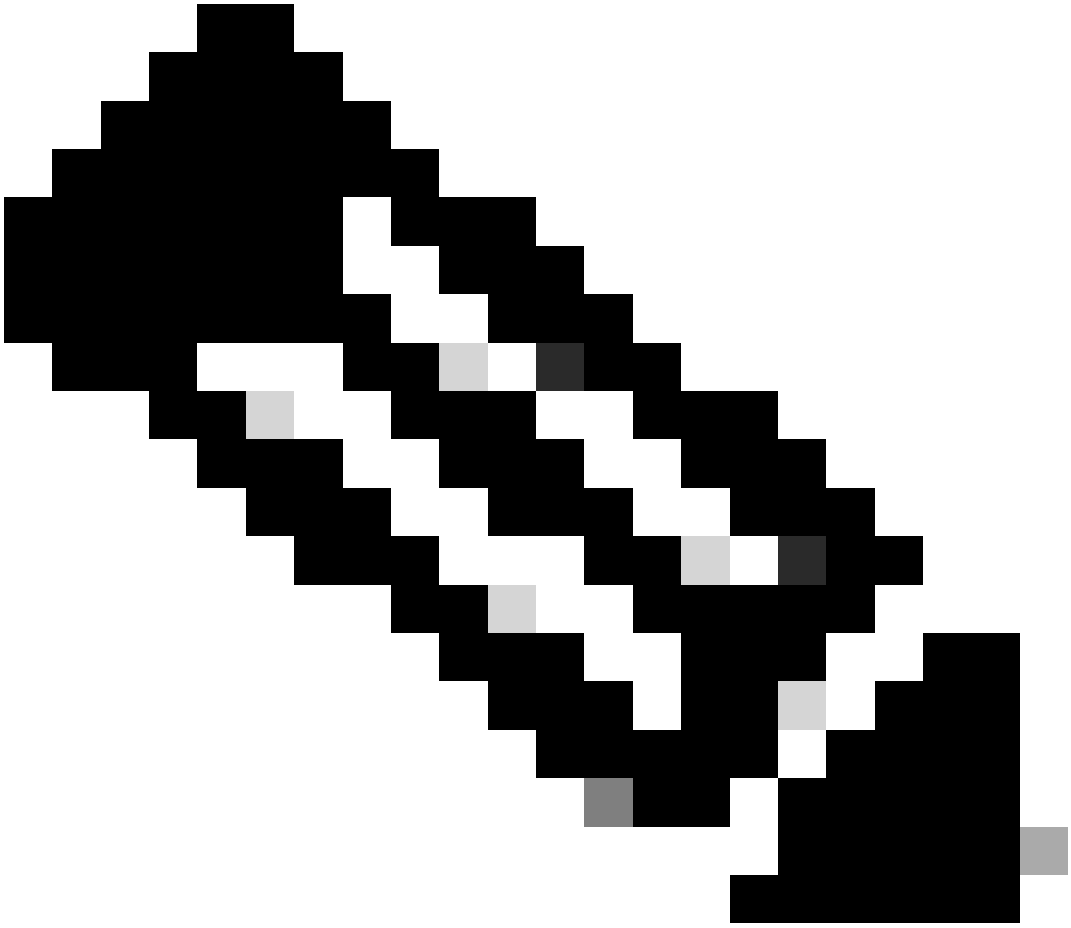
注:x.x.x.x/xおよびy.y.y.y/yはCIDR表記のipv4アドレスを表します。

同様に、SSH接続の場合は、configure ssh-access-listコマンドを1つまたは複数のコマンドで区切って使用します。

```
> 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
```



注：**configure disable-https-access**コマンドまたはconfigure disable-ssh-accessコマンドを使用して、それぞれHTTPSアクセスまたはSSHアクセスを無効にすることができます。セッションからロックアウトされる可能性があるため、これらの変更に注意してください。

確認

CLISHから確認するには、次のコマンドを使用できます。

```
> 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
```

参考資料

Cisco Secure Firewall Threat Defenseコマンドリファレンス

Firepower Device Manager用Cisco Firepower Threat Defense設定ガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。