Konfigurieren des Managementzugriffs für SSH und HTTPS auf FTD über FDM

Inhalt

Einleitung

In diesem Dokument wird das Verfahren zur Konfiguration und Verifizierung der Management-Zugriffsliste für SSH und HTTPS auf lokal oder remote verwaltetem FTD beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

- Cisco Secure Firewall Threat Defense mit Version 7.4.1, verwaltet von FDM

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

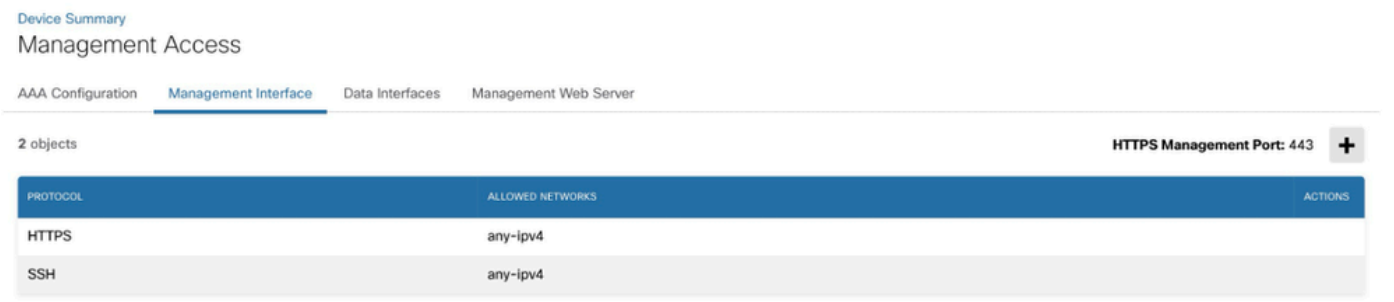
Konfigurieren

FTD kann lokal mithilfe von FDM oder über FMC verwaltet werden. In diesem Dokument liegt der Schwerpunkt auf dem Managementzugriff über FDM und CLI. Mit CLI können Sie Änderungen sowohl für FDM als auch für FMC vornehmen.

Vorsicht: Konfigurieren Sie SSH- oder HTTPS-Zugriffslisten nacheinander, um eine Sitzungssperre zu vermeiden. Aktualisieren und Bereitstellen eines Protokolls, Überprüfen des Zugriffs und Fortfahren mit dem anderen Protokoll

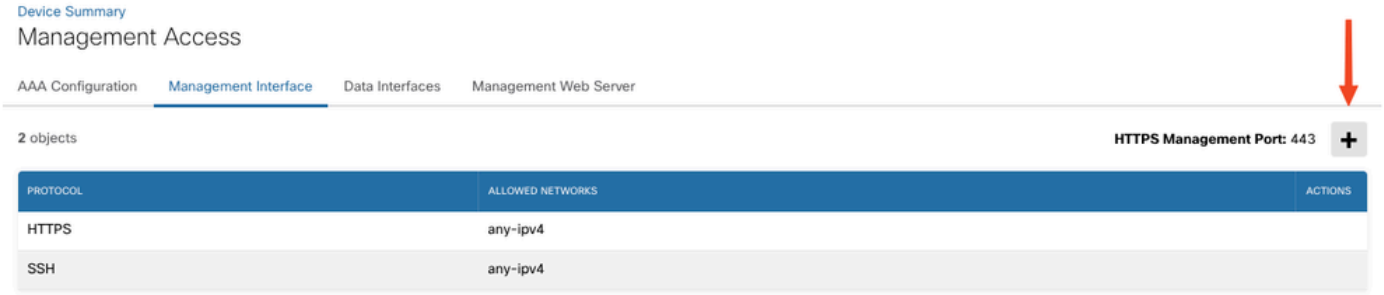
FDM-Schritte:

Schritt 1: Melden Sie sich beim FirePOWER-Gerätemanager (FDM) an, und navigieren Sie zu Systemeinstellungen > Verwaltungszugriff > Verwaltungsschnittstelle .



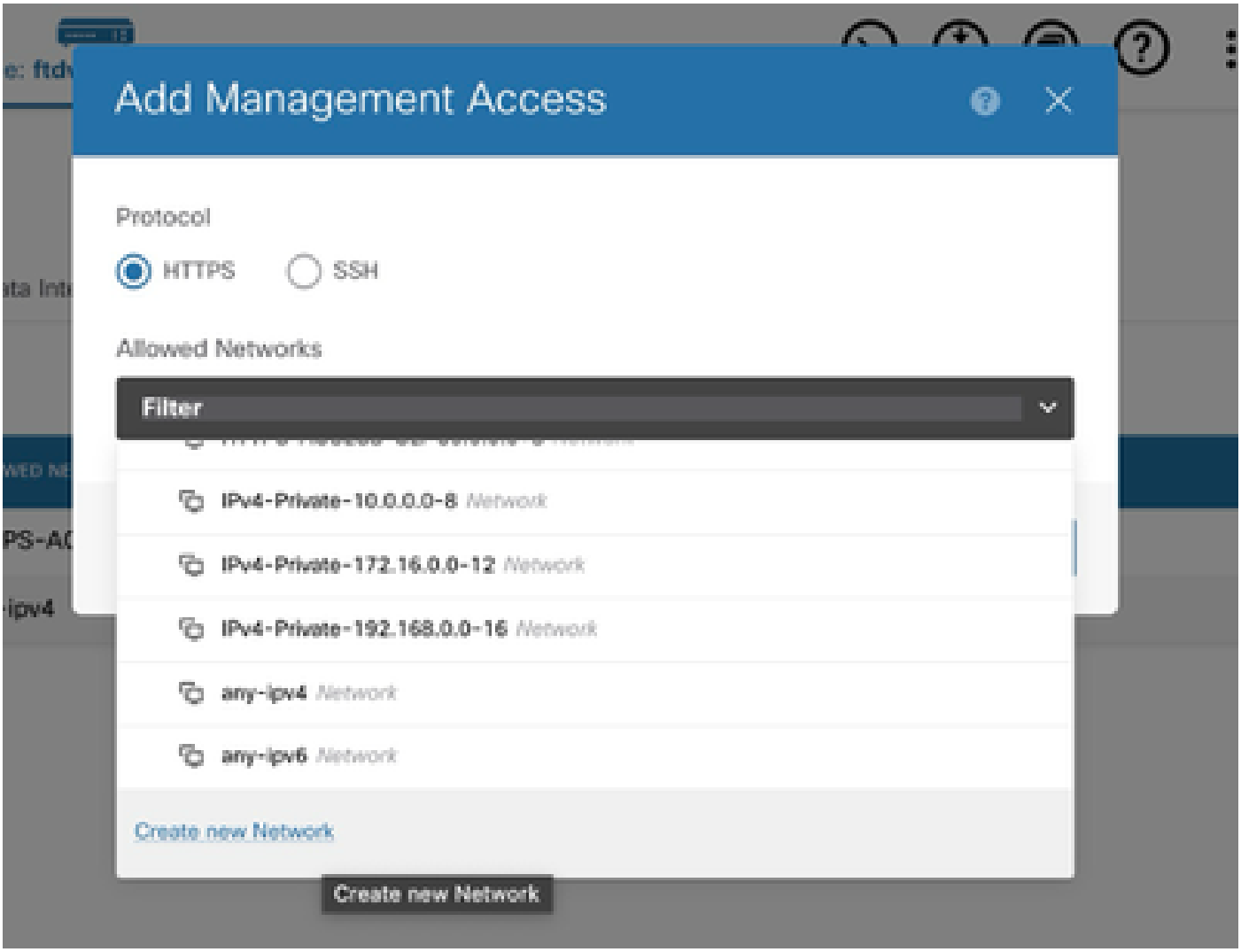
Standardmäßig ist jeder IPv4-Zugriff auf dem Management-Port für SSH und HTTPS zulässig.

Schritt 2: Klicken Sie auf das +-Symbol, um das Fenster zum Hinzufügen des Netzwerks zu öffnen.



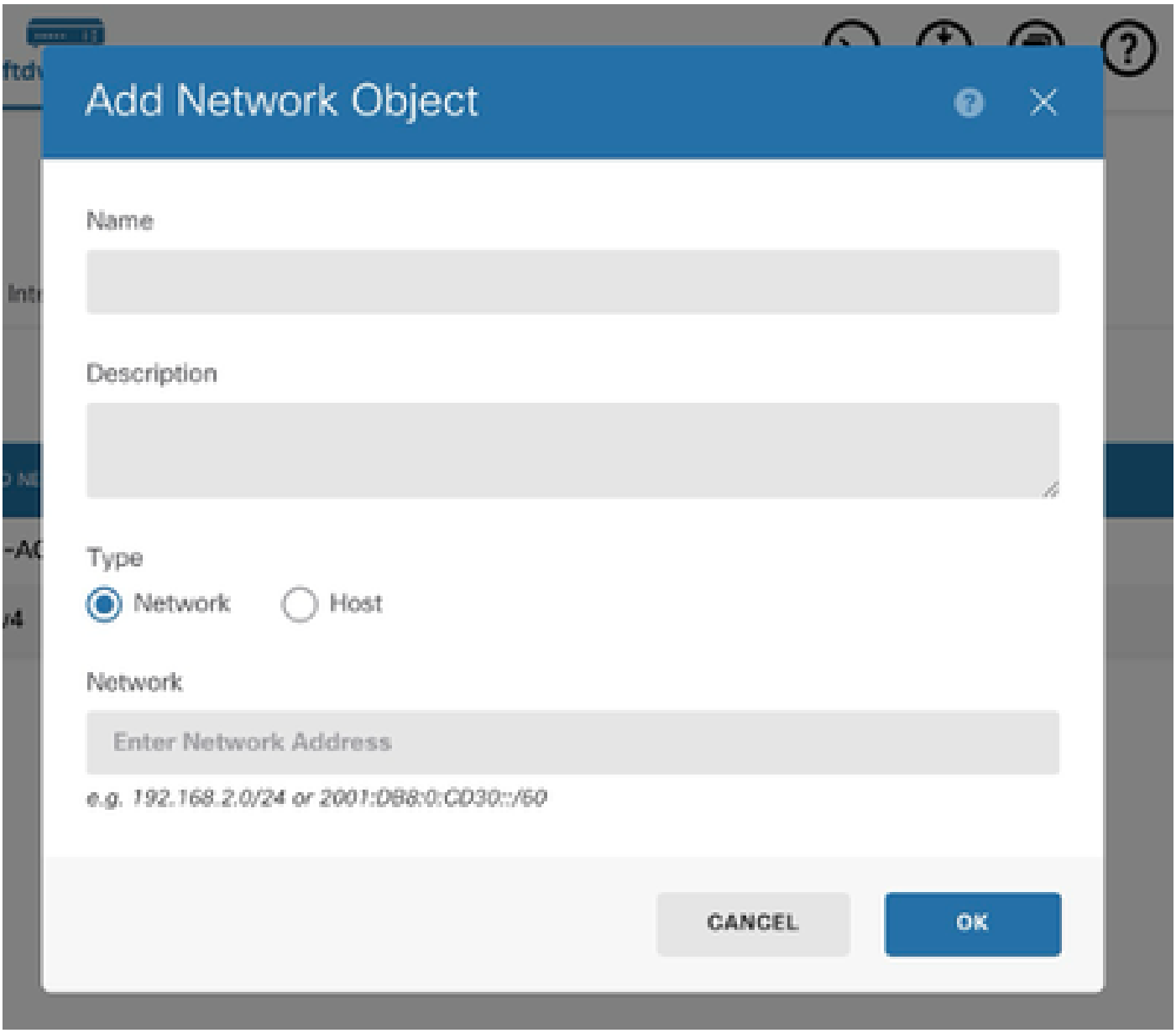
Klicken Sie oben rechts auf die Schaltfläche Hinzufügen.

Schritt 3: Fügen Sie das Netzwerkobjekt hinzu, um SSH- oder HTTPS-Zugriff zu erhalten. Wenn Sie ein neues Netzwerk erstellen müssen, wählen Sie die Option Neues Netzwerk erstellen. Sie können dem Verwaltungszugriff mehrere Einträge für Netzwerke oder Hosts hinzufügen.



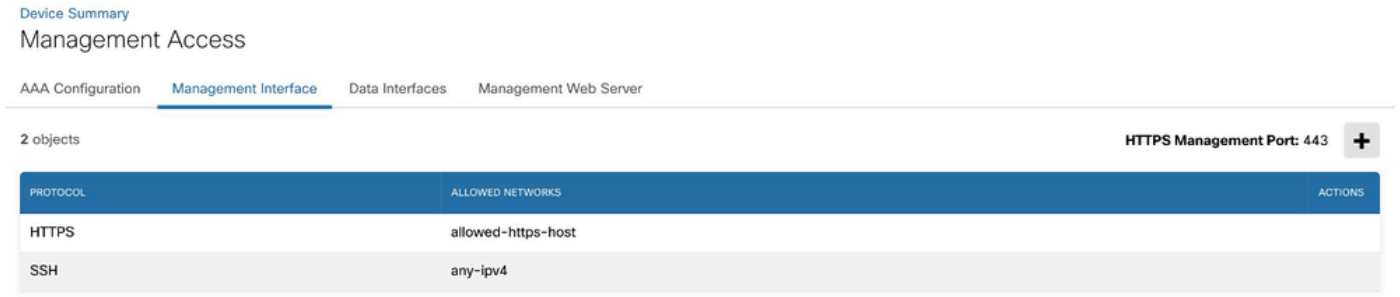
Wählen Sie das Netzwerk aus.

Schritt 4 (optional): Die Option Neues Netzwerk erstellen öffnet das Fenster Netzwerkobjekt hinzufügen.

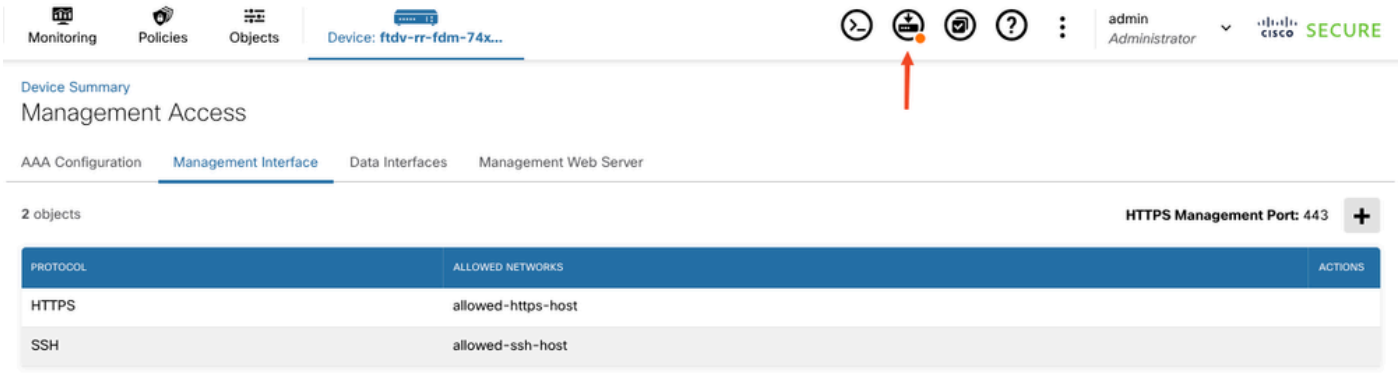


Erstellen Sie ein Netzwerk mit Hosts entsprechend Ihrer Anforderung.

Schritt 5: Überprüfen der vorgenommenen Änderungen und Bereitstellen.

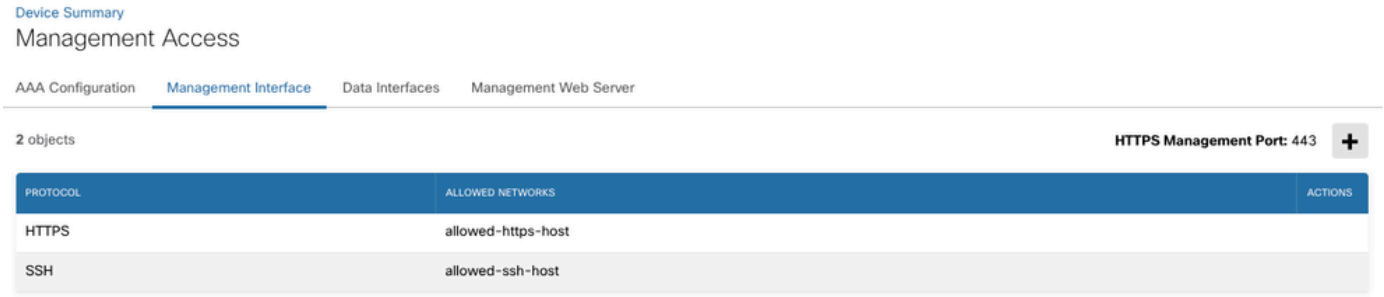


Der HTTPS-Verwaltungszugriff wurde geändert, und any-ipv4 wird entfernt.



Bereitstellung auf FDM

Schritt 6 (optional): Nachdem zuvor für HTTPS durchgeführte Änderungen verifiziert wurden, wiederholen Sie diese für SSH.



Netzwerkobjekt für SSH und HTTPS hinzugefügt.

Schritt 7: Stellen Sie schließlich die Änderungen bereit, und überprüfen Sie Ihren Zugriff auf die FTD vom zugelassenen Netzwerk und Host aus.

Schritte der CLISH:

CLI-Schritte können bei FDM- oder FMC-Management verwendet werden.

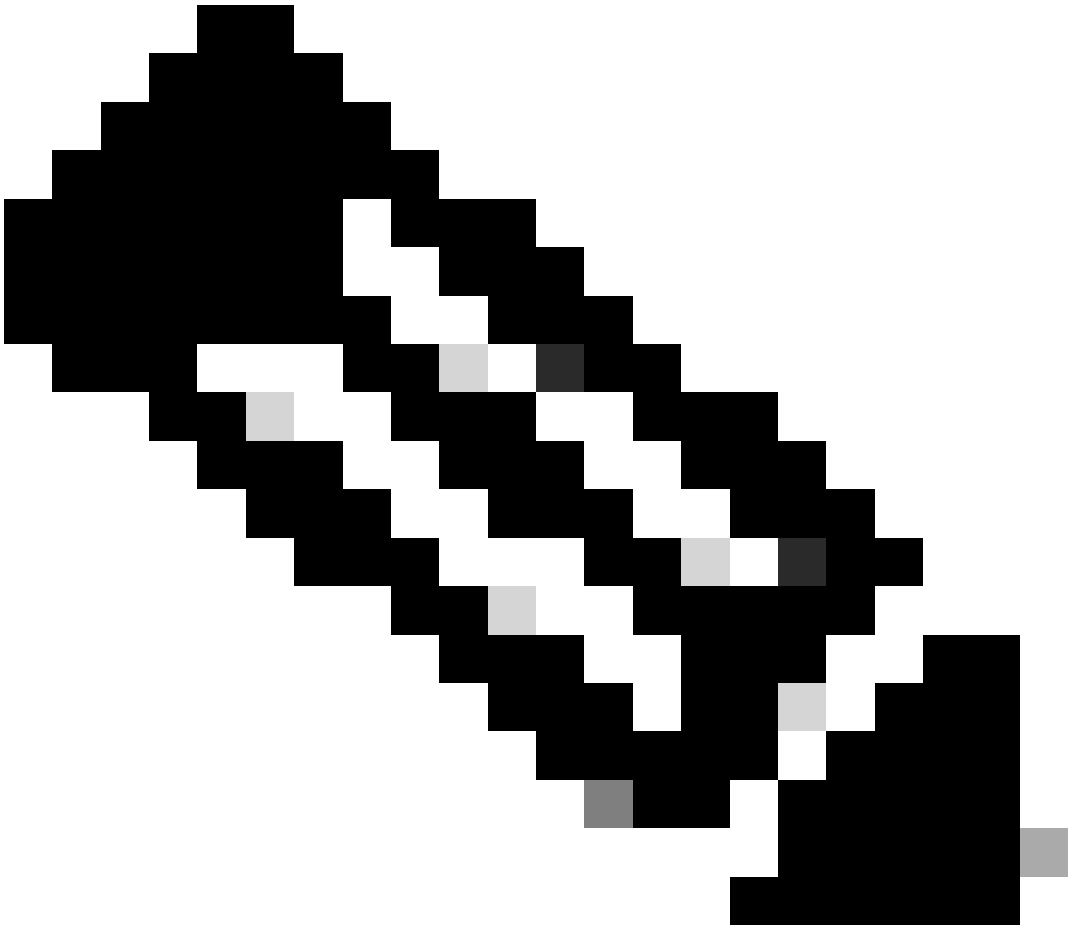
Um das Gerät so zu konfigurieren, dass es HTTPS- oder SSH-Verbindungen von angegebenen IP-Adressen oder Netzwerken akzeptiert, verwenden Sie`configure https-access-list`configure ssh-access-listden Befehl theorcommand.

- Sie müssen alle unterstützten Hosts oder Netzwerke in einem einzigen Befehl einschließen. Die in diesem Befehl angegebenen Adressen überschreiben den aktuellen Inhalt der jeweiligen Zugriffsliste.
- Wenn es sich bei dem Gerät um eine Einheit in einer lokal verwalteten Hochverfügbarkeitsgruppe handelt, werden die Änderungen bei der nächsten Bereitstellung von Konfigurationsaktualisierungen durch die aktive Einheit überschrieben. Wenn es sich hierbei um die aktive Einheit handelt, wird die Änderung während der Bereitstellung an den Peer weitergegeben.

```
> 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
```



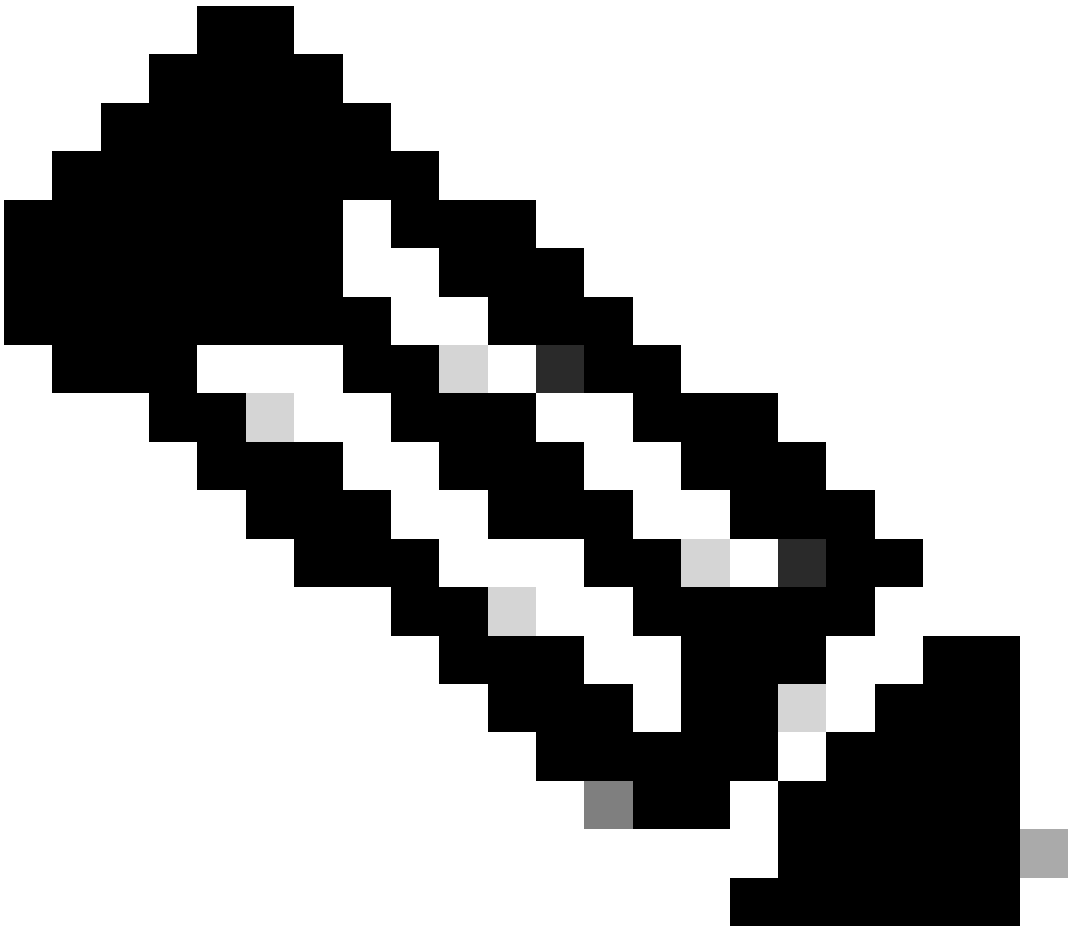
Anmerkung: x.x.x.x/x und y.y.y.y/y repräsentieren eine IPv4-Adresse mit CIDR-Notation.

Ebenso verwenden Sie für SSH-Verbindungen`configure ssh-access-list`den Befehl, wobei ein oder mehrere Befehle getrennt sind.

```
> 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
```



Anmerkung: Sie können Befehle **configure disable-https-access** bzw.configure disable-ssh-accessden HTTPS- oder SSH-Zugriff deaktivieren. Stellen Sie sicher, dass Sie diese Änderungen kennen, da Sie dadurch von der Sitzung ausgeschlossen werden können.

Überprüfung

Um von CLISH aus zu überprüfen, können Sie Befehle verwenden:

```
> 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
```

Referenzen

Cisco Secure Firewall Threat Defense-Befehlsreferenz

Cisco Firepower Threat Defense - Konfigurationsleitfaden für Firepower Device Manager

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.