Configureer beheertoegang voor SSH en HTTPS op FTD via FDM

Inhoud

Inleiding

Dit document beschrijft de procedure om de beheertoegangslijst voor SSH en HTTPS op lokaal of extern beheerde FTD te configureren en te verifiëren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

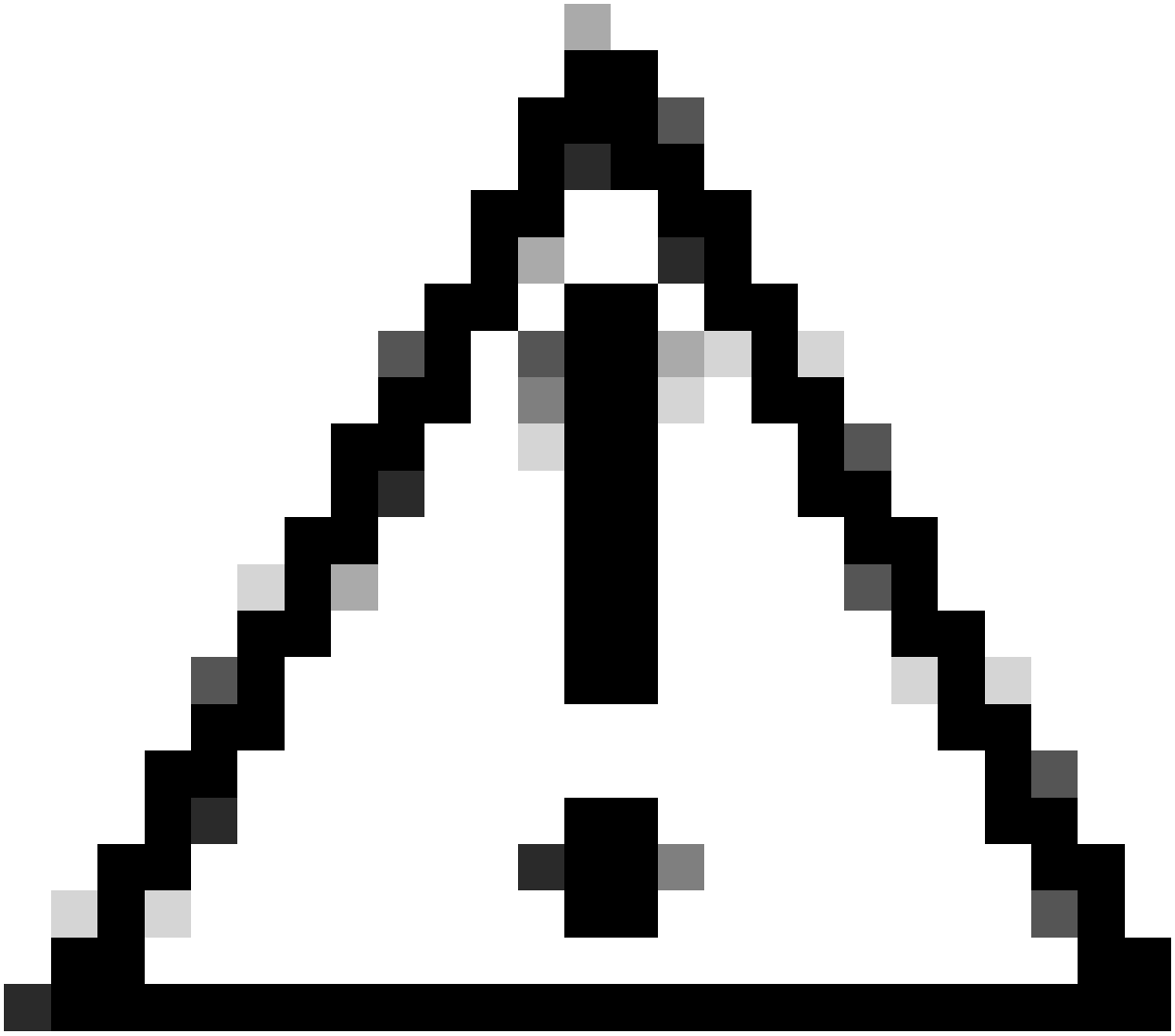
Gebruikte componenten

- Cisco Secure Firewall Threat Defense, versie 7.4.1 uitgevoerd door FDM.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

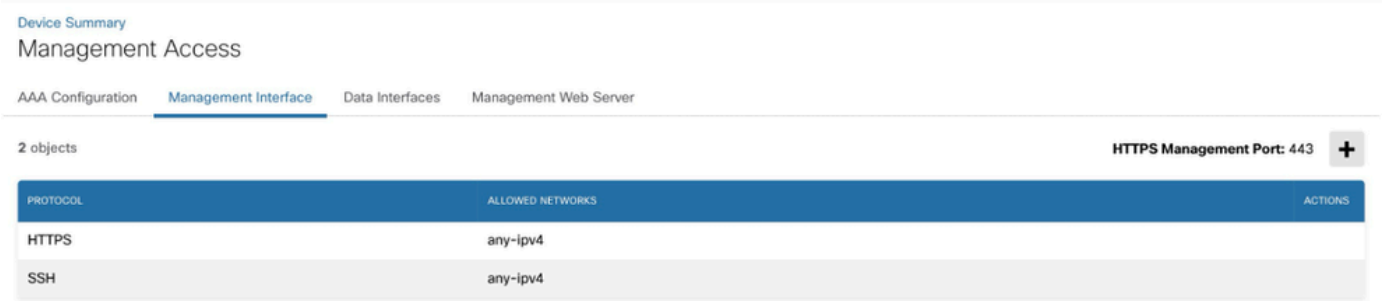
FTD kan lokaal worden beheerd met behulp van FDM of via FMC. In dit document ligt de nadruk op beheertoegang via FDM en CLI. Met CLI kunt u wijzigingen aanbrengen voor zowel FDM als FMC.



Voorzichtig: Configureer SSH- of HTTPS-toegangslijsten één voor één om uitsluiting van sessies te voorkomen. Eerst, update en implementeer één protocol, verifieer toegang, dan ga met andere.

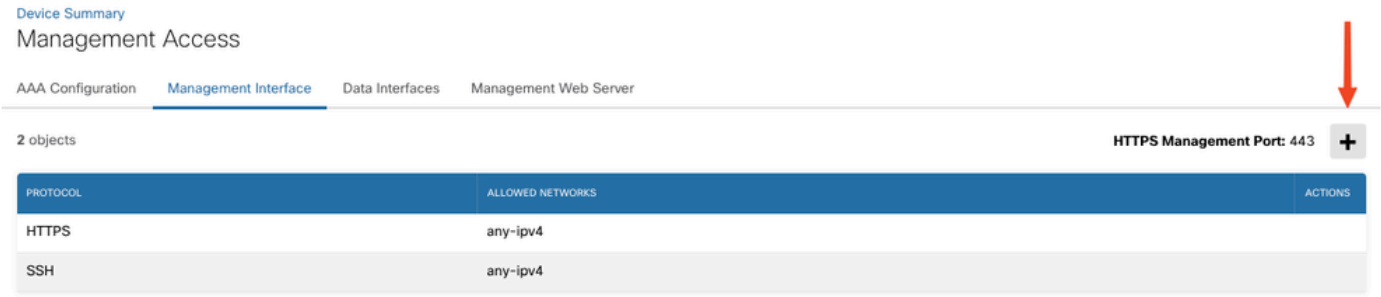
FDM-stappen:

Stap 1: Log in op Firepower Device Manager (FDM) en navigeer naar Systeeminstellingen > Management Access > Management Interface .



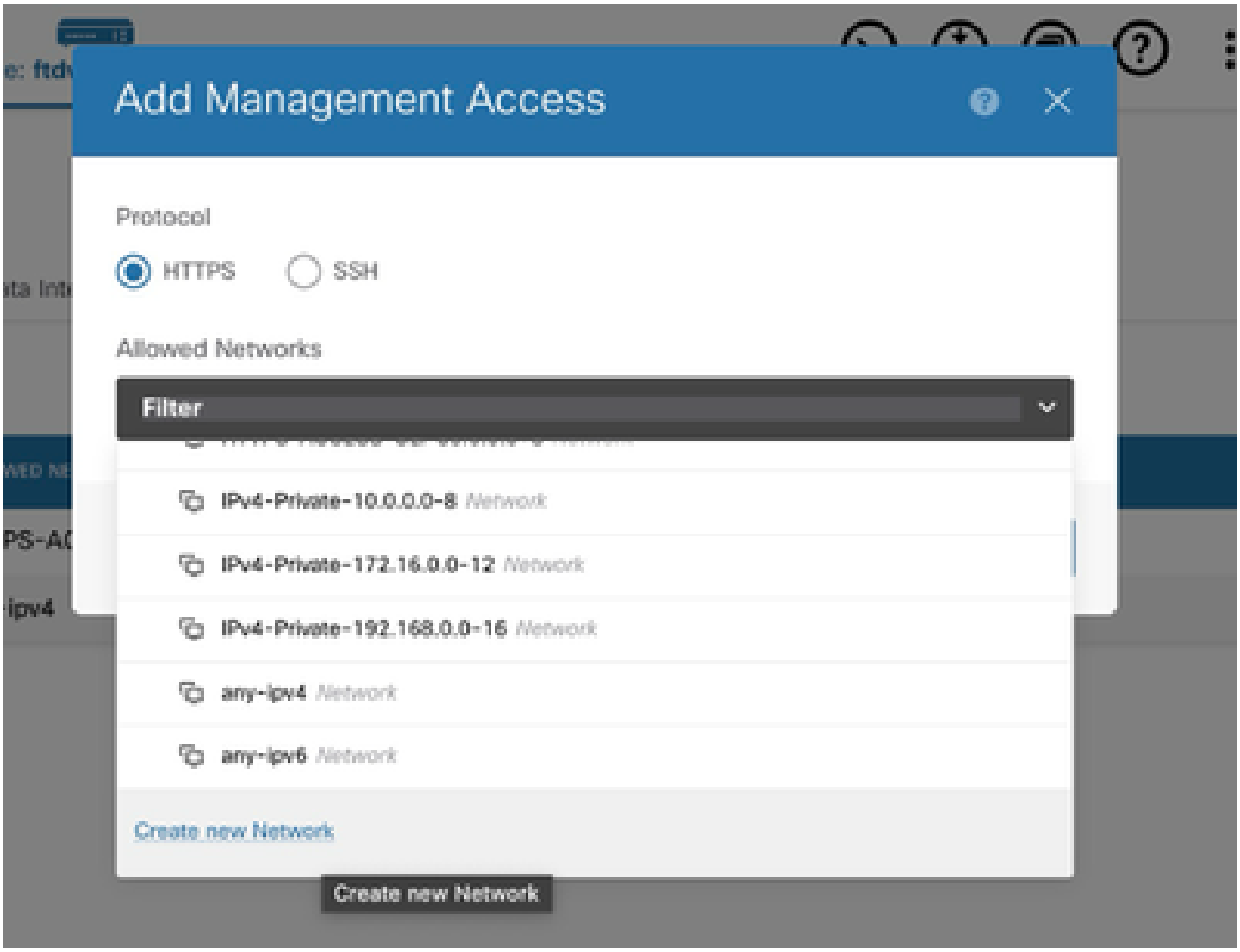
Standaard is elke IPV4-toegang op de beheerpoort voor SSH en HTTPS toegestaan

Stap 2: Klik op het + pictogram om het venster te openen voor het toevoegen van het netwerk.



Klik rechtsboven op de knop Toevoegen.

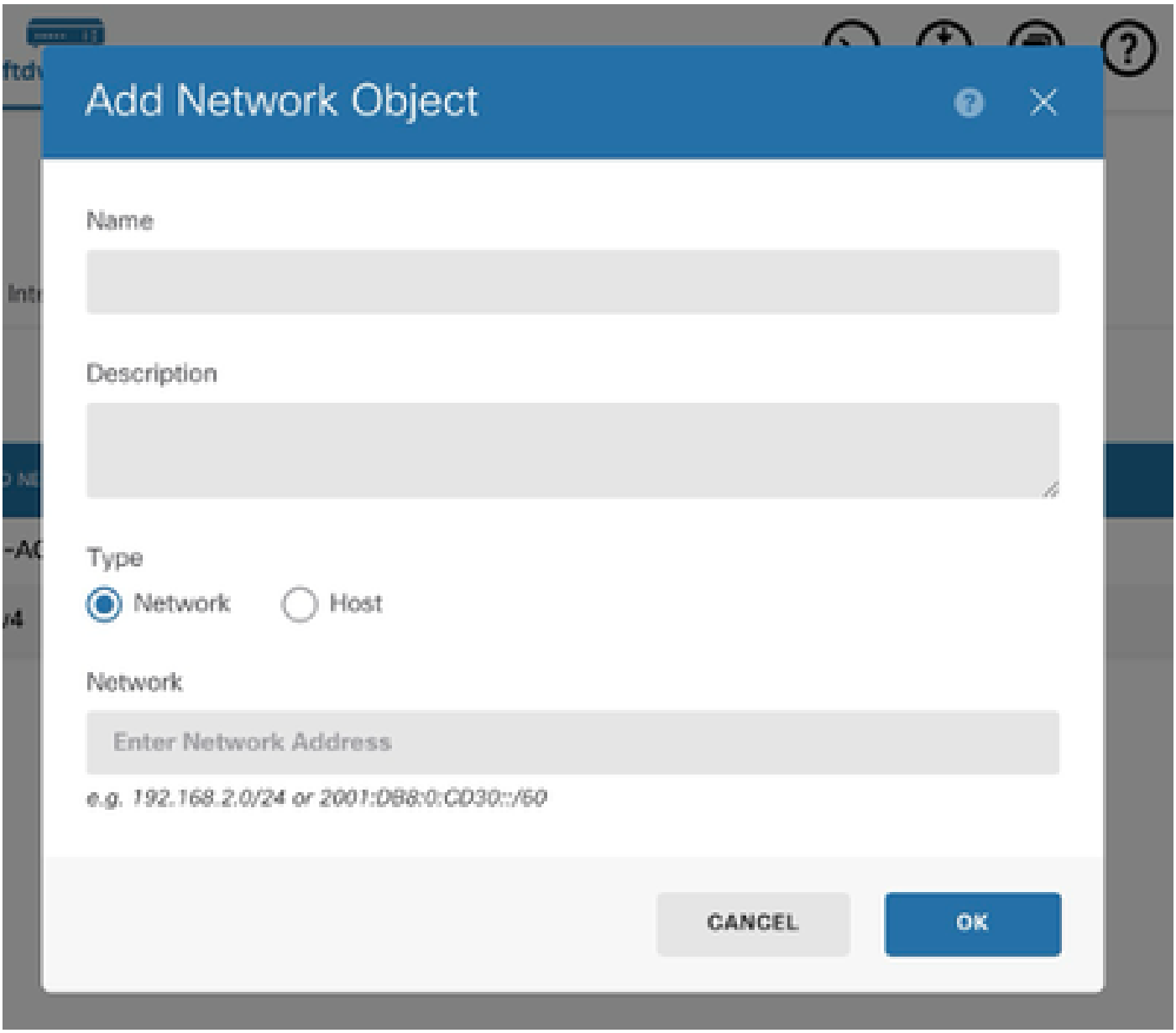
Stap 3: Voeg het netwerkobject toe om SSH- of HTTPS-toegang te hebben. Als u een nieuw netwerk wilt maken, selecteert u de optie Nieuw netwerk maken. U kunt meerdere items toevoegen voor netwerken of host in het beheer.



Selecteer het netwerk.

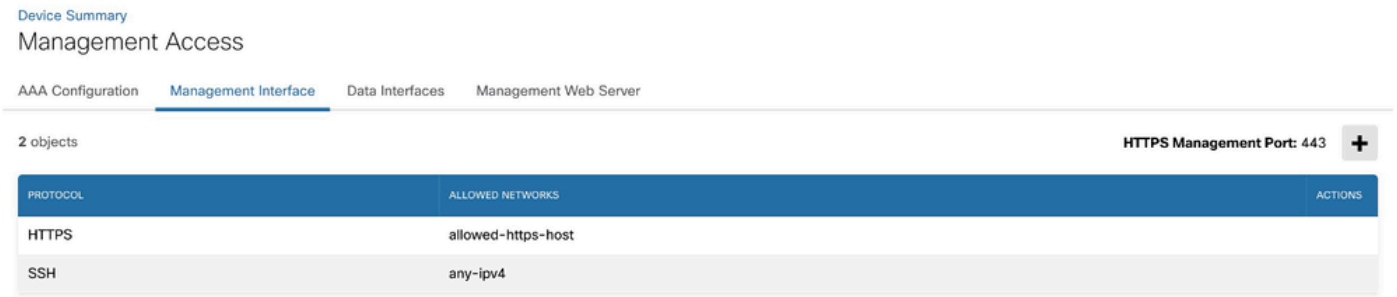
Stap 4 (optioneel): De optie Nieuw netwerk maken wordt geopend in het venster Netwerkobject

toevoegen.

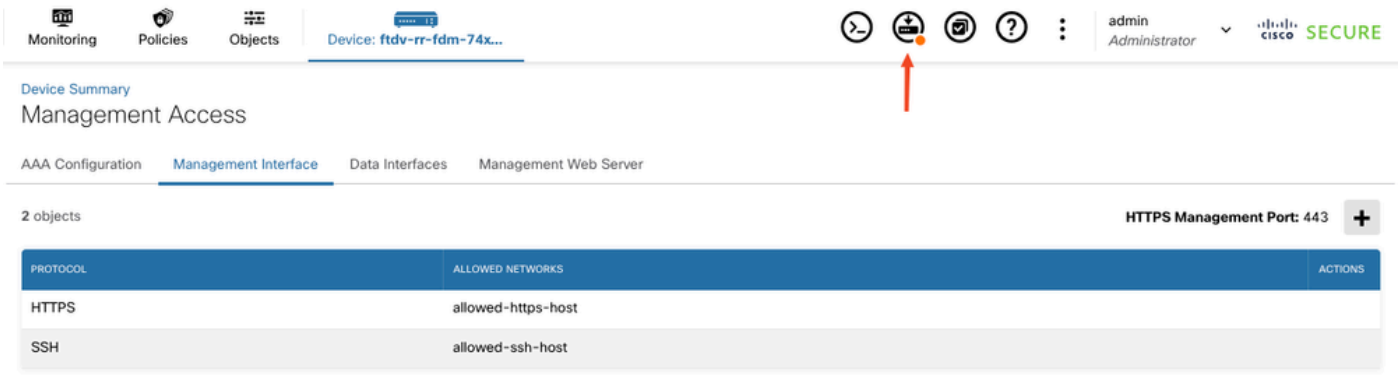


Maak een netwerk van host volgens uw aanvraag.

Stap 5: Controleer de aangebrachte veranderingen en implementeer.

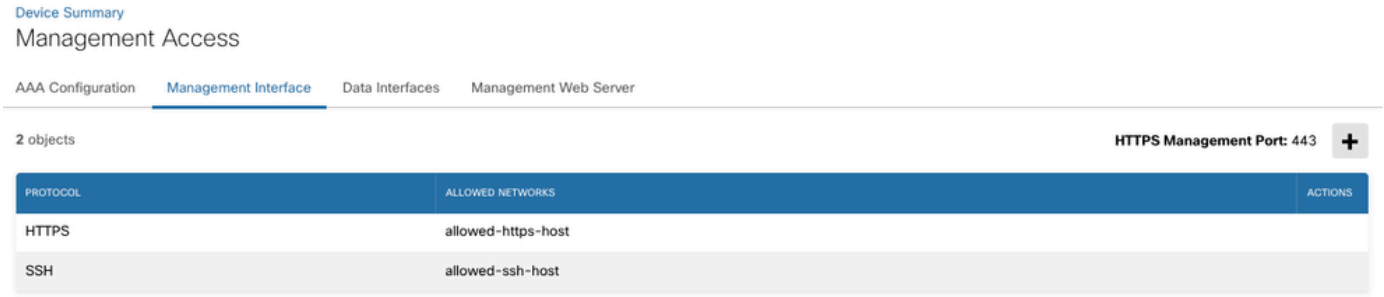


HTTPS-beheertoegang gewijzigd en Any-ipv4 verwijderd.



Implementeren op FDM

Stap 6 (optioneel): Zodra eerder aangebrachte wijzigingen voor HTTPS zijn geverifieerd, herhaalt u hetzelfde voor SSH.



Toegevoegd netwerkobject voor SSH en HTTPS.

Stap 7: Stel tot slot de wijzigingen in en controleer uw toegang tot de FTD vanaf het toegestane netwerk en de host.

CLISH stappen:

CLI-stappen kunnen worden gebruikt in het geval van zowel FDM- als FMC-beheer.

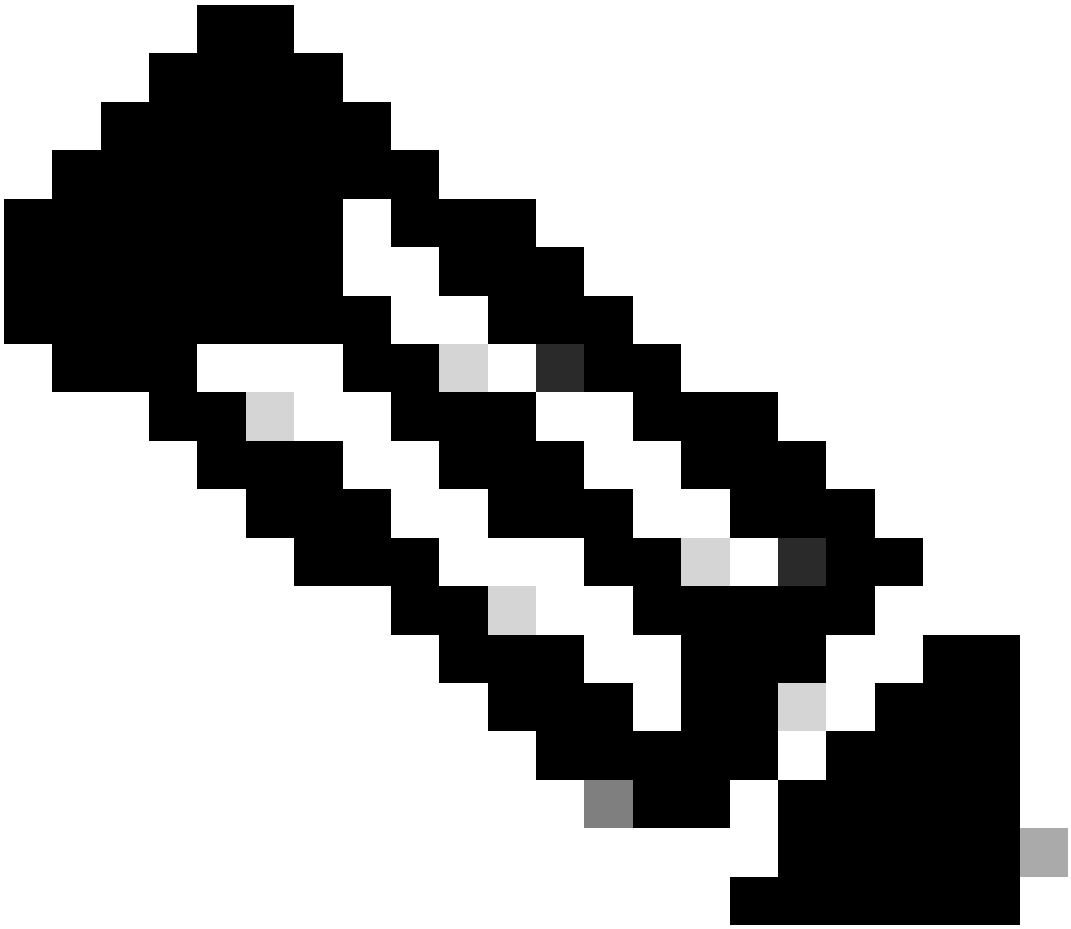
Om het apparaat te configureren om HTTPS- of SSH-verbindingen van gespecificeerde IP-adressen of netwerken te accepteren, gebruikt uconfigure https-access-listconfigure ssh-access-listtheoretisch commando.

- U moet alle ondersteunde hosts of netwerken in één opdracht opnemen. De adressen die in deze opdracht worden gespecificeerd, overschrijven de huidige inhoud van de respectievelijke toegangslijst.
- Als het apparaat een eenheid is in een lokaal beheerde groep met hoge beschikbaarheid, overschrijft uw wijziging de volgende keer dat de actieve eenheid configuratie-updates implementeert. Als dit de actieve eenheid is, wordt de wijziging tijdens de implementatie doorgegeven aan de peer.

```
> 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
```



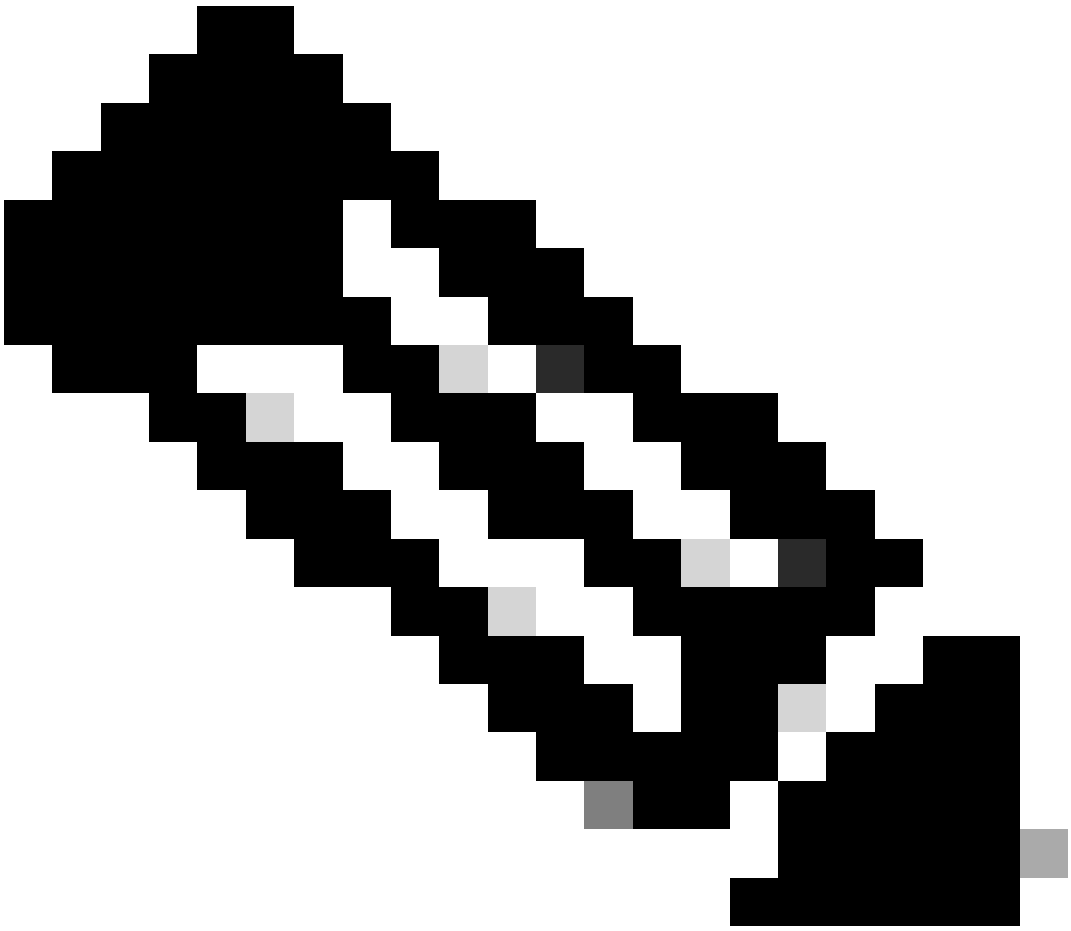
Opmerking: x.x.x.x/x en y.y.y/y vertegenwoordigen ipv4-adres met CIDR-notatie.

Op dezelfde manier voor SSH-verbindingen gebruik`configure ssh-access-list`opdracht met één of meerdere opdracht gescheiden.

```
> 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
```



Opmerking: U kunt opdrachten gebruiken **configure disable-https-access** of HTTPS- of SSH-toegangconfigure disable-ssh-accessuitschakelen. Zorg ervoor dat u zich bewust bent van deze veranderingen, aangezien dit u kan uitsluiten van de sessie.

Verifiëren

Om van CLISH te verifiëren kunt u bevelen gebruiken:

```
> 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
```

Referenties

Naslaghandleiding voor Cisco Secure Firewall Threat Defence

Configuratiehandleiding voor Cisco Firepower Threat Defence voor Firepower Device Manager

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.