

Beheertoegang tot FTD (HTTPS en SSH) configureren via FMC

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Toegang voor beheer instellen](#)

[Stap 1. Configuratie van IP op FTD Interface via FMC GUI.](#)

[Stap 2. Configuratie van externe verificatie.](#)

[Stap 3. Configuratie van SSH-toegang.](#)

[Stap 4. HTTPS-toegang instellen.](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt de configuratie van beheerstoegang tot een Firepower Threat Defense (FTD) (HTTPS en SSH) via FireSIGHT Management Center (FMC) beschreven.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van vuurstechnologie
- Basiskennis van ASA (adaptieve security applicatie)
- Kennis van toegang tot beheer voor ASA via HTTPS en SSH (Secure Shell)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Adaptieve security applicatie (ASA) Firepower Threat Defense Image voor ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X), die werkt op softwareversie 6.0.1 en

hoger.

- ASA Firepower Threat Defense Image voor ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) die op softwareversie 6.0.1 en hoger draait.
- Firepower Management Center (FMC) versie 6.0.1 en hoger.


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.

Achtergrondinformatie

Met het begin van Firepower Threat Defense (FTD) wordt de gehele ASA-gerelateerde configuratie uitgevoerd op GUI.

Op FTD-apparaten die softwareversie 6.0.1 uitvoeren, wordt de ASA diagnostische CLI benaderd terwijl u de **stysteemondersteuning diagnostisch-CLI** ingaat. Op FTD-apparaten die softwareversie 6.1.0 uitvoeren, wordt de CLI geconverteerd en worden alle ASA-opdrachten op de CLISH geconfigureerd.

```
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
```

Om direct toegang tot beheer van een extern netwerk te krijgen, moet u beheerstoegang via HTTPS of SSH configureren. Dit document biedt de configuratie die nodig is om externe toegang tot het beheer te verkrijgen via SSH of HTTPS.

Opmerking: Op FTD-apparaten die softwareversie 6.0.1 gebruiken, kan de CLI niet door een lokale gebruiker worden benaderd, moet een externe verificatie worden geconfigureerd om de gebruikers voor de authenticatie te zorgen. Op FTD-apparaten die softwareversie 6.1.0 uitvoeren, wordt de CLI echter benaderd door de lokale **admin**-gebruiker terwijl een externe authenticatie voor alle andere gebruikers vereist is.

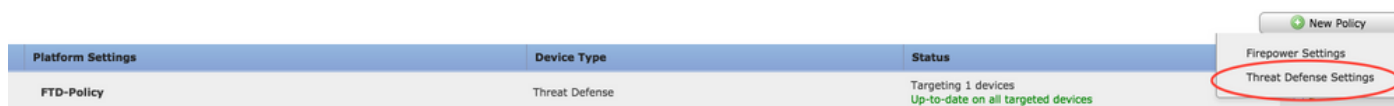
Opmerking: Op FTD-apparaten die softwareversie 6.0.1 uitvoeren, is de diagnostische CLI niet rechtstreeks toegankelijk over de IP die is geconfigureerd voor **br1** van de FTD. Op FTD-apparaten die softwareversie 6.1.0 uitvoeren, is de geconvergeerde CLI toegankelijk over elke interface die is geconfigureerd voor beheertoegang, maar de interface moet worden geconfigureerd met een IP-adres.

Configureren

Alle configuratie met betrekking tot Management Access is ingesteld omdat u naar het tabblad **Platform Settings** in **Devices** navigeert, zoals in de afbeelding:



Bewerk het beleid dat bestaat omdat u op het pictogram van het potlood klikt of maak een nieuw FTD beleid aangezien u op de knop **Nieuw beleid** klikt en selecteer type als **de** instellingen van de **Bedreigingsverdediging**, zoals in de afbeelding getoond:



Selecteer het FTD-apparaat om dit beleid toe te passen en klik op **Opslaan**, zoals in de afbeelding:

New Policy ? X

Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

FTD_HA

Selected Devices

FTD_HA

Toegang voor beheer instellen

Dit zijn de vier belangrijkste stappen die zijn ondernomen om de Management Access te configureren.

Stap 1. Configuratie van IP op FTD Interface via FMC GUI.

Configureer een IP op de interface waarop de FTD via SSH of HTTPS toegankelijk is. Bewerk de interfaces die bestaan terwijl u naar het tabblad **Interfaces** van het FTD navigeert.

Opmerking: Op FTD-apparaten die softwareversie 6.0.1 uitvoeren, is de standaardinstellingen van het beheer interface op de FTD de diagnostische 0/0-interface. Op FTD-apparaten die softwareversie 6.1.0 uitvoeren, ondersteunen alle interfaces echter beheertoegang behalve de diagnostische interface.

Er zijn zes stappen om de diagnostische interface te configureren.

Stap 1. navigeren naar **Apparaat > Apparaatbeheer**.

Stap 2. Selecteer het apparaat of de FTD HA Cluster.

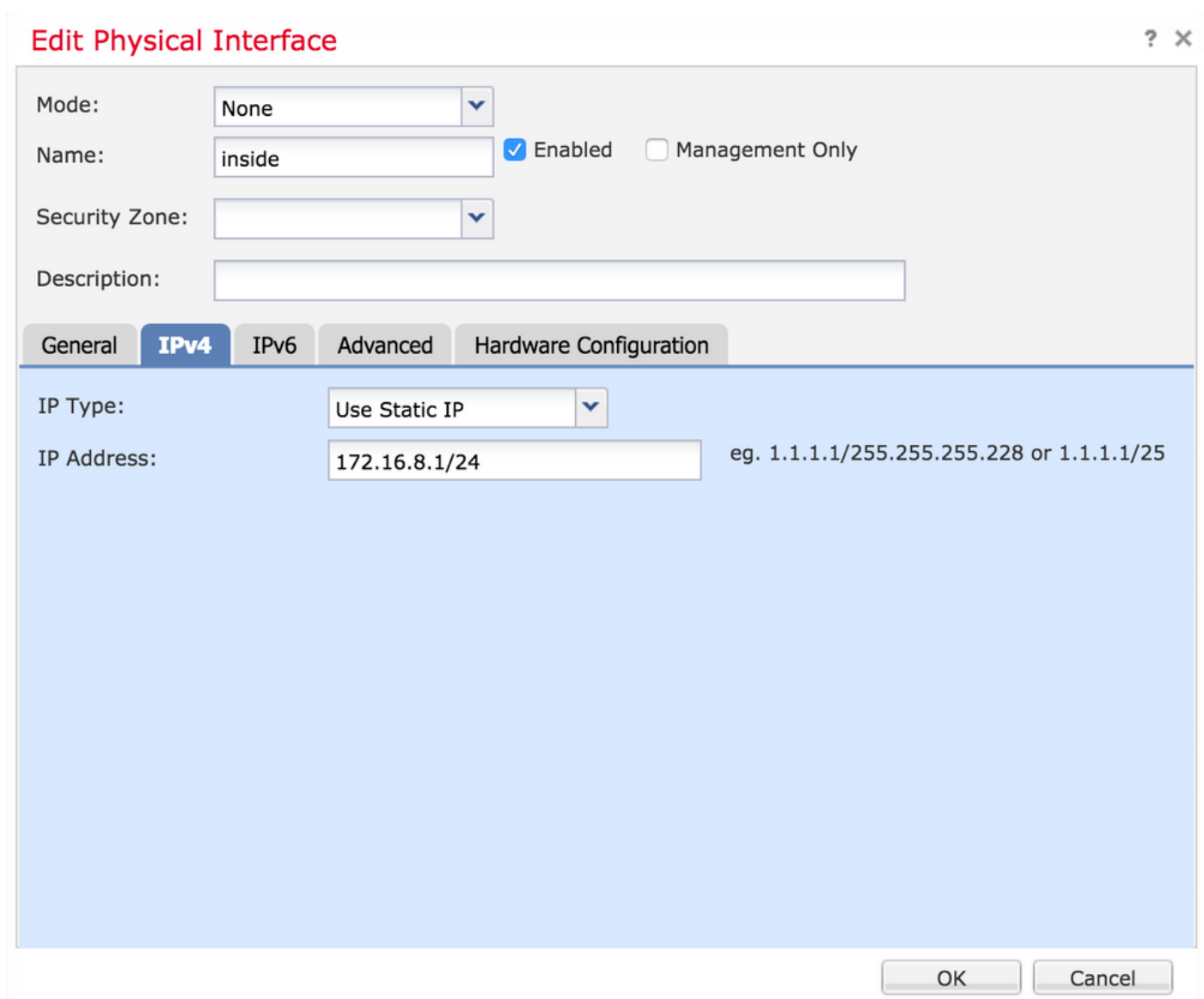
Stap 3. Navigeer naar het tabblad **Interfaces**.

Stap 4. Klik op het **pictogram** pen om de interface te configureren/bewerken om de beheertoegang te verkrijgen, zoals in de afbeelding:



Status	Interface	Logical Name	Type	Interface Objects	MAC Address (Active/Standby)	IP Address
●	GigabitEthernet0/0	transit	Physical			172.16.5.2/30(Static)
●	GigabitEthernet0/1	inside	Physical			172.16.8.1/24(Static)

Stap 5. Selecteer het selectiekader voor **het inschakelen** van de interfaces. Kies het IP-type als **statisch** of **DHCP** aan het tabblad **IP4**. Voer nu een IP-adres voor de interface in en klik op **OK**, zoals in de afbeelding:



Edit Physical Interface ? X

Mode: ▾

Name: Enabled Management Only

Security Zone: ▾

Description:

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: ▾

IP Address: eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25

OK Cancel

Stap 6. Klik op **Save** en voer het beleid vervolgens in op de FTD.

Opmerking: de diagnostische interface kan niet worden gebruikt om toegang te krijgen tot de

geconvergeerde CLI via SSH op apparaten met softwareversie 6.1.0

Stap 2. Configuratie van externe verificatie.

Externe authenticatie vergemakkelijkt de integratie van de FTD in een actieve map of RADIUS-server voor gebruikersverificatie. Dit is een noodzakelijke stap omdat lokaal gevormde gebruikers geen directe toegang tot de diagnostische CLI hebben. De diagnostische CLI en de GUI worden alleen benaderd door gebruikers die echt zijn bevonden via Lichtgewicht Directory Access Protocol (LDAP) of RADIUS.

Er zijn 6 stappen om externe verificatie te configureren.

Stap 1. navigeren naar **Apparaten > Platform-instellingen**.

Stap 2. Bewerk het beleid dat bestaat omdat u op het pictogram van het potlood klikt of maak een nieuw FTD beleid aangezien u op de knop **Nieuw beleid** klikt en type als u selecteert **Instellingen bedreigingsverdediging**

Stap 3. navigeren naar het tabblad **Externe verificatie**, zoals in de afbeelding:



Stap 4. Aangezien u op **Add** klikt, verschijnt een dialoogvenster zoals in de afbeelding:

- **Schakel in voor HTTP** - Schakel deze optie in om toegang tot de FTD over HTTPS te bieden.
- **Inschakelen voor SSH** - Schakel deze optie in om toegang tot de FTD via SSH te bieden.
- **Naam** - Voer de naam in voor de LDAP-verbinding.
- **Beschrijving** - Voer een optionele beschrijving in voor het externe verificatieobject.
- **IP-adres** - Voer een netwerkobject in dat het IP van de externe verificatieserver opslaat. Als er geen netwerkobject is geconfigureerd maakt u een nieuw object. Klik op het pictogram (+).
- **Verificatiemethode**-Selecteer RADIUS- of LDAP-protocol voor verificatie.

- **Schakel SSL**-Schakel deze optie in om het verificatieverkeer te versleutelen.
- **Type server**: selecteer het type server. De bekende servertypen zijn MS Active Directory, Sun, OpenLDAP en Novell. Standaard wordt de optie ingesteld om het servertype automatisch te detecteren.
- **Port**- Voer de poort in waarop de authenticatie plaatsvindt.
- **Time-out** - Voer een tijdelijke waarde in voor de verificatieverzoeken.
- **Base DN** - Voer een basisDN in om een bereik te verstrekken waarbinnen de gebruiker aanwezig kan zijn.
- **LDAP Toepassingsgebied** - Selecteer het te bekijken LDAP-bereik. Het toepassingsgebied is binnen hetzelfde niveau of om binnen de subboom te kijken.
- **Gebruikersnaam** - Voer een gebruikersnaam in om te binden aan de LDAP folder.
- **Verificatiewachtwoord**-Voer het wachtwoord voor deze gebruiker in.
- **Bevestig** - voer het wachtwoord opnieuw in.
- **Beschikbare interfaces** - Er wordt een lijst weergegeven van beschikbare interfaces op de FTD.
- **Geselecteerde zones en interfaces** - Dit toont een lijst van interfaces waarvan de authenticatieserver wordt benaderd.

Voor RADIUS-verificatie is er geen server-type Base DN- of LDAP-bereik. De poort is de RADIUS-poort 1645.

Geheime - Voer de geheime sleutel in voor RADIUS.

Add External Authentication



Enable for HTTP

Enable for SSH

Name*

Description

IP Address*

Authentication Method

Enable SSL

Server Type

Port

Timeout (0 - 300 Seconds)

Base DN ex. dc=cisco,dc=com

Ldap Scope

Username ex. cn=jsmith,dc=cisco,dc=com

Authentication Password

Confirm

Available Zones

Selected Zones/Interfaces

Stap 5. Klik op **OK** als de configuratie is voltooid.

Stap 6 . Bewaar het beleid en implementeer het in het Firepower Threat Defense-apparaat.

Opmerking: Externe verificatie kan niet worden gebruikt voor toegang tot de geconvergeerde CLI via SSH op apparaten met softwareversie 6.1.0

Stap 3. Configuratie van SSH-toegang.

SSH verleent directe toegang tot de geconvergeerde CLI. Gebruik deze optie om direct toegang te hebben tot de CLI en debug-opdrachten uit te voeren. In deze sectie wordt beschreven hoe u SSH moet configureren om toegang te krijgen tot de FTD CLI.

Opmerking: Op FTD-apparaten die softwareversie 6.0.1 uitvoeren, geeft de SSH-configuratie op Platform-instellingen rechtstreeks toegang tot de diagnostische CLI en niet tot de CLISH. U moet verbinding maken met het IP-adres dat ingesteld is op **br1** om toegang te krijgen tot de CLISH. Op FTD-apparaten die softwareversie 6.1.0 uitvoeren, navigeren alle interfaces naar de geconvergeerde CLI wanneer benaderd via SSH

Er zijn 6 stappen om SSH te configureren op de ASA

Uitsluitend op 6.0.1-inrichtingen:

Deze stappen worden uitgevoerd op FTD-apparaten met softwareversie onder 6.1.0 en groter dan 6.0.1. Op 6.1.0-apparaten worden deze parameters geërfd van het besturingssysteem.

Stap 1. navigeren naar **Apparaten>Platform-instellingen**.

Stap 2. Bewerk het beleid dat bestaat terwijl u op het pictogram van het potlood klikt of maak een nieuw beleid van de Bedreigingsdefensie van de Firepower aangezien u op de knop **Nieuw Beleid** klikt en type als **Instellingen van de Bedreigingsverdediging** selecteert.

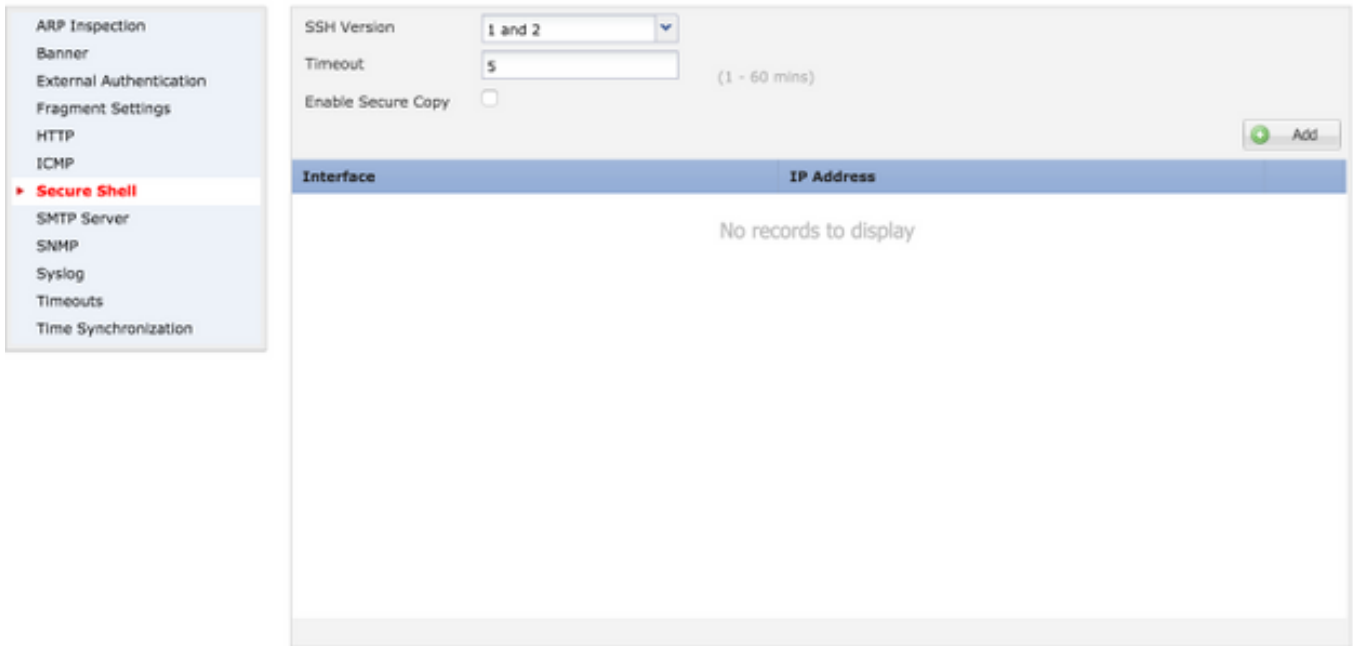
Stap 3. Navigeer naar het gedeelte **Secure Shell**. Er verschijnt een pagina, zoals in de afbeelding:

SSH-versie: Selecteer de SSH-versie om de ASA-toets in te schakelen. Er zijn drie opties:

- **1:** Alleen SSH versie 1 inschakelen
- **2:** Alleen SSH versie 2 inschakelen
- **1 en 2:** Schakel zowel SSH versie 1 als 2 in

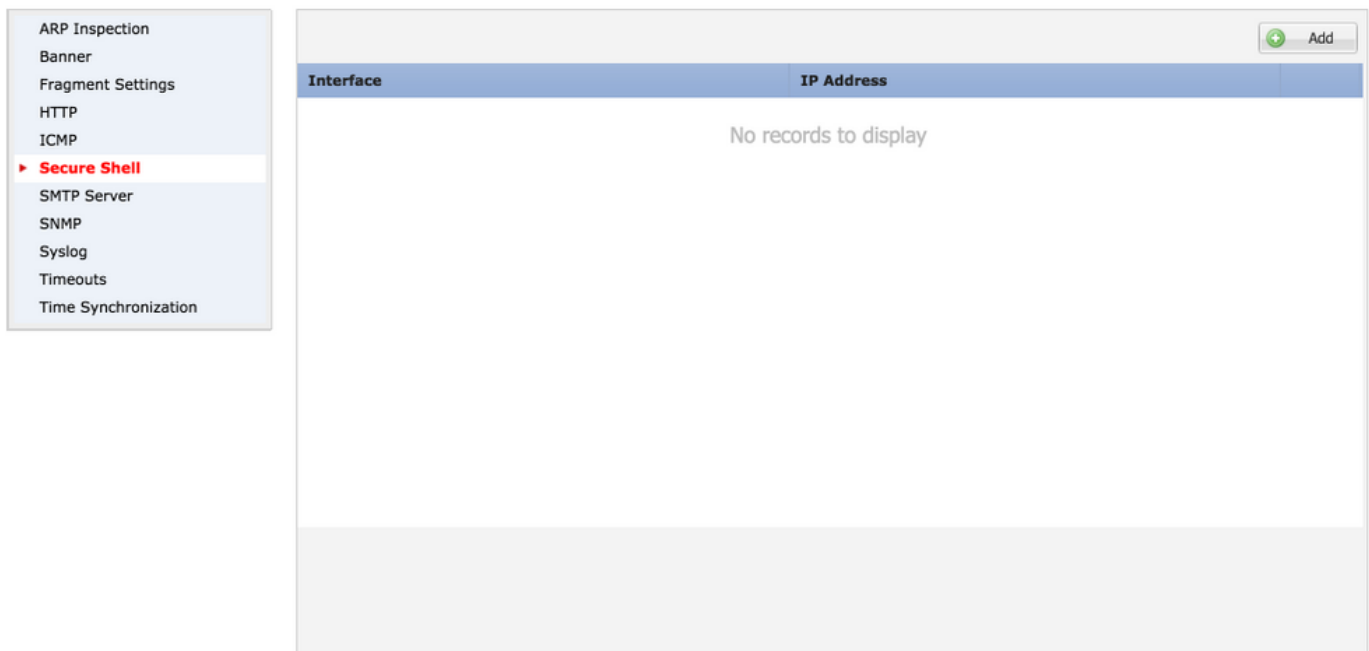
Time-out: Voer de gewenste SSH-tijd in enkele minuten in.

Schakel Secure Kopie in - Schakel deze optie in om het apparaat te configureren zodat Secure Copy (SCP)-verbindingen mogelijk worden en fungeer als een SCP-server.



Op 6.0.1- en 6.1.0-inrichtingen:

Deze stappen worden geconfigureerd om de beheertoegang via SSH te beperken tot specifieke interfaces en tot specifieke IP-adressen.



Stap 1. Klik op **Add** en stel deze opties in:

IP-adres: Selecteer een netwerkobject dat de subnetten bevat die CLI via SSH mogen gebruiken. Als een netwerk object niet aanwezig is, maak er een als u op het (+) pictogram klikt.

Geselecteerde gebieden/interfaces: Selecteer de zones of interfaces waarvan de SSH-server toegang heeft.

Stap 2. Klik op **OK**, zoals in de afbeelding:

Edit Secure Shell Configuration



IP Address*

Available Zones

Selected Zones/Interfaces

outside

Configuratie voor SSH wordt gezien in de geconvergeerde CLI (ASA Diagnostic CLI in 6.0.1-apparaten) met gebruik van deze opdracht.

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

Stap 3. Zodra de SSH-configuratie is uitgevoerd, klikt u op **Opslaan** en vervolgens implementeert u het beleid in de FTD.

Stap 4. HTTPS-toegang instellen.

Om HTTPS toegang tot één of meer interfaces mogelijk te maken, navigeer naar de **HTTP** sectie in platform instellingen. HTTPS-toegang is specifiek nuttig om de pakketvastlegging van de diagnostische veilige web interface rechtstreeks voor de analyse te downloaden.

Er zijn 6 stappen om HTTPS-toegang te configureren.

Stap 1. Navigatie naar **apparaten > Platform-instellingen**

Stap 2. Bewerk het beleid voor platform instellingen dat bestaat omdat u op het **potlood pictogram** naast het beleid klikt of maak een nieuw FTD beleid aangezien u op **Nieuw beleid** klikt. Selecteer het type als **Firepower Threat Defense**.

Stap 3. Aangezien u naar de **HTTP**-sectie navigeert, verschijnt een pagina zoals in de afbeelding.

HTTP-server inschakelen: Schakel deze optie in om HTTP-server op de FTD in te schakelen.

Port: Selecteer de poort waarop de FTD beheerverbindingen accepteert.

FTD-Policy

Enter a description

The screenshot shows the configuration interface for the HTTP server. On the left is a navigation menu with the following items: ARP Inspection, Banner, External Authentication, Fragment Settings, **HTTP** (highlighted), ICMP, Secure Shell, SMTP Server, SNMP, Syslog, Timeouts, and Time Synchronization. The main configuration area has a header 'Enable HTTP Server' with a checked checkbox. Below it is a 'Port' field containing the value '443', with a note '(Please don't use 80 or 1443)'. An 'Add' button is located in the top right corner. Below the configuration fields is a table with two columns: 'Interface' and 'Network'. The table is currently empty, displaying the message 'No records to display'.

Stap 4. Klik op **Add** en pagina zoals in de afbeelding:

IP-adres - Voer de subnetten in die HTTPS-toegang tot de diagnostische interface mogen hebben. Als er geen netwerkobject is, maak er een en gebruik de optie (+).

Geselecteerde zones/interfaces - vergelijkbaar met SSH, moet voor HTTPS-configuratie een interface worden ingesteld waarop deze via HTTPS toegankelijk is. Selecteer de zones of interface waarover de FTD toegankelijk moet zijn via HTTPS.

Edit HTTP Configuration



IP Address* 10.0.0.0_16

Available Zones

Selected Zones/Interfaces

outside

Add

Interface Name Add

OK Cancel

Configuratie voor HTTPS wordt bekeken in de geconvergeerde CLI (ASA Diagnostic CLI in 6.0.1-apparaten) en gebruikt deze opdracht.

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

Stap 5. Zodra de gewenste configuratie is uitgevoerd, selecteert u **OK**.

Stap 6. Nadat alle vereiste informatie is ingevoerd, klikt u op **Opslaan** en stelt u het beleid in op het apparaat.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Dit zijn de basisstappen naar een probleem met de toegang tot probleemoplossing in de FTD.

Stap 1. Zorg ervoor dat de interface is ingeschakeld en met een IP-adres is ingesteld.

Stap 2. Zorg ervoor dat een externe verificatie werkt zoals deze is geconfigureerd en dat deze bereikbaar is via de juiste interface die is gespecificeerd in het gedeelte **Externe verificatie** van de **Platform-instellingen**.

Stap 3. Zorg ervoor dat de routing op de FTD juist is. In FTD softwareversie 6.0.1, navigeer naar **stysteemondersteuning diagnostische-cli**. Start de opdrachten **voor route** en **tonen routebeheer-only** om respectievelijk de routes voor de FTD en de beheerinterfaces te zien.

In FTD softwareversie 6.1.0 voert u de opdrachten rechtstreeks uit in de geconvergeerde CLI.

Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems](#)