

Konfigurieren des Managementzugriffs auf FTD (HTTPS und SSH) über FMC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfigurieren des Managementzugriffs](#)

[Schritt 1: Konfigurieren der IP-Adresse auf der FTD-Schnittstelle über die FMC-GUI](#)

[Schritt 2: Konfigurieren Sie die externe Authentifizierung.](#)

[Schritt 3: Konfigurieren des SSH-Zugriffs](#)

[Schritt 4: Konfigurieren des HTTPS-Zugriffs](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt die Konfiguration des Managementzugriffs auf eine FirePOWER Threat Defense (FTD) (HTTPS und SSH) über das FireSIGHT Management Center (FMC).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse der FirePOWER-Technologie
- Grundkenntnisse der ASA (Adaptive Security Appliance)
- Kenntnisse des Managementzugriffs auf ASA über HTTPS und SSH (Secure Shell)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Adaptive Security Appliance (ASA) Firepower Threat Defense Image für ASA (5506X/5506H-

- X/5506W-X, ASA 5508-X, ASA 5516-X), ausgeführt auf der Softwareversion 6.0.1 und höher.
- ASA FirePOWER Threat Defense-Image für ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X, ASA 5585-X), das auf der Softwareversion 6.0.1 und höher ausgeführt wird.
- FirePOWER Management Center (FMC) ab Version 6.0.1


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 verstehen.

Hintergrundinformationen

Mit Beginn von FirePOWER Threat Defense (FTD) erfolgt die gesamte ASA-bezogene Konfiguration über die Benutzeroberfläche.

Auf FTD-Geräten, auf denen die Software Version 6.0.1 ausgeführt wird, wird auf die ASA-Diagnose-CLI zugegriffen, sobald Sie die **DiagnoseCLI** für **den Systemsupport** eingeben. Auf FTD-Geräten, auf denen die Software Version 6.1.0 ausgeführt wird, ist jedoch die CLI konvergiert, und die gesamten ASA-Befehle werden auf der CLISH konfiguriert.

```
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
```

Um den Managementzugriff direkt von einem externen Netzwerk aus zu erhalten, müssen Sie den Managementzugriff über HTTPS oder SSH konfigurieren. Dieses Dokument enthält die erforderliche Konfiguration für den externen Zugriff auf das Management über SSH oder HTTPS.

Anmerkung: Auf FTD-Geräten, auf denen die Software Version 6.0.1 ausgeführt wird, kann von einem lokalen Benutzer nicht auf die CLI zugegriffen werden. Zur Authentifizierung der Benutzer muss eine externe Authentifizierung konfiguriert werden. Auf FTD-Geräten, auf denen die Software Version 6.1.0 ausgeführt wird, wird jedoch vom lokalen **Admin**-Benutzer auf die CLI zugegriffen, während für alle anderen Benutzer eine externe Authentifizierung erforderlich ist.

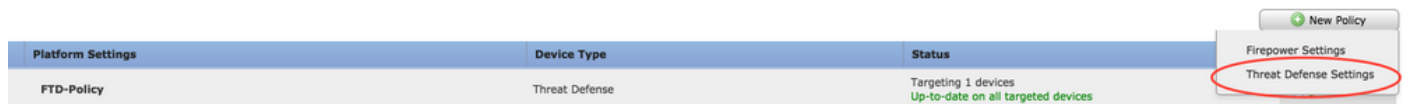
Anmerkung: Auf FTD-Geräten, auf denen die Software Version 6.0.1 ausgeführt wird, ist der direkte Zugriff auf die Diagnose-CLI nicht über die IP möglich, die für **br1** der FTD konfiguriert ist. Auf FTD-Geräten, auf denen die Software Version 6.1.0 ausgeführt wird, ist der Zugriff auf die konvergente CLI jedoch über jede Schnittstelle möglich, die für den Managementzugriff konfiguriert wurde. Die Schnittstelle muss jedoch mit einer IP-Adresse konfiguriert werden.

Konfigurieren

Die Konfiguration der gesamten Konfiguration für den Managementzugriff wird konfiguriert, wenn Sie zur Registerkarte **Plattformeinstellungen** unter **Geräte** navigieren, wie im Bild gezeigt:



Bearbeiten Sie entweder die vorhandene Richtlinie, indem Sie auf das Bleistiftsymbol klicken, oder erstellen Sie eine neue FTD-Richtlinie, während Sie auf die Schaltfläche **Neue Richtlinie** klicken und als **Threat Defense Settings** auswählen, wie im Bild gezeigt:



Wählen Sie die FTD-Appliance aus, um diese Richtlinie anzuwenden, und klicken Sie auf **Speichern**, wie im Bild gezeigt:

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

Konfigurieren des Managementzugriffs

Dies sind die vier wichtigsten Schritte zur Konfiguration des Management-Zugriffs.

Schritt 1: Konfigurieren der IP-Adresse auf der FTD-Schnittstelle über die FMC-GUI

Konfigurieren Sie eine IP-Adresse auf der Schnittstelle, über die der FTD über SSH oder HTTPS erreichbar ist. Bearbeiten Sie die vorhandenen Schnittstellen, während Sie zur Registerkarte **Schnittstellen** des FTD navigieren.

Anmerkung: Auf FTD-Geräten, auf denen die Software Version 6.0.1 ausgeführt wird, ist die Standard-Verwaltungsschnittstelle auf dem FTD die diagnostische0/0-Schnittstelle. Auf FTD-Geräten, auf denen die Software Version 6.1.0 ausgeführt wird, unterstützen alle Schnittstellen jedoch den Verwaltungszugriff mit Ausnahme der Diagnoseschnittstelle.

Die Diagnoseschnittstelle kann in sechs Schritten konfiguriert werden.

Schritt 1: Navigieren zu **Gerät > Gerätemanagement**.

Schritt 2: Wählen Sie das Gerät oder den FTD HA-Cluster aus.

Schritt 3: Navigieren Sie zur Registerkarte **Schnittstellen**.

Schritt 4: Klicken Sie auf das **Bleistiftsymbol**, um die Schnittstelle zu konfigurieren/zu bearbeiten, um den Verwaltungszugriff zu erhalten, wie im Bild gezeigt:

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)

Schritt 5: Aktivieren Sie das Kontrollkästchen **aktivieren**, um die Schnittstellen zu aktivieren. Navigieren Sie zur Registerkarte **Ipv4**, und wählen Sie den IP-Typ als **statisch oder DHCP** aus. Geben Sie nun eine IP-Adresse für die Schnittstelle ein, und klicken Sie auf **OK**, wie im Bild gezeigt:

Edit Physical Interface

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

Schritt 6: Klicken Sie auf **Speichern** und stellen Sie die Richtlinie dann im FTD bereit.

Hinweis: Die Diagnoseschnittstelle kann nicht für den Zugriff auf die konvergente CLI über SSH auf Geräten mit der Softwareversion 6.1.0 verwendet werden.

Schritt 2: Konfigurieren Sie die externe Authentifizierung.

Die externe Authentifizierung vereinfacht die Integration des FTD in ein Active Directory oder einen RADIUS-Server für die Benutzerauthentifizierung. Dies ist ein notwendiger Schritt, da lokal konfigurierte Benutzer keinen direkten Zugriff auf die Diagnose-CLI haben. Auf die Diagnose-CLI und die Benutzeroberfläche wird nur von Benutzern zugegriffen, die über LDAP (Lightweight Directory Access Protocol) oder RADIUS authentifiziert sind.

Die Konfiguration der externen Authentifizierung erfolgt in sechs Schritten.

Schritt 1: Navigieren zu **Geräte > Plattformeinstellungen**.

Schritt 2: Bearbeiten Sie entweder die vorhandene Richtlinie, indem Sie auf das Bleistiftsymbol klicken, oder erstellen Sie eine neue FTD-Richtlinie, während Sie auf die Schaltfläche **Neue Richtlinie** klicken und als Typ auswählen. **Einstellungen für die Bedrohungsabwehr**.

Schritt 3: Navigieren Sie zur Registerkarte **Externe Authentifizierung**, wie im Bild gezeigt:



Schritt 4: Wenn Sie auf **Hinzufügen** klicken, wird ein Dialogfeld angezeigt, wie im Bild gezeigt:

- **Für HTTP aktivieren:** Aktivieren Sie diese Option, um Zugriff auf FTD über HTTPS bereitzustellen.
- **Für SSH aktivieren:** Aktivieren Sie diese Option, um Zugriff auf FTD über SSH bereitzustellen.
- **Name:** Geben Sie den Namen für die LDAP-Verbindung ein.
- **Beschreibung:** Geben Sie eine optionale Beschreibung für das Objekt Externe Authentifizierung ein.
- **IP-Adresse:** Geben Sie ein Netzwerkobjekt ein, in dem die IP-Adresse des externen Authentifizierungsservers gespeichert wird. Wenn kein Netzwerkobjekt konfiguriert ist,

erstellen Sie ein neues. Klicken Sie auf das Symbol (+).

- **Authentifizierungsmethode:** Wählen Sie für die Authentifizierung RADIUS- oder LDAP-Protokoll aus.
- **SSL aktivieren** - Aktivieren Sie diese Option, um den Authentifizierungsdatenverkehr zu verschlüsseln.
- **Servertyp:** Wählen Sie den Servertyp aus. Die bekannten Servertypen sind MS Active Directory, Sun, OpenLDAP und Novell. Standardmäßig ist diese Option so eingestellt, dass der Servertyp automatisch erkannt wird.
- **Port:** Geben Sie den Port ein, über den die Authentifizierung erfolgt.
- **Timeout:** Geben Sie einen Timeout-Wert für die Authentifizierungsanforderungen ein.
- **Basis-DN:** Geben Sie eine Basis-DN ein, um einen Bereich bereitzustellen, in dem der Benutzer vorhanden sein kann.
- **LDAP-Bereich:** Wählen Sie den zu suchenden LDAP-Bereich aus. Der Gültigkeitsbereich befindet sich auf derselben Ebene oder in der Unterstruktur.
- **Benutzername:** Geben Sie einen Benutzernamen ein, der an das LDAP-Verzeichnis gebunden werden soll.
- **Authentifizierungskennwort:** Geben Sie das Kennwort für diesen Benutzer ein.
- **Bestätigen:** Geben Sie das Kennwort erneut ein.
- **Verfügbare Schnittstellen:** Eine Liste der verfügbaren Schnittstellen im FTD wird angezeigt.
- **Ausgewählte Zonen und Schnittstellen:** Diese Liste zeigt eine Liste von Schnittstellen an, über die der Authentifizierungsserver aufgerufen wird.

Für die RADIUS-Authentifizierung gibt es keinen Servertyp Base DN oder LDAP Scope. Der Port ist der RADIUS-Port 1645.

Secret (Geheimschlüssel): Geben Sie den geheimen Schlüssel für RADIUS ein.

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

Schritt 5: Klicken Sie nach Abschluss der Konfiguration auf **OK**.

Schritt 6: Speichern Sie die Richtlinie, und stellen Sie sie auf dem FirePOWER Threat Defense-

Gerät bereit.

Hinweis: Für den Zugriff auf die konvergente CLI über SSH auf Geräten mit Software-Version 6.1.0 kann keine externe Authentifizierung verwendet werden.

Schritt 3: Konfigurieren des SSH-Zugriffs

SSH bietet direkten Zugriff auf die konvergente CLI. Verwenden Sie diese Option, um direkt auf die CLI zuzugreifen und Debug-Befehle auszuführen. In diesem Abschnitt wird beschrieben, wie SSH für den Zugriff auf die FTD-CLI konfiguriert wird.

Anmerkung: Auf FTD-Geräten, auf denen die Software Version 6.0.1 ausgeführt wird, bietet die SSH-Konfiguration unter Plattformeinstellungen direkten Zugriff auf die Diagnose-CLI und nicht auf die CLISH. Sie müssen eine Verbindung zur auf **br1** konfigurierten IP-Adresse herstellen, um auf die CLISH zuzugreifen. Auf FTD-Geräten, auf denen die Software Version 6.1.0 ausgeführt wird, navigieren alle Schnittstellen beim Zugriff über SSH zur konvergenten CLI.

Die SSH-Konfiguration auf der ASA erfolgt in 6 Schritten.

Nur für 6.0.1-Geräte:

Diese Schritte werden auf FTD-Geräten ausgeführt, deren Softwareversion weniger als 6.1.0 und höher als 6.0.1 ist. Auf 6.1.0-Geräten werden diese Parameter vom Betriebssystem geerbt.

Schritt 1: Navigieren Sie zu **Geräte > Plattformeinstellungen**.

Schritt 2: Bearbeiten Sie entweder die vorhandene Richtlinie, indem Sie auf das Bleistiftsymbol klicken, oder erstellen Sie eine neue Firewall-Threat Defense-Richtlinie, während Sie auf die Schaltfläche **New Policy** klicken und als **Threat Defense Settings** auswählen.

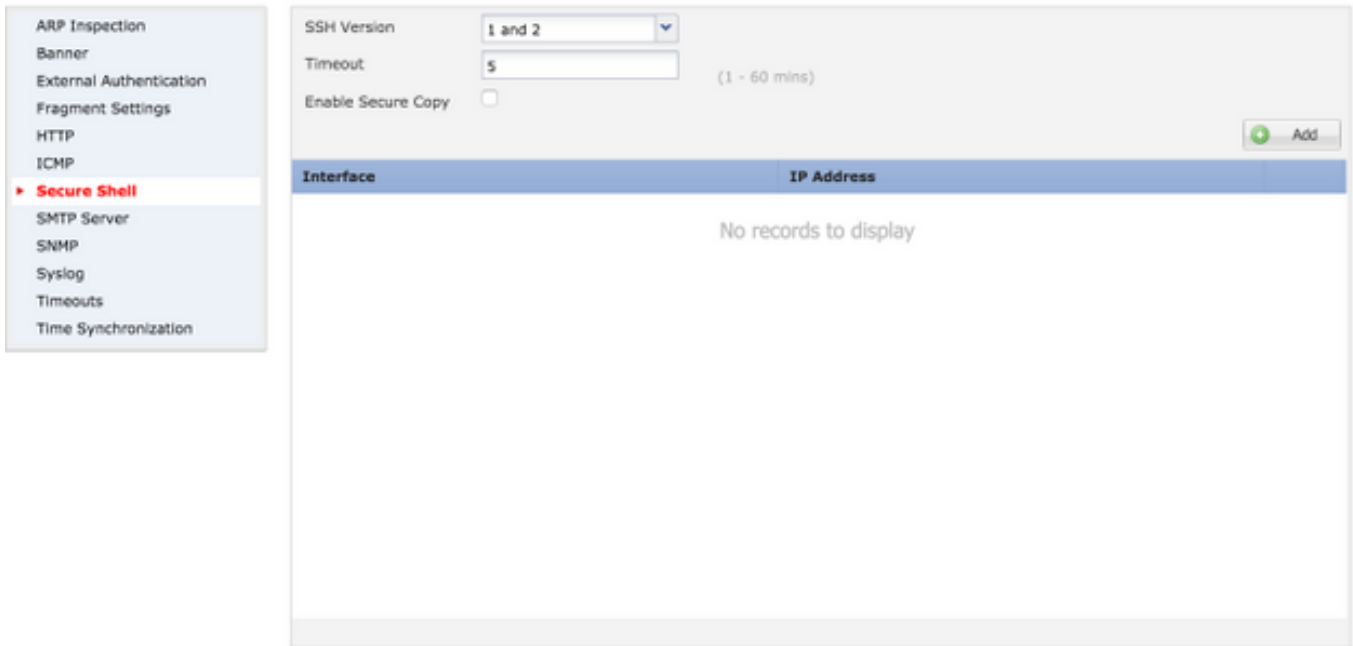
Schritt 3: Navigieren Sie zum Abschnitt **Secure Shell**. Eine Seite wird angezeigt, wie im Bild gezeigt:

SSH-Version: Wählen Sie die SSH-Version aus, die auf der ASA aktiviert werden soll. Es gibt drei Optionen:

- **1:** Nur SSH-Version 1 aktivieren
- **2:** Nur SSH-Version 2 aktivieren
- **1 und 2:** SSH-Version 1 und 2 aktivieren

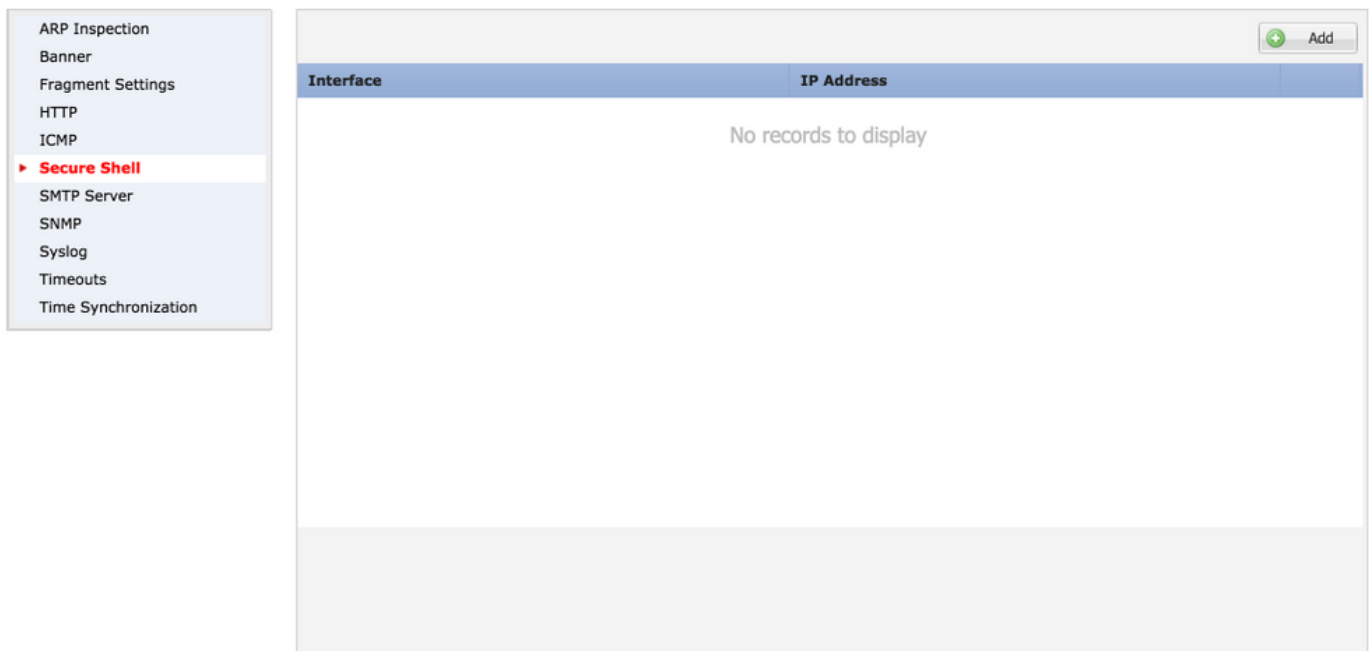
Timeout: Geben Sie das gewünschte SSH-Timeout in Minuten ein.

Sichere Kopie aktivieren: Aktivieren Sie diese Option, um das Gerät so zu konfigurieren, dass SCP-Verbindungen (Secure Copy) zulässig sind und als SCP-Server fungieren.



Auf 6.0.1- und 6.1.0-Geräten:

Diese Schritte werden so konfiguriert, dass der Management-Zugriff über SSH auf bestimmte Schnittstellen und bestimmte IP-Adressen beschränkt wird.

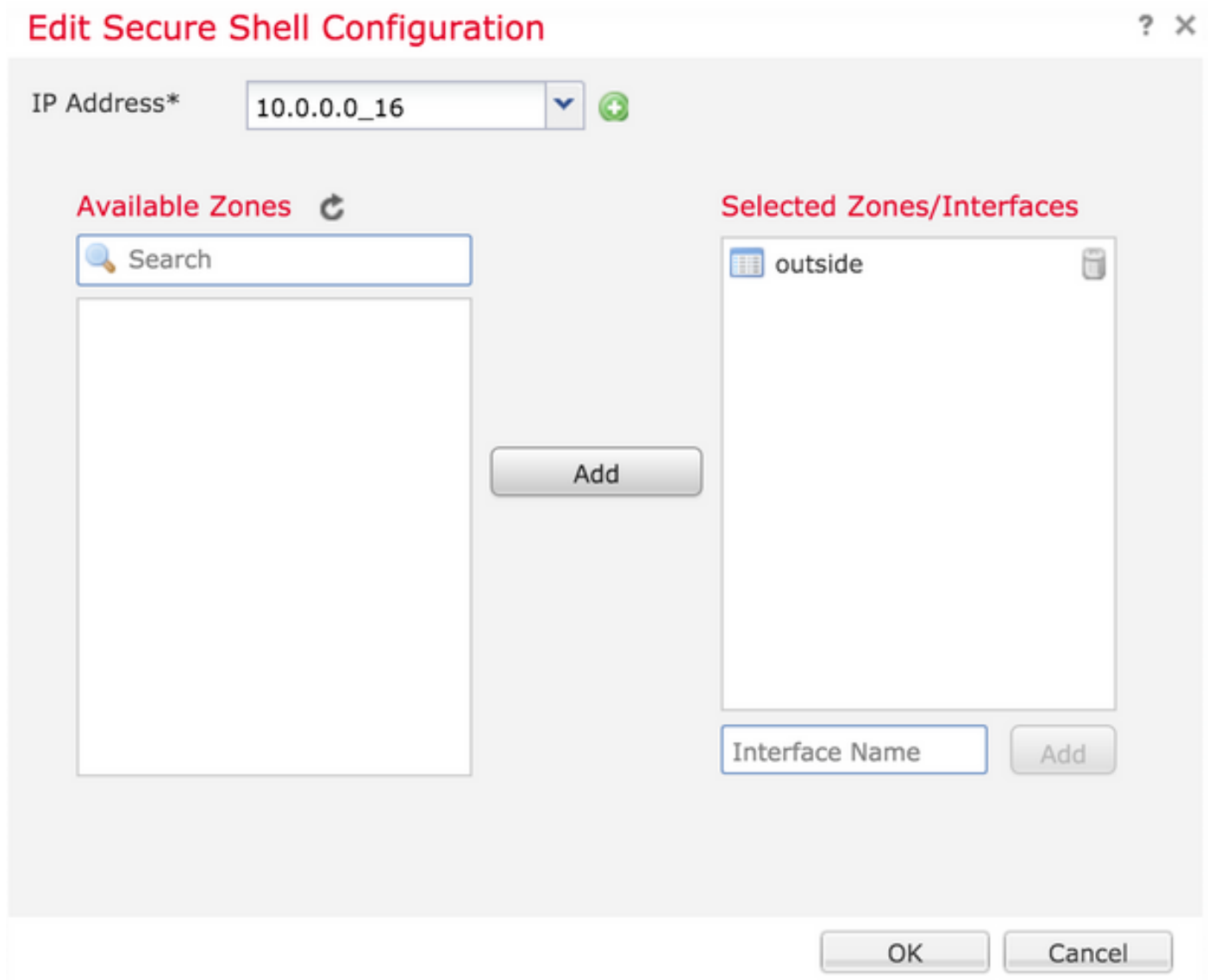


Schritt 1: Klicken Sie auf **Hinzufügen** und konfigurieren Sie diese Optionen:

IP-Adresse: Wählen Sie ein Netzwerkobjekt aus, das die Subnetze enthält, die über SSH auf die CLI zugreifen dürfen. Wenn kein Netzwerkobjekt vorhanden ist, erstellen Sie ein Objekt, indem Sie auf das (+) Symbol klicken.

Ausgewählte Zonen/Schnittstellen: Wählen Sie die Zonen oder Schnittstellen aus, über die auf den SSH-Server zugegriffen wird.

Schritt 2: Klicken Sie auf **OK**, wie im Bild gezeigt:



Die Konfiguration für SSH wird mithilfe dieses Befehls in der konvergenten CLI (ASA Diagnostic CLI in 6.0.1-Geräten) angezeigt.

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

Schritt 3: Wenn die SSH-Konfiguration abgeschlossen ist, klicken Sie auf **Speichern** und geben Sie die Richtlinie dann an die FTD weiter.

Schritt 4: Konfigurieren des HTTPS-Zugriffs

Um HTTPS-Zugriff auf eine oder mehrere Schnittstellen zu aktivieren, navigieren Sie zum **HTTP**-Abschnitt in den Plattformeinstellungen. Der HTTPS-Zugriff ist besonders hilfreich, um die Paketerfassungen direkt von der sicheren Diagnosewebschnittstelle für die Analyse herunterzuladen.

Zum Konfigurieren des HTTPS-Zugriffs sind sechs Schritte erforderlich.

Schritt 1: Navigieren Sie zu **Geräte > Plattformeinstellungen**.

Schritt 2: Bearbeiten Sie entweder die Plattformeinstellungen, die vorhanden sind, während Sie auf das **Bleistiftsymbol** neben der Richtlinie klicken, oder erstellen Sie eine neue FTD-Richtlinie, wenn Sie auf **Neue Richtlinie** klicken. Wählen Sie den Typ als **FirePOWER Threat Defense aus**.

Schritt 3: Wenn Sie zum **HTTP**-Abschnitt navigieren, wird eine Seite angezeigt, wie im Bild gezeigt.

HTTP-Server aktivieren: Aktivieren Sie diese Option, um HTTP-Server in FTD zu aktivieren.

Port: Wählen Sie den Port aus, an dem die FTD Managementverbindungen akzeptiert.

FTD-Policy

Enter a description

The screenshot shows the configuration page for the HTTP section of an FTD Policy. On the left is a navigation menu with options: ARP Inspection, Banner, External Authentication, Fragment Settings, **HTTP** (highlighted), ICMP, Secure Shell, SMTP Server, SNMP, Syslog, Timeouts, and Time Synchronization. The main content area has a header 'Enable HTTP Server' with a checked checkbox. Below it is a 'Port' field containing '443' and a note: '(Please don't use 80 or 1443)'. An 'Add' button is in the top right. A table with columns 'Interface' and 'Network' is shown below, containing the text 'No records to display'.

Schritt 4. Klicken Sie auf **Hinzufügen** und Seite, wie im Bild gezeigt:

IP-Adresse: Geben Sie die Subnetze ein, die HTTPS-Zugriff auf die Diagnoseschnittstelle zulassen. Wenn kein Netzwerkobjekt vorhanden ist, erstellen Sie ein Objekt, und verwenden Sie die Option (+).

Ausgewählte Zonen/Schnittstellen: Ähnlich wie SSH muss für die HTTPS-Konfiguration eine Schnittstelle konfiguriert sein, auf die über HTTPS zugegriffen werden kann. Wählen Sie die Zonen oder Schnittstellen aus, über die der FTD über HTTPS aufgerufen werden soll.

Edit HTTP Configuration



IP Address* 10.0.0.0_16

Available Zones

Selected Zones/Interfaces

outside

Add

Interface Name Add

OK Cancel

Die Konfiguration für HTTPS wird in der konvergenten CLI (ASA Diagnostic CLI in 6.0.1-Geräten) angezeigt und verwendet diesen Befehl.

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

Schritt 5: Wenn die erforderliche Konfiguration abgeschlossen ist, wählen Sie **OK**.

Schritt 6: Nachdem Sie alle erforderlichen Informationen eingegeben haben, klicken Sie auf **Speichern** und stellen Sie die Richtlinie dann auf dem Gerät bereit.

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dies sind die grundlegenden Schritte zur Behebung von Verwaltungsproblemen im FTD.

Schritt 1: Stellen Sie sicher, dass die Schnittstelle aktiviert ist und mit einer IP-Adresse konfiguriert ist.

Schritt 2: Stellen Sie sicher, dass eine externe Authentifizierung wie konfiguriert funktioniert und über die entsprechende, im Abschnitt **Externe Authentifizierung der Plattformeinstellungen** angegebene Schnittstelle erreichbar ist.

Schritt 3: Stellen Sie sicher, dass die FTD-Weiterleitung korrekt ist. Navigieren Sie in FTD-Software Version 6.0.1 zu **Systemsupport-DiagnoseCLI**. Führen Sie die Befehle **show route** und **show route management-only** aus, um die Routen für die FTD bzw. die Management-Schnittstellen anzuzeigen.

Führen Sie die Befehle in der FTD-Software Version 6.1.0 direkt in der konvergenten CLI aus.

Zugehörige Informationen

- [Technischer Support und Dokumentation für Cisco Systeme](#)