Configurazione dell'accesso di gestione a FTD (HTTPS e SSH) tramite FMC

Sommario

Introduzione

In questo documento viene descritta la configurazione dell'accesso di gestione a un Firepower Threat Defense (FTD) (HTTPS e SSH) tramite Firesight Management Center (FMC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza della tecnologia Firepower
- Conoscenze base di ASA (Adaptive Security Appliance)
- Conoscenza dell'accesso alla gestione sull'ASA tramite HTTPS e SSH (Secure Shell)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

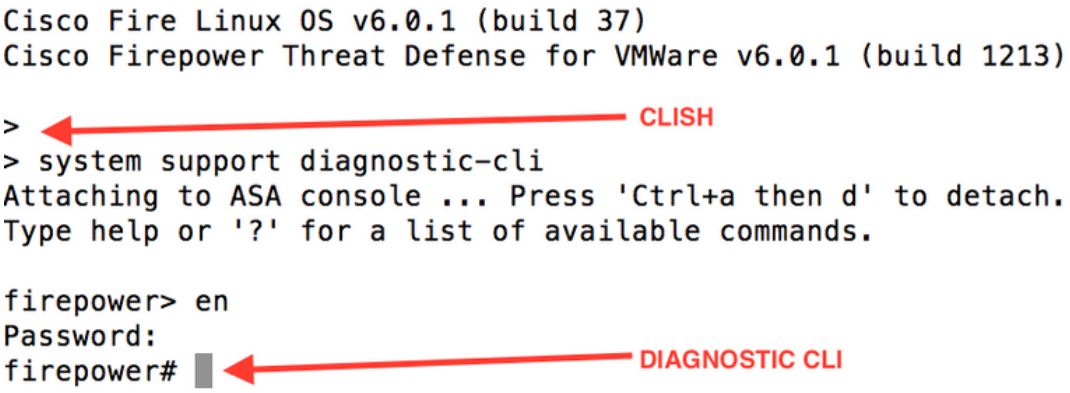
- Adaptive Security Appliance (ASA) Firepower Threat Defense Image per ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X), in esecuzione sul software versione 6.0.1 e successive.
- ASA Firepower Threat Defense Image per ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X), in esecuzione sul software versione 6.0.1 e successive.
- Firepower Management Center (FMC) versione 6.0.1 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Con l'avvio di Firepower Threat Defense (FTD), l'intera configurazione ASA viene eseguita sulla GUI.

Sui dispositivi FTD con software versione 6.0.1, è possibile accedere alla CLI di diagnostica dell'ASA quando si accede al supporto di sistema diagnostic-cli. Tuttavia, sui dispositivi FTD con software versione 6.1.0, la CLI converge e interi comandi ASA vengono configurati sulla CLISH.



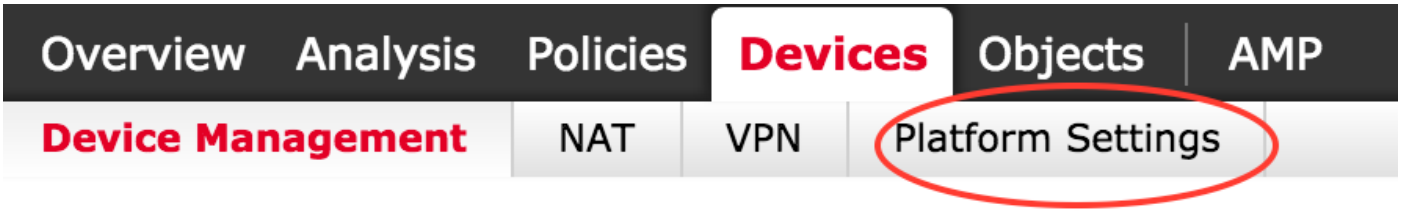
Per ottenere l'accesso alla gestione direttamente da una rete esterna, è necessario configurare l'accesso alla gestione tramite HTTPS o SSH. Questo documento fornisce la configurazione necessaria per ottenere l'accesso alla gestione su SSH o HTTPS esternamente.

Nota: sui dispositivi FTD con software versione 6.0.1, non è possibile accedere alla CLI da parte di un utente locale, è necessario configurare un'autenticazione esterna per autenticare gli utenti. Tuttavia, sui dispositivi FTD con software versione 6.1.0, l'utente admin locale accede alla CLI mentre per tutti gli altri utenti è richiesta un'autenticazione esterna.

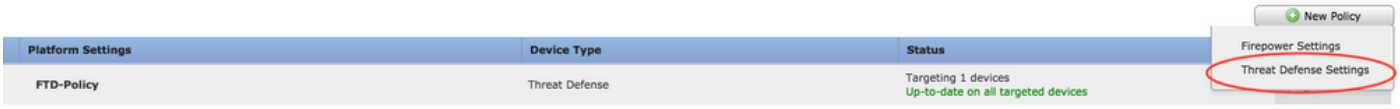
Nota: sui dispositivi FTD con software versione 6.0.1, l'interfaccia CLI di diagnostica non è accessibile direttamente sull'IP configurato per br1 dell'FTD. Tuttavia, sui dispositivi FTD con software versione 6.1.0, la CLI convergente è accessibile su qualsiasi interfaccia configurata per l'accesso di gestione; tuttavia, l'interfaccia deve essere configurata con un indirizzo IP.

Configurazione

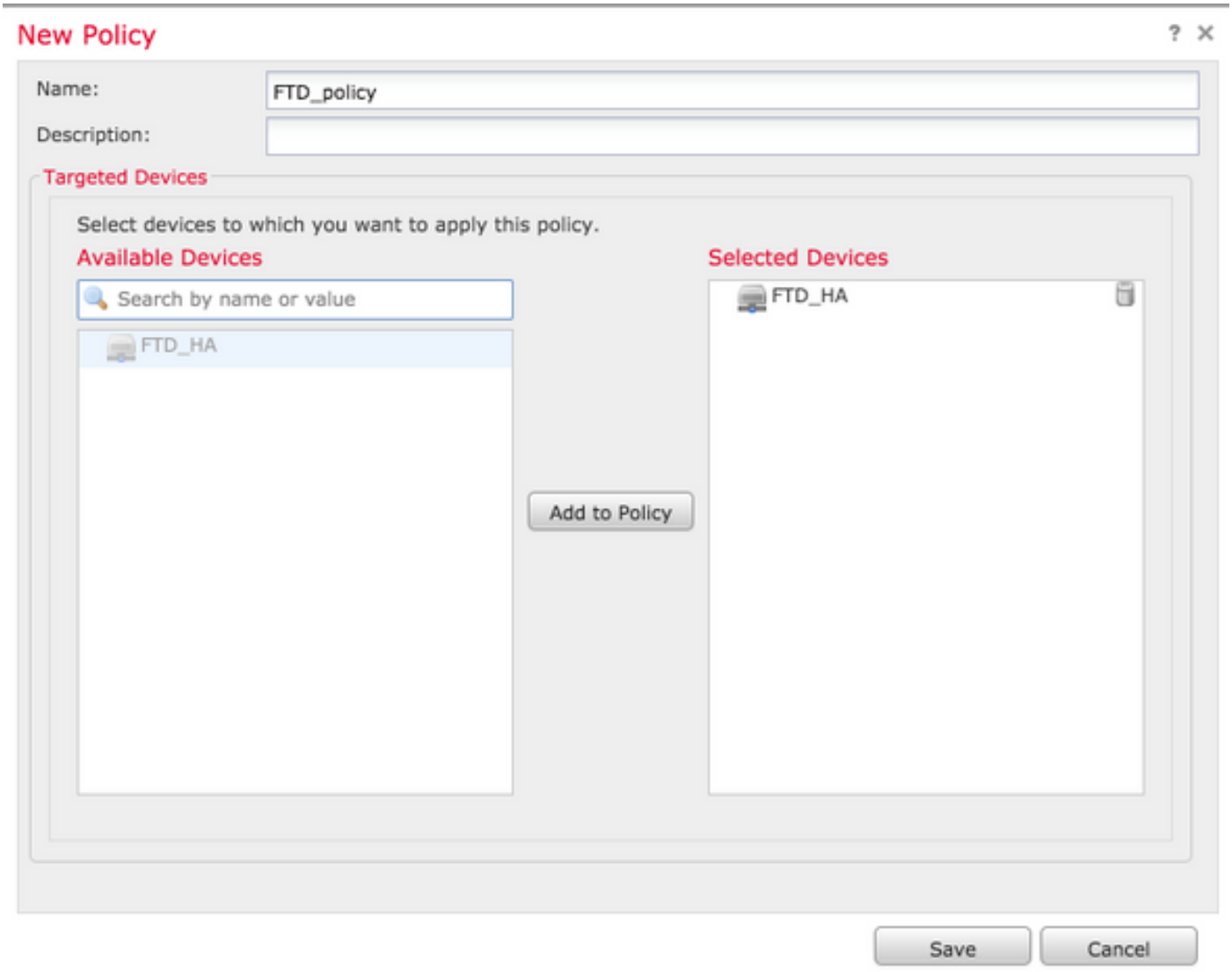
Tutta la configurazione relativa a Management Access viene configurata mentre si passa alla scheda Platform Settings in Devices, come mostrato nell'immagine:



Modificare il criterio esistente facendo clic sull'icona a forma di matita oppure creare un nuovo criterio FTD facendo clic sul pulsante Nuovo criterio e selezionando il tipo Impostazioni di difesa dalle minacce come mostrato nell'immagine:



Selezionare l'accessorio FTD a cui applicare il criterio e fare clic su Salva, come mostrato nell'immagine:



Configura accesso di gestione

Di seguito sono riportati i quattro passaggi principali eseguiti per configurare l'accesso di gestione.

Passaggio 1. Configurare l'indirizzo IP sull'interfaccia FTD tramite l'interfaccia utente di FMC.

Configurare un IP sull'interfaccia su cui è accessibile l'FTD tramite SSH o HTTPS. Modificare le interfacce esistenti mentre si passa alla scheda Interfacce dell'FTD.

> Nota: sui dispositivi FTD con software versione 6.0.1, l'interfaccia di gestione predefinita sull'FTD è l'interfaccia diagnostica 0/0. Tuttavia, sui dispositivi FTD con software versione 6.1.0, tutte le interfacce supportano l'accesso alla gestione ad eccezione dell'interfaccia diagnostica.

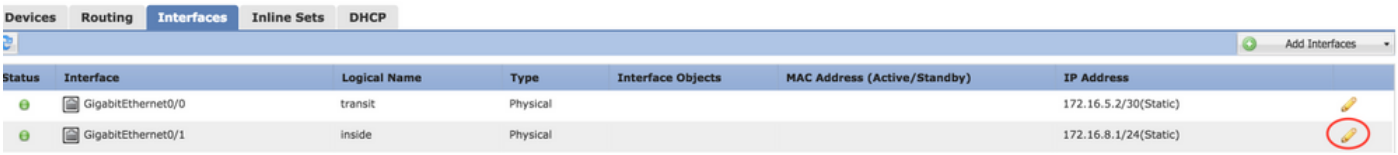
Per configurare l'interfaccia di diagnostica, è necessario eseguire sei passaggi.

Passaggio 1. Passa a Periferica > Gestione periferiche.

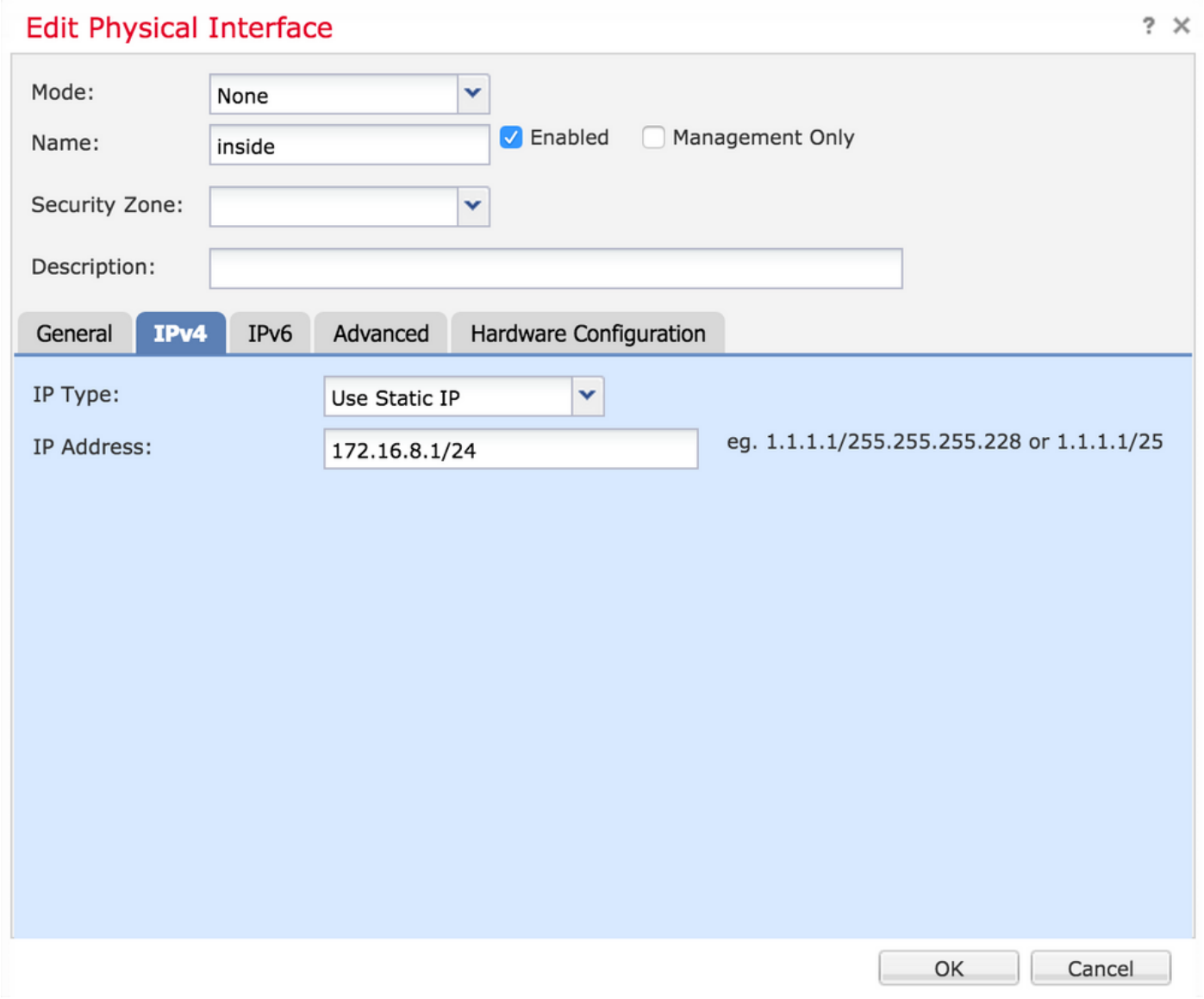
Passaggio 2. Selezionare il dispositivo o il cluster FTD HA.

Passaggio 3. Passare alla scheda Interfacce.

Passaggio 4. Fare clic sull'icona della matita per configurare/modificare l'interfaccia per ottenere l'accesso di gestione, come mostrato nell'immagine:



Passaggio 5. Selezionare la casella di controllo enable per abilitare le interfacce. Selezionare la scheda Ipv4, quindi selezionare il tipo di IP statico o DHCP. Immettere un indirizzo IP per l'interfaccia e fare clic su OK, come mostrato nell'immagine:



Passaggio 6. Fare clic su Salva, quindi distribuire il criterio nell'FTD.

> Nota: l'interfaccia diagnostica non può essere utilizzata per accedere a Converged CLI over SSH sui dispositivi con software versione 6.1.0

Passaggio 2. Configurare l'autenticazione esterna.

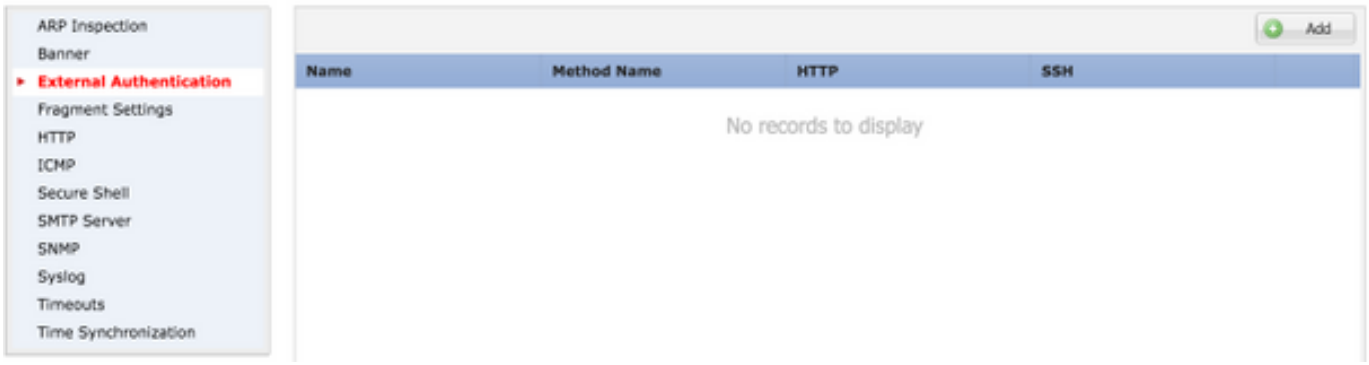
L'autenticazione esterna facilita l'integrazione dell'FTD in un server Active Directory o RADIUS per l'autenticazione degli utenti. Questa operazione è necessaria perché gli utenti configurati localmente non dispongono di accesso diretto alla CLI di diagnostica. La CLI di diagnostica e la GUI sono accessibili solo dagli utenti autenticati tramite LDAP (Lightweight Directory Access Protocol) o RADIUS.

Per configurare l'autenticazione esterna, è necessario eseguire 6 passaggi.

Passaggio 1. Passa a Dispositivi > Impostazioni piattaforma.

Passaggio 2. Modificare il criterio esistente facendo clic sull'icona a forma di matita oppure creare un nuovo criterio FTD facendo clic sul pulsante Nuovo criterio e selezionando il tipo Impostazioni di difesa dalle minacce.

Passaggio 3. Passare alla scheda Autenticazione esterna, come mostrato nell'immagine:



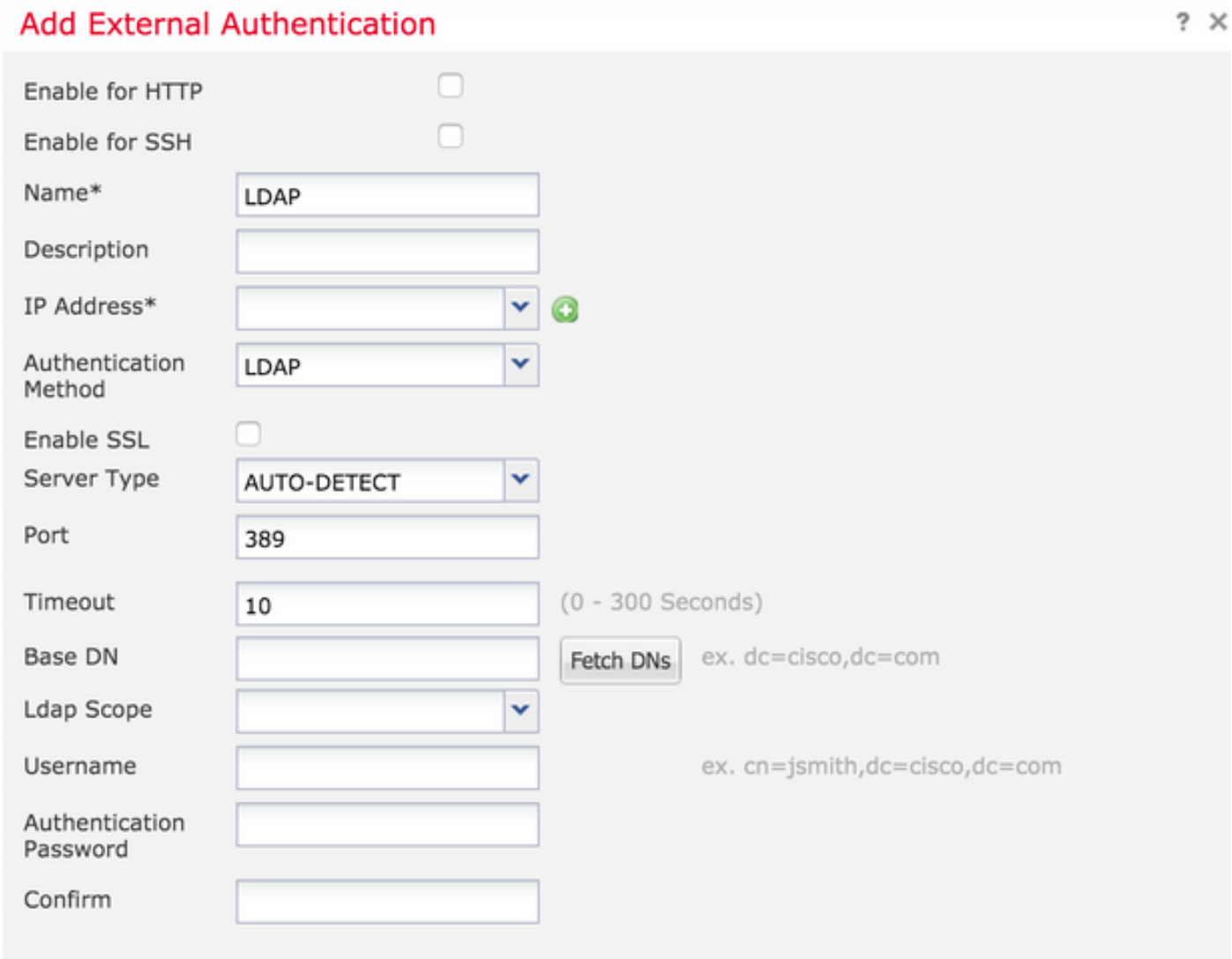
Passaggio 4. Facendo clic su Add, viene visualizzata una finestra di dialogo come mostrato nell'immagine:

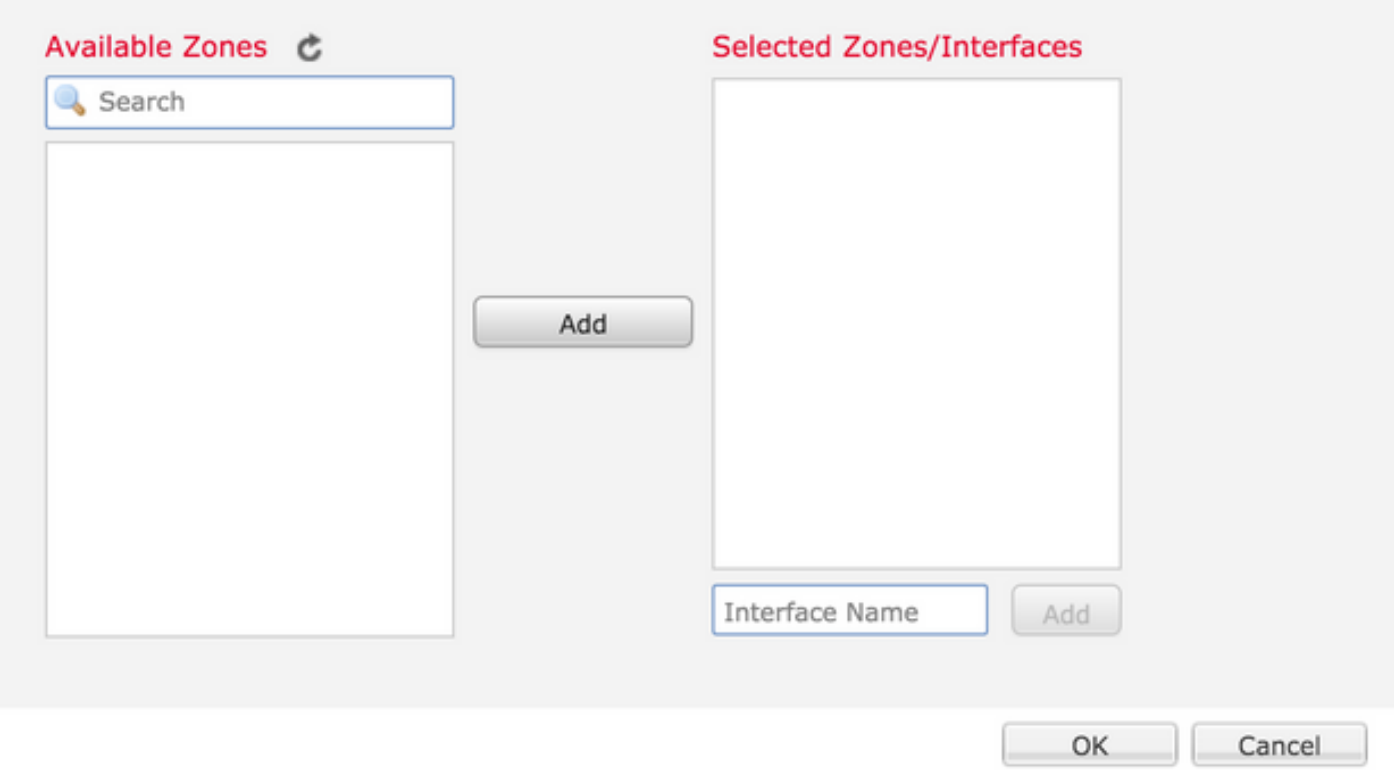
- Abilita per HTTP: abilitare questa opzione per fornire l'accesso al FTD su HTTPS.
- Abilita per SSH: abilitare questa opzione per fornire l'accesso al FTD su SSH.
- Nome: immettere il nome della connessione LDAP.
- Descrizione: immettere una descrizione facoltativa per l'oggetto Autenticazione esterna.
- Indirizzo IP: immettere un oggetto di rete in cui è archiviato l'indirizzo IP del server di autenticazione esterno. Se non è stato configurato alcun oggetto di rete, crearne uno nuovo. Fare clic sull'icona (+).
- Metodo di autenticazione: selezionare il protocollo RADIUS o LDAP per l'autenticazione.
- Abilita SSL-Abilitare questa opzione per crittografare il traffico di autenticazione.
- Tipo di server: selezionare il tipo di server. I tipi di server noti sono MS Active Directory, Sun, OpenLDAP e Novell. Per impostazione predefinita, l'opzione è impostata per il rilevamento automatico del tipo di server.
- Porta: immettere la porta su cui viene eseguita l'autenticazione.
- Timeout: immettere un valore di timeout per le richieste di autenticazione.
- DN di base: immettere un DN di base per fornire un ambito in cui l'utente può essere presente.

- Ambito LDAP: selezionare l'ambito LDAP da cercare. L'ambito si trova all'interno dello stesso livello o per la ricerca all'interno della sottostruttura.
- Nome utente: immettere un nome utente da associare alla directory LDAP.
- Password di autenticazione: immettere la password per l'utente.
- Conferma: immettere nuovamente la password.
- Interfacce disponibili: viene visualizzato un elenco delle interfacce disponibili sull'FTD.
- Zone e interfacce selezionate: visualizza un elenco di interfacce da cui è possibile accedere al server di autenticazione.

Per l'autenticazione RADIUS, non è presente alcun tipo di server DN di base o Ambito LDAP. La porta è la porta RADIUS 1645.

Secret: immettere la chiave segreta per RADIUS.





Passaggio 5. Al termine della configurazione, fare clic su OK.

Passaggio 6. Salvare il criterio e distribuirlo nel dispositivo Firepower Threat Defense.

Nota: l'autenticazione esterna non può essere utilizzata per accedere a Converged CLI over SSH sui dispositivi con software versione 6.1.0

Passaggio 3. Configurare l'accesso SSH.

SSH fornisce accesso diretto alla CLI convergente. Usare questa opzione per accedere direttamente alla CLI ed eseguire i comandi di debug. Questa sezione descrive come configurare SSH per accedere alla CLI dell'FTD.

Nota: sui dispositivi FTD con software versione 6.0.1, la configurazione SSH sulle impostazioni della piattaforma permette di accedere direttamente alla CLI diagnostica e non alla CLISH. Per accedere a CLISH, è necessario collegarsi all'indirizzo IP configurato su br1. Tuttavia, sui dispositivi FTD con software versione 6.1.0, tutte le interfacce passano alla CLI convergente quando vi si accede tramite SSH

Per configurare SSH sull'appliance ASA, è necessario eseguire 6 passaggi

Solo su dispositivi 6.0.1:

Queste operazioni vengono eseguite sui dispositivi FTD con versione software inferiore a 6.1.0 e superiore a 6.0.1. Sui dispositivi 6.1.0 questi parametri sono ereditati dal sistema operativo.

Passaggio 1. Selezionare Dispositivi>Impostazioni piattaforma.

Passaggio 2. Modificare il criterio esistente facendo clic sull'icona a forma di matita o creare un nuovo criterio Firepower Threat Defense facendo clic sul pulsante Nuovo criterio e selezionare il tipo Impostazioni di Threat Defense.

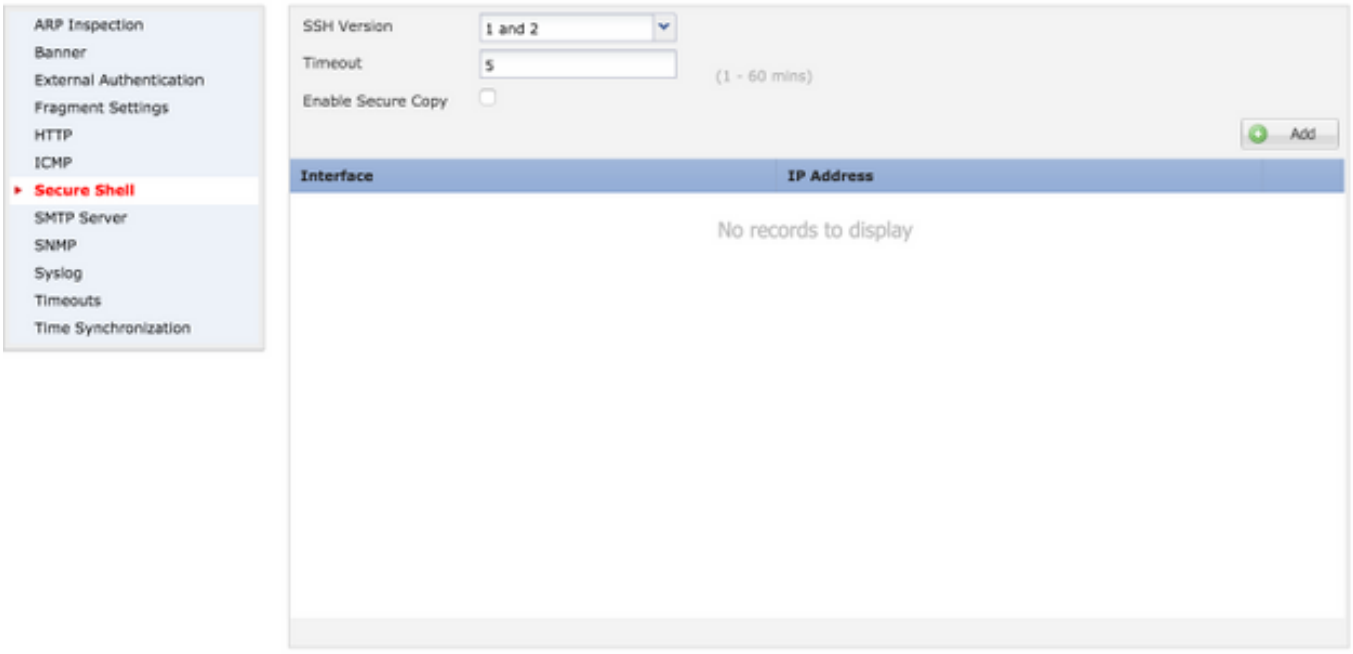
Passaggio 3. Passare alla sezione Secure Shell. Viene visualizzata una pagina, come illustrato nell'immagine:

Versione SSH: selezionare la versione SSH da abilitare sull'appliance ASA. Sono disponibili tre opzioni:

- 1: Abilitare solo SSH versione 1
- 2: Abilitare solo SSH versione 2
- 1 e 2: abilitare SSH versione 1 e 2

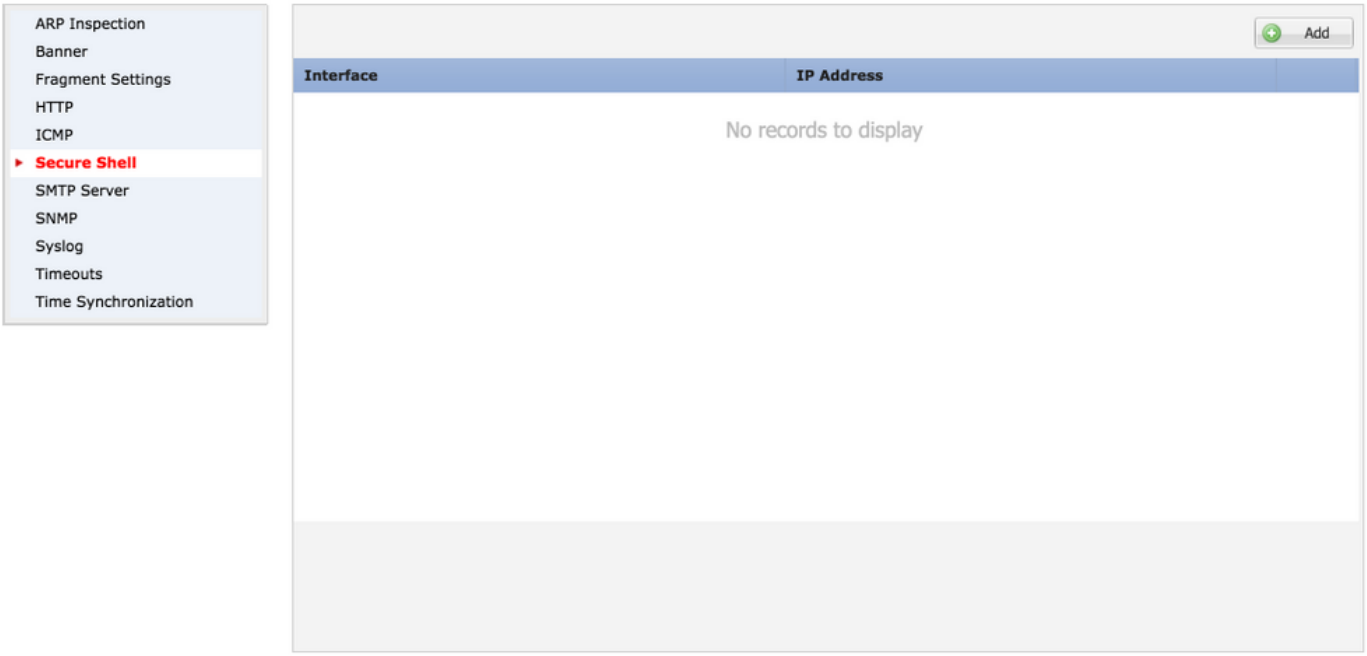
Timeout: immettere il timeout SSH desiderato in minuti.

Abilita copia sicura: selezionare questa opzione per configurare il dispositivo in modo da consentire le connessioni Secure Copy (SCP) e agire come server SCP.



Sui dispositivi 6.0.1 e 6.1.0:

Questa procedura è configurata per limitare l'accesso di gestione tramite SSH a interfacce specifiche e a indirizzi IP specifici.

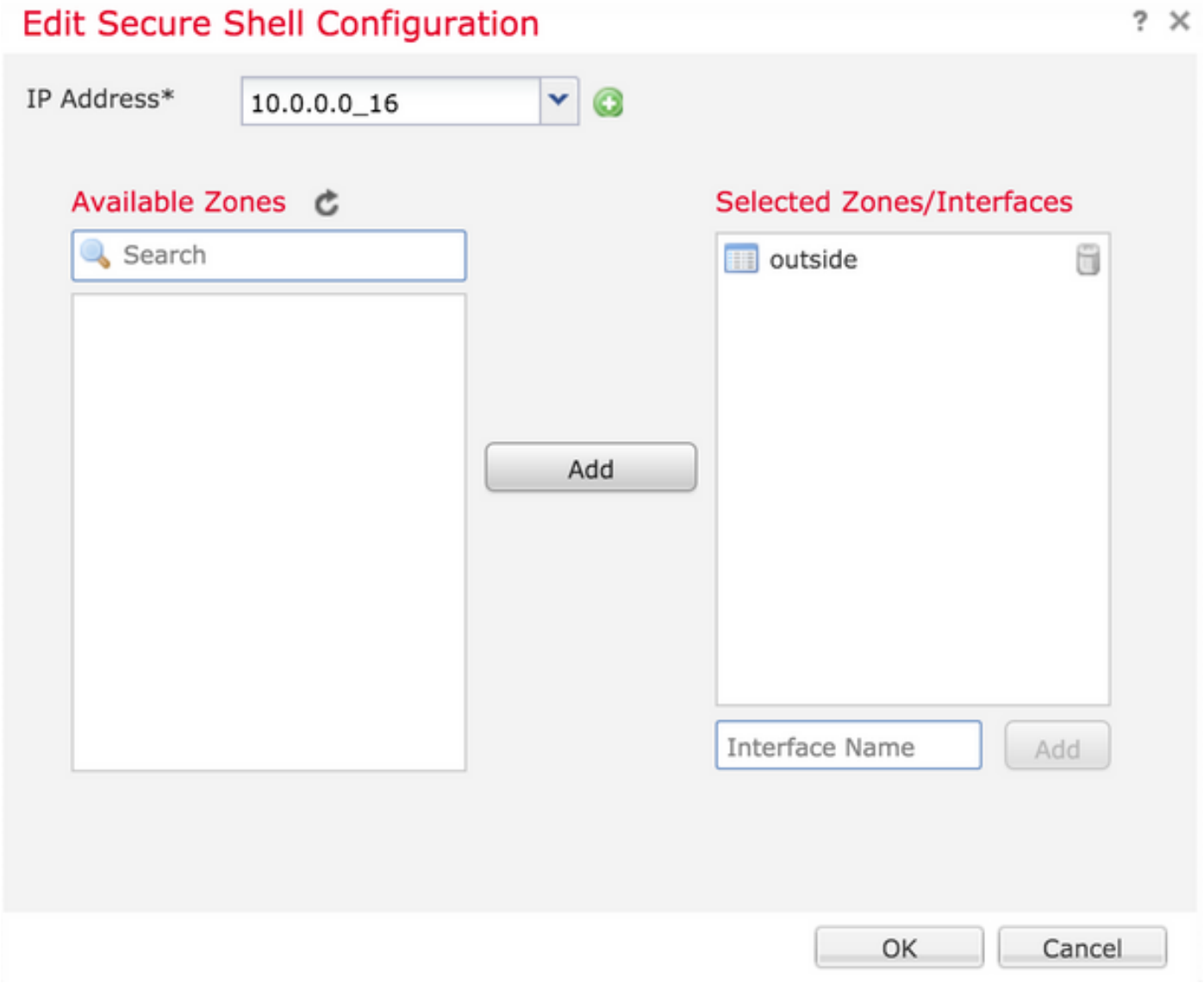


Passaggio 1. Fare clic su Add (Aggiungi) e configurare le seguenti opzioni:

Indirizzo IP: selezionare un oggetto di rete contenente le subnet a cui è consentito accedere alla CLI su SSH. Se un oggetto di rete non è presente, crearne uno facendo clic sull'icona (+).

Zone/interfacce selezionate: selezionare le zone o le interfacce da cui è possibile accedere al server SSH.

Passaggio 2. Fare clic su OK, come mostrato nell'immagine:



La configurazione del protocollo SSH viene visualizzata nella CLI convergente (ASA Diagnostic CLI nei dispositivi 6.0.1) con questo comando.

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

Passaggio 3. Al termine della configurazione SSH, fare clic su Save, quindi distribuire il criterio nell'FTD.

Passaggio 4. Configura accesso HTTPS.

Per abilitare l'accesso HTTPS a una o più interfacce, passare alla sezione HTTP nelle impostazioni della piattaforma. L'accesso HTTPS è particolarmente utile per scaricare le clip dei pacchetti dall'interfaccia Web sicura per la diagnostica direttamente per l'analisi.

Per configurare l'accesso HTTPS è necessario eseguire 6 passaggi.

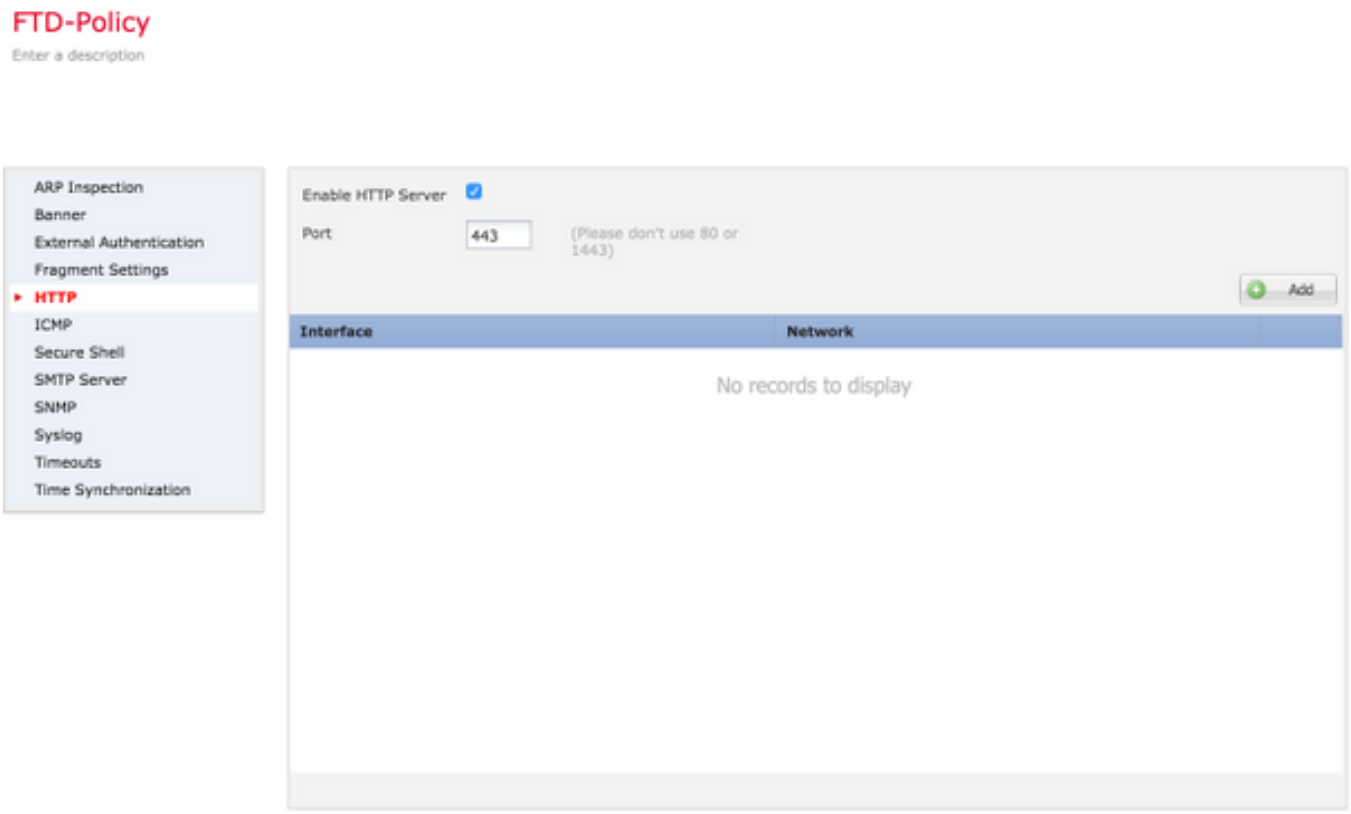
Passaggio 1. Selezionare Dispositivi > Impostazioni piattaforma

Passaggio 2. Modificare il criterio di impostazioni della piattaforma esistente facendo clic sull'icona a forma di matita accanto al criterio oppure creare un nuovo criterio FTD facendo clic su Nuovo criterio. Selezionare il tipo come Firepower Threat Defense.

Passaggio 3. Quando si passa alla sezione HTTP, viene visualizzata una pagina come illustrato nell'immagine.

Abilita server HTTP: abilitare questa opzione per abilitare il server HTTP sull'FTD.

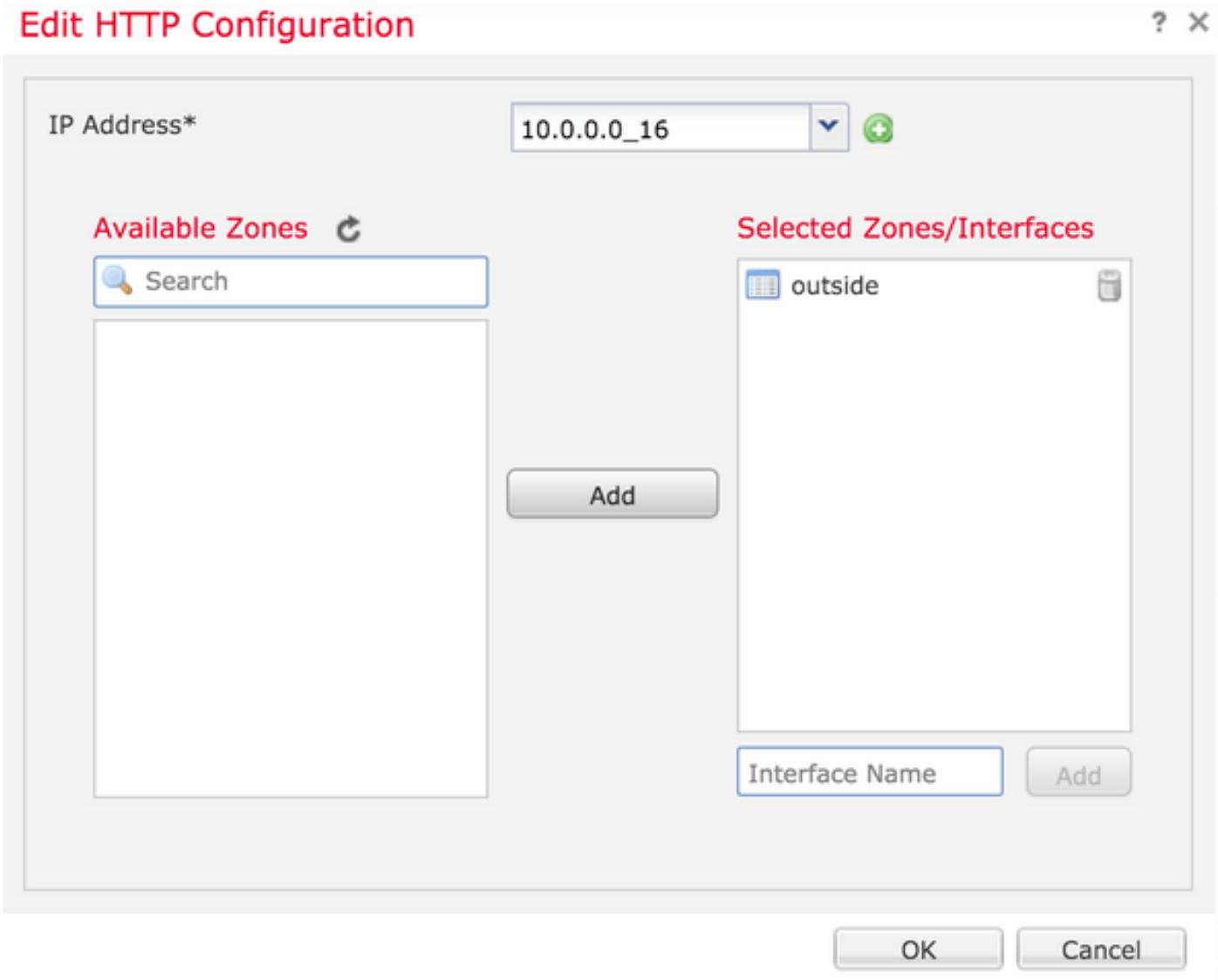
Porta: selezionare la porta su cui l'FTD accetta le connessioni di gestione.



Passaggio 4. Fare clic su Add (Aggiungi) per visualizzare la pagina come mostrato nell'immagine:

Indirizzo IP: immettere le subnet a cui è consentito l'accesso HTTPS all'interfaccia di diagnostica. Se non è presente alcun oggetto di rete, crearne uno e utilizzare l'opzione (+).

Zone/interfacce selezionate: come il protocollo SSH, la configurazione HTTPS deve avere un'interfaccia configurata su cui sia accessibile tramite HTTPS. Selezionare le zone o l'interfaccia su cui accedere all'FTD tramite HTTPS.



La configurazione per HTTPS viene visualizzata nella CLI convergente (ASA Diagnostic CLI nei dispositivi 6.0.1) e utilizza questo comando.

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

Passaggio 5. Una volta completata la configurazione necessaria, selezionare OK.

Passaggio 6. Dopo aver immesso tutte le informazioni richieste, fare clic su Salva e quindi distribuire il criterio nel dispositivo.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Di seguito vengono riportati i passaggi di base per risolvere i problemi di accesso alla gestione sull'FTD.

Passaggio 1. Verificare che l'interfaccia sia abilitata e configurata con un indirizzo IP.

Passaggio 2. Verificare che l'autenticazione esterna funzioni come configurato e che sia raggiungibile dall'interfaccia appropriata specificata nella sezione Autenticazione esterna di Impostazioni piattaforma.

Passaggio 3. Assicurarsi che il routing sull'FTD sia accurato. Nel software FTD versione 6.0.1, passare a system support diagnostic-cli. Eseguire i comandi show route e show route management-only per visualizzare i percorsi rispettivamente per l'FTD e le interfacce di gestione.

Nel software FTD versione 6.1.0, eseguire i comandi direttamente nella CLI convergente.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).