# Configurazione dell'accesso di gestione per SSH e HTTPS su FTD tramite FDM

## Sommario



## Introduzione

Questo documento descrive la procedura per configurare e verificare l'elenco degli accessi alla gestione per SSH e HTTPS su FTD gestito in locale o in remoto.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

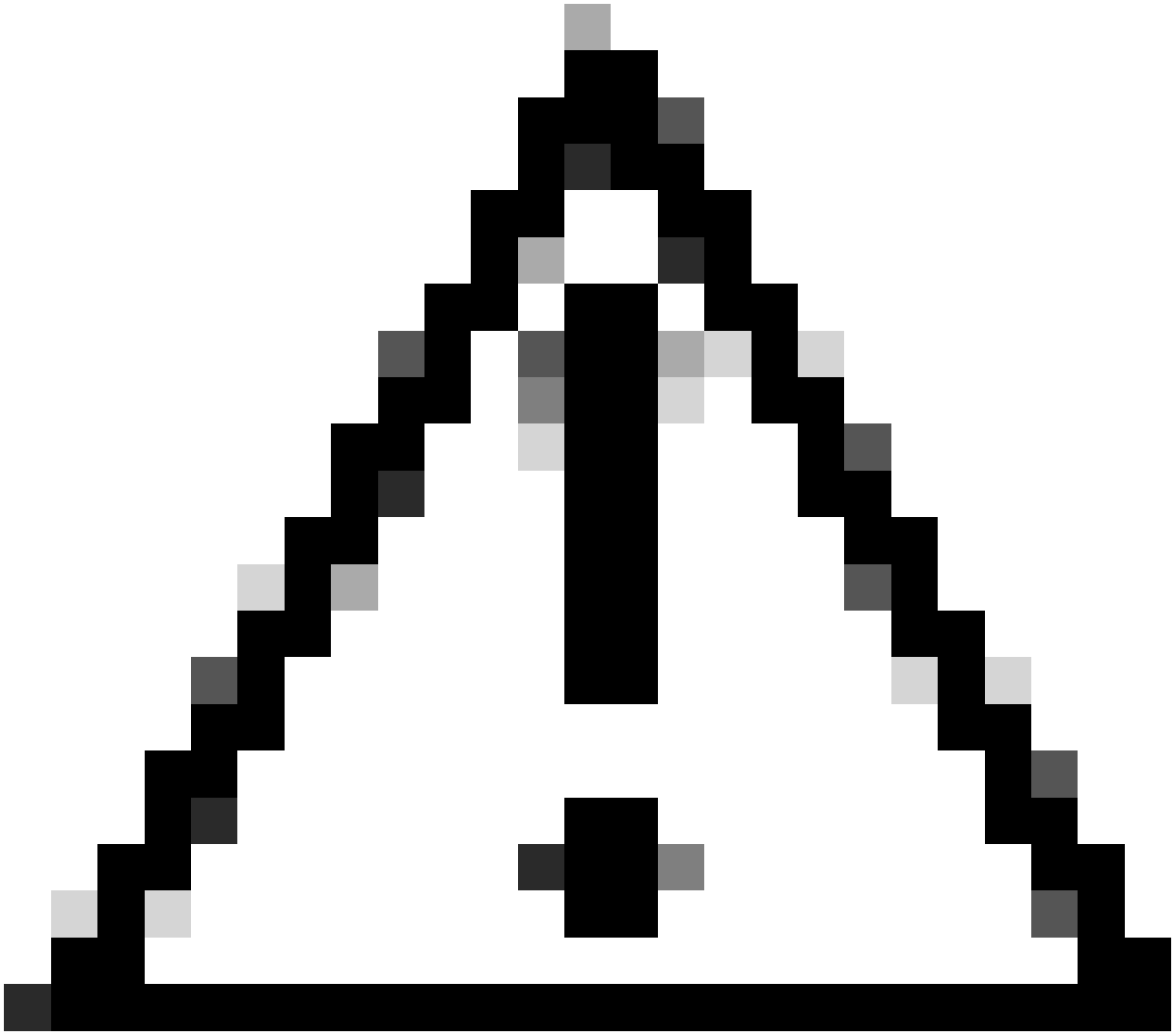
### Componenti usati

- Cisco Secure Firewall Threat Defense con versione 7.4.1 gestito da FDM.

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.

## Configurazione

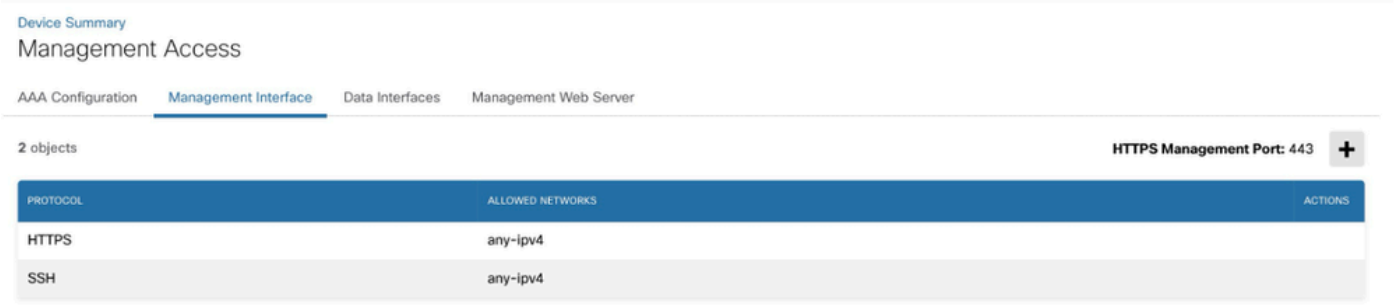
FTD può essere gestito localmente tramite FDM o FMC. In questo documento, l'attenzione si concentra sull'accesso alla gestione tramite FDM e CLI. Utilizzando CLI è possibile apportare modifiche sia per lo scenario FDM che per FMC.



Attenzione: Configurare gli elenchi degli accessi SSH o HTTPS uno alla volta per evitare il blocco delle sessioni. Aggiornare e distribuire un protocollo, verificare l'accesso e procedere con l'altro.

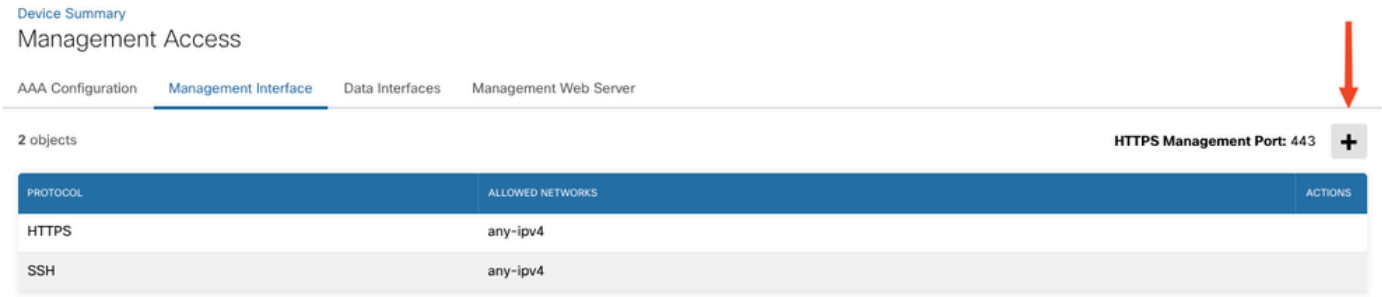
## FDM:

Passaggio 1: Accedere a Firepower Device Manager (FDM) e selezionare Impostazioni di sistema > Accesso gestione > Interfaccia di gestione.



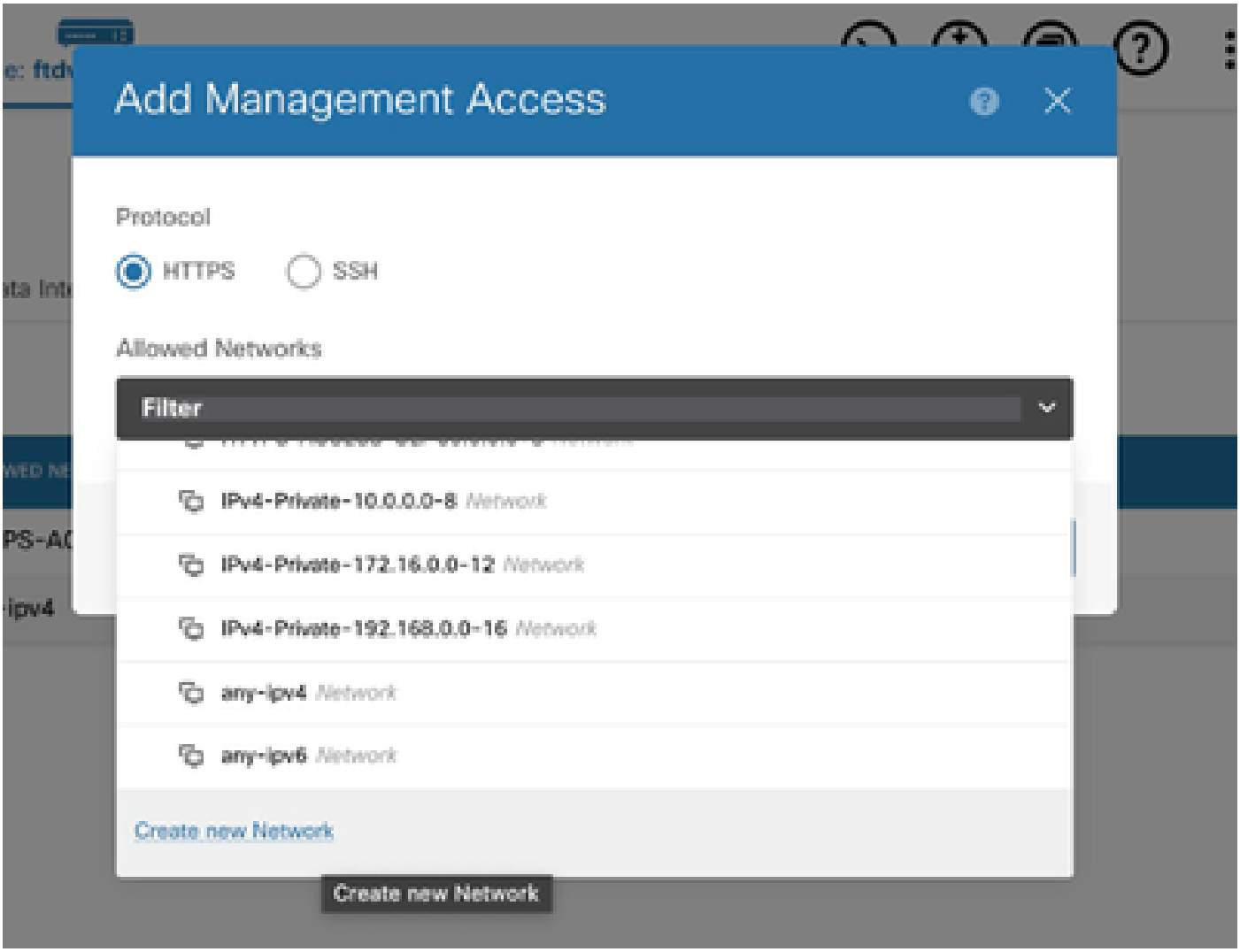
Per impostazione predefinita, l'accesso any-ipv4 è consentito sulla porta di gestione per SSH e HTTPS

Passaggio 2: fare clic sull'icona + per aprire la finestra per l'aggiunta della rete.



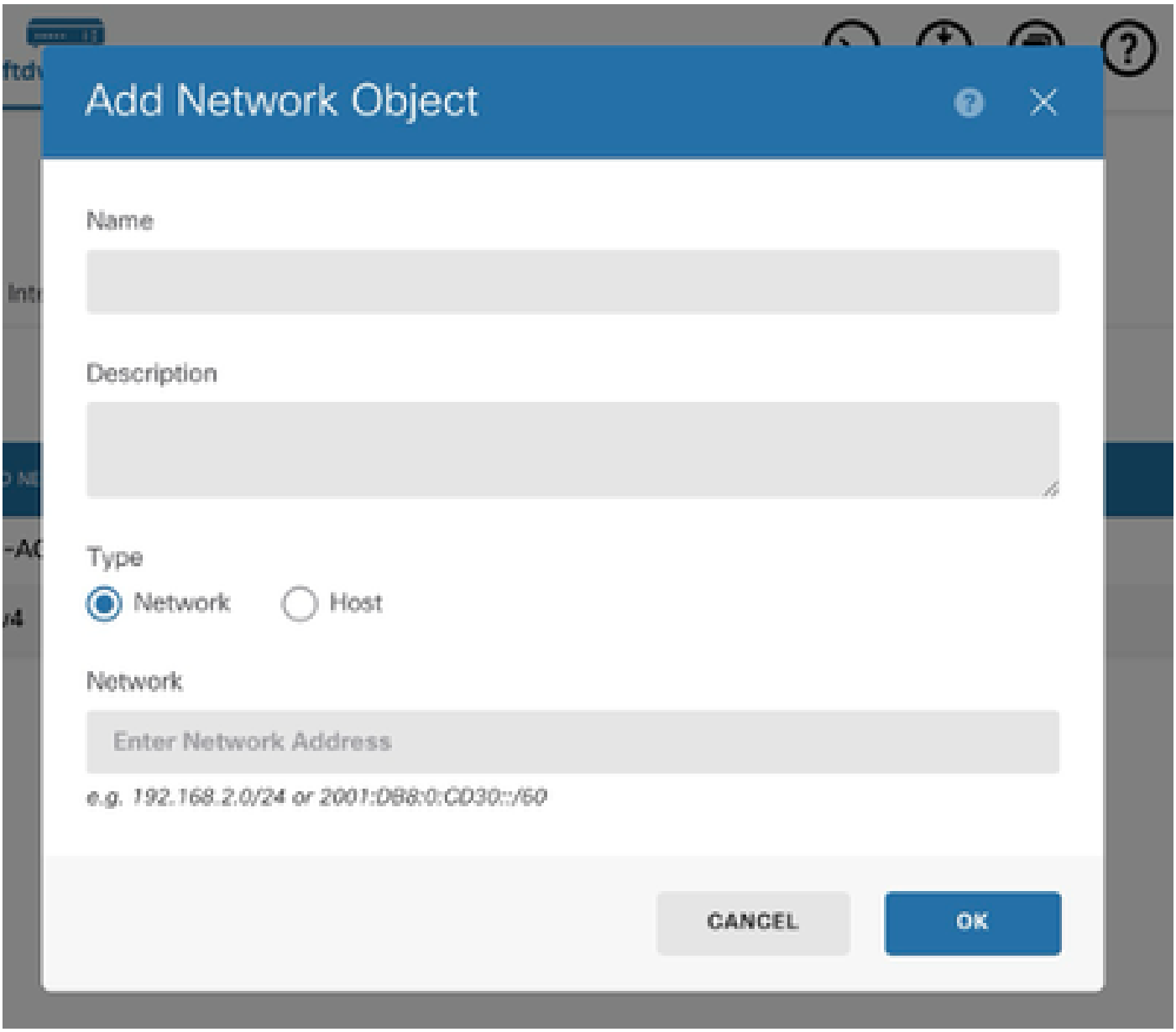

Fare clic sul pulsante Aggiungi in alto a destra.

Passaggio 3: aggiungere l'oggetto di rete per disporre dell'accesso SSH o HTTPS. Se è necessario creare una nuova rete, selezionare l'opzione Crea nuova rete. È possibile aggiungere più voci per reti o host nell'accesso di gestione.



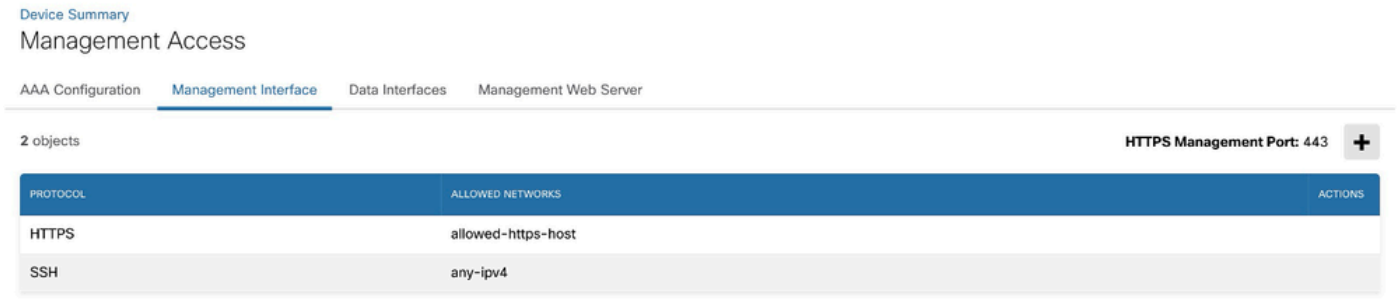

Selezionare la rete.

Passaggio 4 (facoltativo): L'opzione Crea nuova rete apre la finestra Aggiungi oggetto di rete.

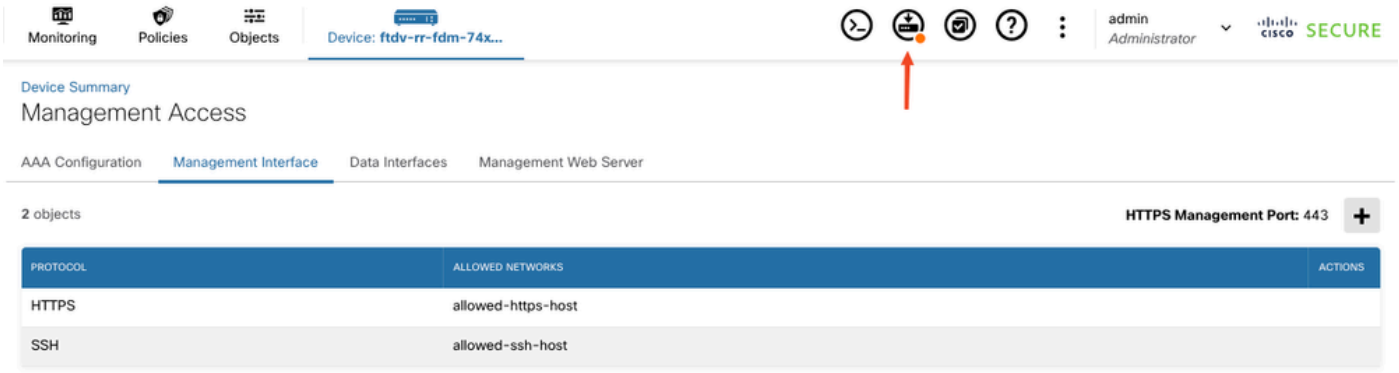



Creare una rete di host in base alle proprie esigenze.

## Passaggio 5: verificare le modifiche apportate e distribuire.

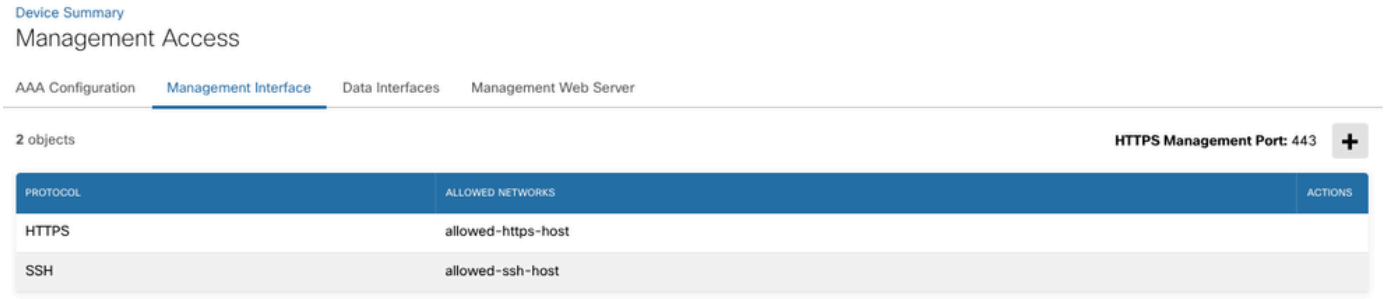



Accesso alla gestione HTTPS modificato. Any-ipv4 viene rimosso.




Distribuisci in FDM

Passaggio 6 (Facoltativo): dopo aver verificato le modifiche apportate in precedenza per HTTPS, ripetere lo stesso operazione per SSH.




Aggiunto oggetto di rete per SSH e HTTPS.

Passaggio 7: Infine, distribuire le modifiche e verificare l'accesso all'FTD dalla rete e dall'host consentiti.

## Fasi di CLISH:

I passaggi CLI possono essere utilizzati in caso di gestione di FDM o FMC.

Per configurare il dispositivo in modo che accetti connessioni HTTPS o SSH da indirizzi IP o rete specificati, utilizzare`configure https-access-list`il `configure ssh-access-list` comando teorico.

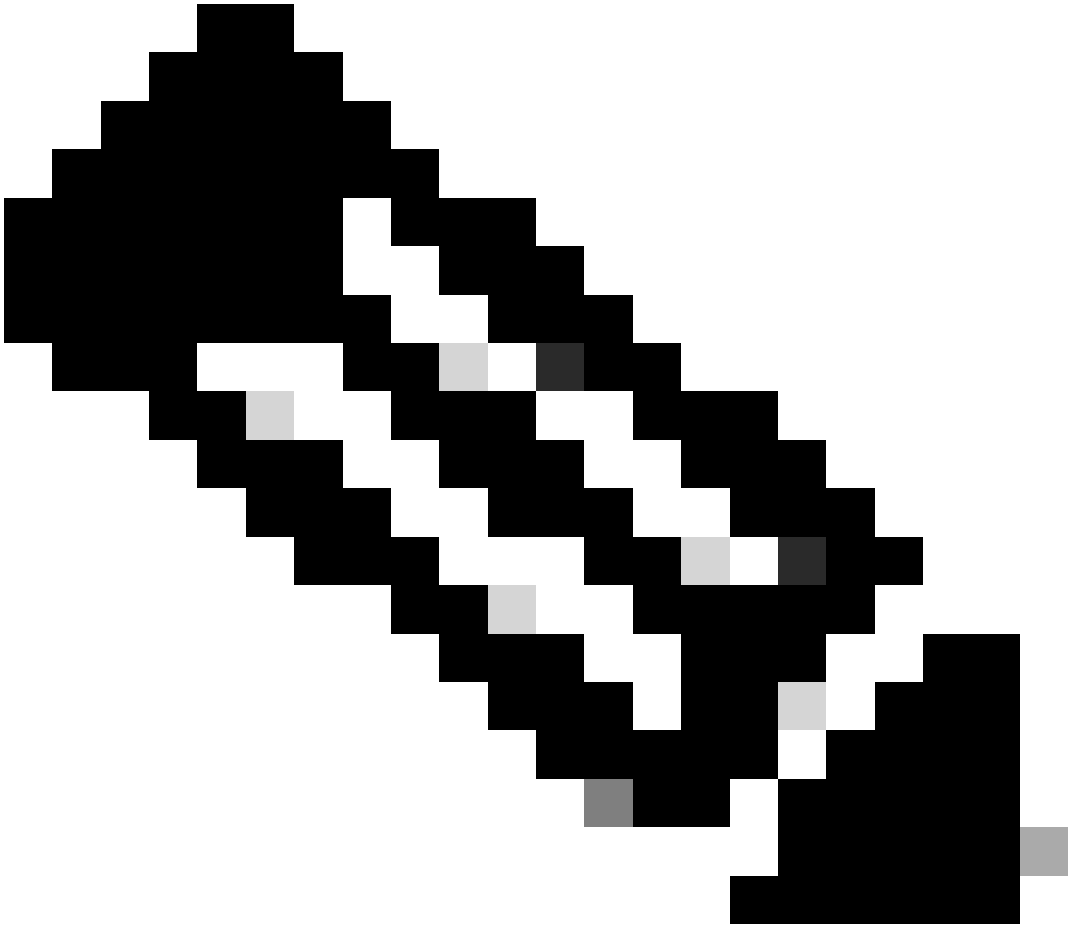
- È necessario includere tutti gli host o le reti supportate in un unico comando. Gli indirizzi specificati in questo comando sovrascrivono il contenuto corrente del rispettivo elenco degli accessi.
- Se il dispositivo è un'unità in un gruppo di disponibilità elevata gestito localmente, la modifica sovrascrive la volta successiva che l'unità attiva distribuisce gli aggiornamenti della configurazione. Se si tratta dell'unità attiva, la modifica viene propagata al peer durante la distribuzione.

```
> 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
```

---



Nota: x.x.x.x/x e y.y.y/y rappresentano l'indirizzo ipv4 con notazione CIDR.

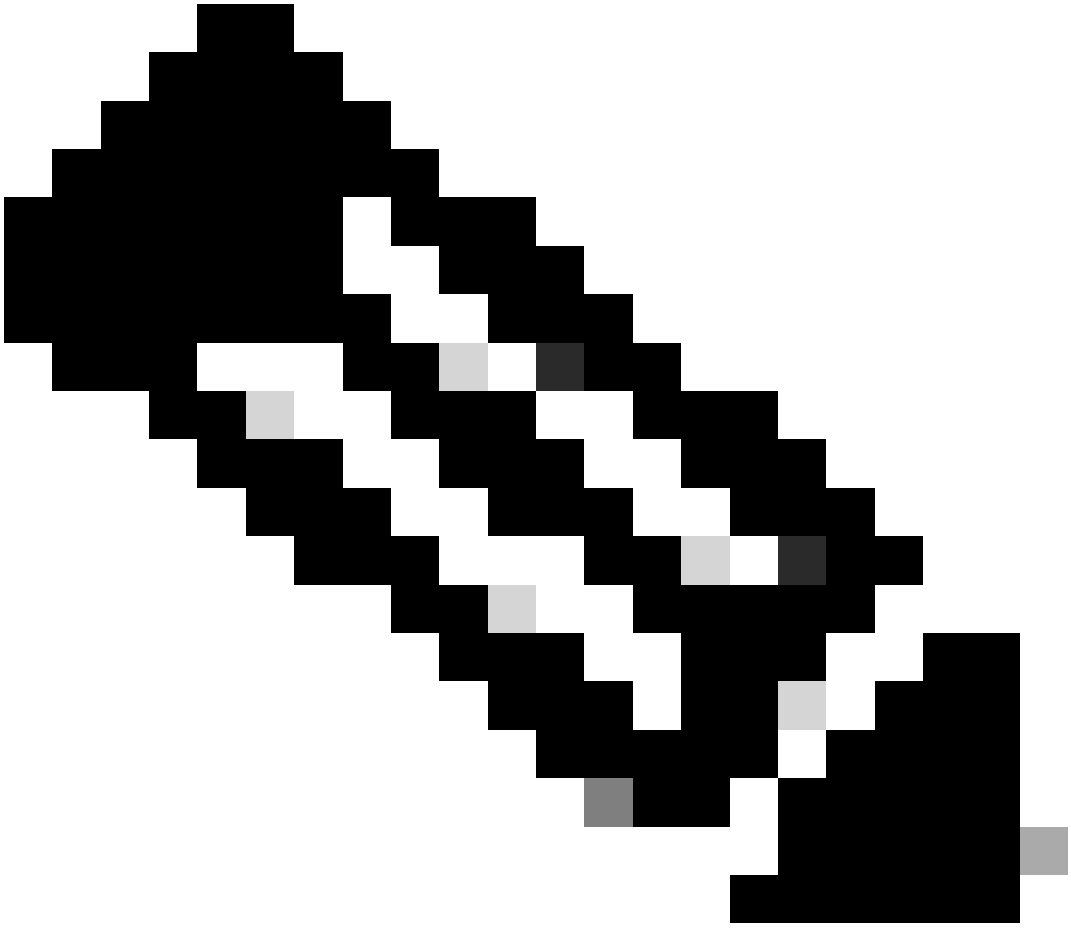
---

Analogamente, per le connessioni SSH, usare`configure ssh-access-list`il comando con uno o più comandi separati.

```
> 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
```



Nota: È possibile utilizzare i comandi **configure disable-https-access** oconfigure disable-ssh-accessper disabilitare l'accesso HTTPS o SSH, rispettivamente. Accertarsi di essere a conoscenza di queste modifiche in quanto ciò può bloccare l'utente fuori dalla sessione.

## Verifica

Per verificare da CLISH è possibile utilizzare i seguenti comandi:

```
> 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
```

# Riferimenti

Guida di riferimento ai comandi di Cisco Secure Firewall Threat Defense

Guida alla configurazione di Cisco Firepower Threat Defense per Firepower Device Manager

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).