

Configurazione dei criteri di controllo di accesso del Control Plane per la difesa dalle minacce del firewall protetto e l'appliance ASA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazioni](#)

[Configurazione di un ACL del control plane per FTD gestito da FMC](#)

[Configurare un ACL del control plane per FTD gestito da FDM](#)

[Configurazione di un ACL del control plane per un'ASA tramite CLI](#)

[Configurazione alternativa per bloccare gli attacchi per un firewall protetto tramite il comando 'shun'](#)

[Verifica](#)

[Bug correlati](#)

Introduzione

In questo documento viene descritto il processo di configurazione delle regole di accesso al control plane per Secure Firewall Threat Defense e Adaptive Security Appliance (ASA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Secure Firewall Threat Defense (FTD)
- Secure Firewall Device Manager (FDM)
- Centro gestione firewall protetto (FMC)
- Secure Firewall ASA
- Access Control List (ACL)
- FlexConfiguration

Componenti usati

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

hardware:

- Secure Firewall Threat Defense versione 7.2.5
- Secure Firewall Manager Center versione 7.2.5
- Secure Firewall Device Manager versione 7.2.5
- Secure Firewall ASA versione 9.18.3

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

Il traffico in genere attraversa un firewall e viene instradato tra le interfacce dati; in alcune circostanze, è utile impedire il traffico destinato al firewall sicuro. Il firewall sicuro Cisco può utilizzare un ACL (Control-Plane Access Control List) per limitare il traffico "diretto". Un esempio di quando un ACL control-plane può essere utile è controllare quali peer possono stabilire un tunnel VPN (da sito a sito o VPN ad accesso remoto) per il firewall sicuro.

Protezione del traffico "through-the-box" del firewall

Il traffico in genere attraversa i firewall da un'interfaccia (in entrata) a un'altra interfaccia (in uscita). Questo tipo di traffico è noto come traffico "through-the-box" ed è gestito da entrambe le regole, ACP (Access Control Policies) e Pre-filter.

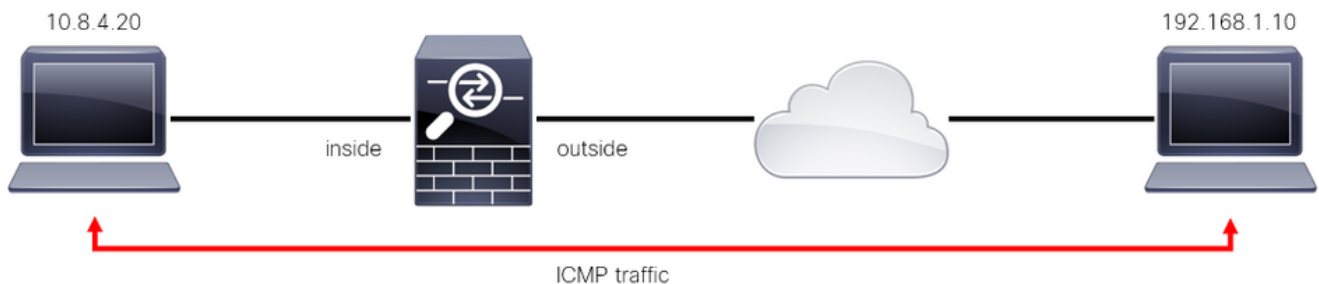


Immagine 1. Esempio di traffico integrato

Protezione del traffico "diretto" del firewall

In altri casi, il traffico è destinato direttamente a un'interfaccia FTD (da sito a sito o VPN ad accesso remoto), ovvero al traffico "diretto", ed è gestito dal control plane dell'interfaccia specifica.

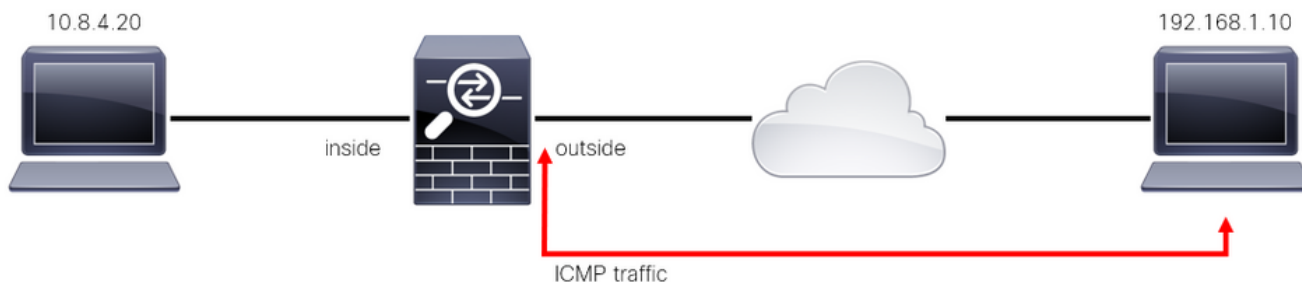


Immagine 2. Esempio di traffico diretto

Considerazioni importanti sugli ACL dei Control Plane

- A partire dalla versione 7.0 di FMC/FTD, un ACL del control plane deve essere configurato utilizzando FlexConfig, utilizzando la stessa sintassi del comando utilizzata sull'appliance ASA.
- La parola chiave control-plane viene aggiunta alla configurazione del gruppo di accesso, che attiverà il traffico 'verso' l'interfaccia protetta del firewall. Senza la parola control-plane aggiunta al comando, l'ACL limiterebbe il traffico 'attraverso' il firewall protetto.
- Un ACL control-plane non limita il protocollo SSH, ICMP o TELNET in entrata a un'interfaccia firewall sicura. Questi vengono elaborati (consentiti/negati) in base ai criteri di impostazioni della piattaforma e hanno una precedenza più alta.
- Un ACL control-plane restringe il traffico 'verso' il firewall sicuro stesso, mentre i criteri di controllo dell'accesso per l'FTD o gli ACL normali per l'ASA controllano il traffico 'attraverso' il firewall sicuro.
- A differenza di un ACL normale, alla fine dell'ACL non è presente un 'rifiuto' implicito.
- Al momento della creazione del documento, la funzione di georilevazione FTD non può essere utilizzata per limitare l'accesso 'a' FTD.

Configurazione

Nell'esempio successivo, un gruppo di indirizzi IP di un determinato paese cerca di forzare la VPN nella rete tentando di accedere all'FTD RAVPN. L'opzione migliore per proteggere l'FTD da questi attacchi VPN con forza bruta è configurare un ACL del control plane in modo da bloccare queste connessioni all'interfaccia FTD esterna.

Configurazioni

Configurazione di un ACL del control plane per FTD gestito da FMC

Questa è la procedura da seguire in un FMC per configurare un ACL del control plane in modo da bloccare gli attacchi VPN con forza bruta in arrivo sull'interfaccia FTD esterna:

Passaggio 1. Aprire l'interfaccia grafica utente (GUI) di FMC tramite HTTPS ed eseguire l'accesso con le credenziali dell'utente.



Immagine 3. Pagina Log In di FMC

Passaggio 2. È necessario creare un ACL esteso. A tale scopo, selezionare Oggetti > Gestione oggetti.

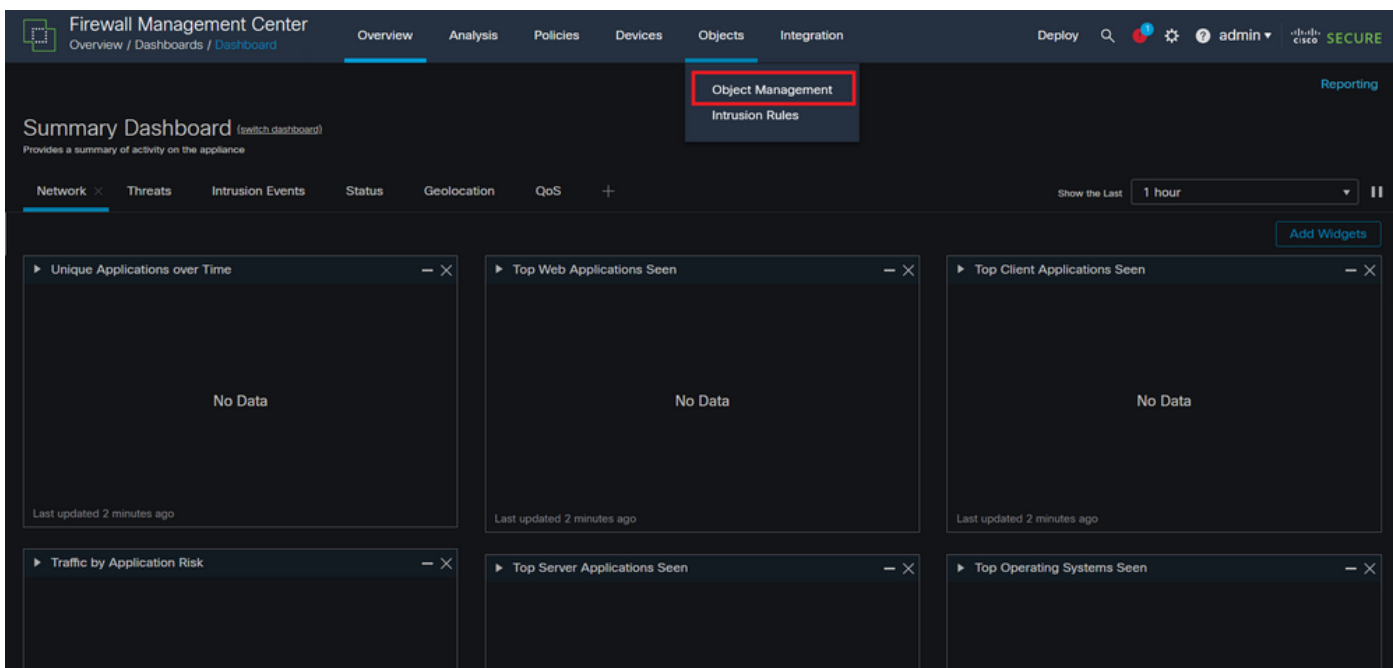


Immagine 4. Gestione oggetti

Passaggio 2.1. Dal pannello di sinistra, selezionare Access List > Extended (Elenco accessi > Esteso) per creare un ACL esteso.

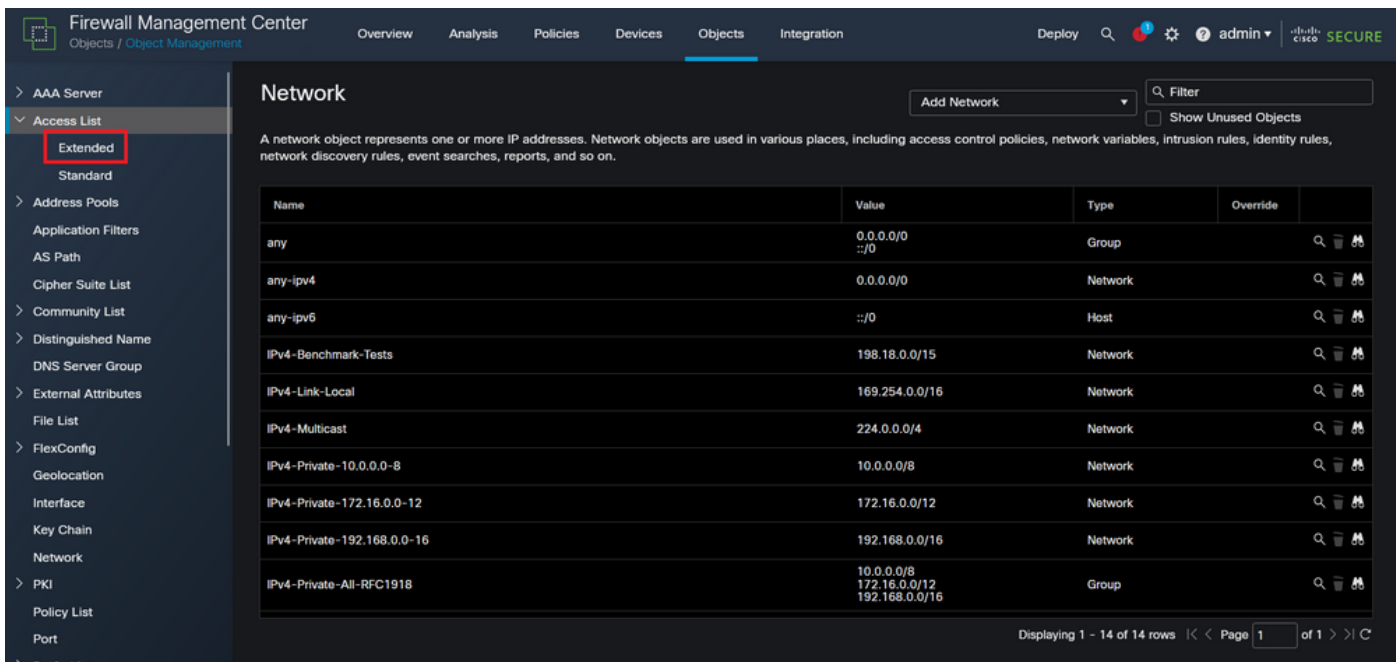


Immagine 5. Menu ACL esteso

Passaggio 2.2. Quindi, selezionare Aggiungi elenco accessi esteso.

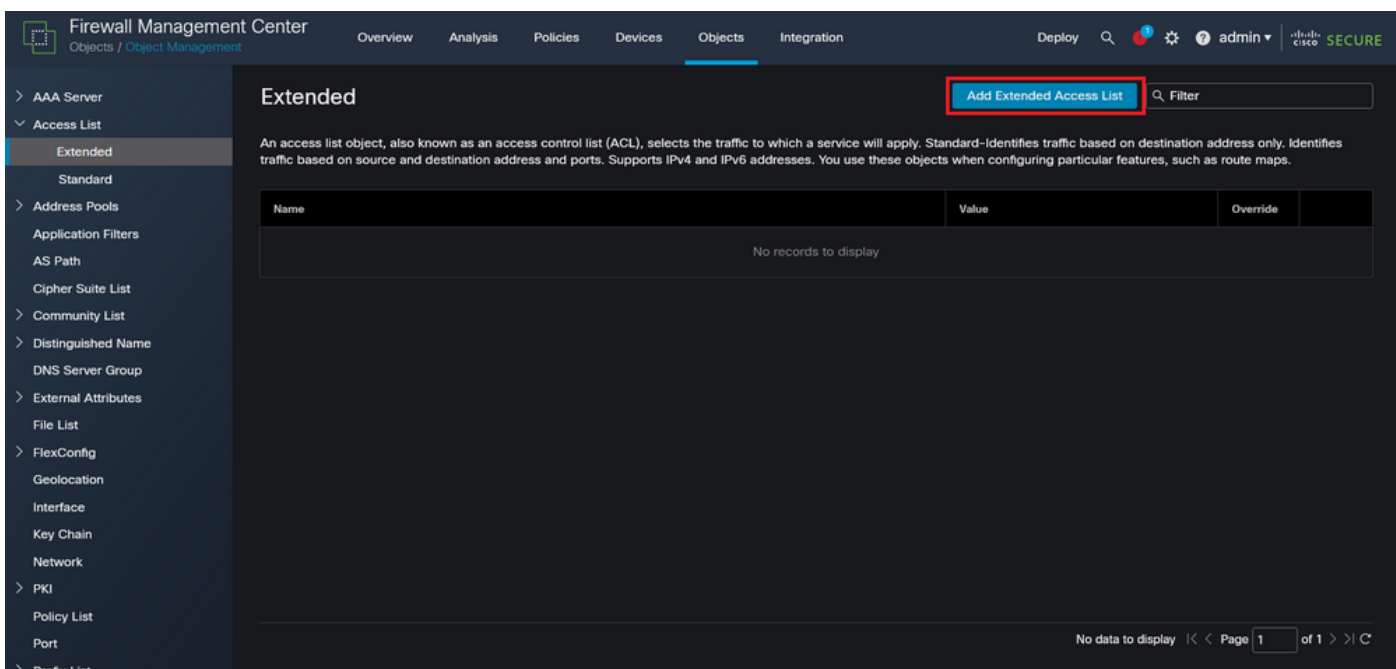


Immagine 6. Aggiungi ACL esteso

Passaggio 2.3. Digitare un nome per l'ACL esteso e quindi fare clic sul pulsante Aggiungi per creare una voce di controllo di accesso (ACE):

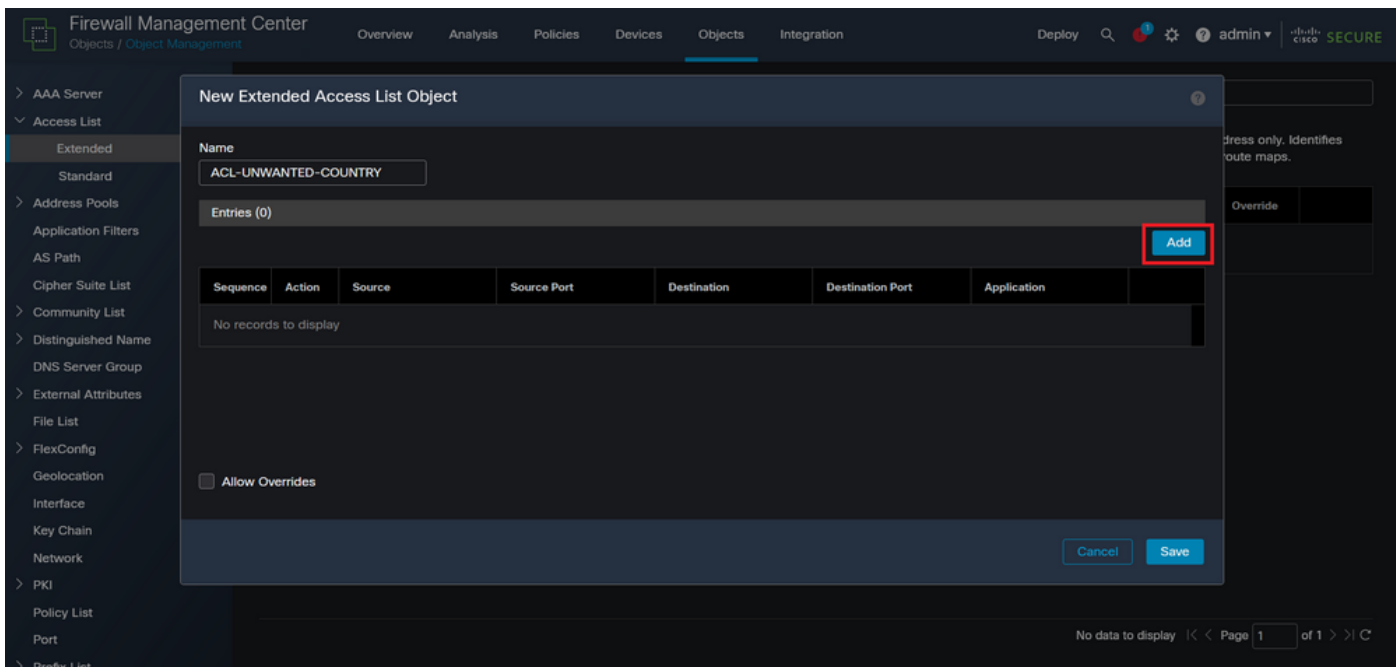


Immagine 7. Voci ACL estese

Passaggio 2.4. Modificare l'azione ACE in Blocca, quindi aggiungere la rete di origine in modo che corrisponda al traffico che deve essere rifiutato all'FTD, mantenere la rete di destinazione come Qualsiasi e fare clic sul pulsante Aggiungi per completare la voce ACE:

- Nell'esempio, la voce ACE configurata bloccherà gli attacchi di forza bruta VPN provenienti dalla subnet 192.168.1.0/24.

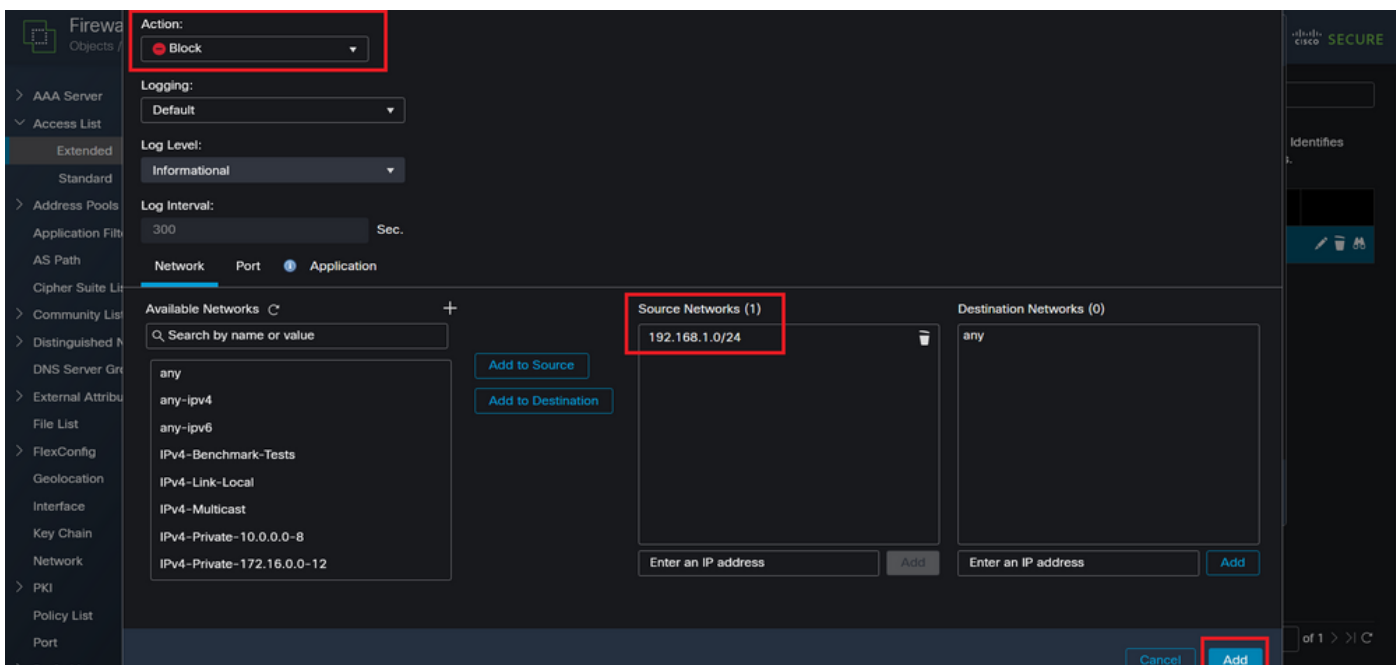


Immagine 8. Reti negate

Passaggio 2.5. Se è necessario aggiungere altre voci ACE, fare di nuovo clic sul pulsante Aggiungi e ripetere il passaggio 2.4. Quindi, fare clic sul pulsante Save (Salva) per completare la configurazione dell'ACL.

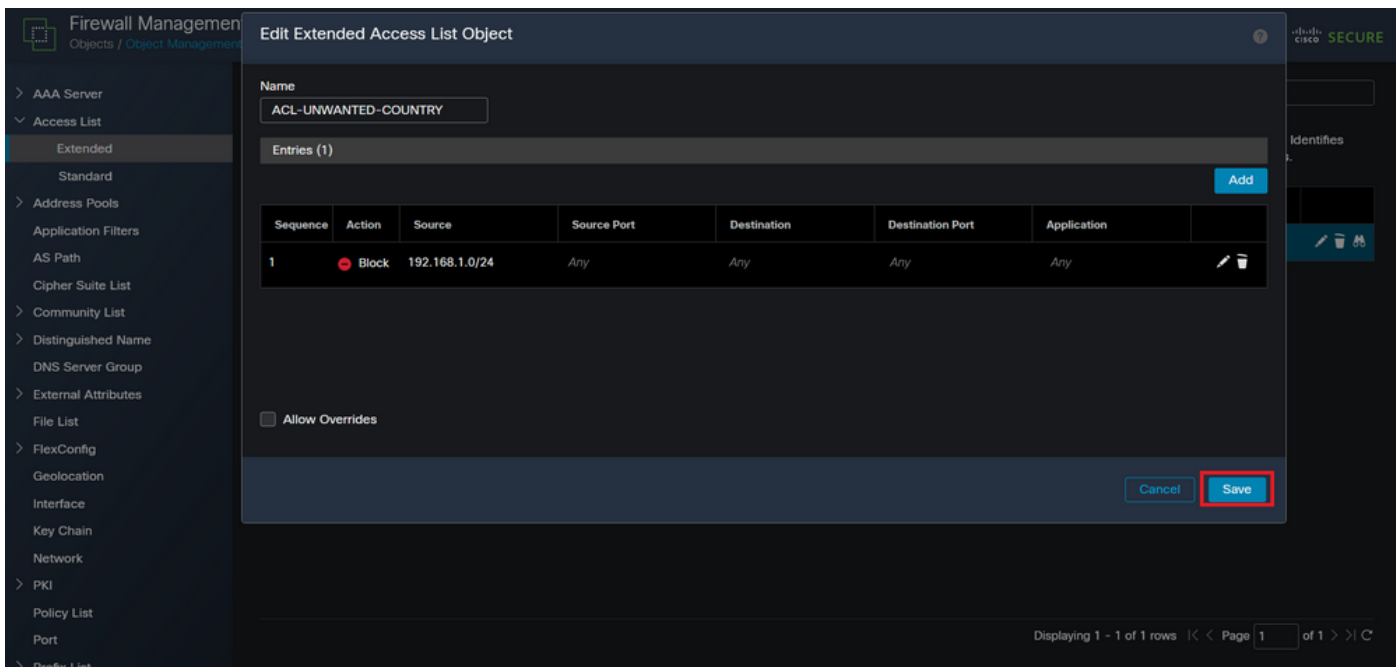


Immagine 9. Voci ACL estese completate

Passaggio 3. Quindi, è necessario configurare un oggetto Flex-Config per applicare l'ACL del piano di controllo all'interfaccia FTD esterna. A tale scopo, spostarsi nel pannello sinistro e selezionare l'opzione FlexConfig > Oggetto FlexConfig.

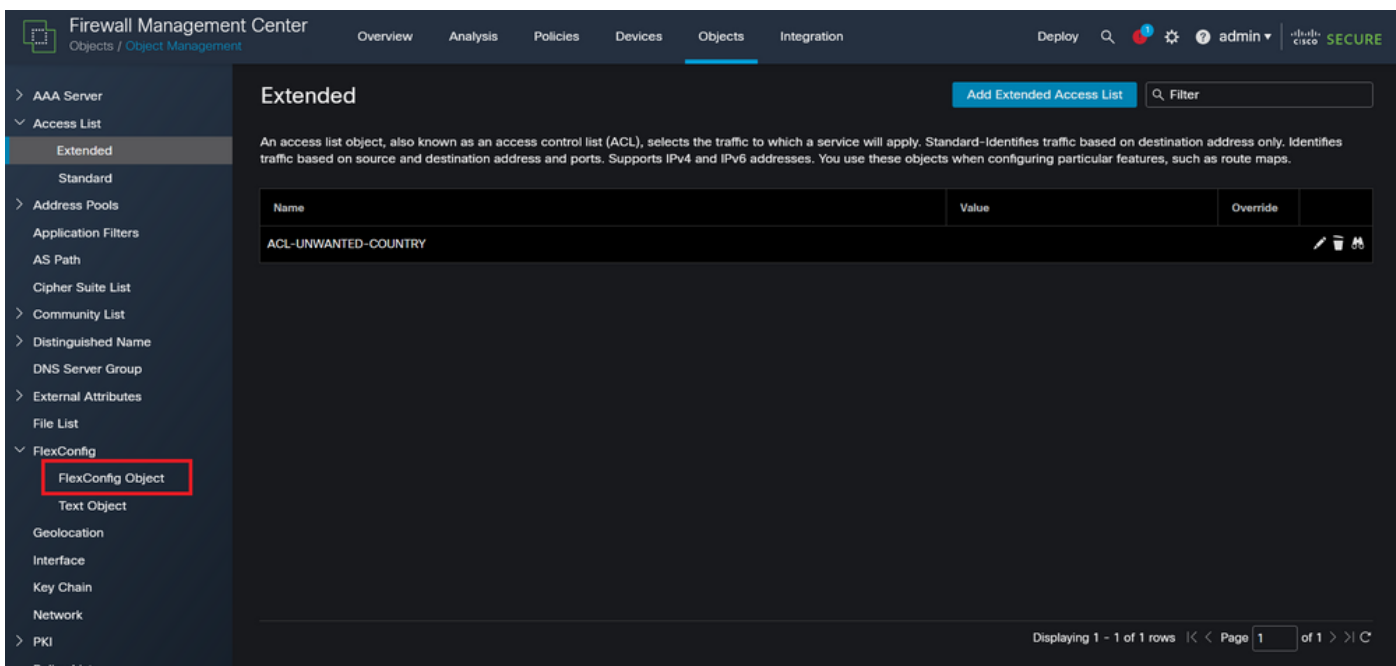


Immagine 10. Menu Oggetto FlexConfig

Passaggio 3.1. Fare clic su Aggiungi oggetto FlexConfig.

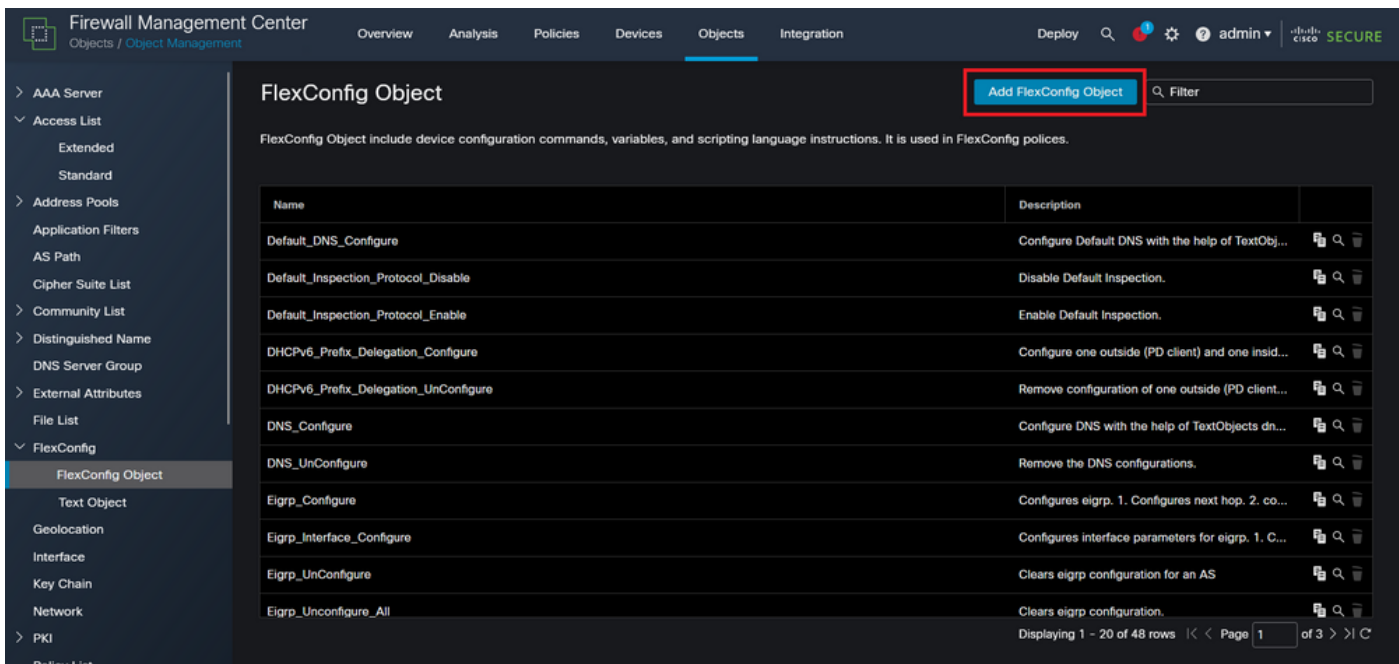


Immagine 11. Aggiungi oggetto Flexconfig

Passaggio 3.2. Aggiungere un nome per l'oggetto FlexConfig, quindi inserire un oggetto criterio ACL. A tale scopo, selezionare Inserisci > Inserisci oggetto criterio > Oggetto ACL esteso.

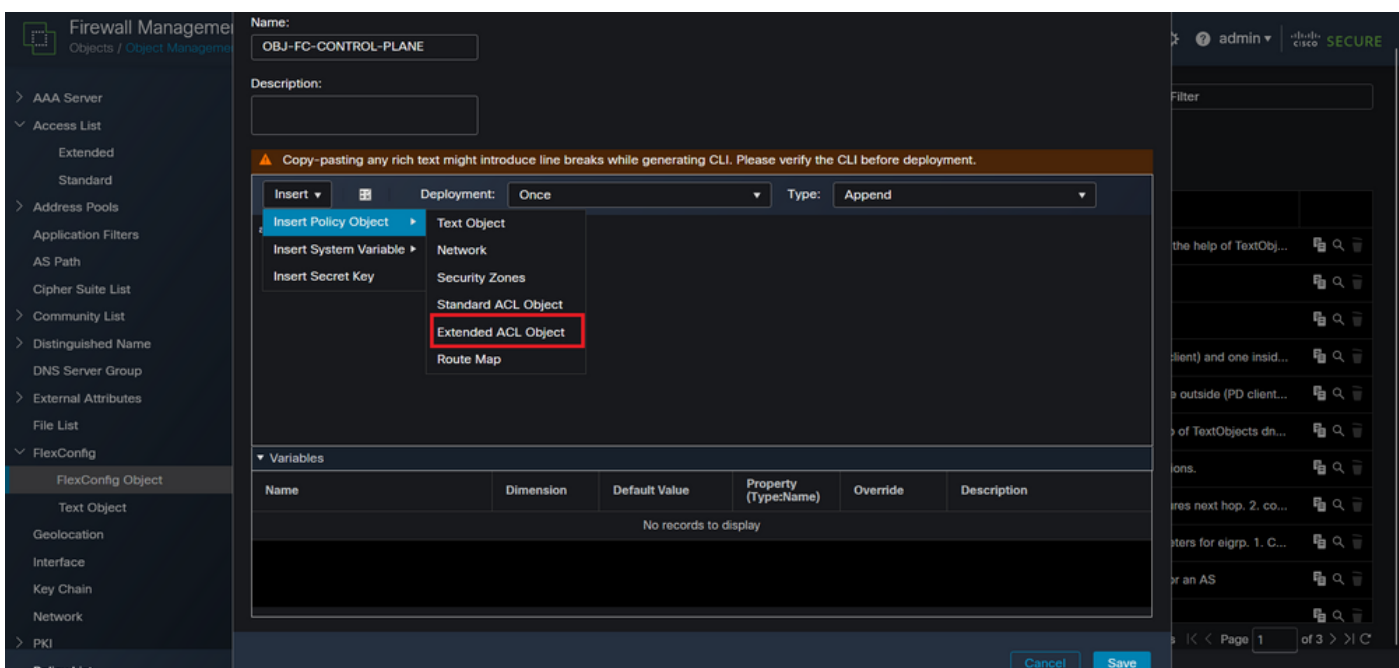


Immagine 12. Variabile oggetto FlexConfig

Passaggio 3.3. Aggiungere un nome per la variabile oggetto ACL e quindi selezionare l'ACL esteso creato nel passaggio 2.3. Quindi, fare clic sul pulsante Save (Salva).

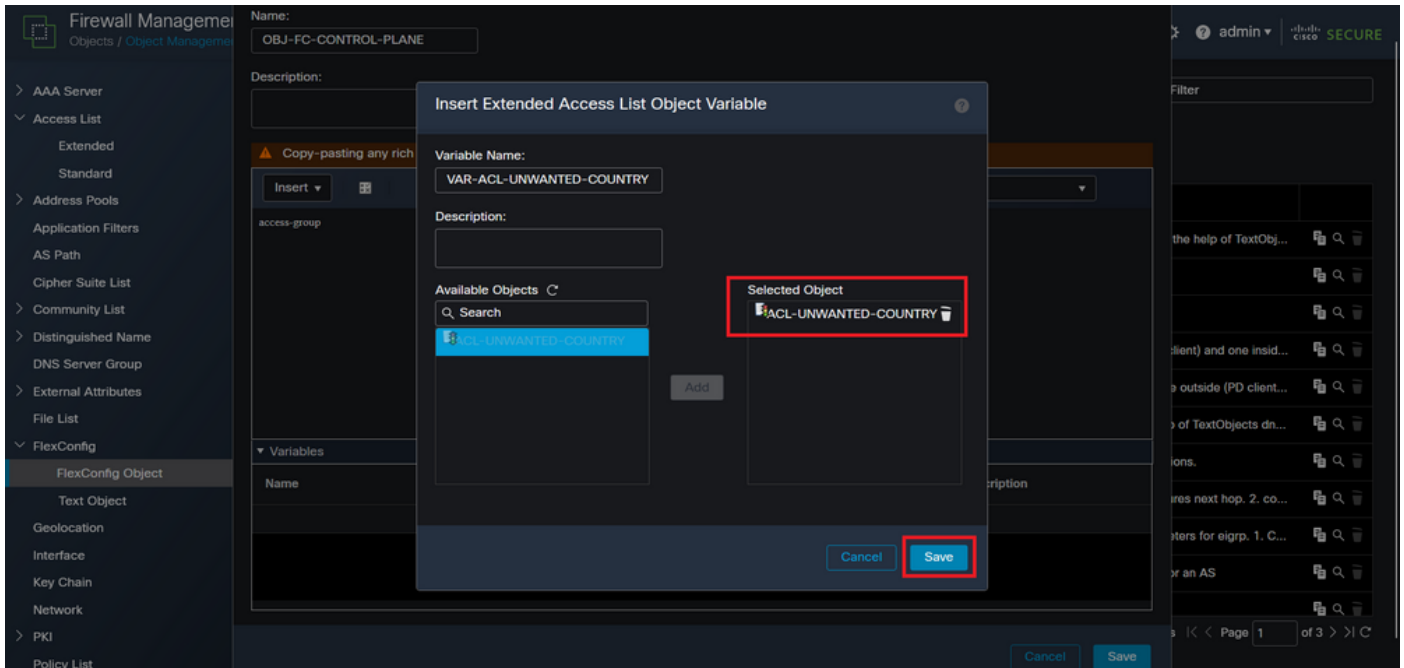


Immagine 13. Assegnazione ACL variabile oggetto FlexConfig

Passaggio 3.4. Quindi, configurare l'ACL del piano di controllo come in entrata per l'interfaccia esterna nel modo seguente.

Sintassi della riga di comando:

```
access-group "variable name starting with $ symbol" in interface "interface-name" control-plane
```

In questo esempio viene illustrato il comando successivo, che utilizza la variabile ACL creata nel passaggio 2.3 'VAR-ACL-UNWANTED-COUNTRY' come segue:

```
access-group $VAR-ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Per completare l'oggetto FlexConfig, selezionare il pulsante Save (Salva) nella finestra oggetto FlexConfig.

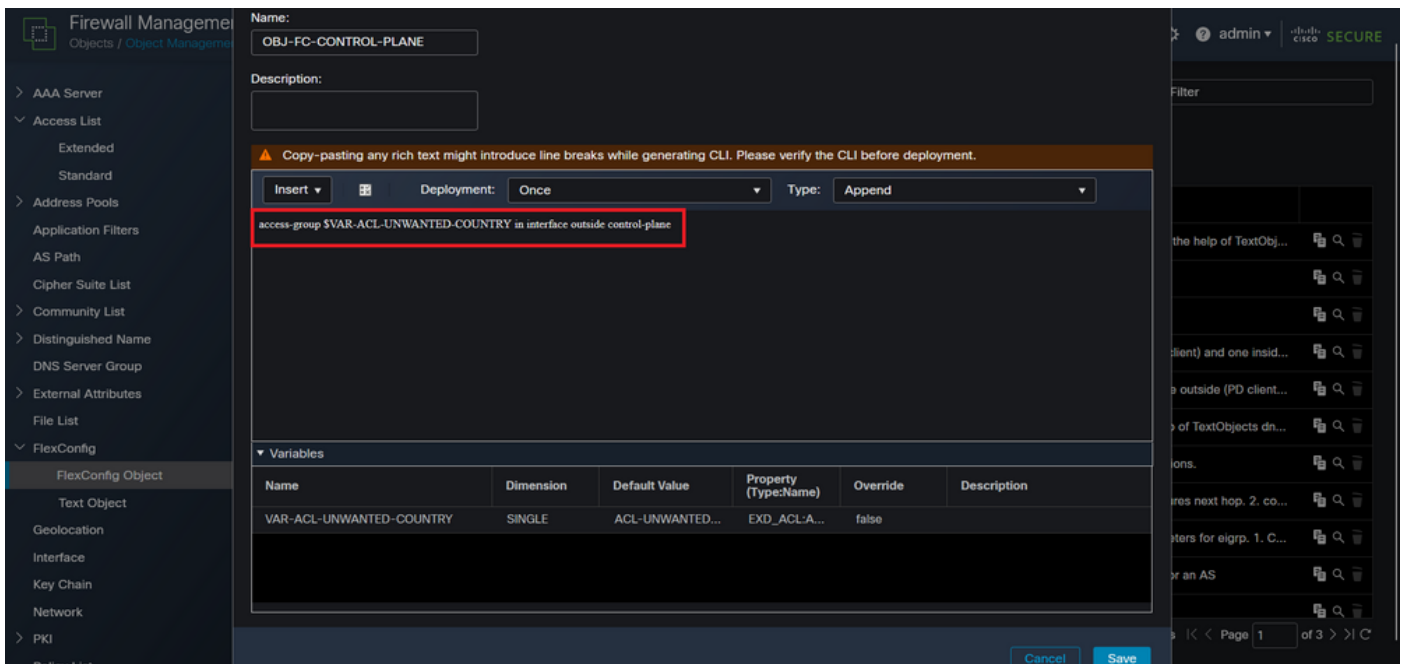


Immagine 14. Riga di comando per il completamento dell'oggetto Flexconfig

Passaggio 4. È necessario applicare la configurazione dell'oggetto FlexConfig all'FTD. A tale scopo, selezionare Dispositivi > FlexConfig.

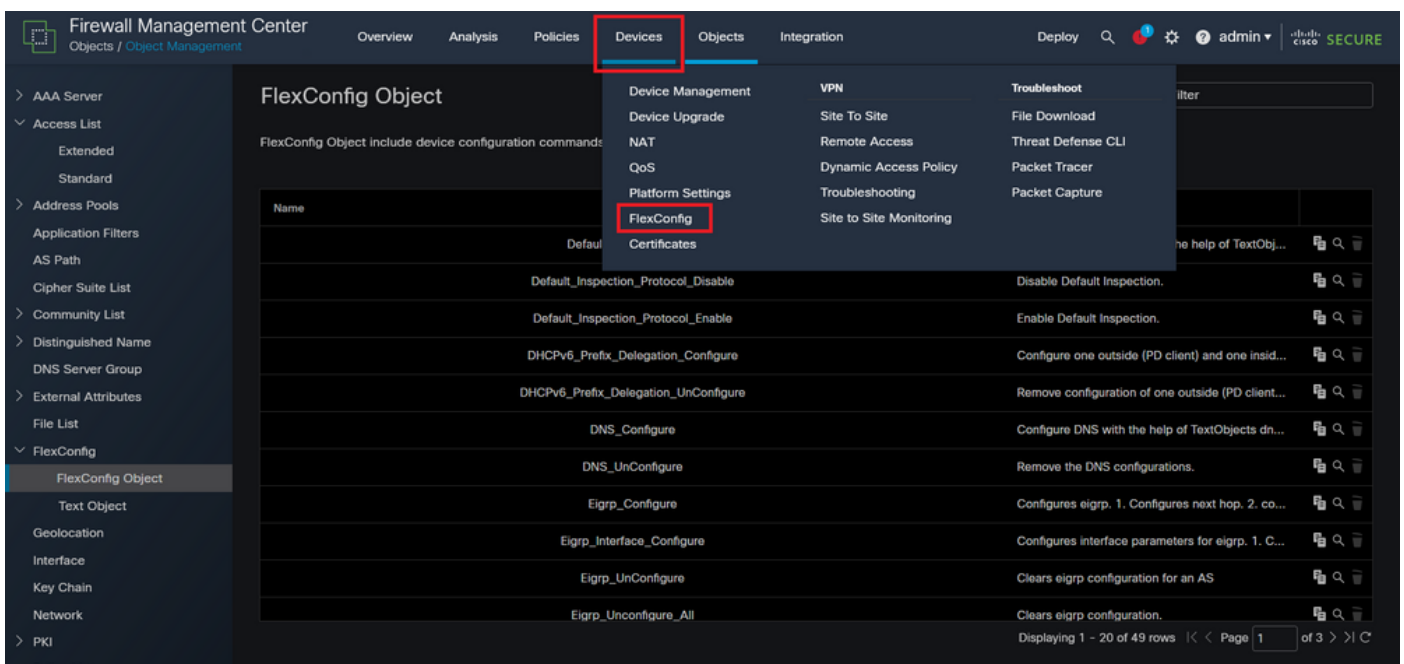


Immagine 15. Menu criteri di FlexConfig

Passaggio 4.1. Quindi, fare clic su Nuovo criterio se non è già stato creato un FlexConfig per il FTD o modificare il criterio FlexConfig esistente.

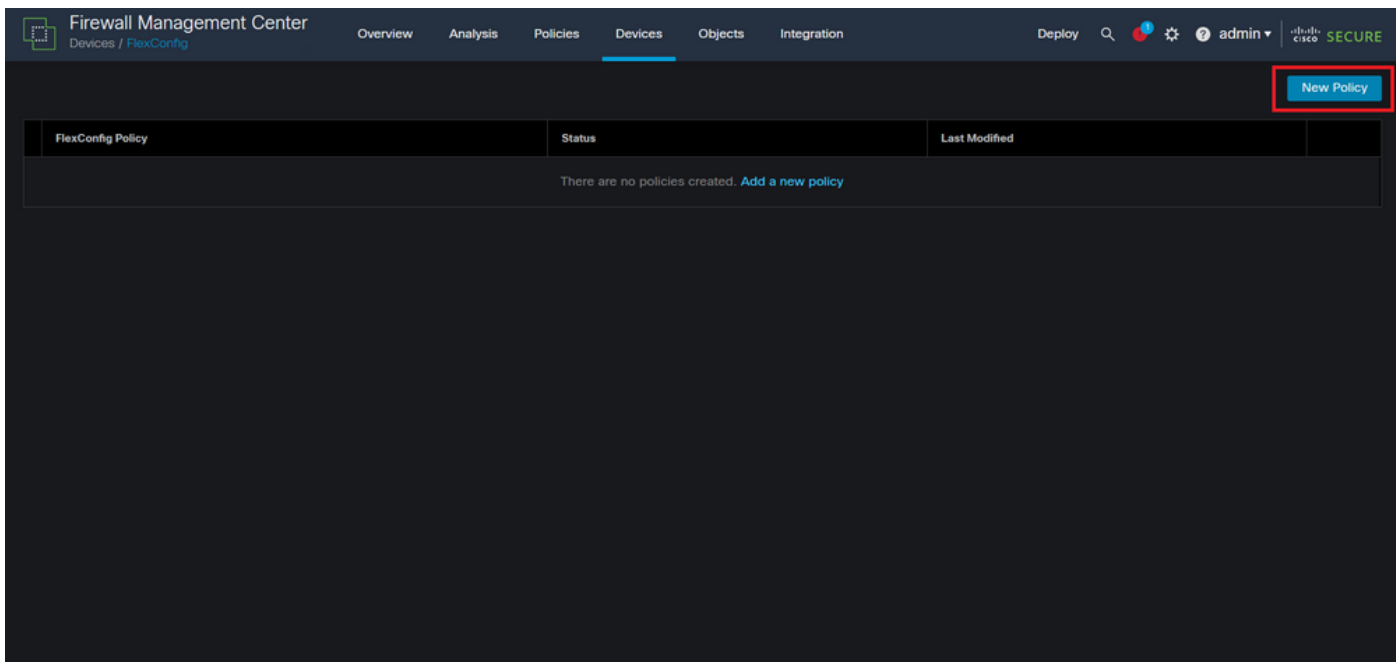


Immagine 16. Creazione criteri FlexConfig

Passaggio 4.2. Aggiungere un nome per il nuovo criterio FlexConfig e selezionare l'FTD a cui si desidera applicare l'ACL del control plane creato.

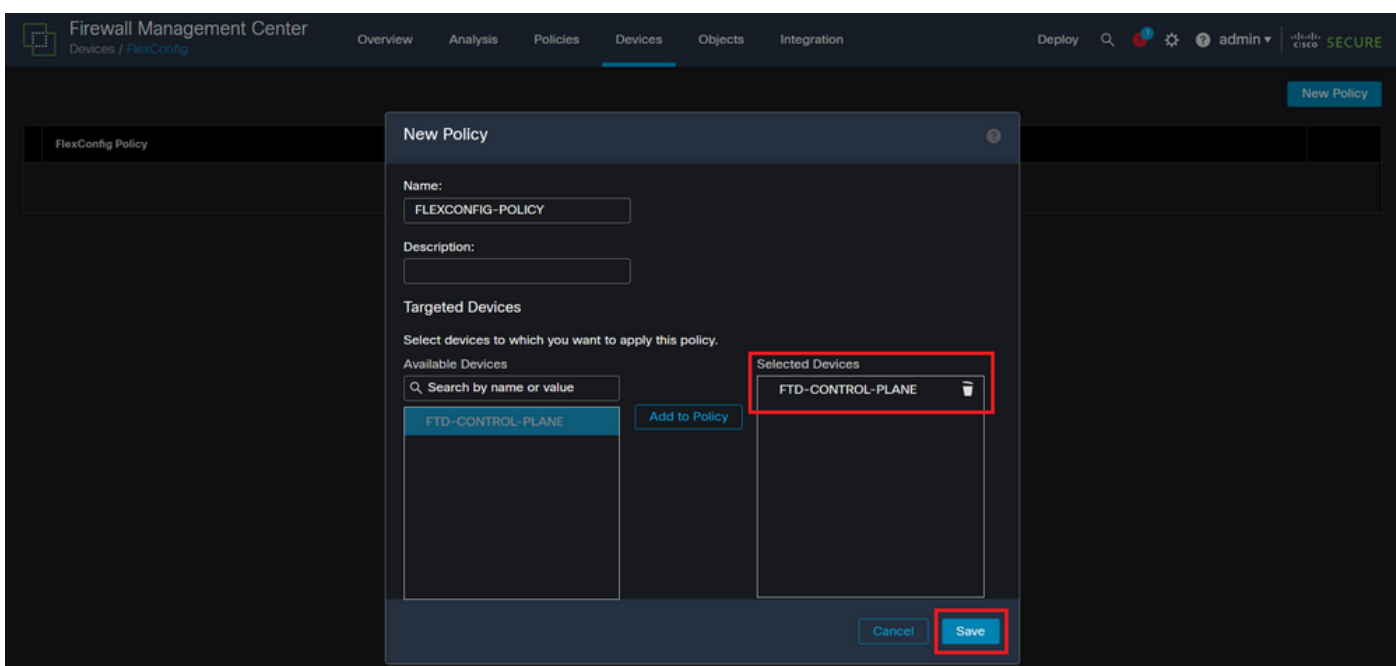


Immagine 17. Assegnazione dispositivo criteri FlexConfig

Passaggio 4.3. Dal pannello sinistro, cercare l'oggetto FlexConfig creato nel passaggio precedente 3.2, quindi aggiungerlo al criterio FlexConfig facendo clic sulla freccia destra al centro della finestra, quindi fare clic sul pulsante Salva.

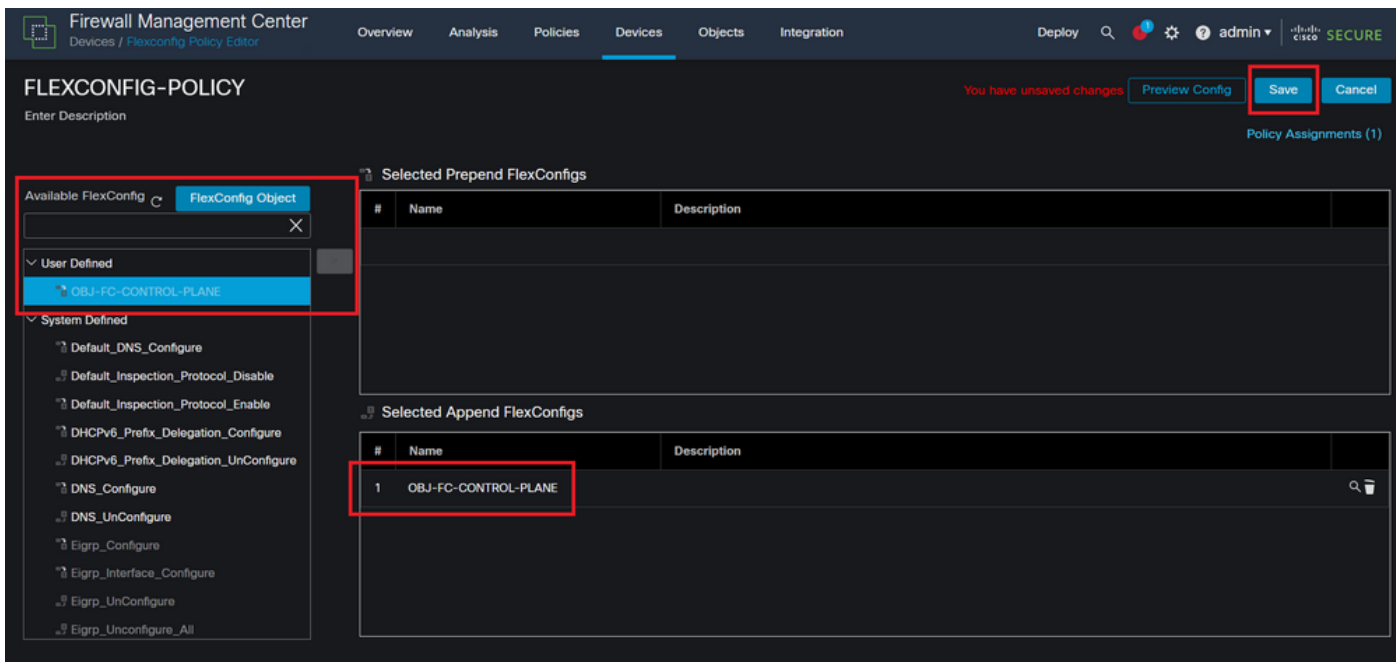


Immagine 18. Assegnazione oggetto criteri FlexConfig

Passaggio 5. Continuare a distribuire la modifica della configurazione nell'FTD. Per questo, passare a Distribuisci > Distribuzione avanzata.

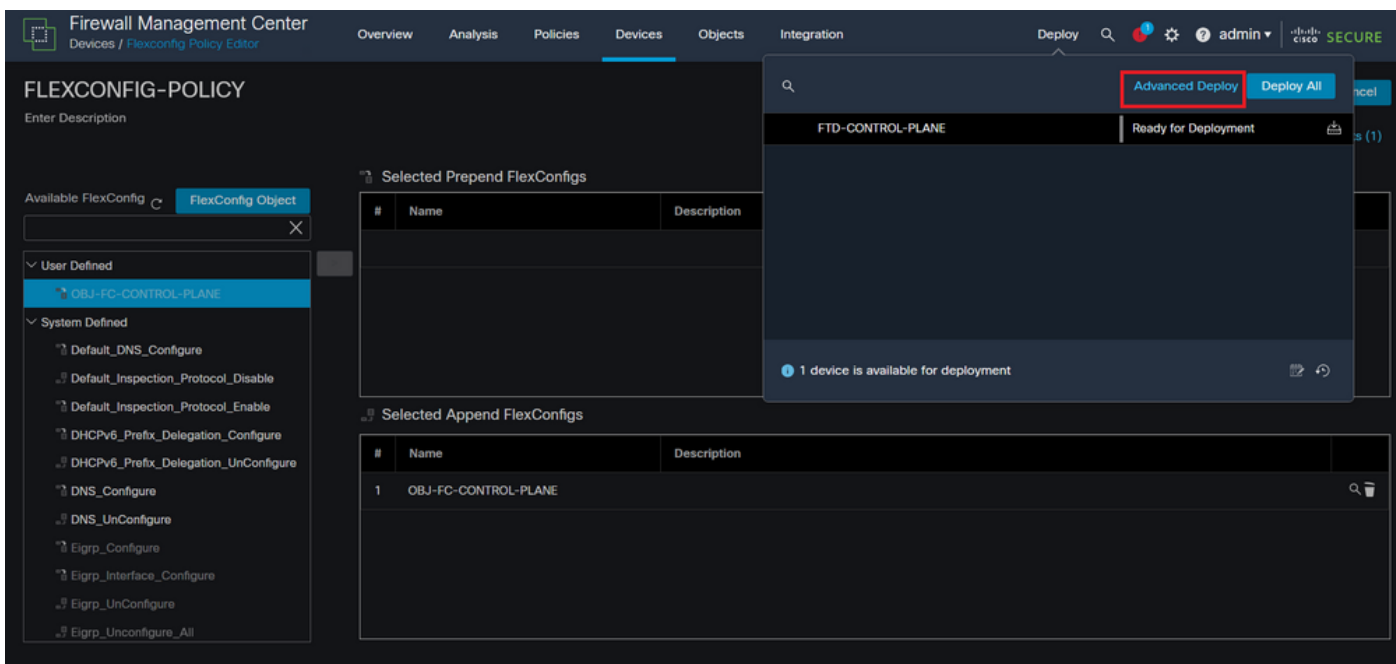


Immagine 19. Distribuzione avanzata FTD

Passaggio 5.1. Quindi, selezionare l'FTD a cui si desidera applicare il criterio FlexConfig. Se tutto è corretto, fare clic su Distribuisci.

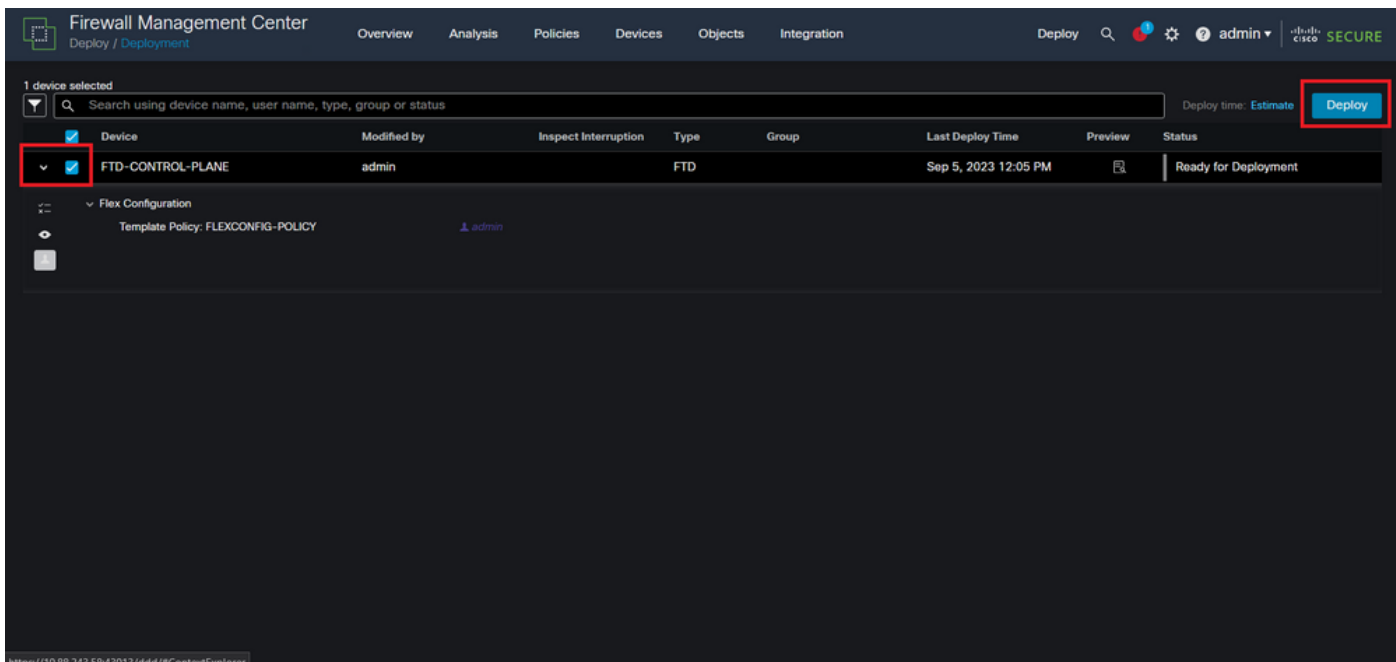


Immagine 20. Convalida distribuzione FTD

Passaggio 5.2. Al termine, verrà visualizzata una finestra di conferma della distribuzione, verrà aggiunto un commento per tenere traccia della distribuzione e si procederà alla distribuzione.

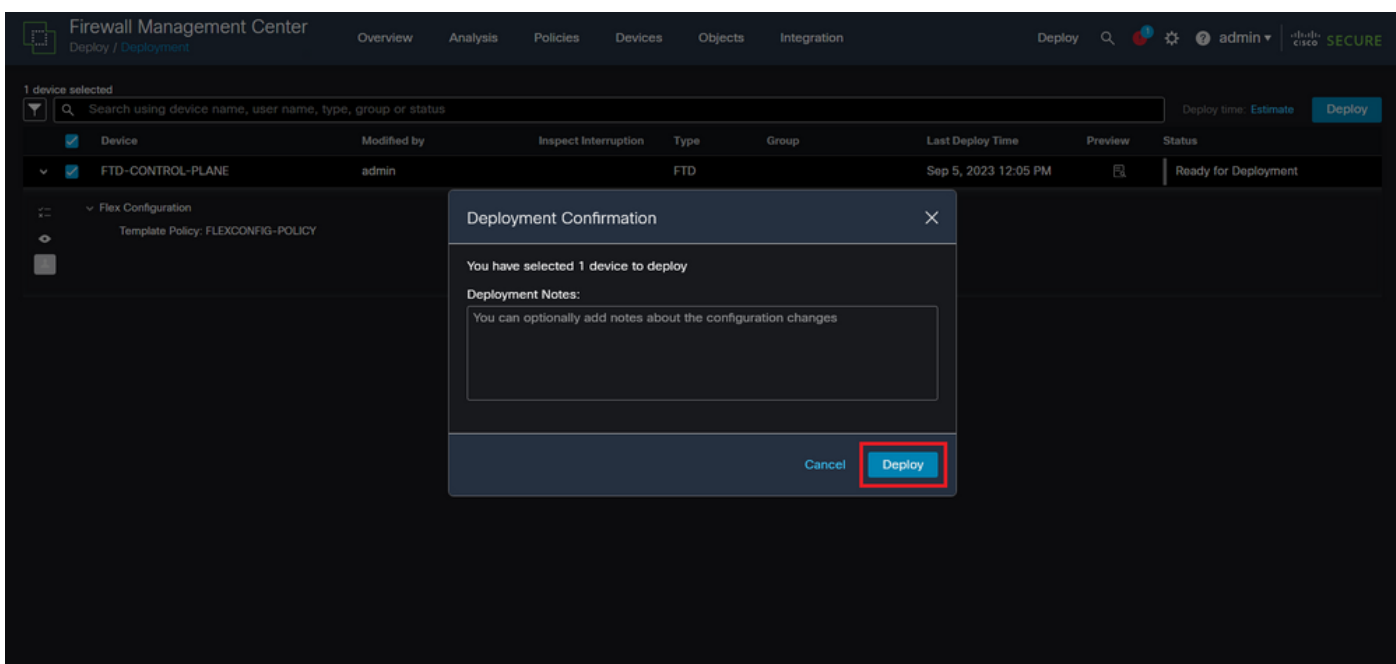


Immagine 21. Commenti distribuzione FTD

Passaggio 5.3. Durante la distribuzione delle modifiche di FlexConfig potrebbe essere visualizzato un messaggio di avviso. Fare clic su Distribuisci solo se si è completamente certi che la configurazione dei criteri sia corretta.

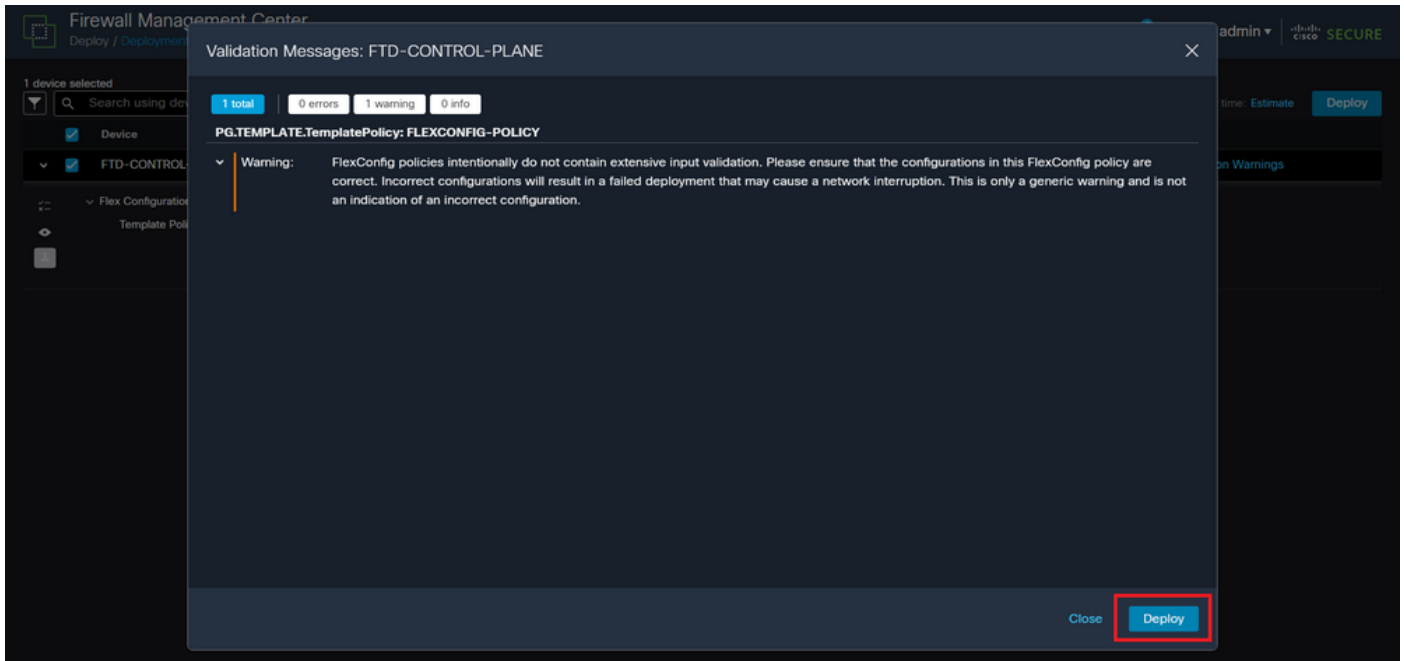


Immagine 22. Avviso Flexconfig di distribuzione FTD

Passaggio 5.4. Confermare che la distribuzione dei criteri per l'FTD è riuscita.

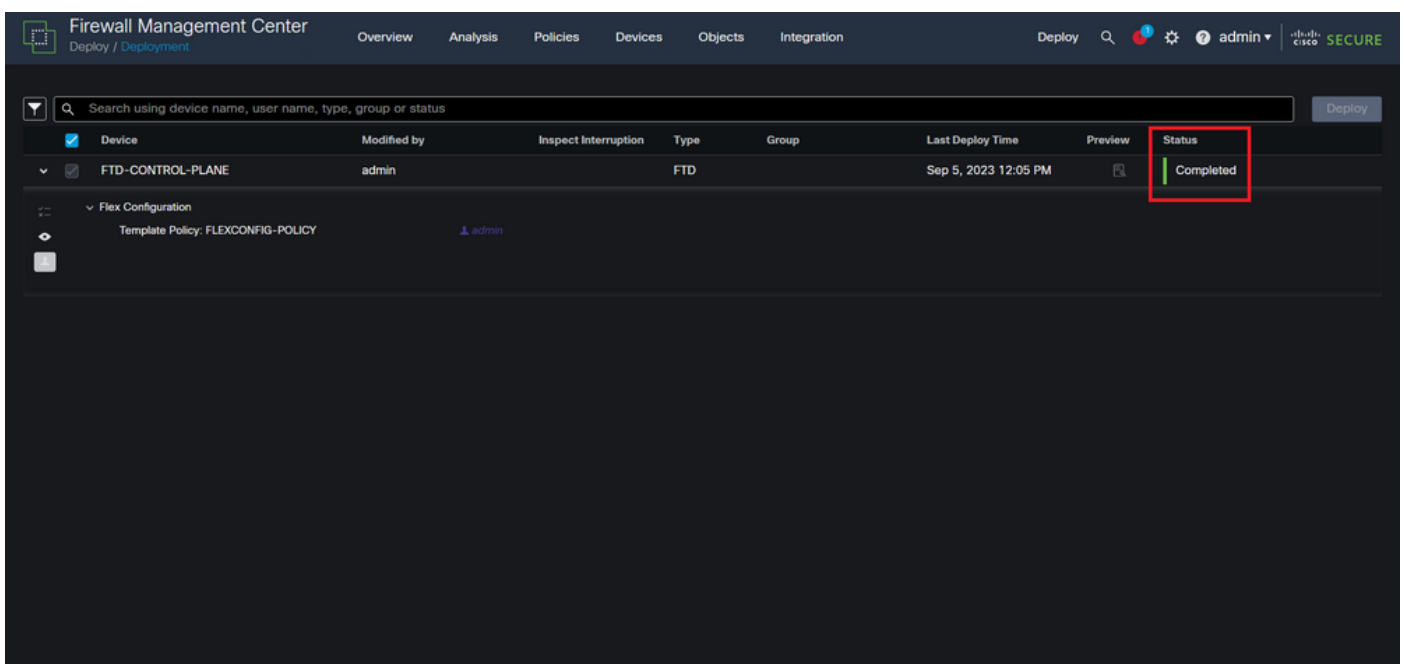


Immagine 23. Distribuzione FTD completata

Passaggio 6. Se si crea un nuovo ACL del piano di controllo per l'FTD o se ne è stato modificato uno esistente che è attivamente in uso, è importante sottolineare che le modifiche apportate alla configurazione non si applicano alle connessioni già stabilite all'FTD; pertanto, è necessario cancellare manualmente i tentativi di connessione attivi all'FTD. Per questo, collegarsi alla CLI dell'FTD e cancellare le connessioni attive come segue.

Per cancellare la connessione attiva per un indirizzo IP host specifico:


```
> clear conn address 192.168.1.10 a11
```

Per cancellare le connessioni attive per un'intera rete di subnet:

```
> clear conn address 192.168.1.0 netmask 255.255.255.0 a11
```

Per cancellare le connessioni attive per un intervallo di indirizzi IP:

```
> clear conn address 192.168.1.1-192.168.1.10 a11
```

 Nota: si consiglia di usare la parola chiave 'all' alla fine del comando clear conn address per forzare la cancellazione dei tentativi di connessione VPN brute force attivi verso il firewall sicuro, soprattutto quando la natura dell'attacco VPN brute force sta lanciando un'esplosione di tentativi di connessione costanti.

Configurare un ACL del control plane per FTD gestito da FDM

Questa è la procedura che è necessario seguire in un FDM per configurare un ACL del control plane in modo da bloccare gli attacchi di forza bruta VPN in ingresso sull'interfaccia FTD esterna:

Passaggio 1. Aprire l'interfaccia utente grafica di FDM tramite HTTPS ed eseguire l'accesso con le credenziali.

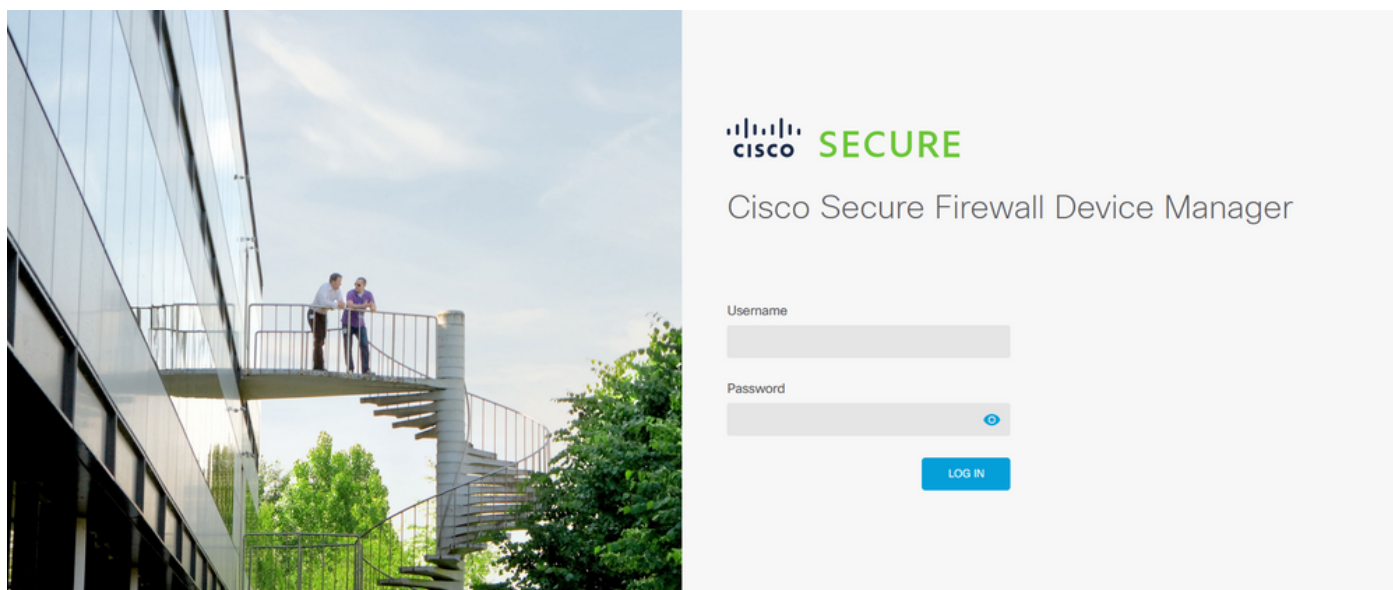


Immagine 24. Pagina Log In di FDM

Passaggio 2. È necessario creare una rete di oggetti. A tale scopo, passare a Oggetti:

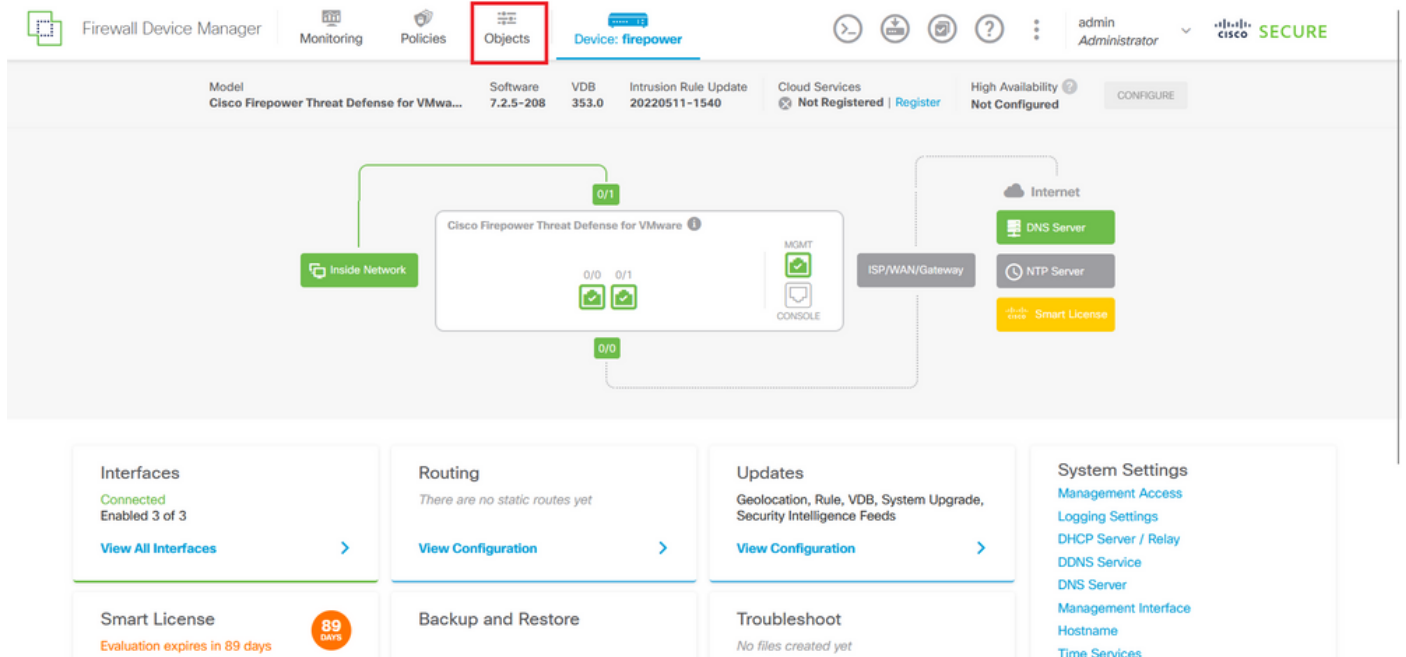


Immagine 25. Dashboard principale di FDM

Passaggio 2.1. Dal pannello sinistro, selezionare Reti, quindi fare clic sul pulsante '+' per creare un nuovo oggetto di rete.

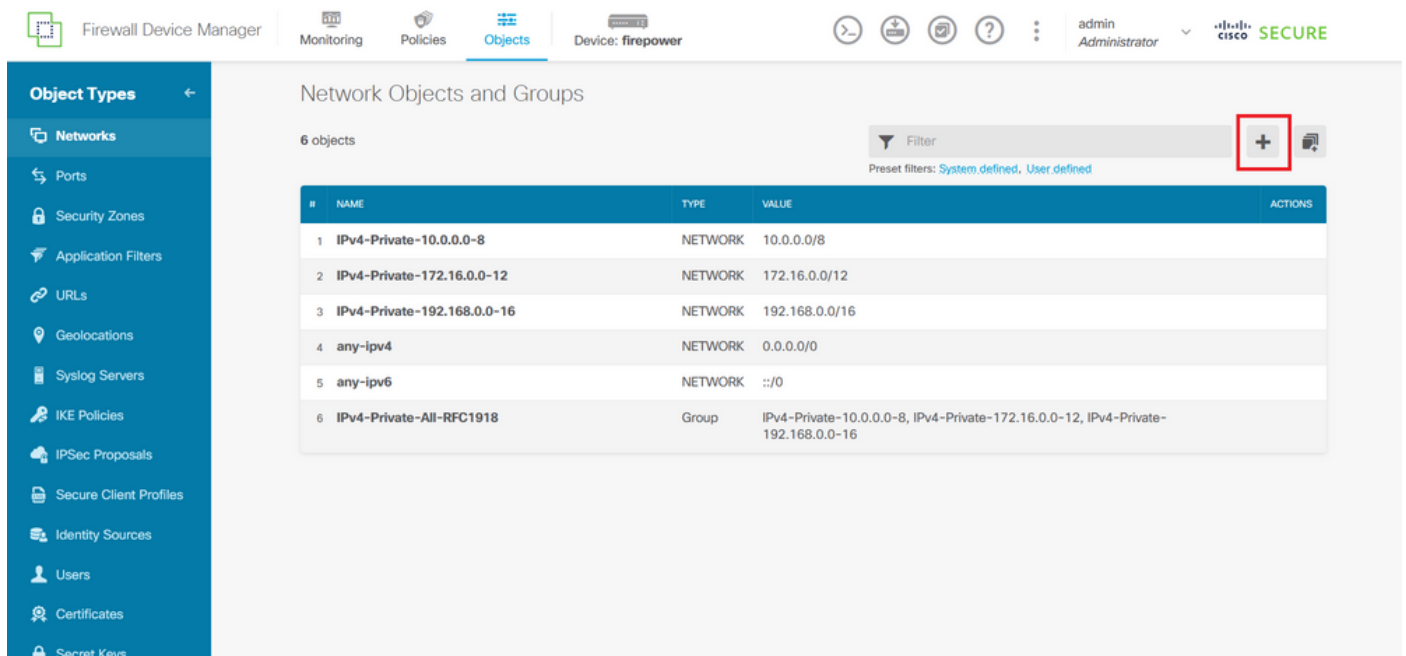


Immagine 26. Creazione di oggetti

Passaggio 2.2. Aggiungere un nome per l'oggetto di rete, selezionare il tipo di rete per l'oggetto, aggiungere l'indirizzo IP, l'indirizzo di rete o l'intervallo di IP in modo che corrisponda al traffico che deve essere negato all'FTD. Quindi, fare clic sul pulsante OK per completare la rete di oggetti.

- Nell'esempio, la rete di oggetti configurata ha lo scopo di bloccare gli attacchi di forza bruta VPN provenienti dalla subnet 192.168.1.0/24.

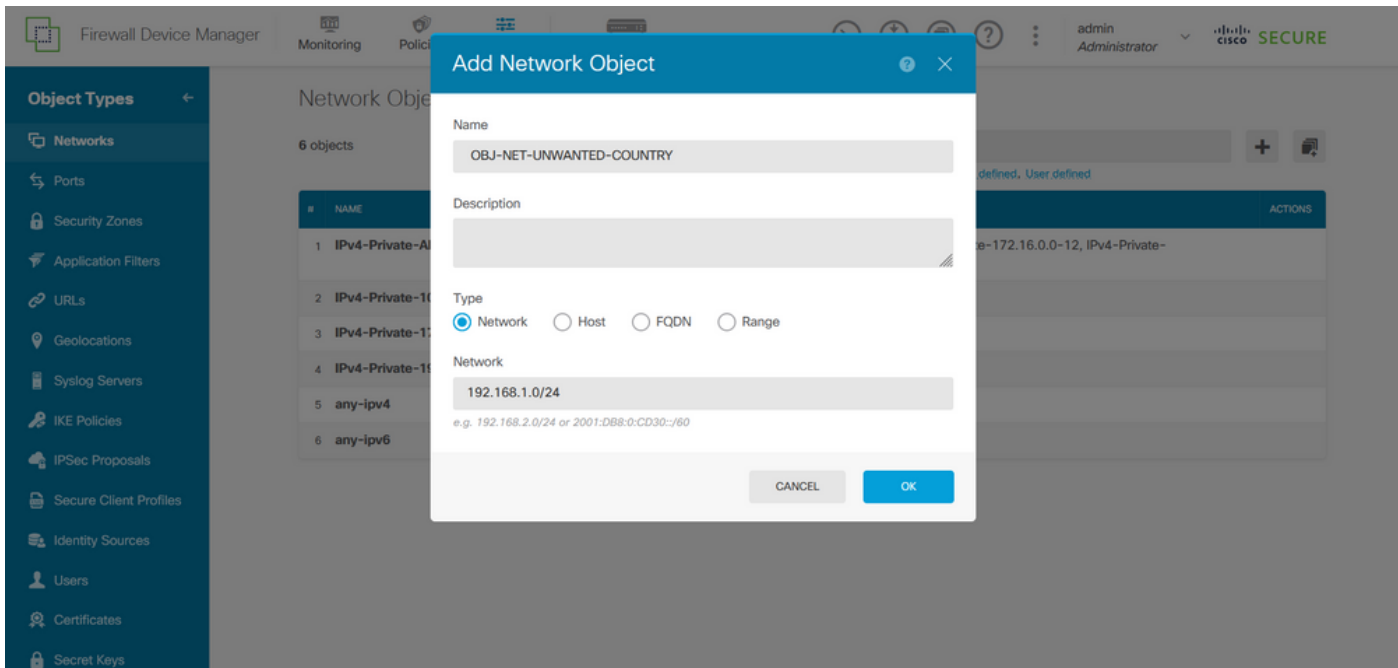


Immagine 27. Aggiungi oggetto di rete

Passaggio 3. Quindi, è necessario creare un ACL esteso; a questo scopo, selezionare la scheda Device (Dispositivo) nel menu superiore.

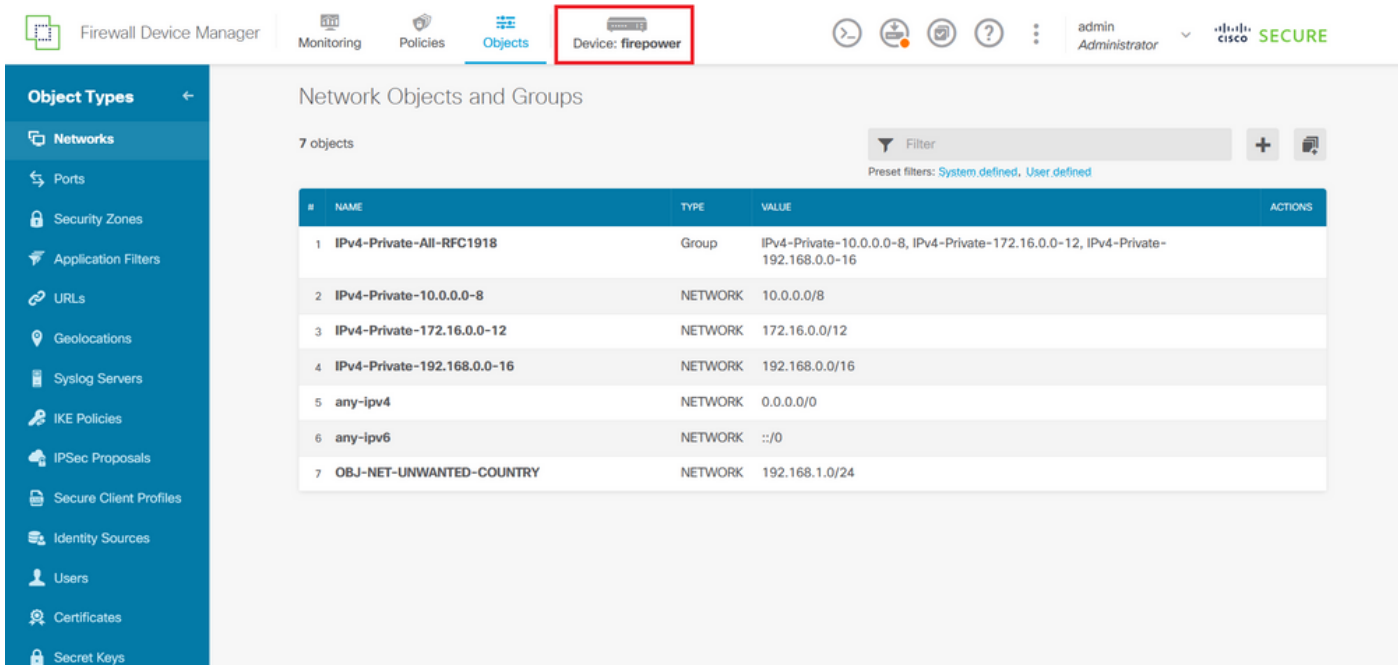


Immagine 28. Pagina Impostazioni dispositivo

Passaggio 3.1. Scorrere verso il basso e selezionare Visualizza configurazione dal riquadro Configurazione avanzata come indicato di seguito.

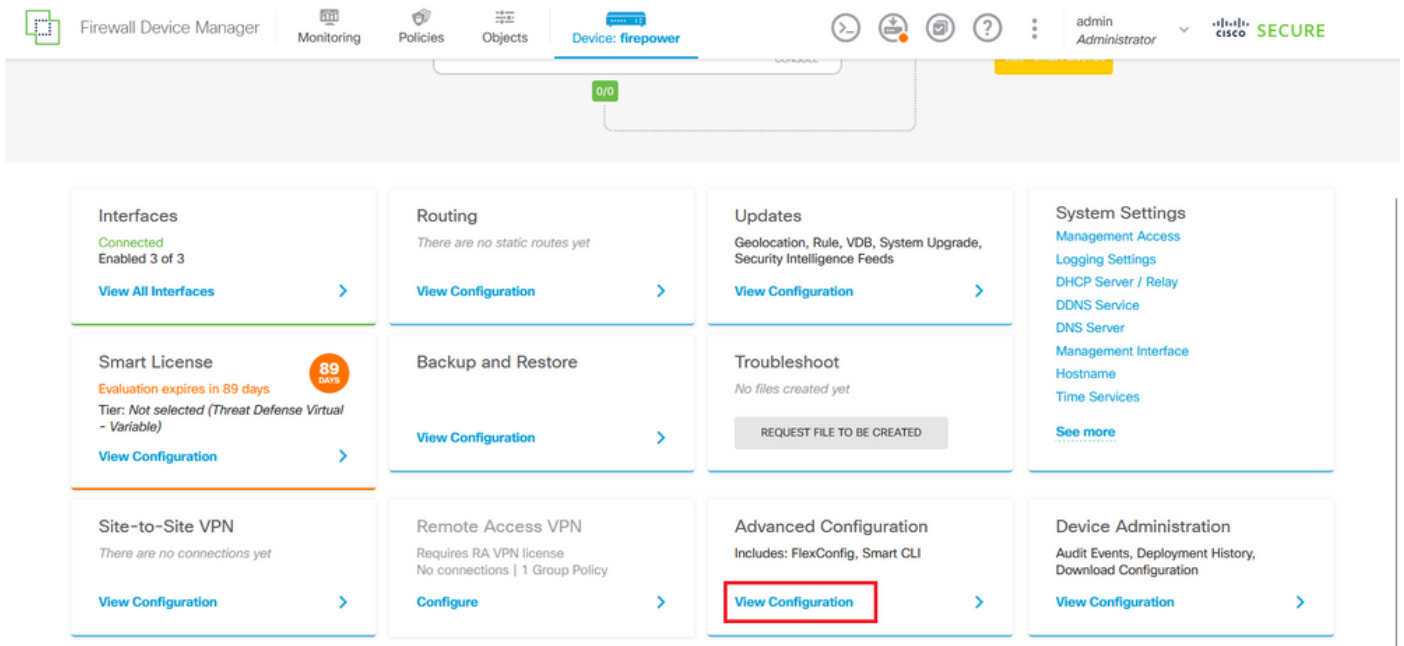


Immagine 29. Configurazione avanzata FDM

Passaggio 3.2. Quindi, dal pannello sinistro, passare a Smart CLI > Oggetti e fare clic su CREA OGGETTO SMART CLI.

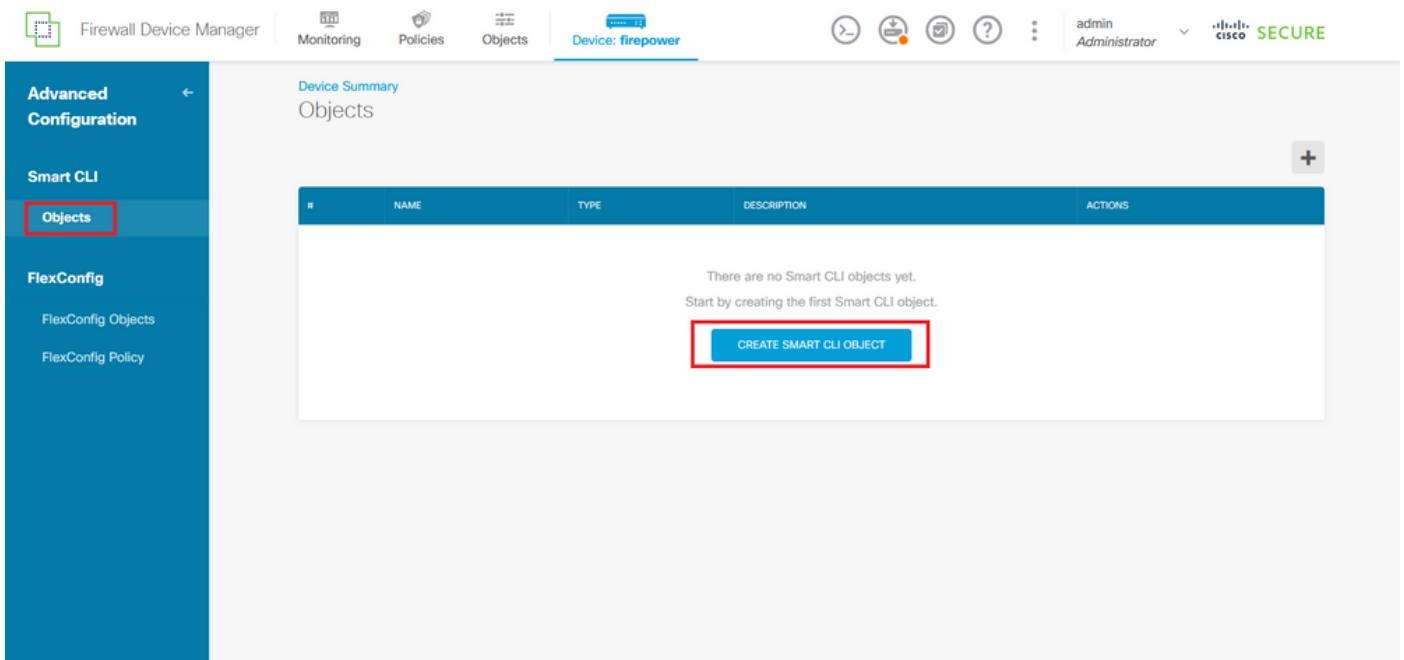


Immagine 30. Oggetti Smart CLI

Passaggio 3.3. Aggiungere un nome per l'ACL esteso da creare, selezionare Elenco accessi esteso dal menu a discesa del modello CLI, configurare le voci di controllo di accesso richieste dall'oggetto di rete creato nel passaggio precedente, 2.2, quindi fare clic sul pulsante OK per completare l'ACL.

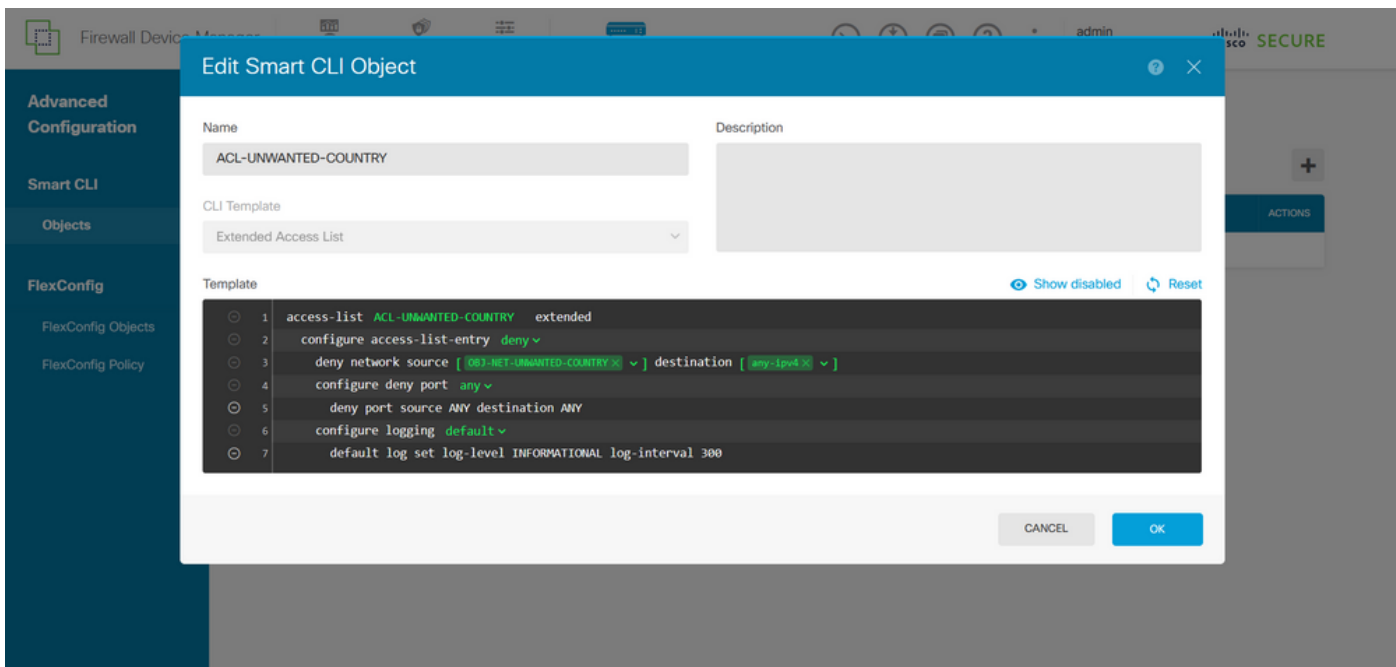



Immagine 31. Creazione di ACL estesi

 Nota: se è necessario aggiungere altre voci di controllo di accesso per l'ACL, è possibile farlo posizionando il mouse sulla sinistra della voce di controllo di accesso corrente. Verranno quindi visualizzati tre punti su cui è possibile fare clic. Fare clic su di esse e selezionare **Duplica** per aggiungere altre voci ACE.

Passaggio 4. Quindi, è necessario creare un oggetto FlexConfig. Per questo, spostarsi sul pannello sinistro e selezionare **FlexConfig > Oggetti FlexConfig**, quindi fare clic su **CREATE FLEXCONFIG OBJECT**.

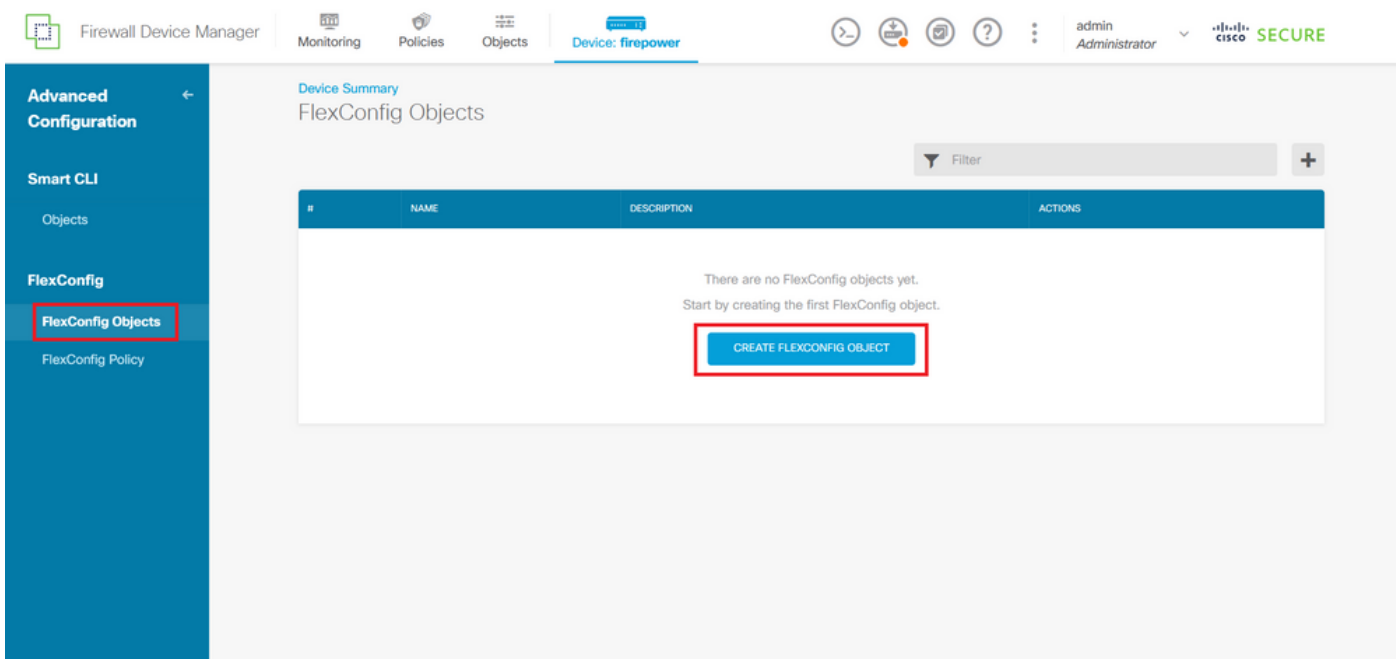


Immagine 32. Oggetti FlexConfig

Passaggio 4.1. Aggiungere un nome per l'oggetto FlexConfig per creare e configurare l'ACL del

piano di controllo come in entrata per l'interfaccia esterna, come indicato di seguito.

Sintassi della riga di comando:

```
access-group "ACL-name" in interface "interface-name" control-plane
```

Questo si traduce nell'esempio di comando successivo, che usa l'ACL esteso creato nel passaggio 3.3 'ACL-UNWANTED-COUNTRY' come segue:

```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Di seguito viene riportata la modalità di configurazione dell'oggetto FlexConfig nella finestra oggetto FlexConfig. A questo punto, selezionare il pulsante OK per completare l'oggetto FlexConfig.

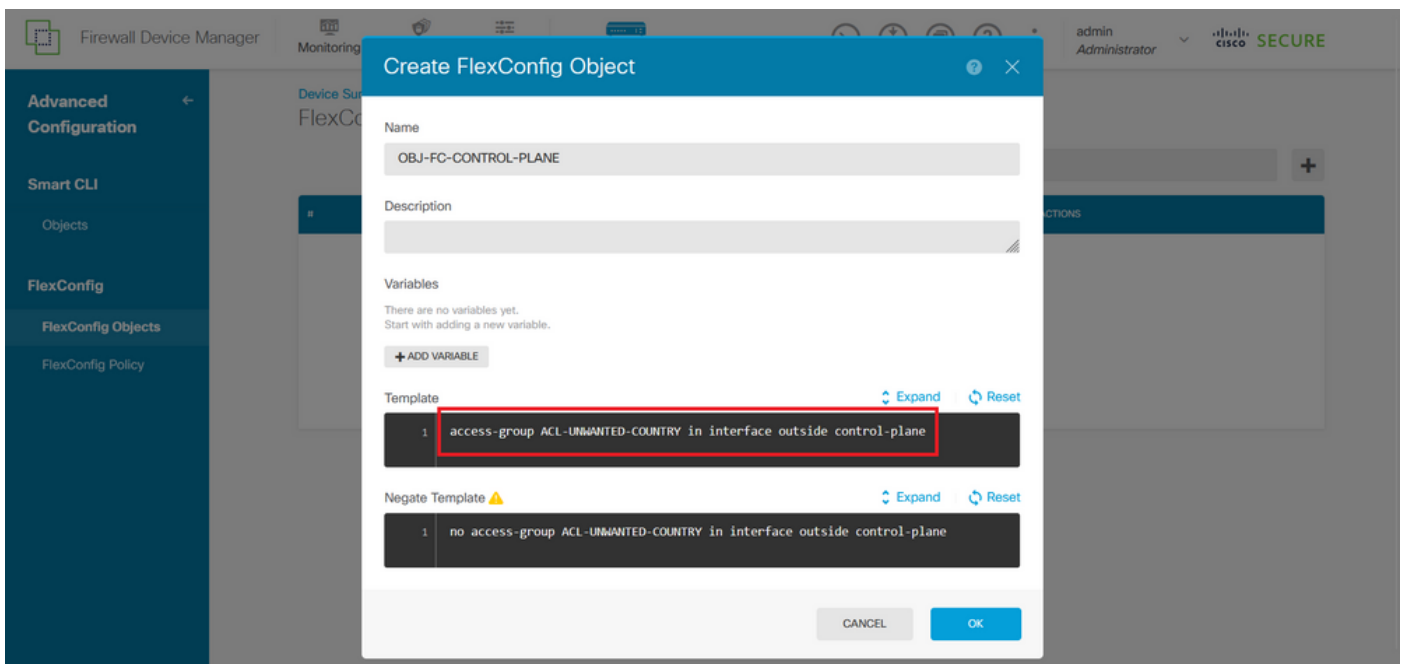


Immagine 33. Creazione oggetto FlexConfig

Passaggio 5. Procedere alla creazione di un criterio FlexConfig. A tale scopo, selezionare Flexconfig > Criterio FlexConfig, fare clic sul pulsante '+' e selezionare l'oggetto FlexConfig creato nel passaggio 4.1 precedente.

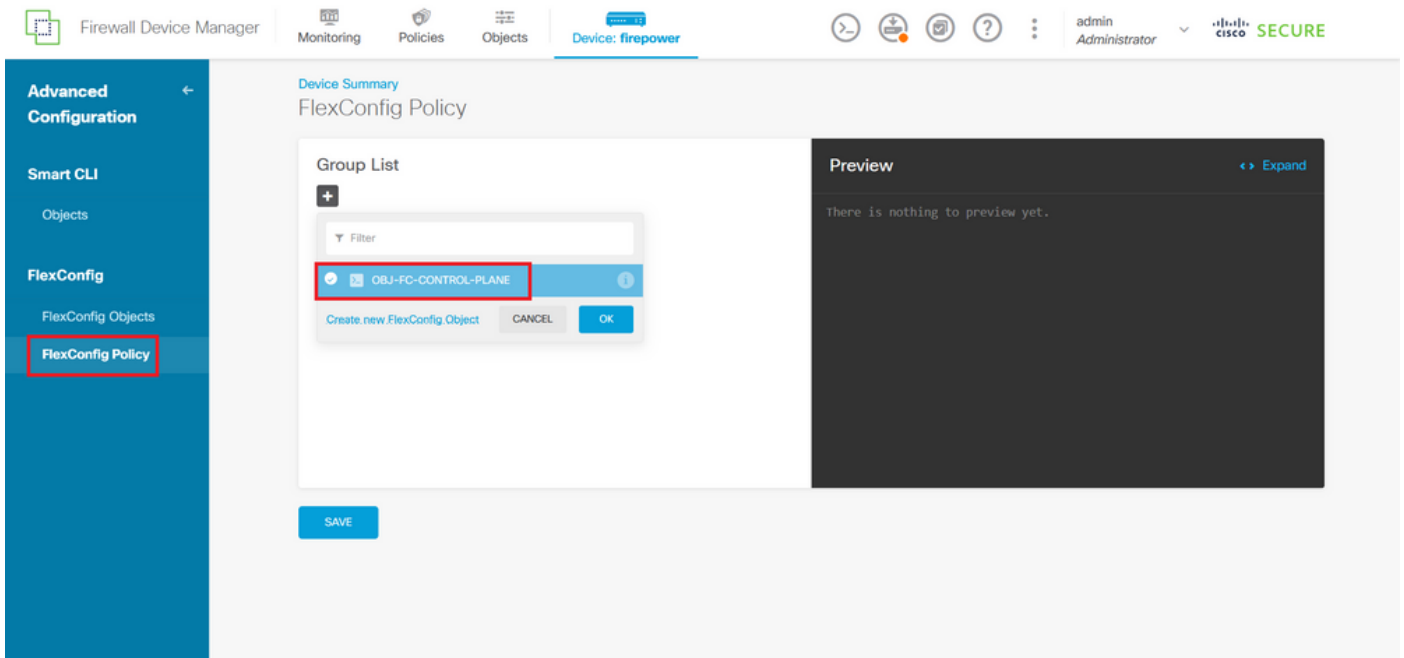


Immagine 34. Criteri FlexConfig

Passaggio 5.1. Verificare che nell'anteprima di FlexConfig sia visualizzata la configurazione corretta per l'ACL del piano di controllo creato e fare clic sul pulsante Save (Salva).

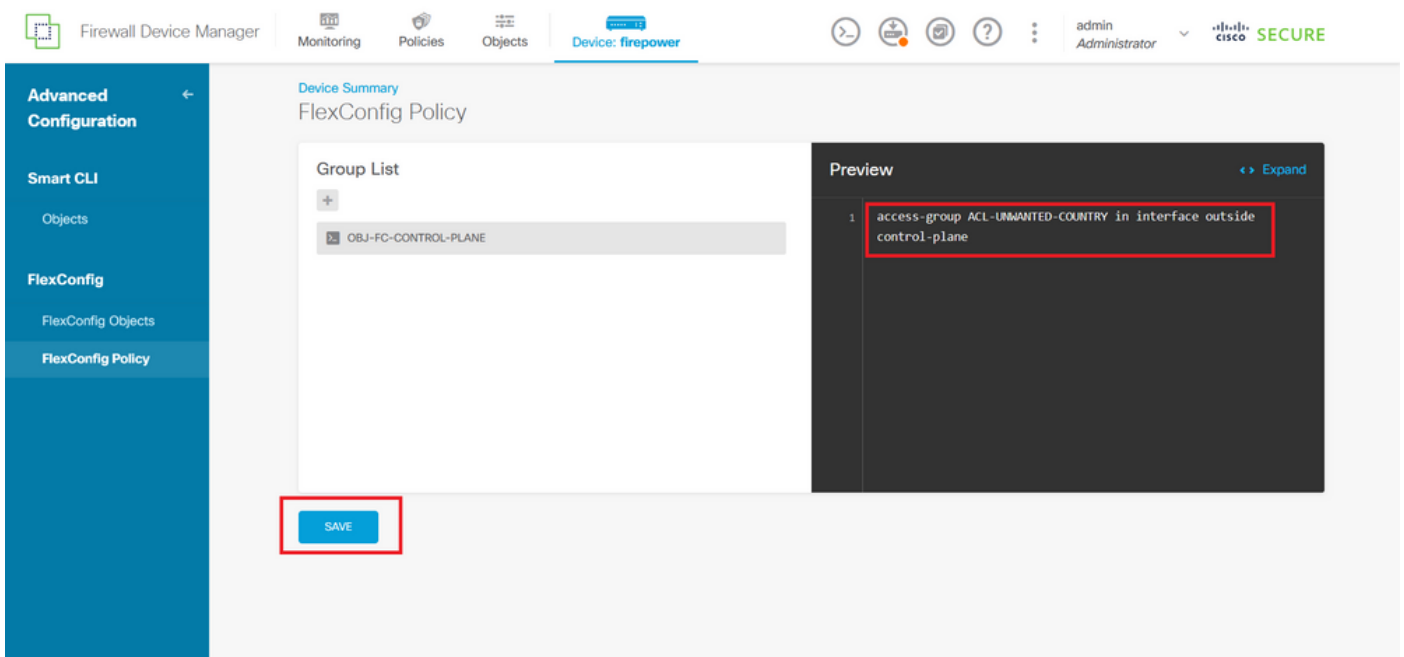


Immagine 35. Anteprima criteri FlexConfig

Passaggio 6. Distribuire le modifiche della configurazione all'FTD che si desidera proteggere dagli attacchi di forza brute della VPN. A tale scopo, fare clic sul pulsante Deployment nel menu superiore, verificare che le modifiche della configurazione da distribuire siano corrette e quindi fare clic su DEPLOY NOW.

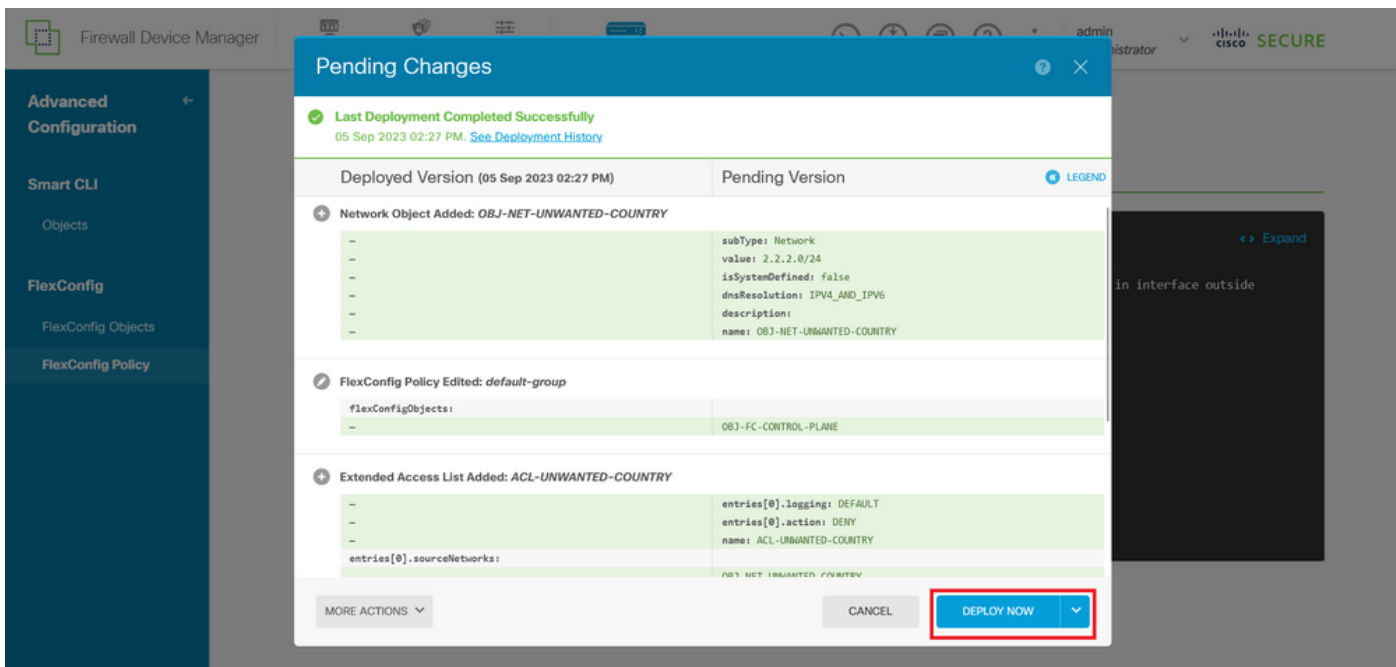


Immagine 36. Distribuzione in sospenso

Passaggio 6.1. Verificare che la distribuzione dei criteri sia stata completata.

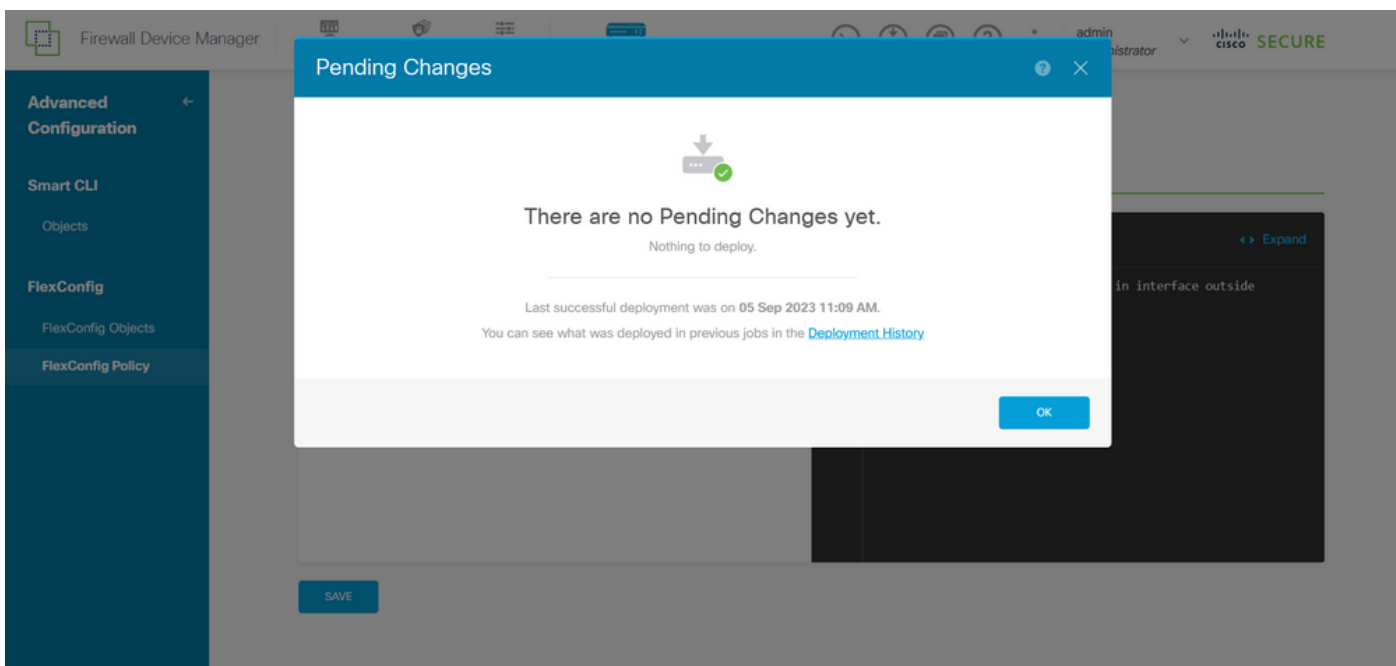


Immagine 37. Distribuzione completata

Passaggio 7. Se si crea un nuovo ACL del piano di controllo per l'FTD o se ne è stato modificato uno esistente che è attivamente in uso, è importante sottolineare che le modifiche apportate alla configurazione non si applicano alle connessioni già stabilite all'FTD; pertanto, è necessario cancellare manualmente i tentativi di connessione attivi all'FTD. Per questo, collegarsi alla CLI dell'FTD e cancellare le connessioni attive come segue.

Per cancellare la connessione attiva per un indirizzo IP host specifico:


```
> clear conn address 192.168.1.10 all
```

Per cancellare le connessioni attive per un'intera rete di subnet:

```
> clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

Per cancellare le connessioni attive per un intervallo di indirizzi IP:

```
> clear conn address 192.168.1.1-192.168.1.10 all
```

 Nota: si consiglia di usare la parola chiave 'all' alla fine del comando clear conn address per forzare la cancellazione dei tentativi di connessione VPN brute force attivi verso il firewall sicuro, soprattutto quando la natura dell'attacco VPN brute force sta lanciando un'esplosione di tentativi di connessione costanti.

Configurazione di un ACL del control plane per un'ASA tramite CLI

Questa è la procedura da seguire in una CLI ASA per configurare un ACL del control plane in modo da bloccare gli attacchi VPN con forza bruta in arrivo sull'interfaccia esterna:

Passaggio 1. Accedere all'appliance ASA del firewall sicuro tramite la CLI e configurare il terminale come segue.

```
asa# configure terminal
```

Passaggio 2. Usare il comando successivo per configurare un ACL esteso in modo che blocchi un indirizzo IP host o un indirizzo di rete per il traffico che deve essere bloccato sull'appliance ASA.

- Nell'esempio, viene creato un nuovo ACL chiamato 'ACL-UNWANTED-COUNTRY' e la voce ACE configurata blocca gli attacchi della forza bruta VPN provenienti dalla subnet 192.168.1.0/24.

```
asa(config)# access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any
```

Passaggio 3. Usare il comando access-group successivo per configurare l'ACL 'ACL-

UNWANTED-COUNTRY' come ACL del piano di controllo per l'interfaccia ASA esterna.

```
asa(config)# access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Passaggio 4. Se si crea un nuovo ACL del piano di controllo o se ne è stato modificato uno esistente e in uso, è importante sottolineare che le modifiche apportate alla configurazione non si applicano alle connessioni già stabilite all'appliance ASA. Pertanto, è necessario cancellare manualmente i tentativi di connessione attiva all'appliance. A tale scopo, deselezionare le connessioni attive nel modo seguente.

Per cancellare la connessione attiva per un indirizzo IP host specifico:


```
asa# clear conn address 192.168.1.10 all
```

Per cancellare le connessioni attive per un'intera rete di subnet:

```
asa# clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

Per cancellare le connessioni attive per un intervallo di indirizzi IP:

```
asa# clear conn address 192.168.1.1-192.168.1.10 all
```

 Nota: si consiglia di usare la parola chiave 'all' alla fine del comando clear conn address per forzare la cancellazione dei tentativi di connessione VPN brute force attivi verso il firewall sicuro, soprattutto quando la natura dell'attacco VPN brute force sta lanciando un'esplosione di tentativi di connessione costanti.

Configurazione alternativa per bloccare gli attacchi per un firewall protetto tramite il comando 'shun'

In caso di un'opzione immediata per bloccare gli attacchi per il firewall protetto, è possibile utilizzare il comando 'shun'. Il comando theshun consente di bloccare le connessioni da un host in attacco.

- Una volta evitato un indirizzo IP, tutte le connessioni future dall'indirizzo IP di origine vengono interrotte e registrate fino a quando la funzione di blocco non viene rimossa manualmente.
- La funzione di blocco del comando `shun` viene applicata indipendentemente dal fatto che sia attiva o meno una connessione con l'indirizzo host specificato.
- Se si specificano l'indirizzo di destinazione, le porte di origine e di destinazione e il protocollo, si elimina la connessione corrispondente e si rimuove l'indirizzo da tutte le connessioni future dell'IP di origine

indirizzo; verranno ignorate tutte le connessioni future, non solo quelle che corrispondono a questi parametri di connessione specifici.

- È possibile avere solo un comando per indirizzo IP di origine.
- Poiché viene utilizzato per bloccare gli attacchi in modo dinamico, il comando `shun` viene visualizzato nella configurazione del dispositivo di difesa delle minacce.
- Quando si rimuove la configurazione di un'interfaccia, vengono rimossi anche tutti gli `shun` collegati a quell'interfaccia.
- Sintassi del comando `Shun`:

```
shun source_ip [ dest_ip source_port dest_port [ protocol]] [ vlan vlan_id]
```

- Per disabilitare un `shun`, utilizzare la forma `no` di questo comando:

```
no shun source_ip [ vlan vlan_id]
```

Per evitare un indirizzo IP host, procedere come segue per il firewall protetto. Nell'esempio, il comando `'shun'` viene usato per bloccare gli attacchi di forza bruta VPN provenienti dall'indirizzo IP di origine 192.168.1.10.

Esempio di configurazione per FTD.

Passaggio 1. Accedere al FTD tramite CLI e applicare il comando `shun` come indicato di seguito.

```
<#root>
```

```
>
```

```
shun 192.168.1.10
```

```
Shun 192.168.1.10 added in context: single_vf
```

```
Shun 192.168.1.10 successful
```

Passaggio 2. È possibile utilizzare i seguenti comandi show per confermare gli indirizzi IP di shun nel FTD e per monitorare il conteggio delle visite di shun per indirizzo IP:

```
<#root>
```

```
>
```

```
show shun
```

```
shun (outside) 192.168.1.10 0.0.0.0 0 0 0
```

```
>
```

```
show shun statistics
```

```
diagnostic=OFF, cnt=0
```

```
outside=ON, cnt=0
```

```
Shun 192.168.1.10 cnt=0, time=(0:00:28)
```

Esempio di configurazione dell'appliance ASA

Passaggio 1. Accedere all'ASA tramite la CLI e applicare il comando shun come indicato di seguito.

```
<#root>
```

```
asa#
```

```
shun 192.168.1.10
```

```
Shun 192.168.1.10 added in context: single_vf
```

```
Shun 192.168.1.10 successful
```

Passaggio 2. È possibile usare i seguenti comandi show per confermare gli indirizzi IP shun nell'appliance ASA e monitorare il numero di accessi shun per indirizzo IP:

```
<#root>
```

```
asa#
```

```
show shun

shun (outside) 192.168.1.10 0.0.0.0 0 0 0

asa#

show shun statistics

outside=ON, cnt=0
inside=OFF, cnt=0
dmz=OFF, cnt=0
outside1=OFF, cnt=0
mgmt=OFF, cnt=0

Shun 192.168.1.10 cnt=0, time=(0:01:39)
```



Nota: per ulteriori informazioni sul comando secure firewall shun, consultare la [guida di riferimento dei comandi di Cisco Secure Firewall Threat Defense](#)

Verifica

Per verificare che la configurazione dell'ACL del control plane sia attiva per il firewall protetto, procedere come segue:

Passaggio 1. Accedere al firewall protetto tramite CLI ed eseguire i comandi successivi per verificare che la configurazione dell'ACL del control plane sia stata applicata.

Esempio di output per l'FTD gestito da FMC:

```
<#root>
>
show running-config access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any
>
show running-config access-group

***OUTPUT OMITTED FOR BREVITY***
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Esempio di output per l'FTD gestito da FDM:

```
<#root>
> show running-config object id OBJ-NET-UNWANTED-COUNTRY
```

```
object network OBJ-NET-UNWANTED-COUNTRY
subnet 192.168.1.0 255.255.255.0
```

```
>
```

```
show running-config access-list ACL-UNWANTED-COUNTRY
```

```
access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any4 log default
```

```
> show running-config access-group
```

```
***OUTPUT OMITTED FOR BREVITY***
```

```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Esempio di output per l'appliance ASA:

```
<#root>
```

```
asa#
```

```
show running-config access-list ACL-UNWANTED-COUNTRY
```

```
access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any
```

```
asa#
```

```
show running-config access-group
```

```
***OUTPUT OMITTED FOR BREVITY***
```

```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Passaggio 2. Per verificare che l'ACL del control-plane stia bloccando il traffico richiesto, usare il comando packet-tracer per simulare una connessione TCP 443 in entrata all'interfaccia esterna del firewall protetto, quindi usare il comando show access-list <acl-name> per aumentare il numero di accessi all'ACL ogni volta che una connessione VPN con forza brute al firewall protetto viene bloccata dall'ACL del control-plane:

- Nell'esempio, il comando packet-tracer simula una connessione TCP 443 in entrata originata dall'host 192.168.1.10 e destinata all'indirizzo IP esterno del nostro firewall sicuro. L'output 'packet-tracer' conferma che il traffico viene interrotto e l'output 'show access-list' visualizza gli incrementi del numero di accessi per l'ACL del control plane sul posto:

Esempio di output per FTD

<#root>

>

packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.251 443

Phase: 1

Type:

ACCESS-LIST

Subtype: log

Result: DROP

Elapsed time: 21700 ns

Config:

Additional Information:

Result:

input-interface: outside(vrfid:0)

input-status: up

input-line-status: up

Action: drop

Time Taken: 21700 ns

Drop-reason: (acl-drop) Flow is denied by configured rule

, Drop-location: frame 0x00005623c7f324e7 flow (NA)/NA

>

show access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f

access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any (

hitcnt=1

) 0x142f69bf

Esempio di output per l'appliance ASA

<#root>

asa#

packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.5 443

Phase: 1

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Elapsed time: 19688 ns

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 2

Type:

ACCESS-LIST

Subtype: log

Result: DROP

Elapsed time: 17833 ns

Config:

Additional Information:

Result:

input-interface: outside

input-status: up

input-line-status: up

Action: drop

Time Taken: 37521 ns

Drop-reason: (acl-drop) Flow is denied by configured rule

, Drop-location: frame 0x0000556e6808cac8 flow (NA)/NA

asa#


show access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f

access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any

(hitcnt=1)

0x9b4d26ac

 Nota: se nel firewall sicuro è implementata una soluzione VPN come la VPN Cisco Secure Client, è possibile eseguire un reale tentativo di connessione al firewall sicuro per verificare che l'ACL del control plane stia funzionando come previsto per bloccare il traffico richiesto.

Bug correlati

- ENH | Connessioni client AnyConnect basate sulla località geografica: ID bug Cisco [CSCvs65322](#)

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).