

為安全防火牆威脅防禦和ASA配置控制平面訪問控制策略

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[組態](#)

[為FMC管理的FTD設定控制平面ACL](#)

[為FDM管理的FTD配置控制平面ACL](#)

[使用CLI為ASA配置控制平面ACL](#)

[使用「shun」命令阻止安全防火牆攻擊的備用配置](#)

[驗證](#)

[相關錯誤](#)

簡介

本文檔介紹為安全防火牆威脅防禦和自適應安全裝置(ASA)配置控制平面訪問規則的過程。

必要條件

需求

思科建議您瞭解以下主題：

- 安全防火牆威脅防禦(FTD)
- 安全防火牆裝置管理員(FDM)
- 安全防火牆管理中心(FMC)
- 安全防火牆ASA
- 存取控制清單(ACL)
- FlexConfig

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 安全防火牆威脅防禦版本7.2.5
- 安全防火牆管理器中心版本7.2.5
- 安全防火牆裝置管理員版本7.2.5

- 安全防火牆ASA版本9.18.3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

流量通常通過防火牆，並在資料介面之間路由；在某些情況下，拒絕發往「到」安全防火牆的流量是有益的。思科安全防火牆可以使用控制平面訪問控制清單(ACL)來限制「機箱內」流量。控制平面ACL何時有用的示例是控制哪些對等體可以建立到安全防火牆的VPN（站點到站點或遠端訪問VPN）隧道。

安全防火牆「機箱內」流量

流量通常從一個介面（入站）穿過防火牆到達另一個介面（出站），這稱為「通過機箱式」流量，由訪問控制策略(ACP)和預過濾器規則共同管理。

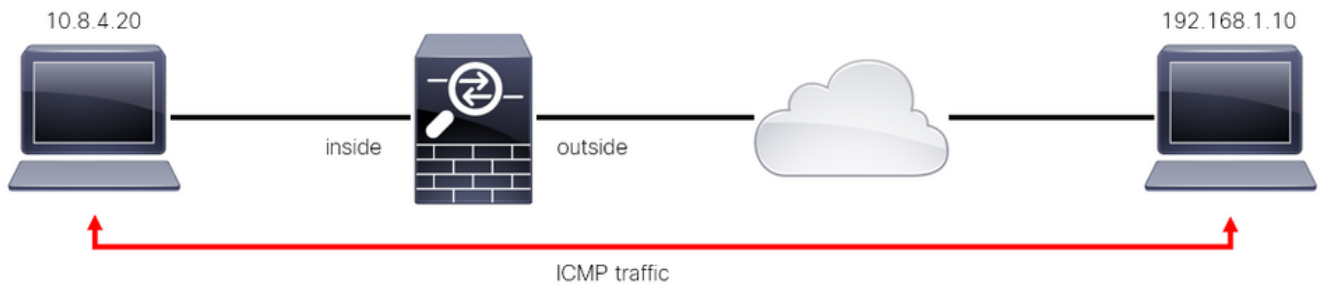


圖1.通過機箱的流量示例

安全防火牆的「機箱內」流量

在其他情況下，流量直接目的地為FTD介面（站對站或遠端存取VPN），這稱為「到箱」流量，由該特定介面的控制平面管理。

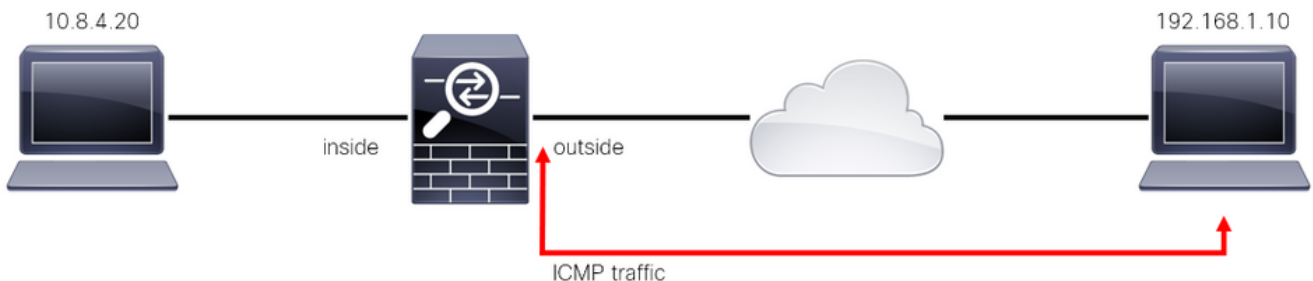


圖2.即插即用流量示例

有關控制平面ACL的重要注意事項

- 自FMC/FTD 7.0版起，必須使用FlexConfig使用ASA上使用的相同命令語法配置控制平面ACL。

- 關鍵字control-plane被附加到訪問組配置中，該配置會將流量「強制」到安全防火牆介面。如果沒有在命令後附加控制平面字，ACL將限制通過「安全」防火牆的流量。
- 控制平面ACL不會限制安全防火牆介面的SSH、ICMP或TELNET入站。根據平台設定策略處理（允許/拒絕），並且具有更高的優先順序。
- 控制平面ACL將流量限制為「進入」安全防火牆本身，而FTD的訪問控制策略或ASA的正常ACL則控制流量「通過」安全防火牆。
- 與普通ACL不同，ACL的結尾沒有隱含的「deny」。
- 建立本檔案時，FTD地理定位功能無法用於限制「訪問」FTD。

設定

在下一個範例中，來自特定國家的一組IP位址嘗試登入FTD RAVPN，從而VPN強行進入網路。保護FTD免受這些VPN暴力攻擊的最佳選項是設定控制平面ACL，以阻擋這些連線到外部FTD介面。

組態

為FMC管理的FTD設定控制平面ACL

您可以在FMC中按照以下步驟操作，以設定控制平面ACL來阻止傳入VPN暴力攻擊到外部FTD介面：

步驟 1.通過HTTPS開啟FMC圖形使用者介面(GUI)並使用您的憑證登入。



圖3.FMC登入頁

步驟 2.您需要建立延伸型ACL。為此，請導航到Objects > Object Management。

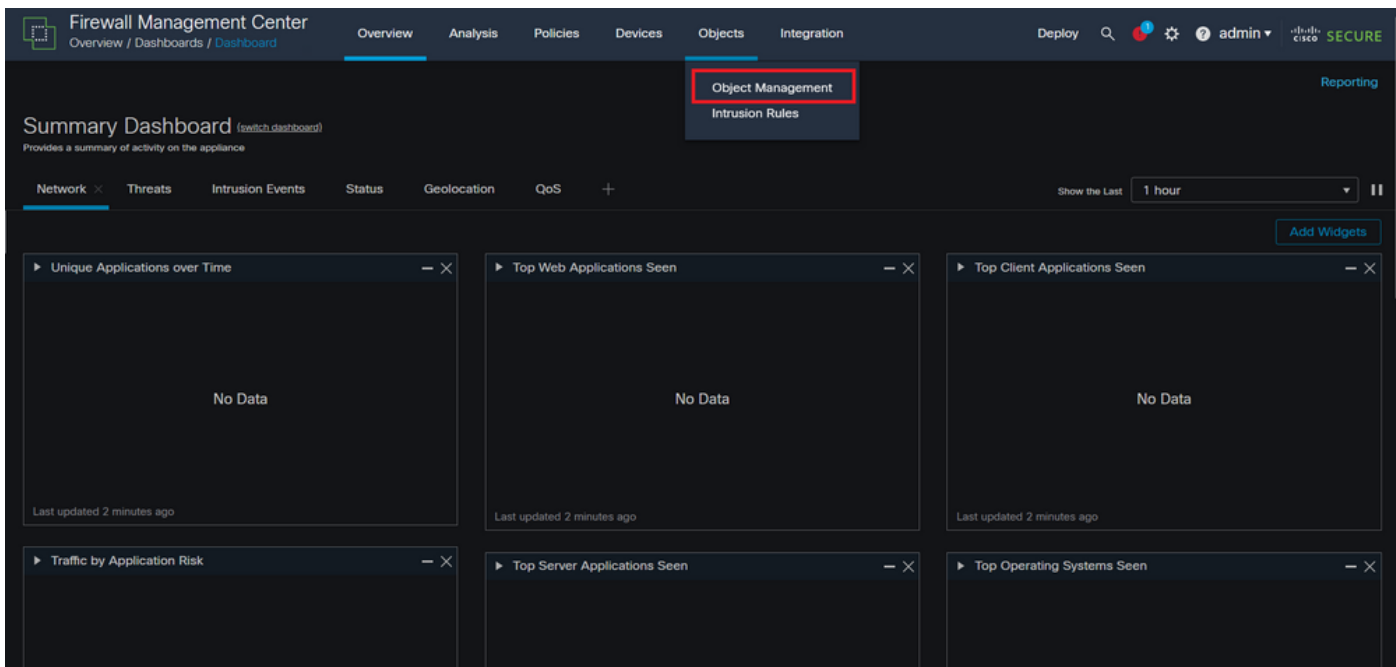


圖4.物件管理

步驟 2.1.從左側面板導航到Access List > Extended以建立擴展ACL。

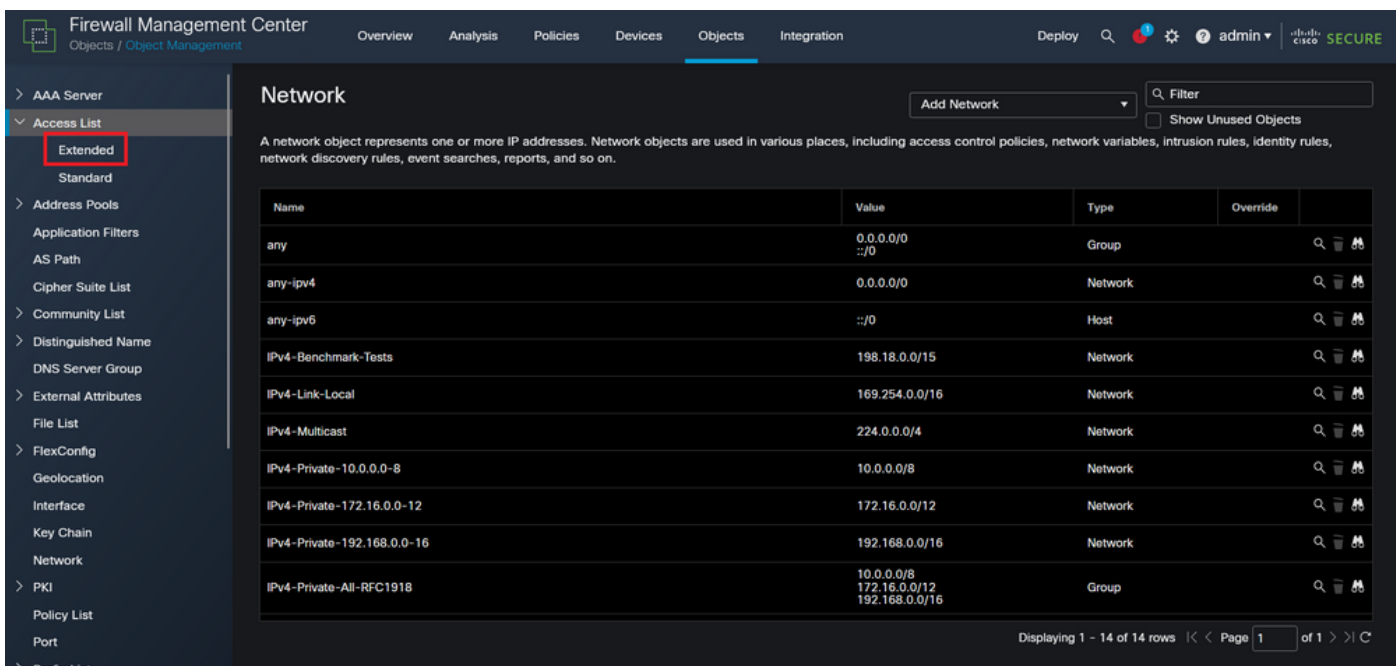


圖5.擴展ACL選單

步驟 2.2.然後，選擇Add Extended Access List。

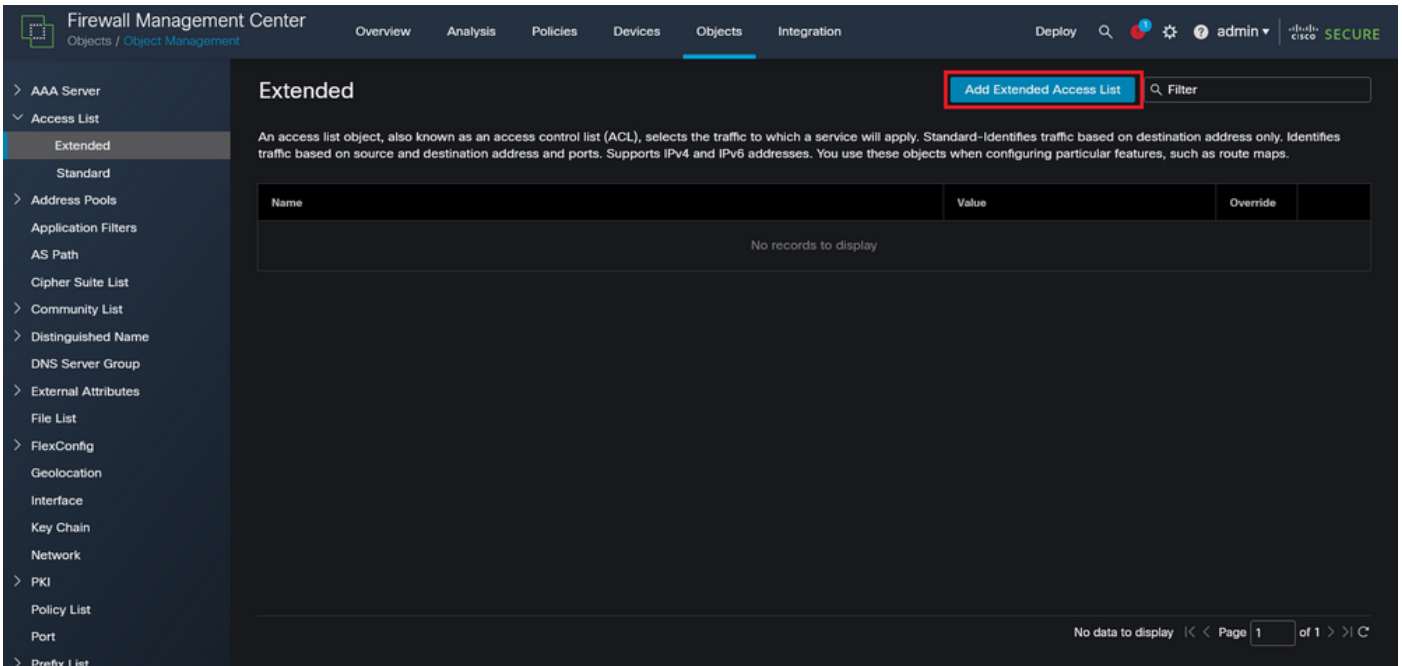


圖6.新增擴展ACL

步驟 2.3.鍵入擴展ACL的名稱，然後按一下Add按鈕建立訪問控制條目(ACE):

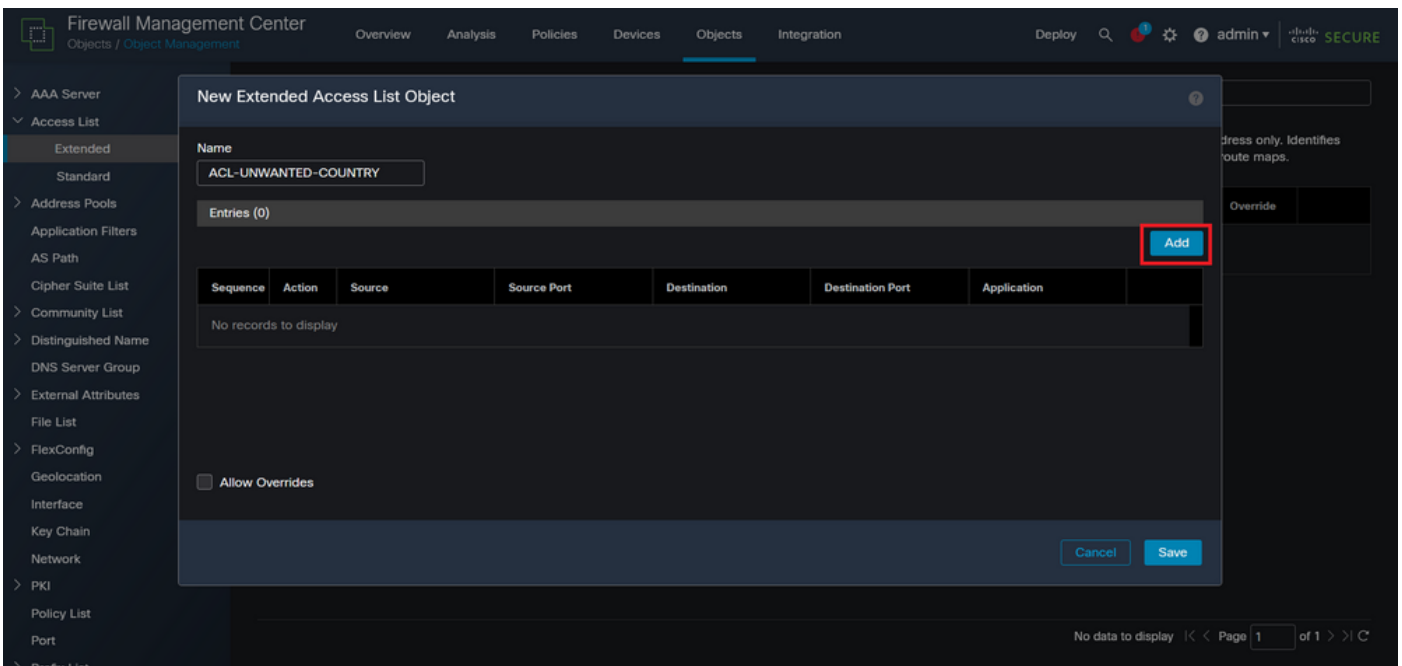


圖7.延伸型ACL專案

步驟 2.4.將ACE操作更改為Block，然後新增源網路以匹配需要拒絕到FTD的流量，將目標網路保留為Any，然後按一下Add按鈕完成ACE條目：

— 在本示例中，配置的ACE條目將阻止來自192.168.1.0/24子網的VPN暴力攻擊。

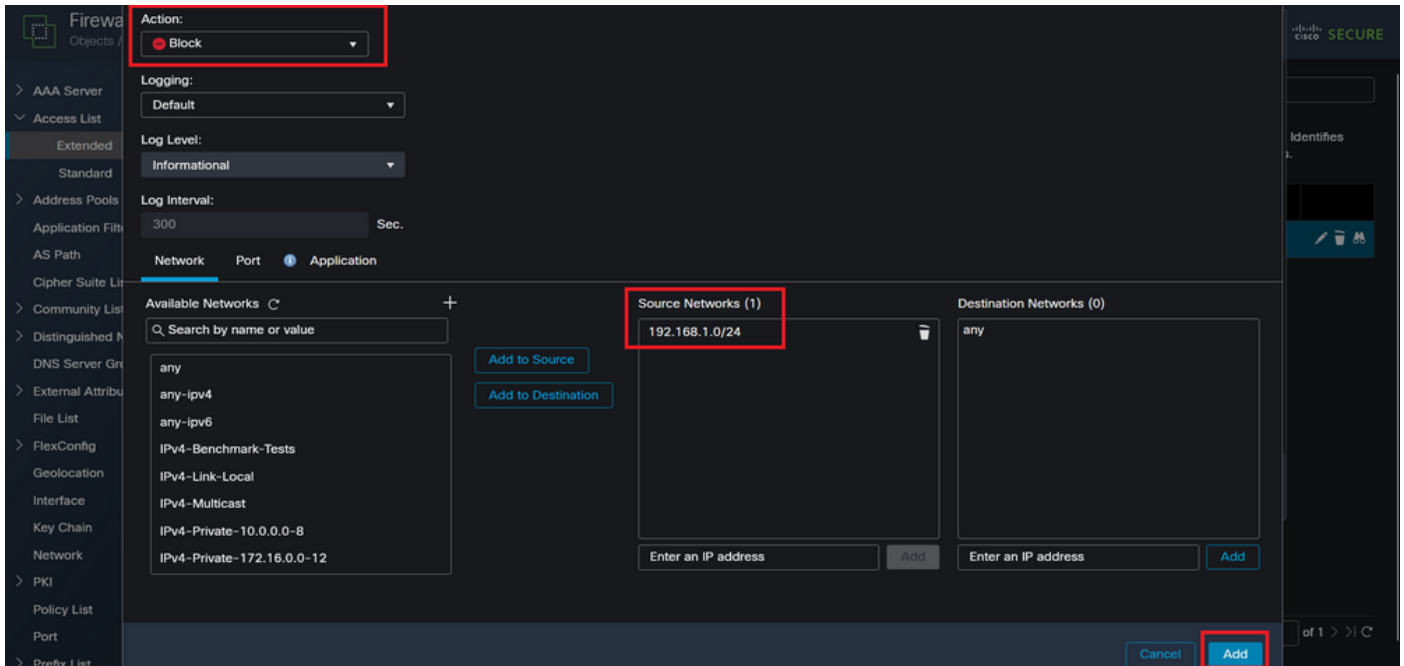


圖8.拒絕的網路

步驟 2.5. 如果需要新增更多ACE條目，請再次按一下Add按鈕並重複步驟2.4。完成後，點選Save按鈕完成ACL配置。

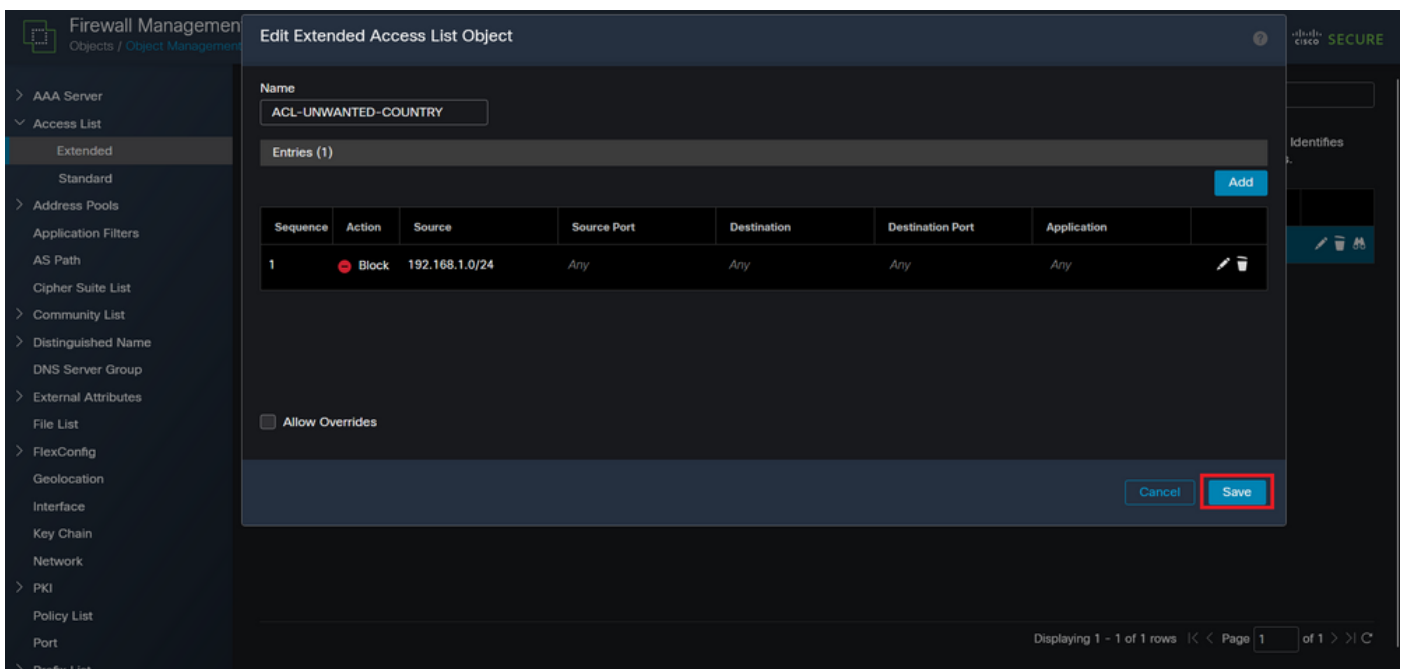


圖9.完成的擴展ACL條目

步驟 3. 接下來，您需要設定Flex-Config對象，以將控制平面ACL套用到外部FTD介面。為此，導航到左側面板，然後選擇選項FlexConfig > FlexConfig Object。

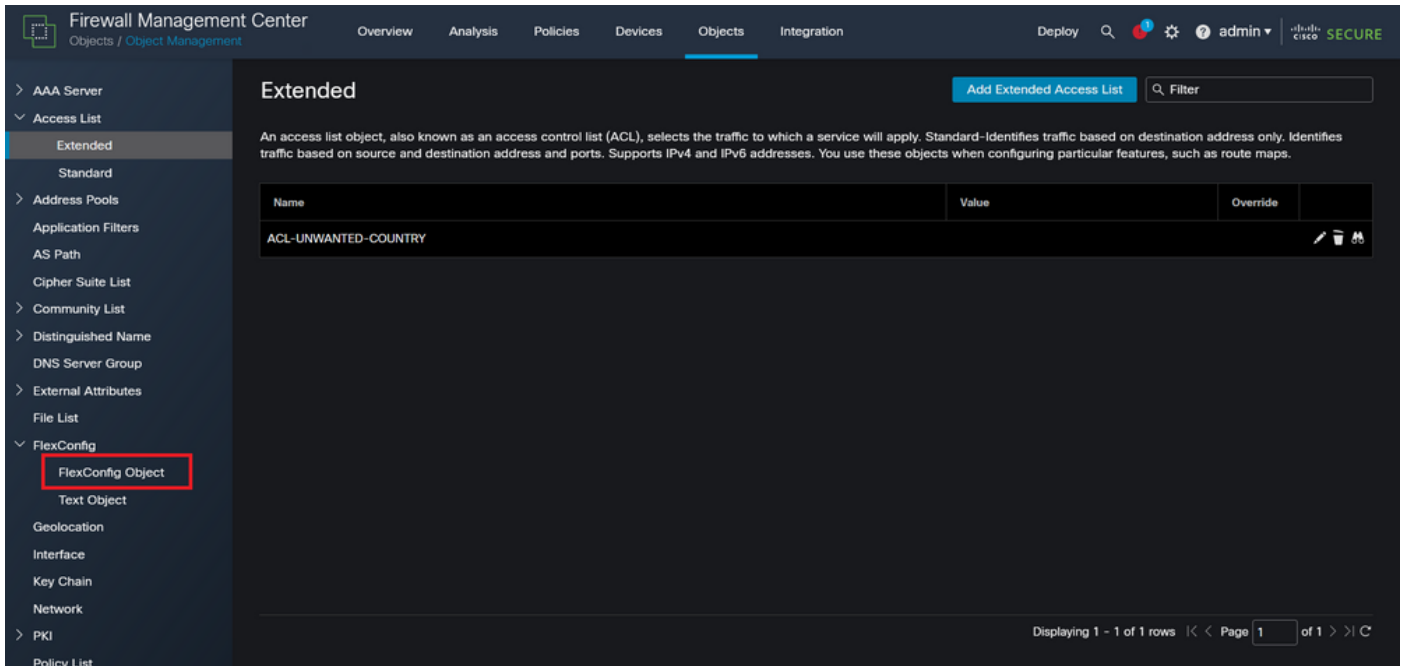


圖10.FlexConfig對象選單

步驟 3.1.按一下新增FlexConfig對象。

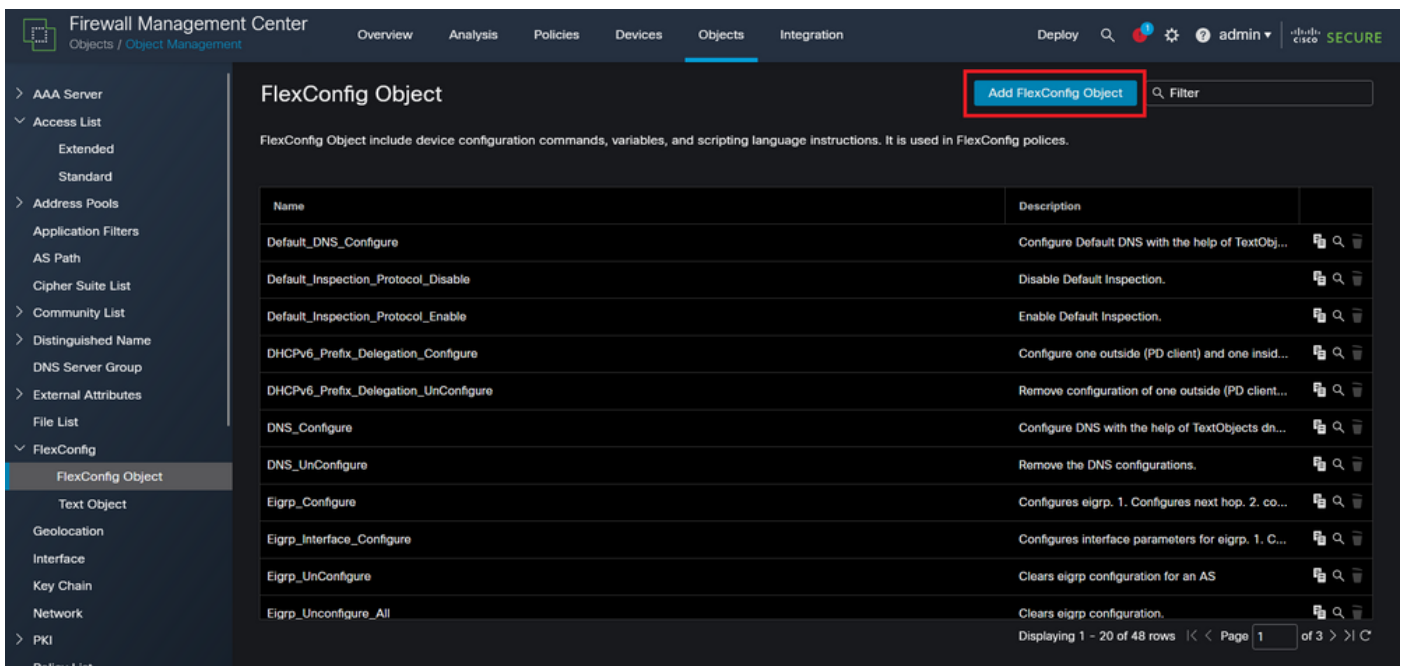


圖11.新增Flexconfig對象

步驟 3.2.為FlexConfig對象新增名稱，然後插入ACL策略對象。為此，請選擇Insert > Insert Policy Object > Extended ACL Object。

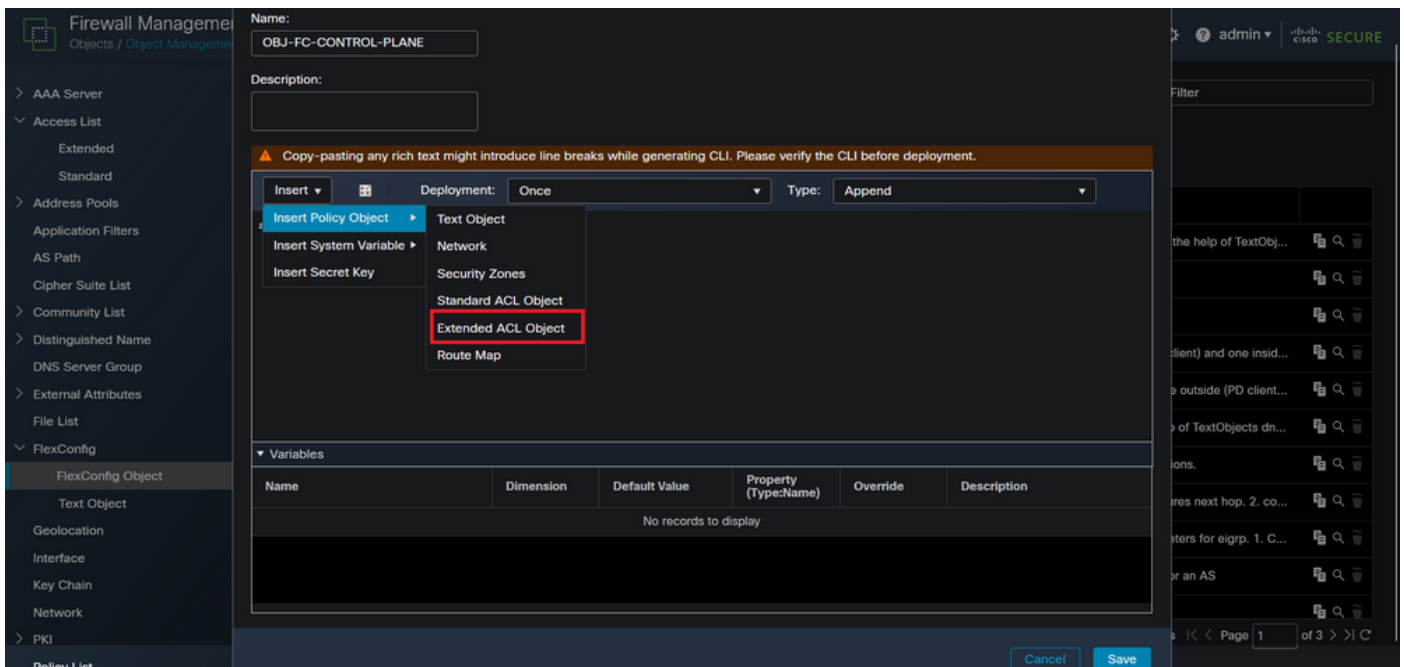


圖12.FlexConfig對象變數

步驟 3.3.為ACL對象變數新增名稱，然後選擇在步驟2.3中建立的擴展ACL，然後點選Save按鈕。

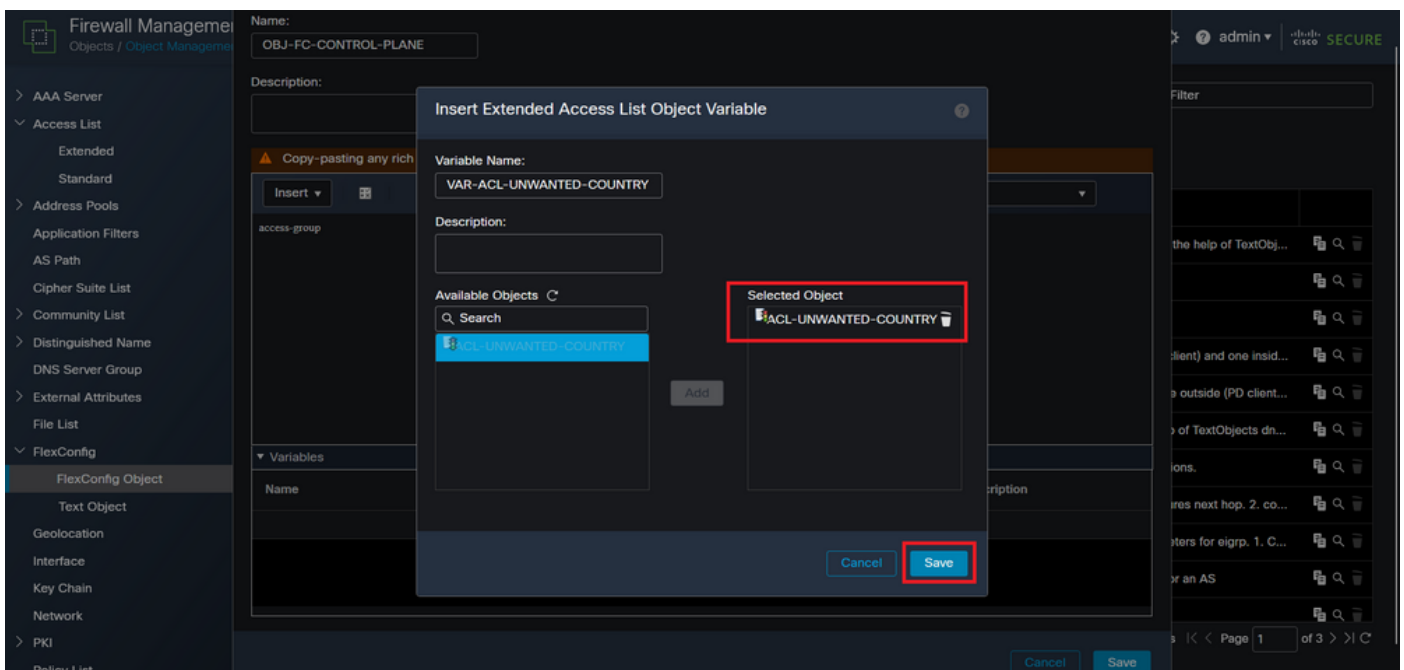


圖13.FlexConfig對象變數ACL分配

步驟 3.4.然後，將控制平面ACL配置為外部介面的入站流量，如下所示。

命令列語法：

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


此命令轉換為下一個命令示例，該示例使用在以上步驟2.3「VAR-ACL-UNWANTED-COUNTRY」中建立的ACL變數，如下所示：

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

這是必須配置到FlexConfig對象視窗中的方法，之後，選擇「儲存」按鈕完成FlexConfig對象。

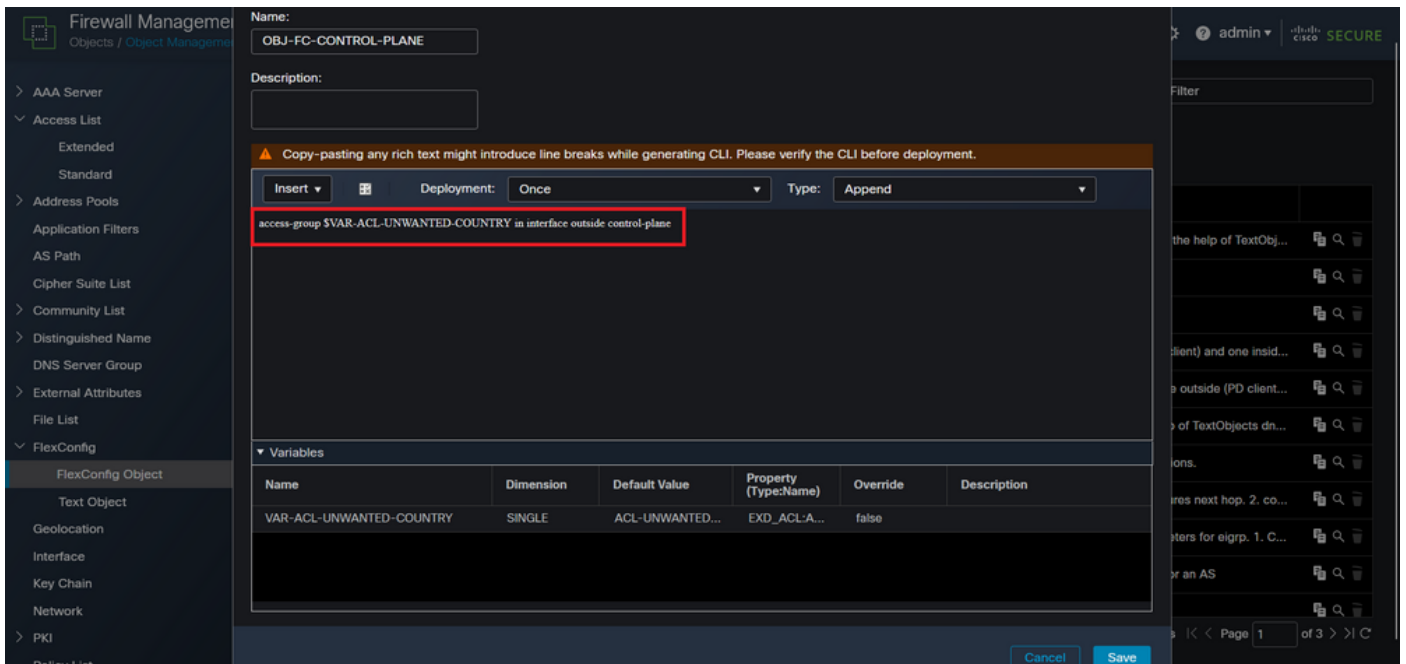


圖14.Flexconfig Object complete命令列

步驟 4.您需要將FlexConfig對象配置應用於FTD，為此，請轉至Devices > FlexConfig。

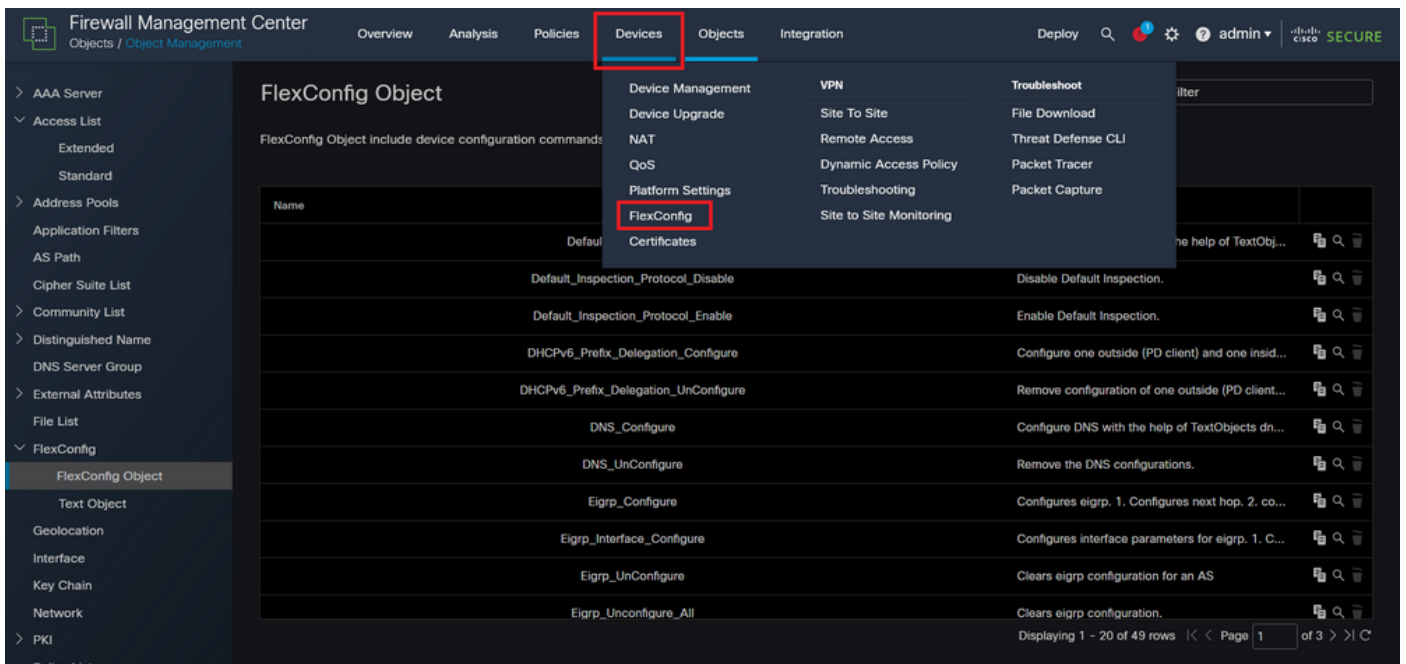


圖15.FlexConfig Policy選單

步驟 4.1.然後，如果沒有為FTD建立的FlexConfig，則點選New Policy，或編輯現有的FlexConfig策略。

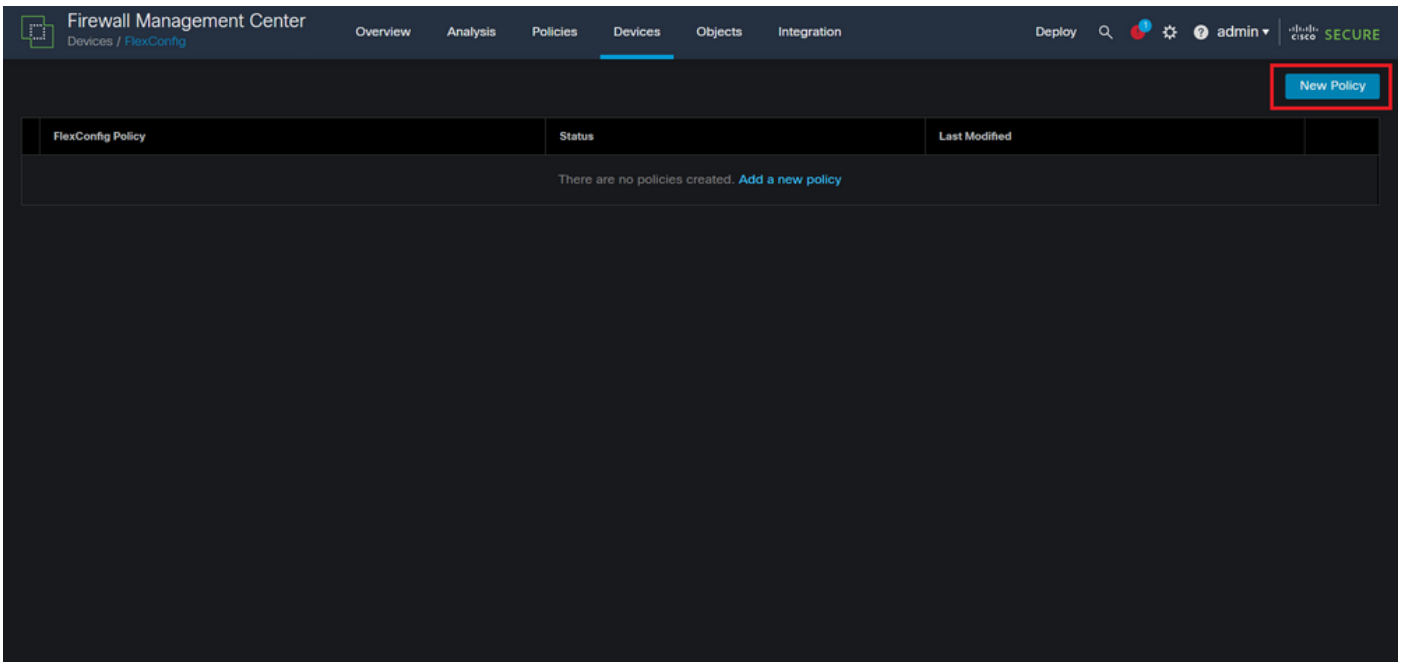


圖16.FlexConfig策略建立

步驟 4.2.為新的FlexConfig策略新增名稱，並選擇要應用建立的Control Plane ACL的FTD。

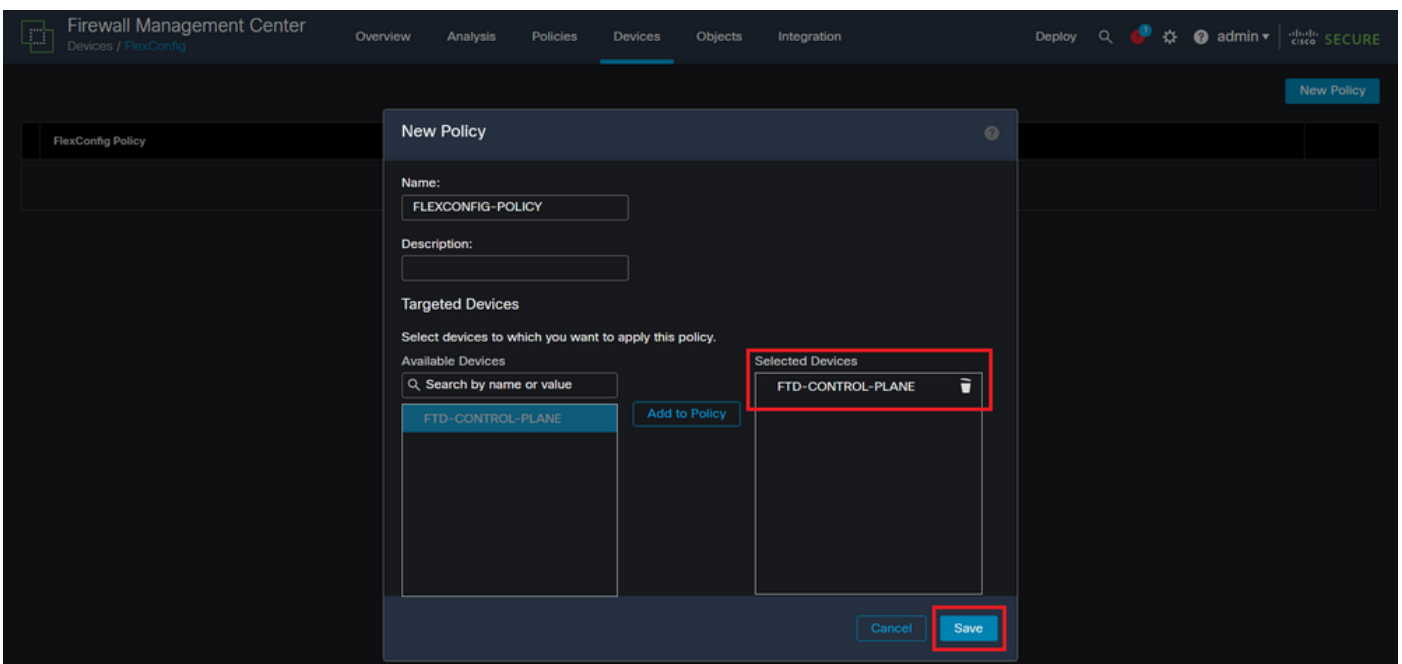


圖17.FlexConfig策略裝置分配

步驟 4.3.在左側面板中，搜尋在上面的步驟3.2中建立的FlexConfig對象，然後通過按一下位於視窗中間的右箭頭將其新增到FlexConfig策略中，然後點選Save按鈕。

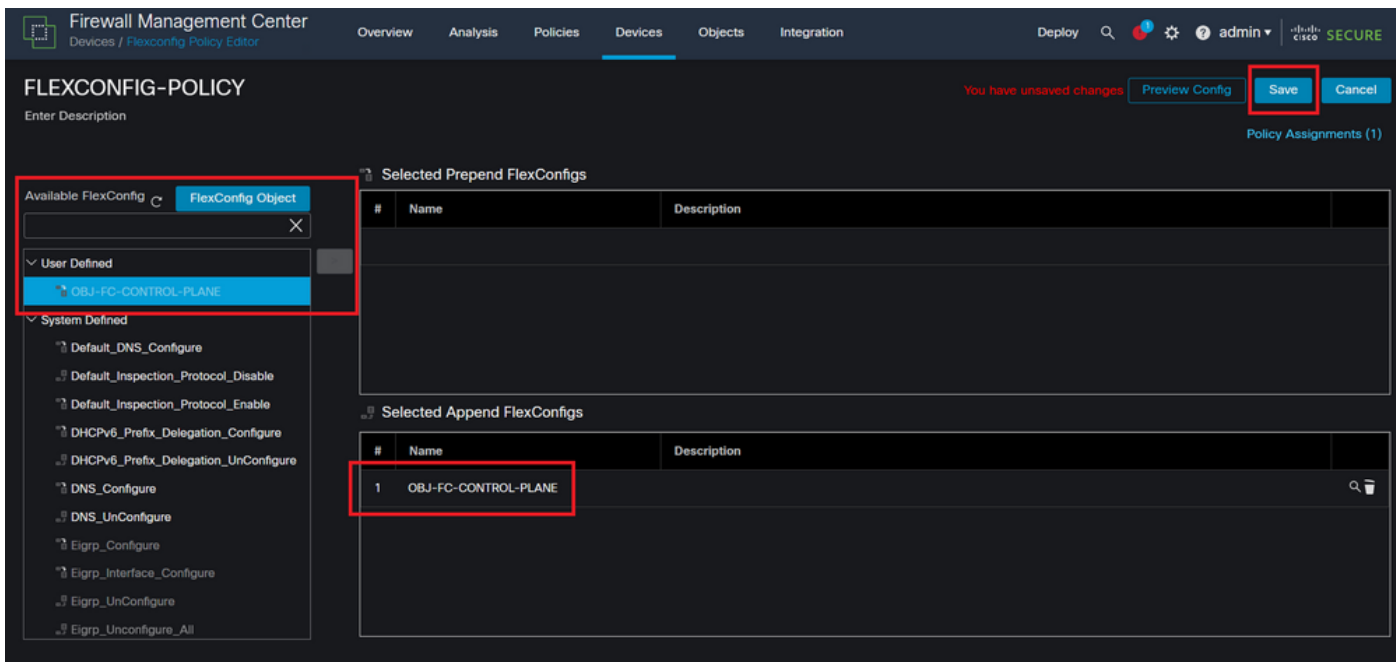


圖18.FlexConfig策略對象分配

步驟 5.繼續將組態變更部署到FTD，並為此請導覽至Deploy > Advanced Deploy。

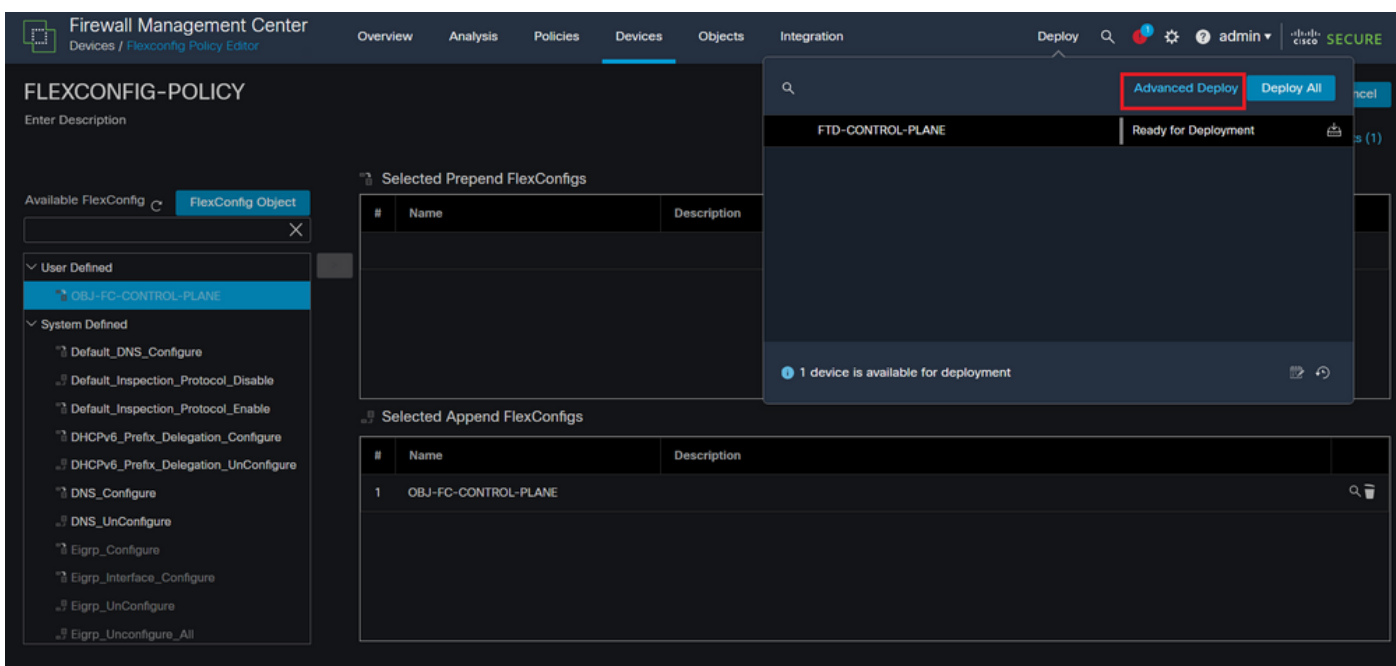


圖19.FTD進階部署

步驟 5.1.然後，選擇要應用FlexConfig策略的FTD。如果一切正常，則按一下「部署」。

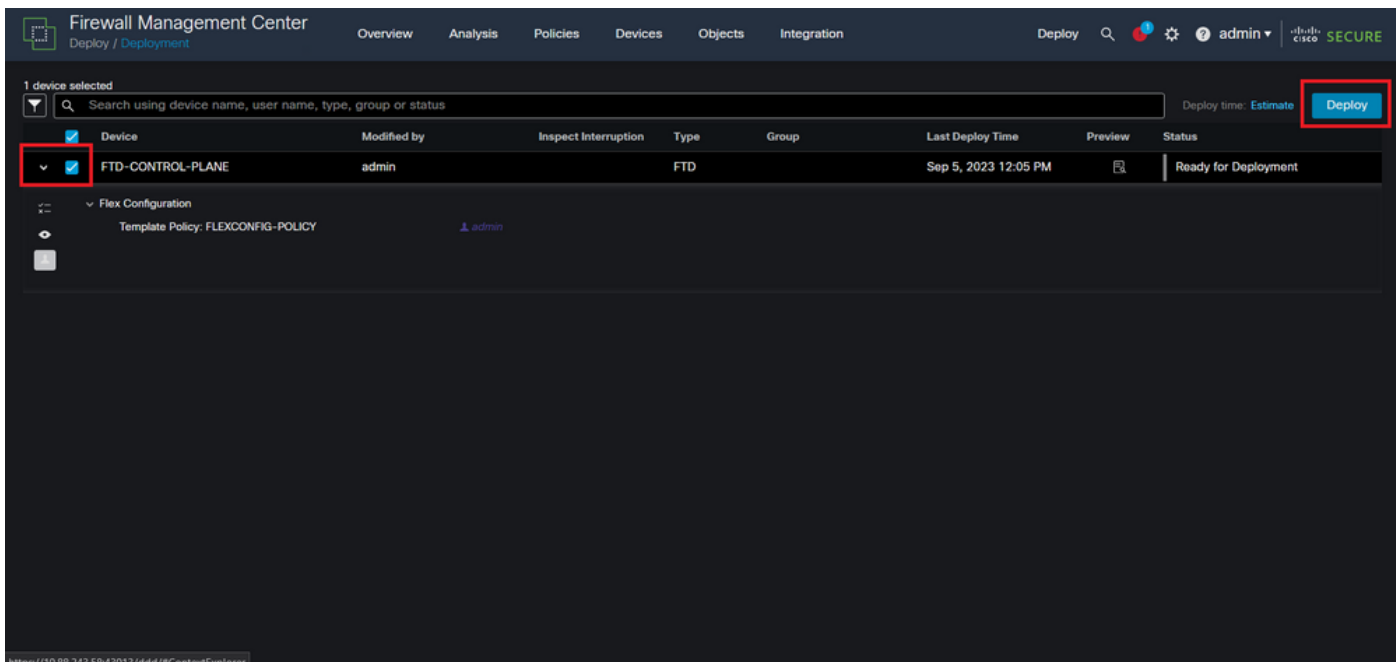


圖20.FTD部署驗證

步驟 5.2.之後，將彈出一個「部署確認」視窗，新增註釋以跟蹤部署並繼續進行「部署」。

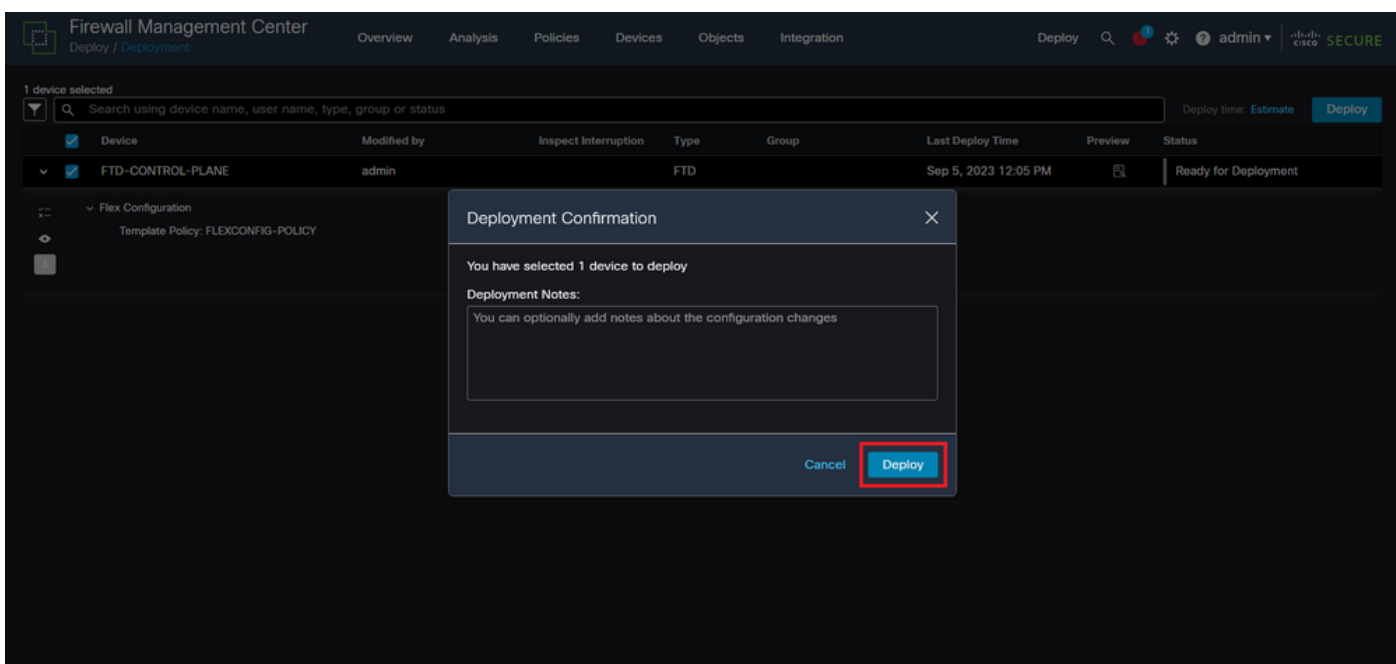


圖21.FTD部署註釋

步驟 5.3.部署FlexConfig更改時可能會出現警告消息。只有完全確定策略配置正確時，才按一下 Deploy。

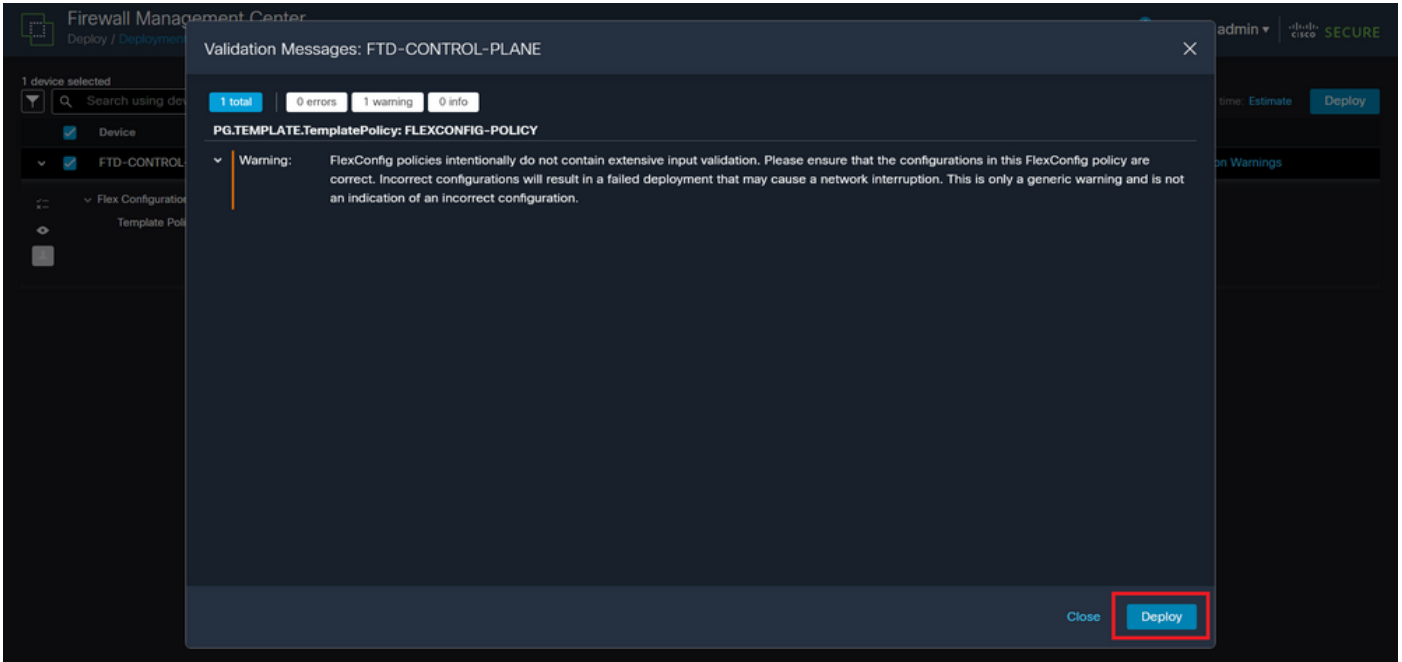


圖22.FTD部署Flexconfig警告

步驟 5.4.確認FTD的原則部署成功。

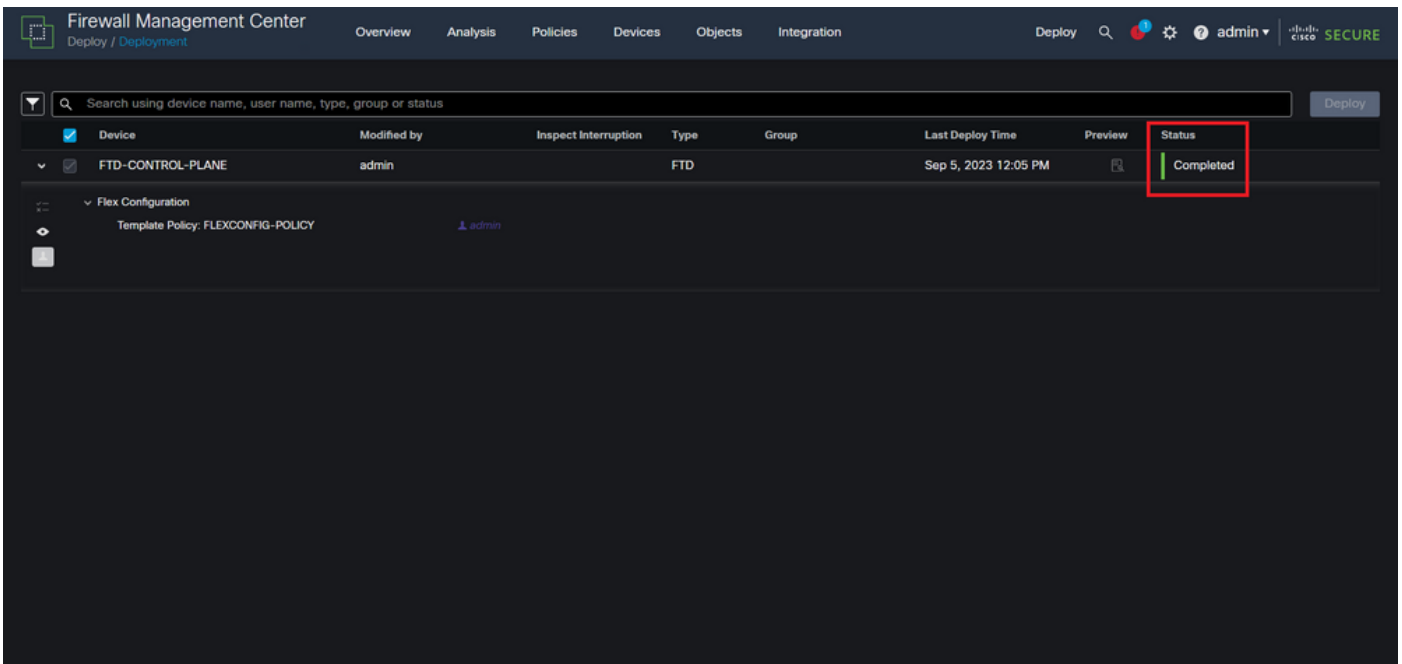


圖23.FTD部署成功

步驟 6. 如果您為FTD建立新控制平面ACL，或編輯現有控制平面ACL且現有控制平面ACL處於使用中，則務必強調所作的組態變更不適用於已建立與FTD的連線，因此，您需要手動清除與FTD的連線嘗試。為此，請連線到FTD的CLI並清除作用中連線，如下所示。

要清除特定主機IP地址的活動連線：


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

要清除整個子網網路的活動連線，請執行以下操作：

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

要清除IP地址範圍的活動連線，請執行以下操作：

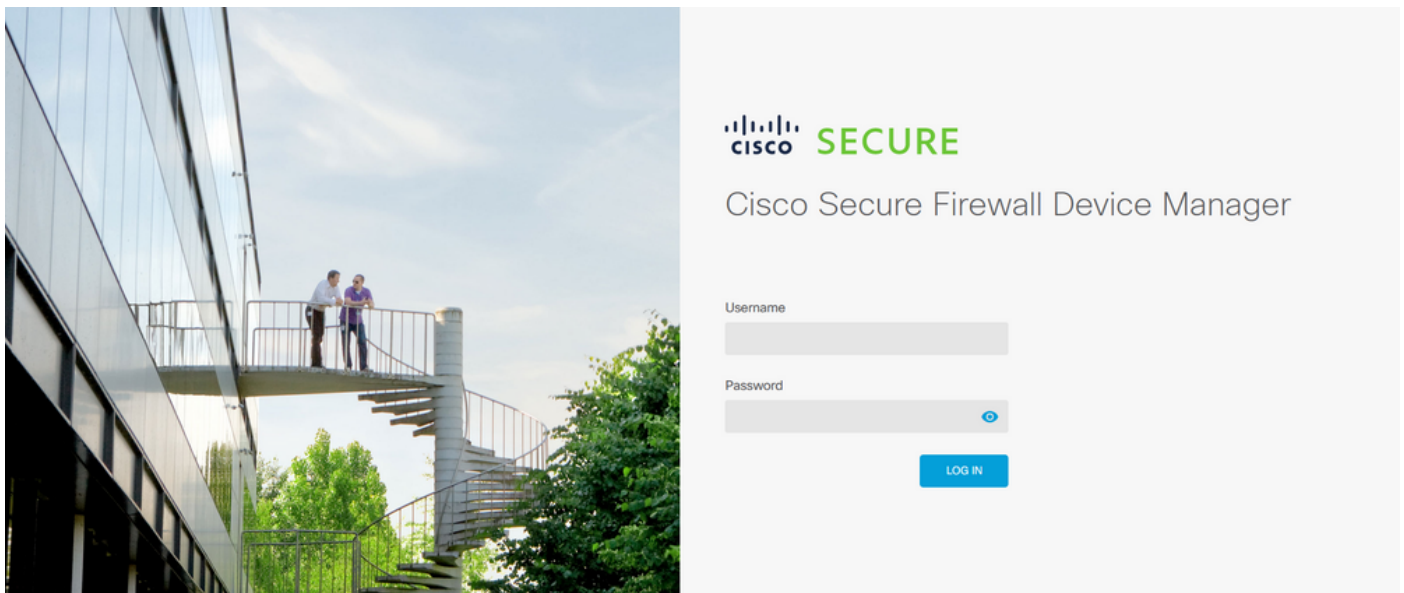
```
> clear conn address 192.168.1.1-192.168.1.10 all
```

 注意：強烈建議在clear conn address命令末尾使用關鍵字「all」，強制清除對安全防火牆的活動的VPN暴力連線嘗試，主要在VPN暴力攻擊的性質正在引發大量持續連線嘗試時。

為FDM管理的FTD配置控制平面ACL

在FDM中，需要遵循以下步驟來配置控制平面ACL，以阻止傳入VPN暴力攻擊到外部FTD介面：

步驟 1.通過HTTPS開啟FDM GUI並使用您的憑據登入。



© 2015-2023 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. This product contains some software licensed under the "GNU Lesser General Public License, versions: 2, 2.1 and 3" provided with ABSOLUTELY NO WARRANTY under the terms of "GNU Lesser General Public License, [version 2](#), [version 2.1](#) and [version 3](#)".

圖24. 「FDM登入」頁

步驟 2.您需要建立對象網路。為此，請導航到Objects:

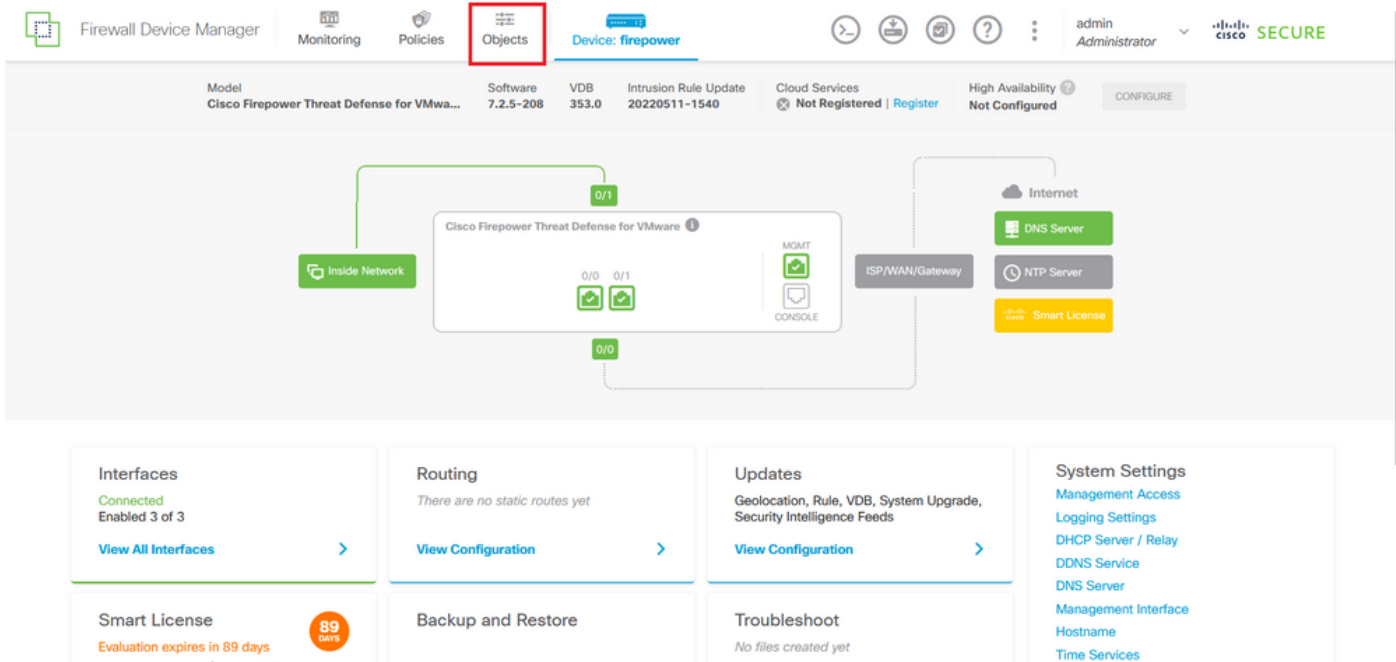


圖25.FDM主儀表板

步驟 2.1.在左側面板中選擇Networks，然後按一下「+」按鈕建立新的網路對象。

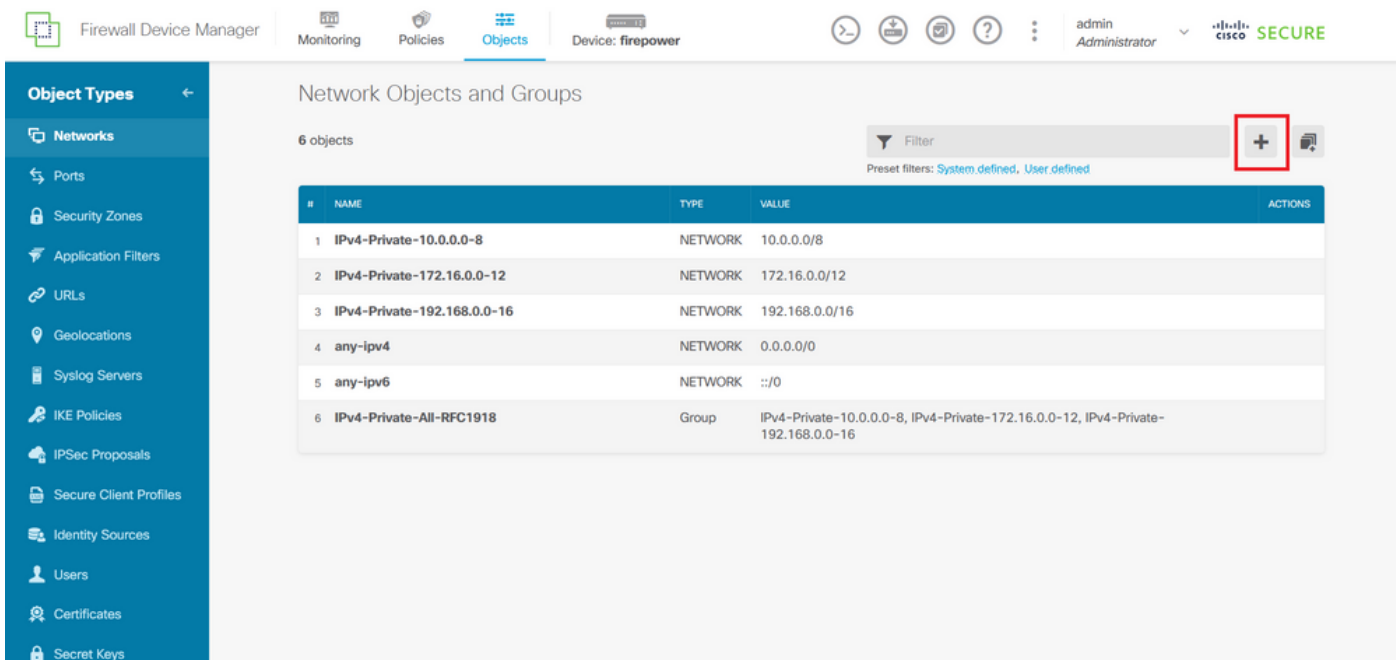


圖26.對象建立

步驟 2.2.為網路物件新增名稱，為物件選取網路型別，並新增IP位址、網路位址或IP範圍，以與需要拒絕到FTD的流量相符。然後，按一下「確定」(OK)按鈕完成對象網路。

— 在本示例中，配置的對象網路旨在阻止來自192.168.1.0/24子網的VPN暴力攻擊。

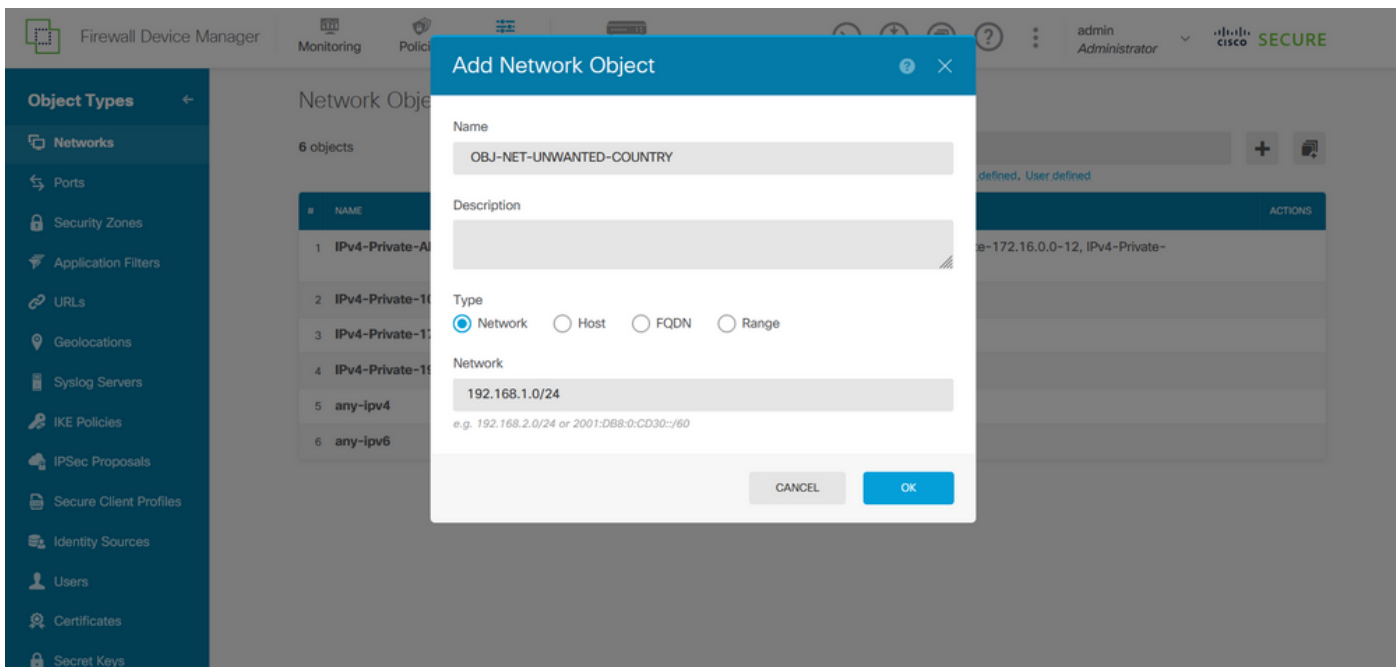


圖27.新增網路對象

步驟 3.然後，您需要建立一個延伸型ACL，為此，請導航到頂部選單的「Device (裝置)」頁籤。

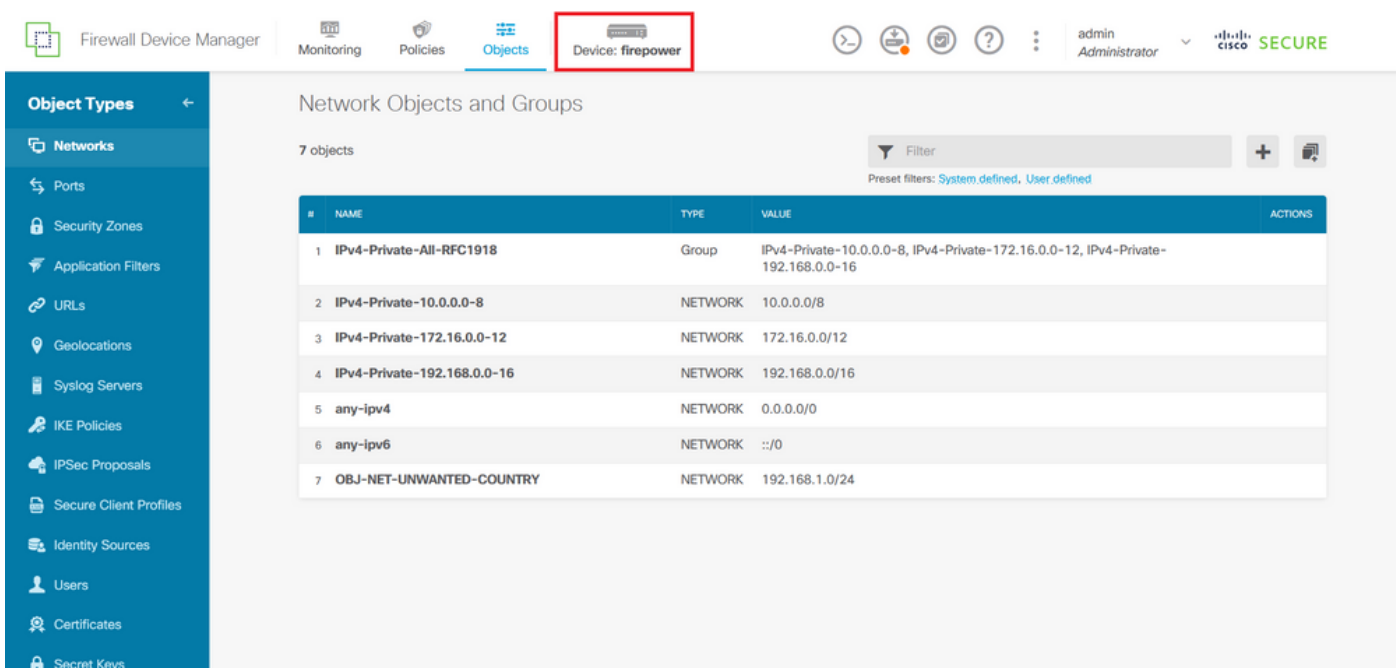


圖28.「裝置設定」頁

步驟 3.1.向下滾動，從Advanced Configuration (高級配置) 方塊中選擇View Configuration (檢視配置)，如下所示。

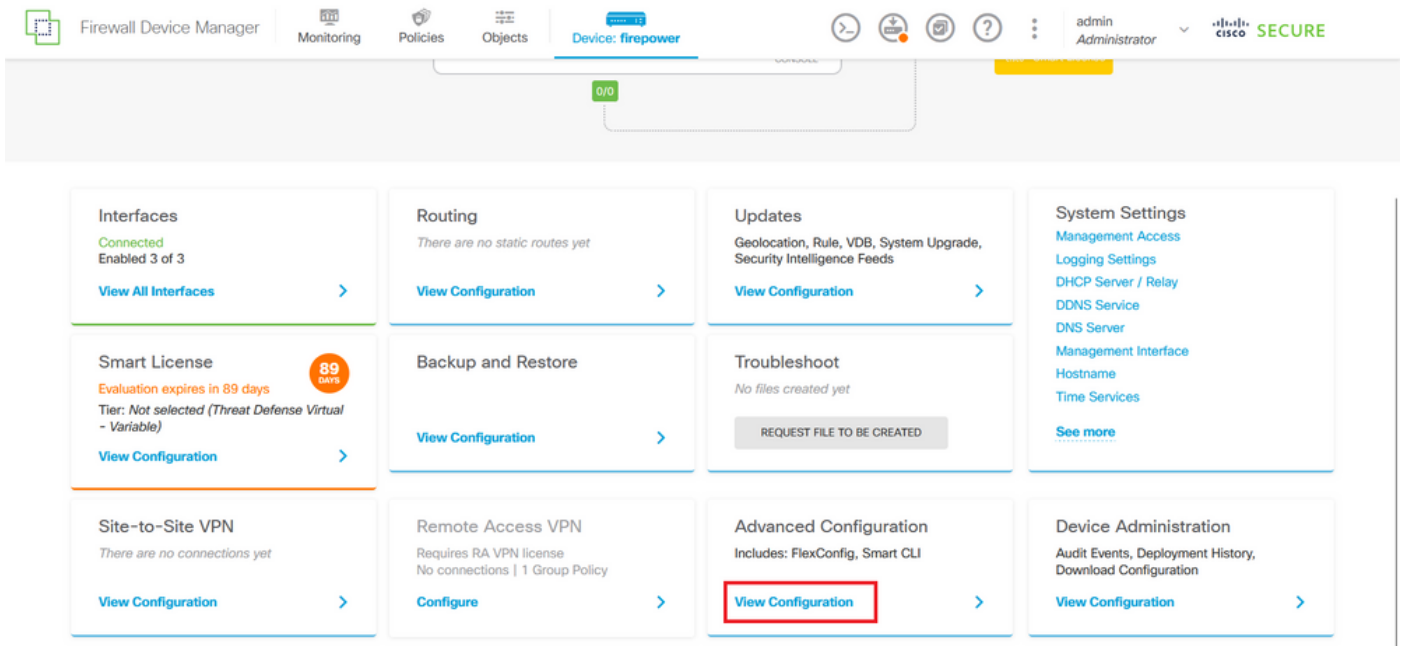


圖29.FDM高級配置

步驟 3.2.然後，從左側面板導航到Smart CLI > Objects，然後點選CREATE SMART CLI OBJECT。

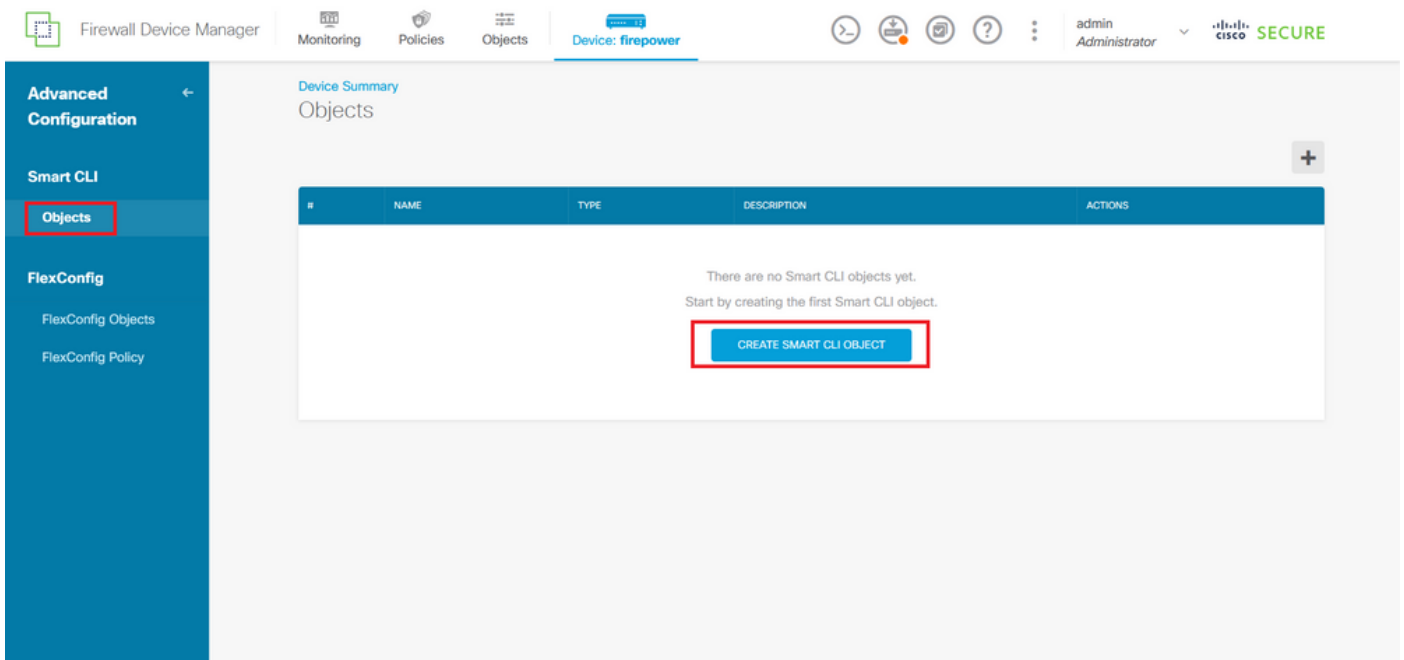


圖30.智慧CLI對象

步驟 3.3.為要建立的擴展ACL新增名稱，從CLI模板下拉選單中選擇Extended Access List，並使用在上面的步驟2.2中建立的網路對象配置所需的ACE，然後按一下OK按鈕完成ACL。

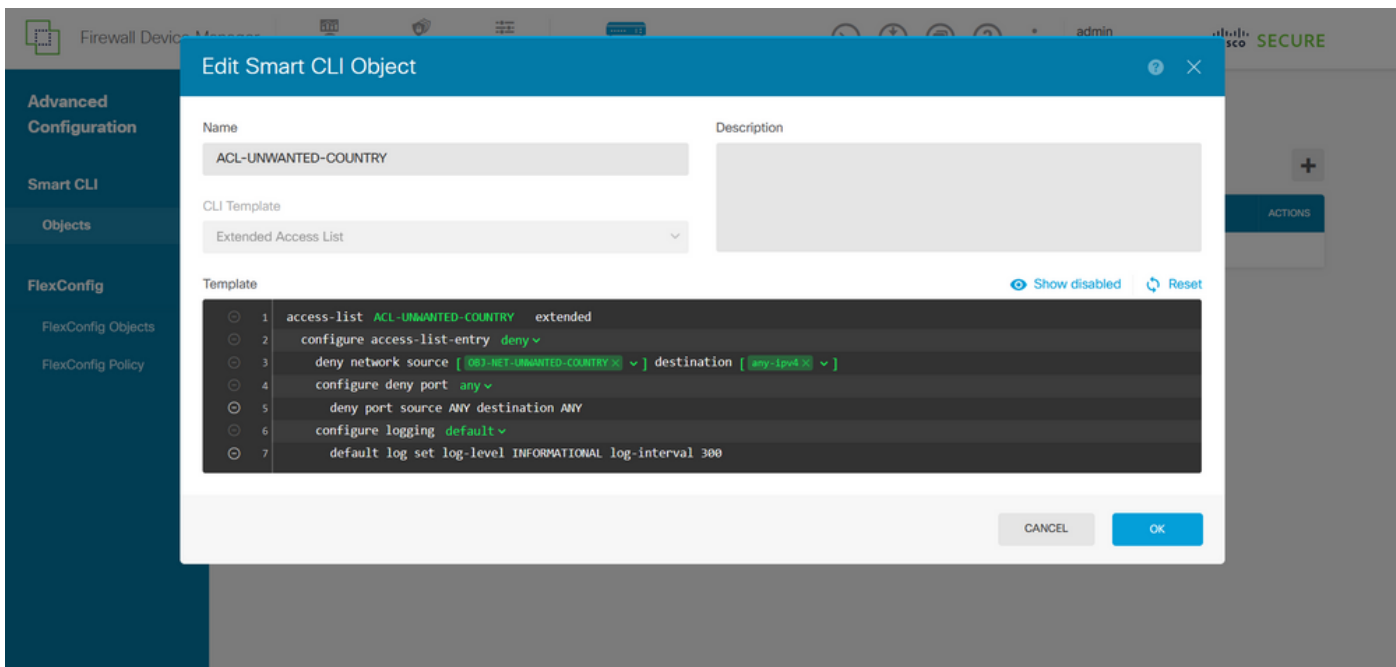



圖31.擴展ACL建立

 注意：如果需要為ACL新增更多ACE，可以將滑鼠懸停在當前ACE的左側，這樣就會出現三個可點選的點。按一下它們並選擇「複製」以新增更多ACE。

步驟 4. 然後，您需要建立FlexConfig對象，為此，請導航到左側面板並選擇FlexConfig > FlexConfig對象，然後按一下CREATE FLEXCONFIG OBJECT。

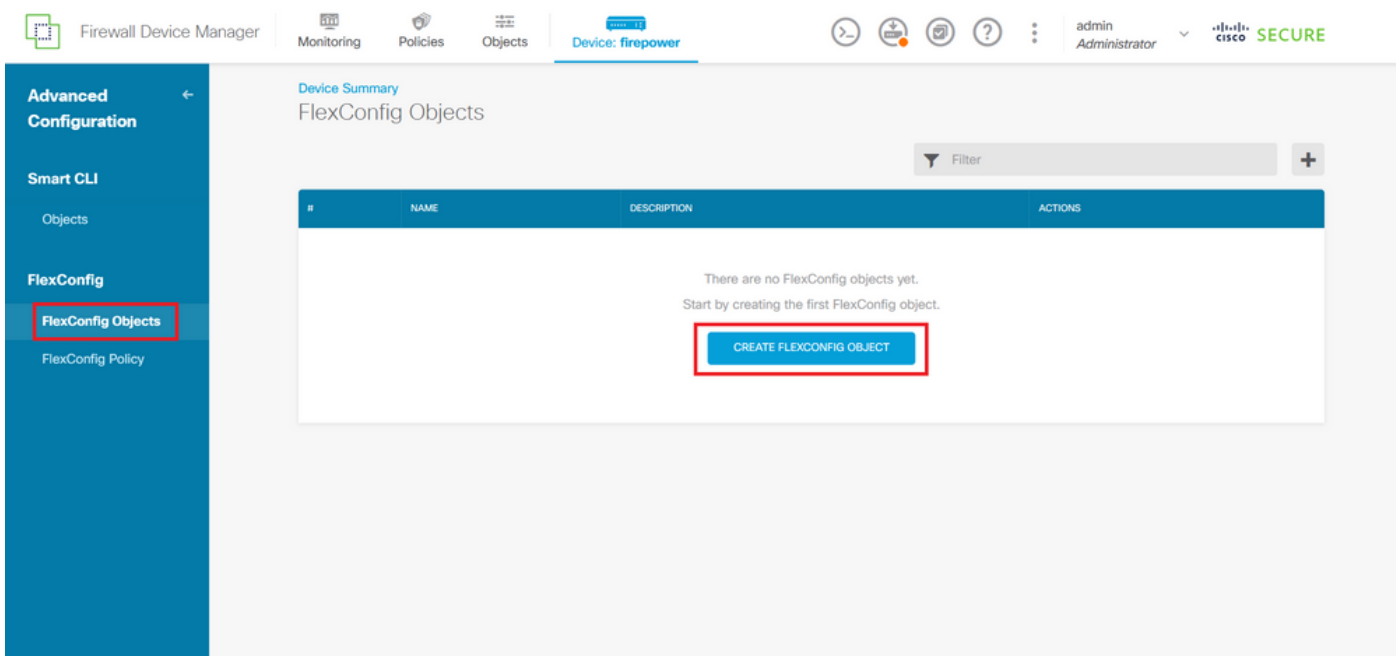


圖32.FlexConfig對象

步驟 4.1. 為FlexConfig對象新增名稱，以建立控制平面ACL並將其配置為外部介面的入站流量，如下所示。

命令列語法：

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

這轉換為下一個命令示例，該示例使用在以上步驟3.3「ACL-UNWANTED-COUNTRY」中建立的擴展ACL，如下所示：

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

這是將其配置到FlexConfig對象視窗的方式，之後，選擇「確定」(OK)按鈕完成FlexConfig對象。

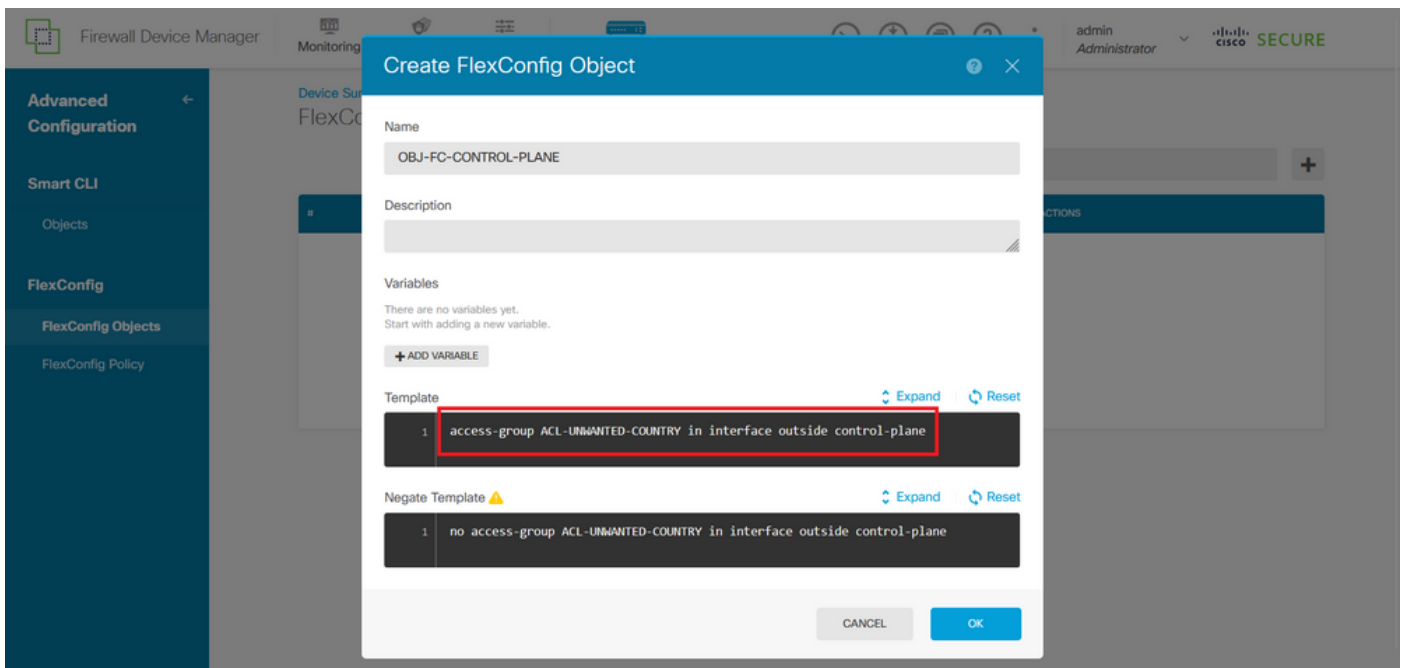


圖33.FlexConfig對象建立

步驟 5.繼續建立FlexConfig策略，為此，請導航到Flexconfig > FlexConfig Policy，按一下「+」按鈕，然後選擇在上面的步驟4.1中建立的FlexConfig對象。

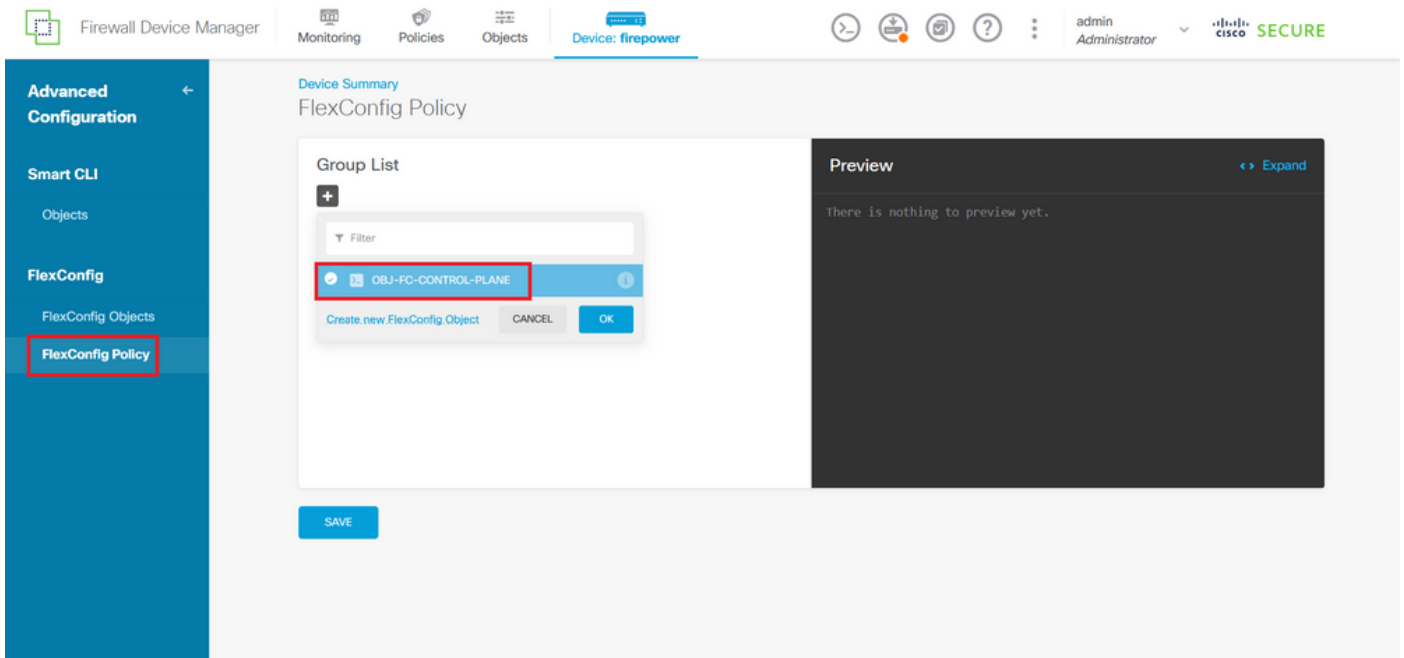


圖34.FlexConfig策略

步驟 5.1. 驗證FlexConfig預覽是否顯示所建立的控制平面ACL的正確配置，然後按一下「Save (儲存)」按鈕。

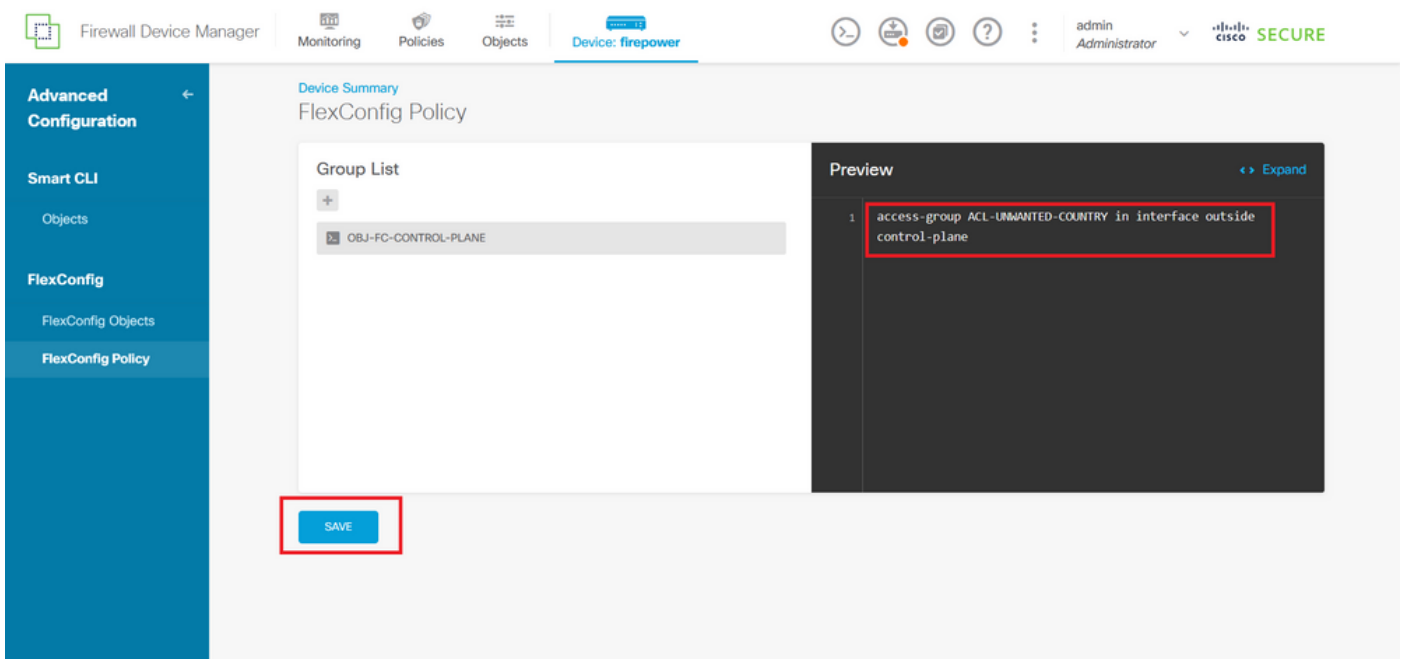


圖35.FlexConfig策略預覽

步驟 6. 將配置更改部署到要防禦VPN暴力攻擊的FTD，為此，按一下頂部選單上的Deployment按鈕，驗證要部署的配置更改是否正確，然後按一下DEPLOY NOW。

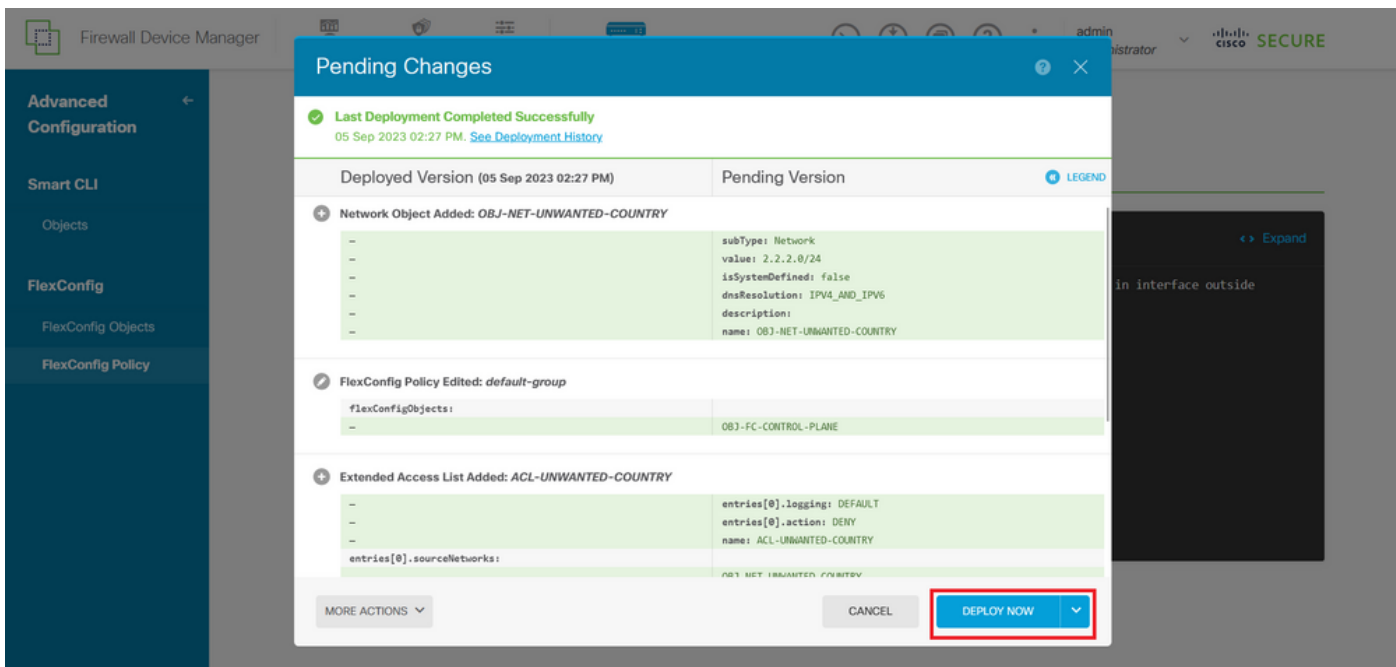


圖36.掛起的部署

步驟 6.1.驗證策略部署是否成功。

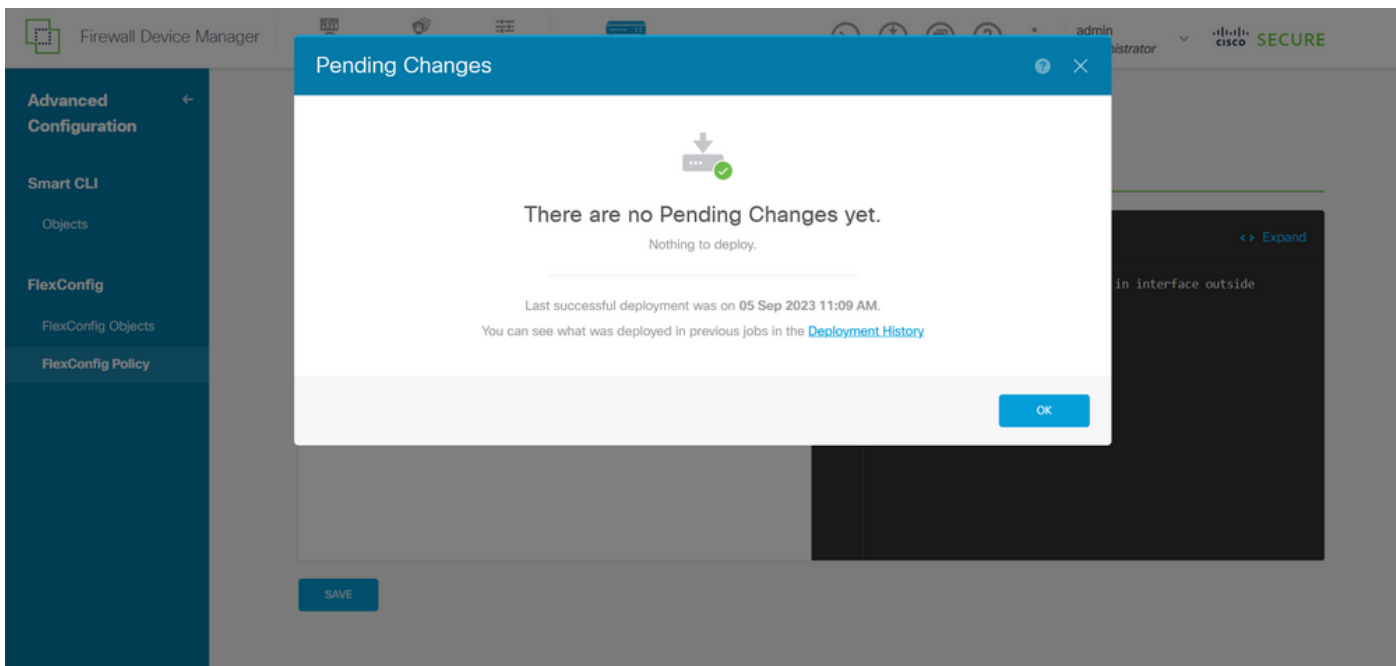


圖37.部署成功

步驟 7. 如果您為FTD建立新控制平面ACL，或編輯現有控制平面ACL且現有控制平面ACL處於使用中，則務必強調所作的組態變更不適用於已建立與FTD的連線，因此，您需要手動清除與FTD的連線嘗試。為此，請連線到FTD的CLI並清除作用中連線，如下所示。

要清除特定主機IP地址的活動連線：


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

要清除整個子網網路的活動連線，請執行以下操作：

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

要清除IP地址範圍的活動連線，請執行以下操作：

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

 注意：強烈建議在clear conn address命令末尾使用關鍵字「all」，強制清除對安全防火牆的活動的VPN暴力連線嘗試，主要在VPN暴力攻擊的性質正在引發大量持續連線嘗試時。

使用CLI為ASA配置控制平面ACL

您需要在ASA CLI中按照以下步驟配置控制平面ACL以阻止傳入的VPN暴力攻擊到外部介面：

步驟 1.通過CLI登入安全防火牆ASA並訪問「配置終端」，如下所示。

```
asa# configure terminal
```

步驟 2.使用next命令配置擴展ACL，以阻止需要阻止到ASA的流量的主機IP地址或網路地址。

— 在本示例中，您將建立一個名為「ACL-WANTED-COUNTRY」的新ACL，並且配置的ACE條目將阻止來自192.168.1.0/24子網的VPN暴力攻擊。

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

步驟 3.使用next access-group命令將「ACL-UNWANTED-COUNTRY」ACL配置為外部ASA介面的控制平面ACL。

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

步驟 4. 如果建立新的控制平面ACL或編輯了正在使用的現有控制平面ACL，則必須強調所做的配置

更改不適用於已建立到ASA的連線，因此，您需要手動清除對ASA的活動連線嘗試。為此，請按如下所示清除活動連線。

要清除特定主機IP地址的活動連線：


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

要清除整個子網網路的活動連線，請執行以下操作：

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

要清除IP地址範圍的活動連線，請執行以下操作：

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

 **注意：**強烈建議在clear conn address命令末尾使用關鍵字「all」，強制清除對安全防火牆的活動的VPN暴力連線嘗試，主要在VPN暴力攻擊的性質正在引發大量持續連線嘗試時。

使用「shun」命令阻止安全防火牆攻擊的備用配置

如果存在阻止安全防火牆攻擊的立即選項，則可以使用「shun」命令。使用Thuncommand可以阻止來自攻擊主機的連線。

— 迴避IP地址後，源IP地址的所有未來連線都會被丟棄並記錄，直到手動刪除阻止功能為止。

— 無論具有指定主機地址的連線當前是否處於活動狀態，都會應用thuncommand的阻止功能。

— 如果指定目的地地址、來源和目的地連線埠和通訊協定，則會捨棄相符的連線，並對來自來源IP的所有未來連線設定迴避

地址；將來所有連線都將被迴避，而不僅僅是那些匹配這些特定連線引數的連線。

— 每個源IP地址只能使用oneshuncommand。

— 由於thuncommand用於動態阻止攻擊，因此它不會顯示在威脅防禦設備配置中。

— 每當刪除介面配置時，也會刪除連線到該介面的所有分路。

- Shun命令語法：

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

— 要禁用shun，請使用此命令的no形式：

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

要避開主機IP地址，請按照以下步驟處理安全防火牆。在本示例中，「shun」命令用於阻止來自源IP地址192.168.1.10的VPN暴力攻擊。

FTD的組態範例。

步驟 1.透過CLI登入FTD，然後按以下方式套用shun指令。

```
<#root>
```

```
>
```

```
shun 192.168.1.10
```

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

```
Shun 192.168.1.10 successful
```

步驟 2. 您可以使用以下show命令確認FTD中的shun IP位址，並監控每個IP位址的shun命中次數：

```
<#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)
```

ASA配置示例

步驟 1. 通過CLI登入到ASA並按如下方式應用shun命令。

```
<#root>
asa#
  shun 192.168.1.10
Shun 192.168.1.10 added in context: single_vf

Shun 192.168.1.10 successful
```

步驟 2. 您可以使用以下show命令確認ASA中的shun IP地址並監控每個IP地址的shun命中數：

```
<#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)
```

 注意：有關secure firewall shun命令的詳細資訊，請檢視[思科安全防火牆威脅防禦命令參考](#)

驗證

要確認安全防火牆的控制平面ACL配置已就緒，請按照以下步驟操作：

步驟 1. 通過CLI登入安全防火牆，並運行以下命令以確認已應用控制平面ACL配置。

FMC管理的FTD的輸出示例：

```
<#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
```

FDM管理的FTD的输出示例：

```
<#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
```

ASA的输出示例：

```
<#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
```

步驟 2. 要確認控制平面ACL正在阻止所需的流量，請使用packet-tracer命令模擬到安全防火牆外部介面的傳入TCP 443連線，然後使用show access-list <acl-name> 命令，每當到安全防火牆的VPN暴力連線被控制平面ACL阻止時，ACL命中計數都會增加：

— 在本例中，packet Tracer命令模擬從主機192.168.1.10發往安全防火牆外部IP地址的傳入TCP 443連線。「packet Tracer」輸出確認流量被丟棄，而「show access-list」輸出則顯示現有控制平面ACL的命中計數增量：

FTD的輸出範例

```
<#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
```

ASA的輸出示例

```
<#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
```

 注意：如果在安全防火牆中實施類似Cisco安全客戶端VPN的RAVPN解決方案，則可能會執行到安全防火牆的真實連線嘗試，以確認控制平面ACL是否按預期工作，從而阻止所需的流量。

相關錯誤

- ENH | 基於地理位置的AnyConnect客戶端連線：思科錯誤ID [CSCvs65322](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。