

# Konfigurieren von Zugriffskontrollrichtlinien auf Kontrollebene für sicheren Schutz vor Bedrohungen durch Firewalls und ASA

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfigurationen](#)

[Konfigurieren einer von FMC verwalteten Kontrollebenen-ACL für FTD](#)

[Konfigurieren einer von FDM verwalteten Kontrollebenen-ACL für FTD](#)

[Konfigurieren einer Kontrollebenen-ACL für ASA mit CLI](#)

[Alternative Konfiguration zum Blockieren von Angriffen für eine sichere Firewall mithilfe des Befehls "shun"](#)

[Überprüfung](#)

[Verwandte Fehler](#)

---

## Einleitung

In diesem Dokument wird der Prozess zur Konfiguration von Zugriffsregeln auf Kontrollebene für die Secure Firewall Threat Defense- und die Adaptive Security Appliance (ASA) beschrieben.

## Voraussetzungen

### Anforderungen

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

- Sichere Firewall-Bedrohungsabwehr (FTD)
- Sicherer Firewall-Gerätanager (FDM)
- Secure Firewall Management Center (FMC)
- Sichere Firewall ASA
- Zugriffskontrollliste (ACL)
- FlexConfig

### Verwendete Komponenten

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

Versionen:

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

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 kennen.

## Hintergrundinformationen

Der Datenverkehr durchläuft in der Regel eine Firewall und wird zwischen Datenschnittstellen weitergeleitet. In manchen Fällen ist es sinnvoll, den Datenverkehr, der für die sichere Firewall bestimmt ist, zu verweigern. Die sichere Cisco Firewall kann mithilfe einer Zugriffskontrollliste auf Kontrollebene (Control-Plane Access Control List, ACL) den einsatzbereiten Datenverkehr beschränken. Ein Beispiel für den Fall, dass eine Kontrollebenen-ACL nützlich sein kann, wäre die Kontrolle darüber, welche Peers einen VPN-Tunnel (Site-to-Site oder Remote Access VPN) zur sicheren Firewall einrichten können.

Sichere Firewall durch einsatzbereiten Datenverkehr

Der Datenverkehr durchläuft in der Regel Firewalls von einer Schnittstelle (eingehend) zu einer anderen Schnittstelle (ausgehend). Dies wird als Durchgangsverkehr bezeichnet und wird von den Zugriffskontrollrichtlinien (ACP) und den Vorfilterregeln verwaltet.

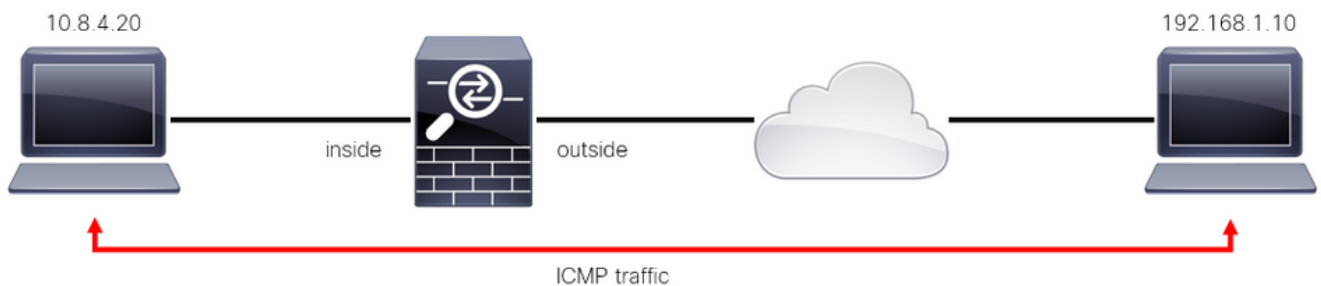


Bild 1. Beispiel für Datenverkehr durch die Box

Sicherer, sofort einsatzbereiter Firewall-Datenverkehr

Es gibt andere Fälle, in denen der Datenverkehr direkt an eine FTD-Schnittstelle (Site-to-Site- oder Remote Access-VPN) gerichtet ist. Dies wird als einsatzbereiter Datenverkehr bezeichnet und von der Kontrollebene dieser Schnittstelle verwaltet.

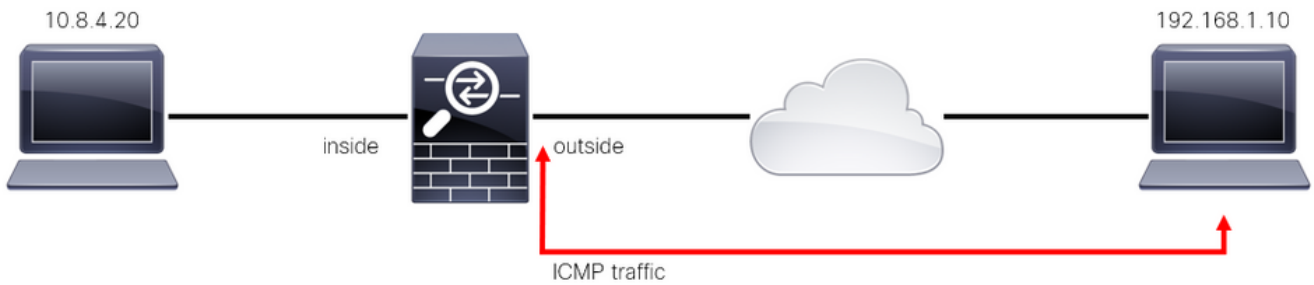


Bild 2. Beispiel für standortunabhängigen Datenverkehr

## Wichtige Überlegungen zu ACLs auf Kontrollebene

- Ab FMC/FTD Version 7.0 muss eine ACL der Kontrollebene mit FlexConfig konfiguriert werden, wobei dieselbe Befehlssyntax wie für die ASA verwendet wird.
- Das Schlüsselwort "control-plane" wird an die Zugriffsgruppenkonfiguration angefügt, die den Datenverkehr "zur" sicheren Firewall-Schnittstelle erzwingt. Ohne das an den Befehl angehängte Wort für die Kontrollebene würde die ACL den Datenverkehr "durch" die sichere Firewall einschränken.
- Eine Kontrollebenen-ACL schränkt den eingehenden SSH-, ICMP- oder TELNET-Verkehr zu einer sicheren Firewall-Schnittstelle nicht ein. Diese werden gemäß den Plattformeinstellungsrichtlinien verarbeitet (zugelassen/abgelehnt) und haben eine höhere Priorität.
- Eine ACL auf Kontrollebene beschränkt den Datenverkehr "zur" sicheren Firewall selbst, während die Zugriffskontrollrichtlinie für FTD oder die normalen ACLs für ASA den Datenverkehr "durch" die sichere Firewall steuert.
- Im Gegensatz zu einer normalen ACL wird am Ende der ACL kein implizites "deny" (Verweigern) angezeigt.
- Zum Zeitpunkt der Erstellung dieses Dokuments kann die FTD-Standortbestimmung nicht verwendet werden, um den Zugriff auf das FTD einzuschränken.

## Konfigurieren

Im nächsten Beispiel versucht eine Gruppe von IP-Adressen aus einem bestimmten Land, VPN-Brute-Force-Angriffe auf das Netzwerk auszuführen, indem sie versucht, sich beim FTD RAVPN anzumelden. Die beste Option zum Schutz des FTD vor diesen VPN-Brute-Force-Angriffen ist die Konfiguration einer Kontrollebenen-ACL, um diese Verbindungen zur externen FTD-Schnittstelle zu blockieren.

## Konfigurationen

Konfigurieren einer von FMC verwalteten Kontrollebenen-ACL für FTD

Mit diesem Verfahren müssen Sie in einem FMC eine Kontrollebenen-ACL konfigurieren, um eingehende VPN-Brute-Force-Angriffe auf die externe FTD-Schnittstelle zu blockieren:

Schritt 1: Öffnen Sie die grafische Benutzeroberfläche (GUI) von FMC über HTTPS, und melden Sie sich mit Ihren Anmeldeinformationen an.



Bild 3. FMC-Anmeldeseite

Schritt 2: Sie müssen eine erweiterte Zugriffskontrollliste erstellen. Navigieren Sie dazu zu Objekte > Objektverwaltung.

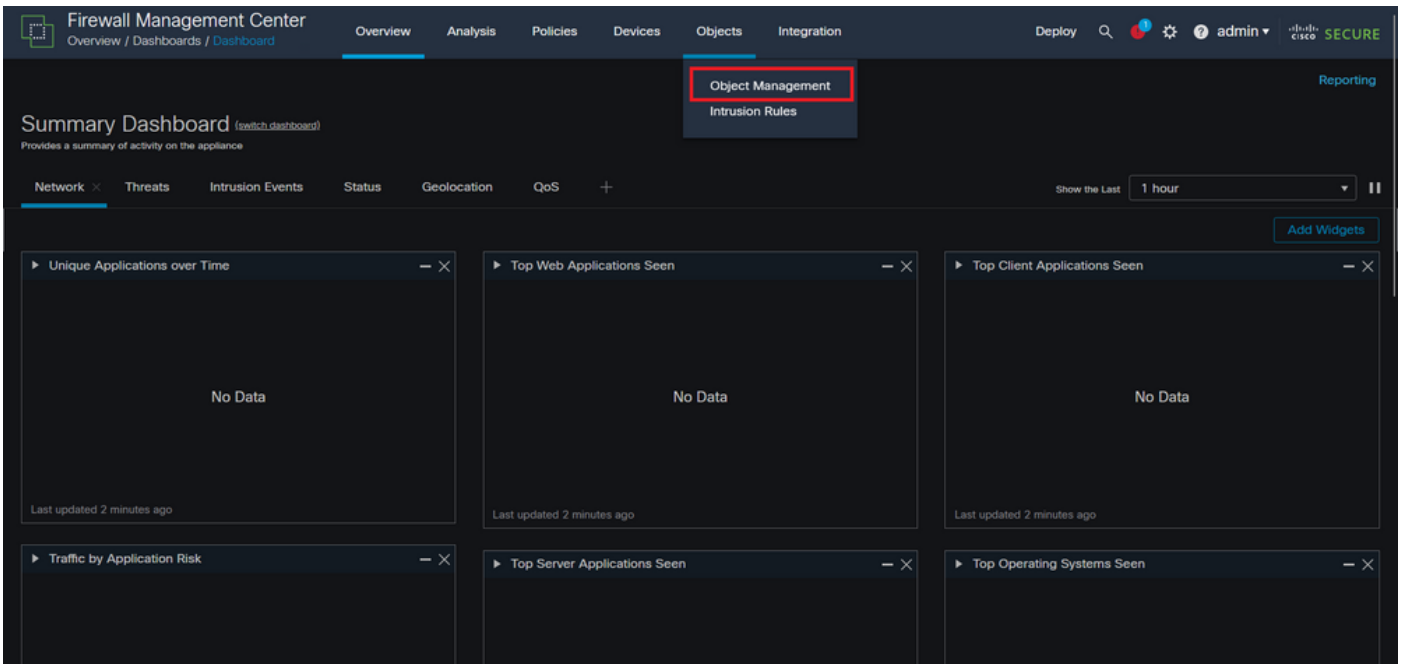


Abbildung 4: Objektmanagement

Schritt 2.1: Navigieren Sie im linken Bereich zu Access List > Extended (Zugriffsliste > Erweitert), um eine erweiterte ACL zu erstellen.

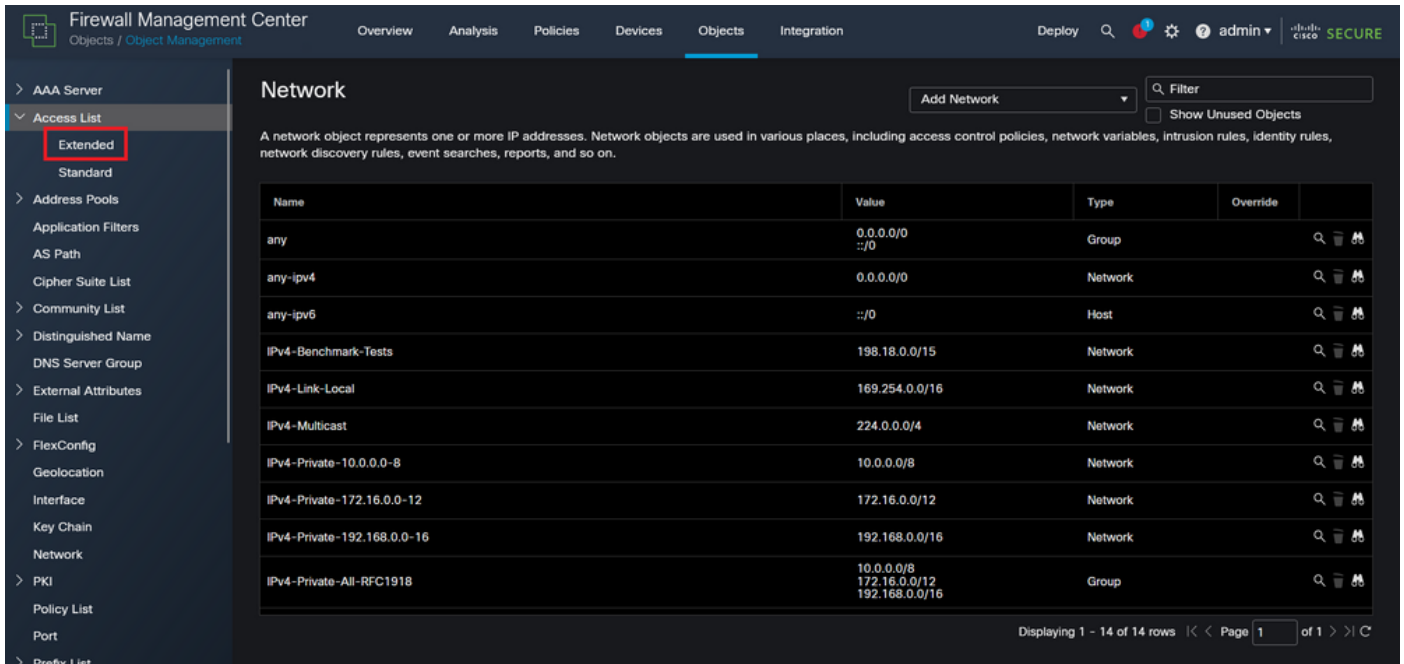


Bild 5. Erweitertes ACL-Menü

Schritt 2.2: Wählen Sie dann Erweiterte Zugriffsliste hinzufügen aus.

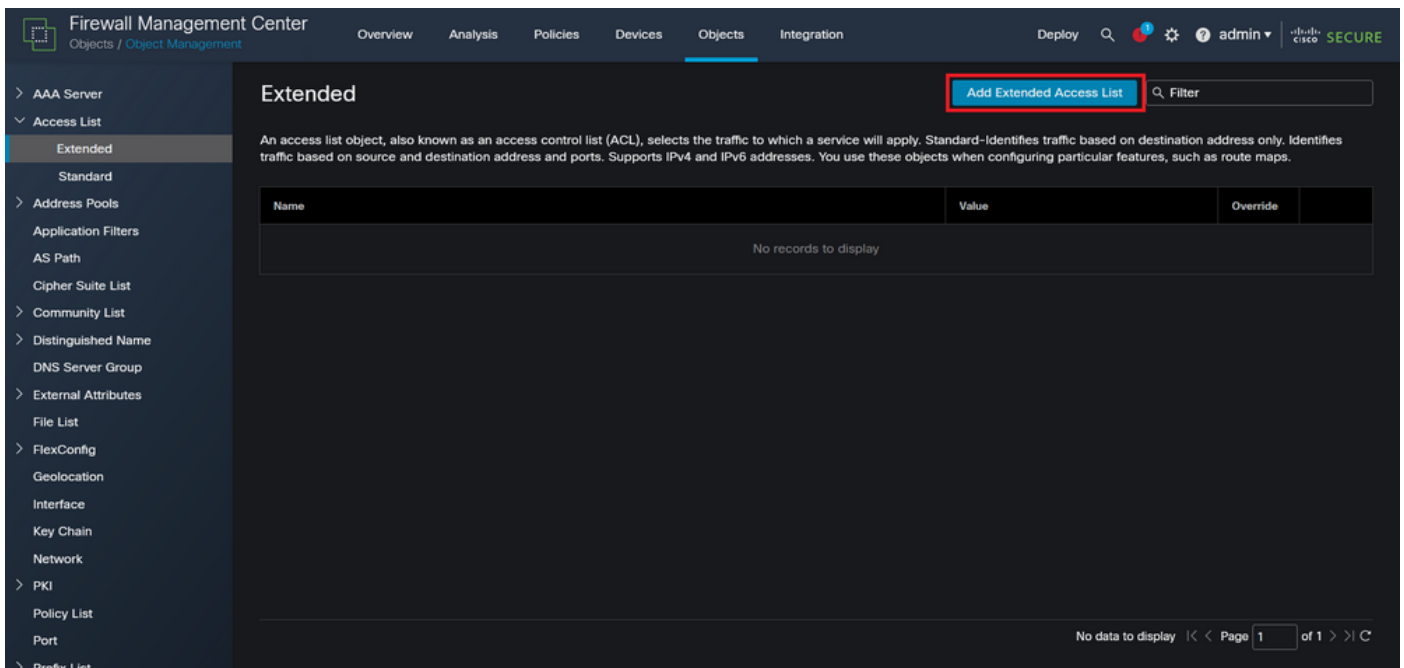


Bild 6. Erweiterte ACL hinzufügen

Schritt 2.3: Geben Sie einen Namen für die erweiterte Zugriffskontrollliste ein, und klicken Sie dann auf die Schaltfläche Hinzufügen, um einen Zugriffskontrolleintrag (ACE) zu erstellen:

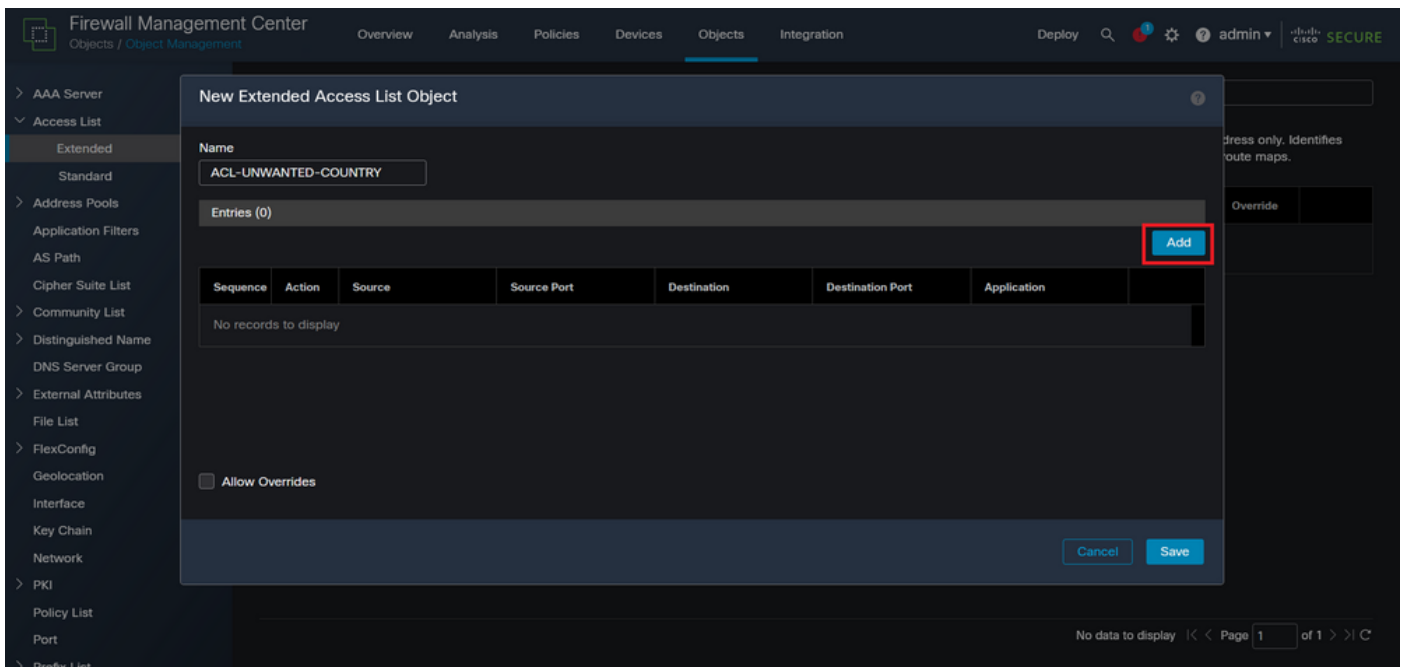


Bild 7. Erweiterte ACL-Einträge

Schritt 2.4: Ändern Sie die ACE-Aktion in Block (Blockieren), fügen Sie dann das Quellnetzwerk hinzu, damit es mit dem Datenverkehr übereinstimmt, der dem FTD verweigert werden muss, und belassen Sie das Zielnetzwerk auf Any (Beliebig), und klicken Sie auf die Schaltfläche Add (Hinzufügen), um den ACE-Eintrag zu vervollständigen:

- In diesem Beispiel blockiert der konfigurierte ACE-Eintrag Brute-Force-VPN-Angriffe aus dem Subnetz 192.168.1.0/24.

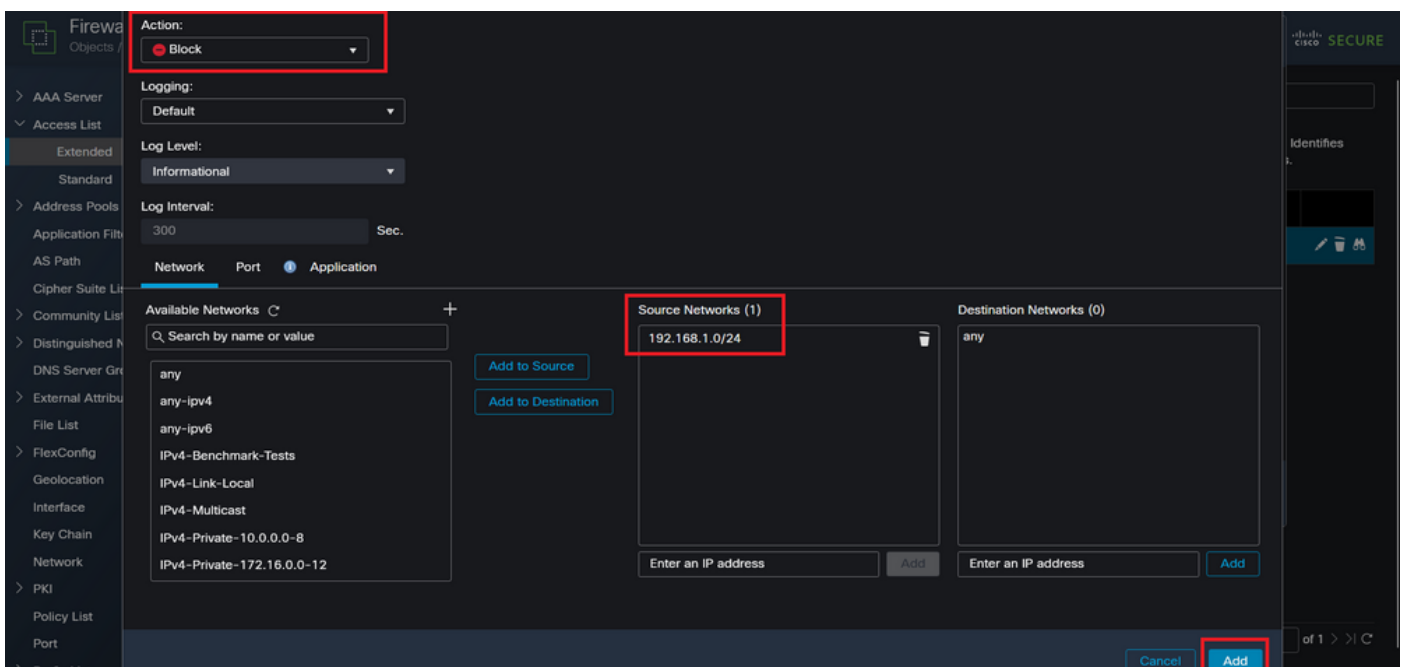


Bild 8. Abgelehnte Netzwerke

Schritt 2.5: Falls Sie weitere ACE-Einträge hinzufügen müssen, klicken Sie erneut auf die Schaltfläche Hinzufügen und wiederholen Sie Schritt 2.4. Klicken Sie anschließend auf Save (Speichern), um die ACL-Konfiguration abzuschließen.

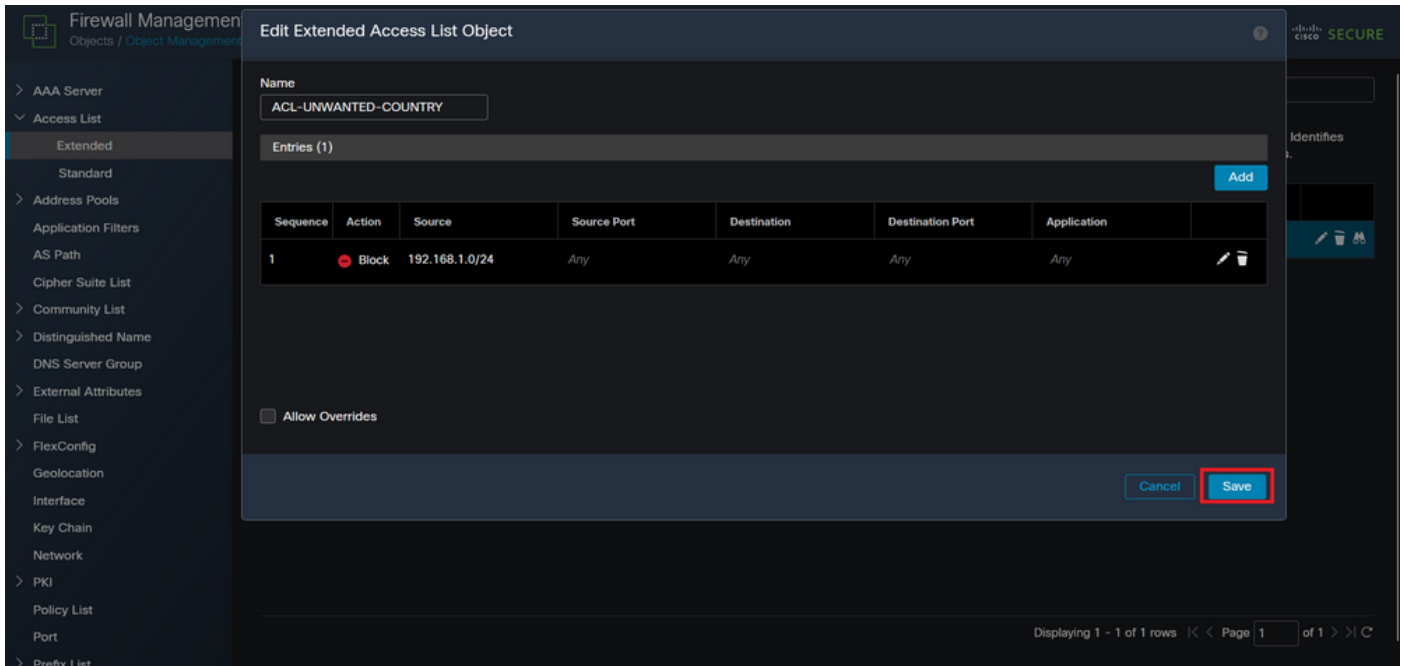


Bild 9. Abgeschlossene erweiterte ACL-Einträge

Schritt 3: Anschließend müssen Sie ein Flex-Config-Objekt konfigurieren, um die Kontrollebenen-ACL auf die externe FTD-Schnittstelle anzuwenden. Navigieren Sie dazu zum linken Bereich, und wählen Sie die Option FlexConfig > FlexConfig Object (FlexConfig > FlexConfig-Objekt) aus.

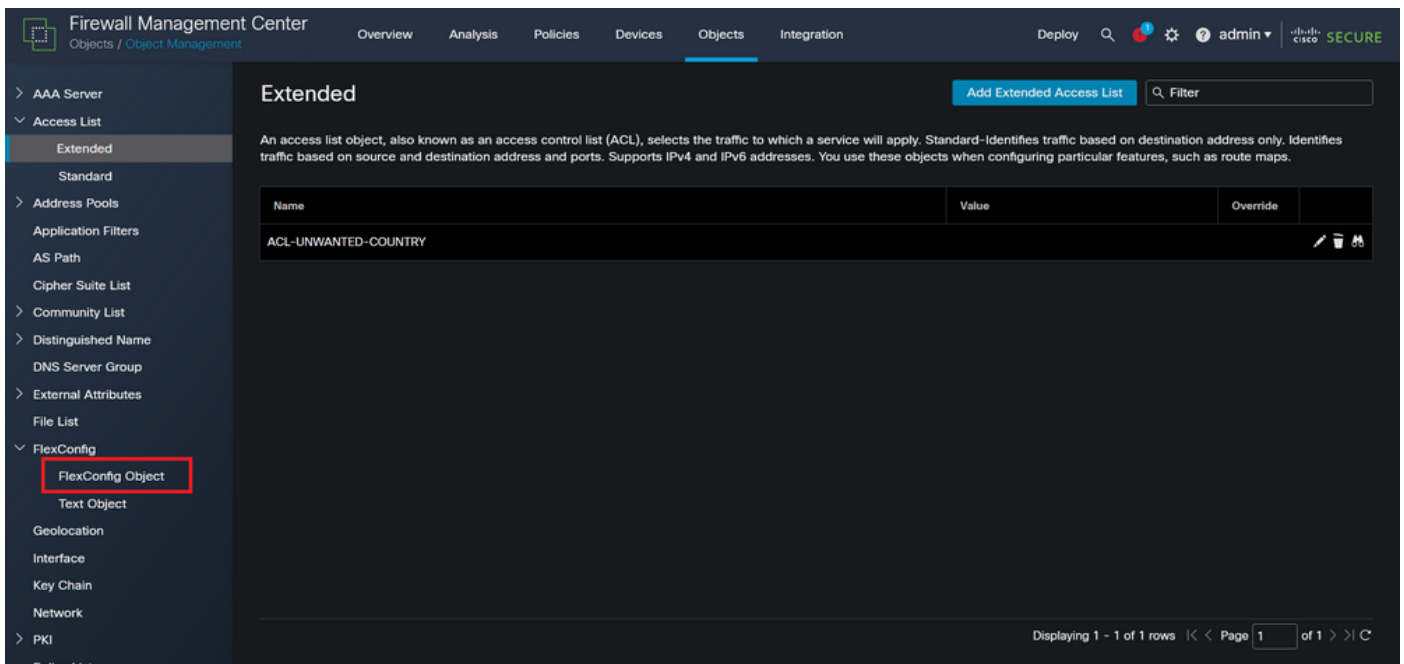


Bild 10. Menü "FlexConfig-Objekt"

Schritt 3.1: Klicken Sie auf FlexConfig Objekt hinzufügen.

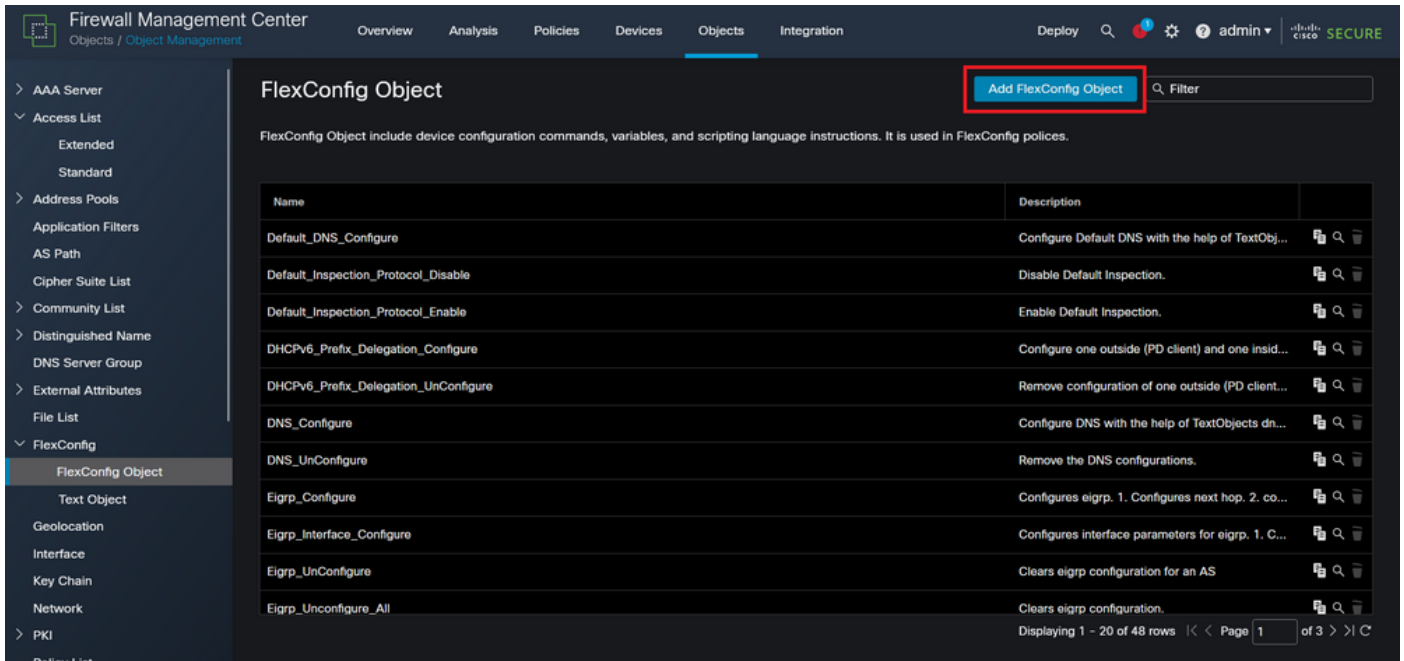


Bild 11. Flexconfig-Objekt hinzufügen

Schritt 3.2: Fügen Sie einen Namen für das FlexConfig-Objekt hinzu, und fügen Sie dann ein ACL-Richtlinienobjekt ein. Wählen Sie dazu Einfügen > Richtlinienobjekt einfügen > Erweitertes ACL-Objekt.

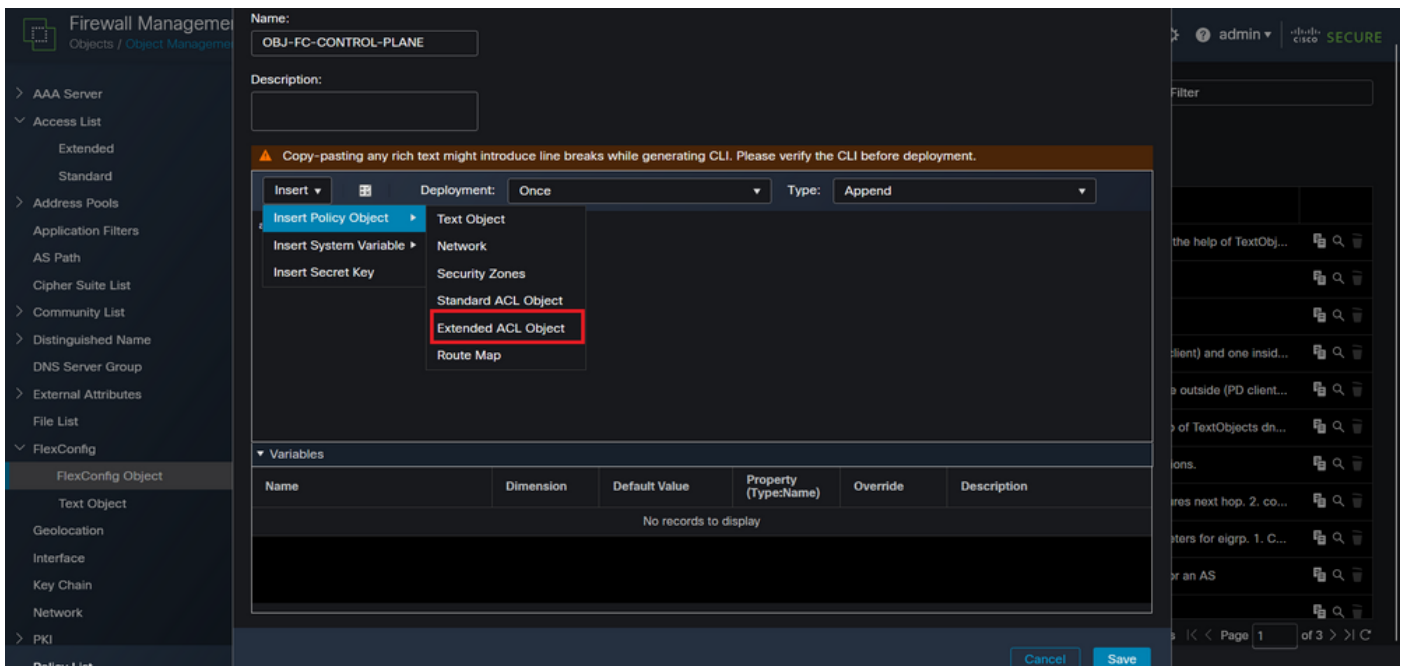


Bild 12. FlexConfig-Objektvariable

Schritt 3.3: Fügen Sie einen Namen für die ACL-Objektvariable hinzu, und wählen Sie dann die erweiterte ACL aus, die in Schritt 2.3 erstellt wurde. Klicken Sie anschließend auf die Schaltfläche Speichern.



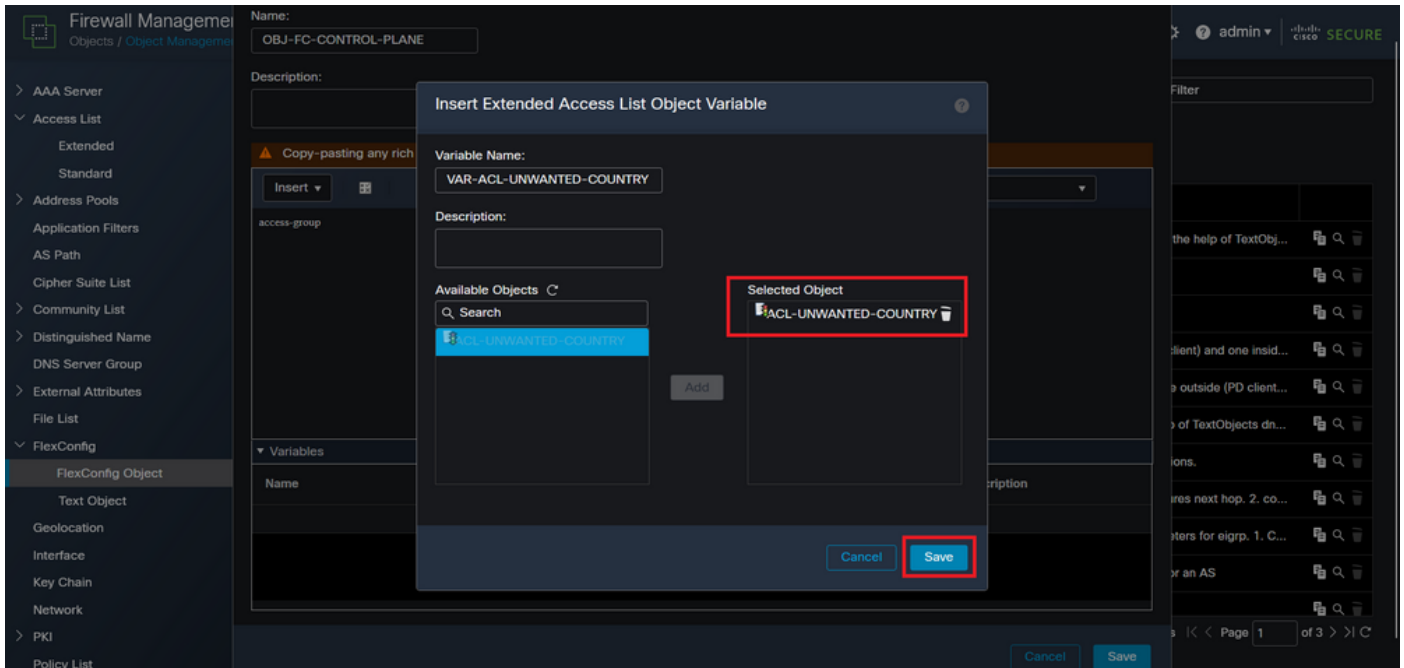


Bild 13. FlexConfig-Objektvariable ACL-Zuweisung

Schritt 3.4: Konfigurieren Sie dann die ACL der Kontrollebene als eingehend für die externe Schnittstelle wie folgt.

### Befehlszeilensyntax

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

Dies wird in das nächste Befehlsbeispiel übersetzt, das die ACL-Variable verwendet, die in Schritt 2.3 "VAR-ACL-UNWANTED-COUNTRY" wie folgt erstellt wurde:

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

Auf diese Weise muss sie im FlexConfig-Objektfenster konfiguriert werden. Wählen Sie anschließend die Schaltfläche "Save" (Speichern), um das FlexConfig-Objekt abzuschließen.

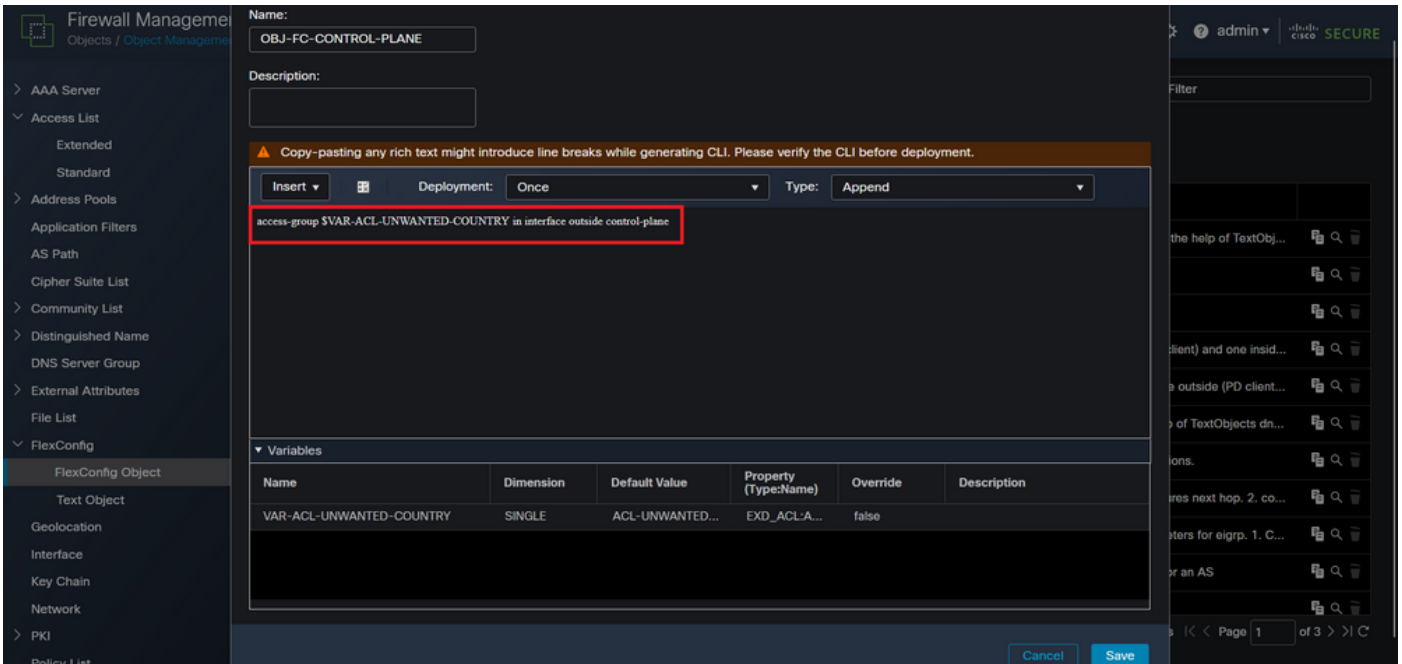


Bild 14. Flexconfig-Objekt - vollständige Befehlszeile

Schritt 4: Sie müssen die Konfiguration des FlexConfig-Objekts auf das FTD anwenden. Gehen Sie dazu zu Devices (Geräte) > FlexConfig (FlexConfig-Objekt).

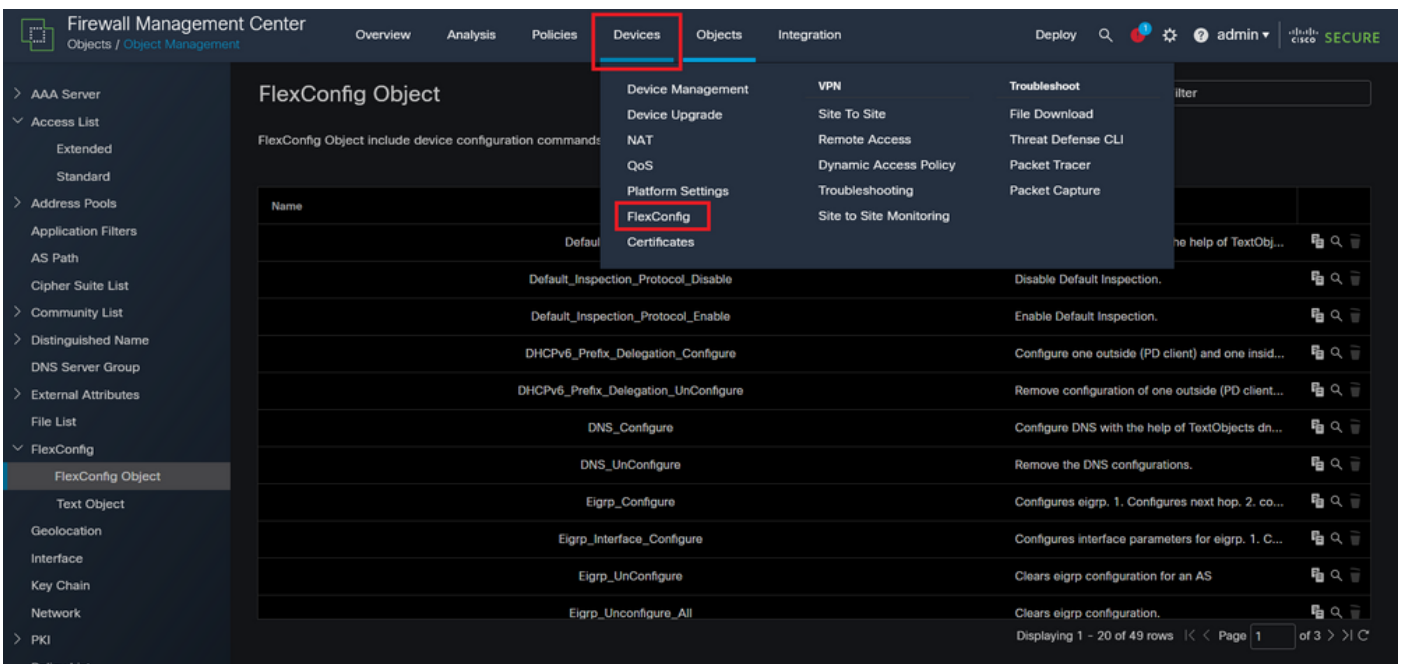


Bild 15. Menü "FlexConfig Policy"

Schritt 4.1: Klicken Sie dann auf New Policy (Neue Richtlinie), wenn noch keine FlexConfig-Option für Ihr FTD erstellt wurde, oder bearbeiten Sie die bestehende FlexConfig-Richtlinie.

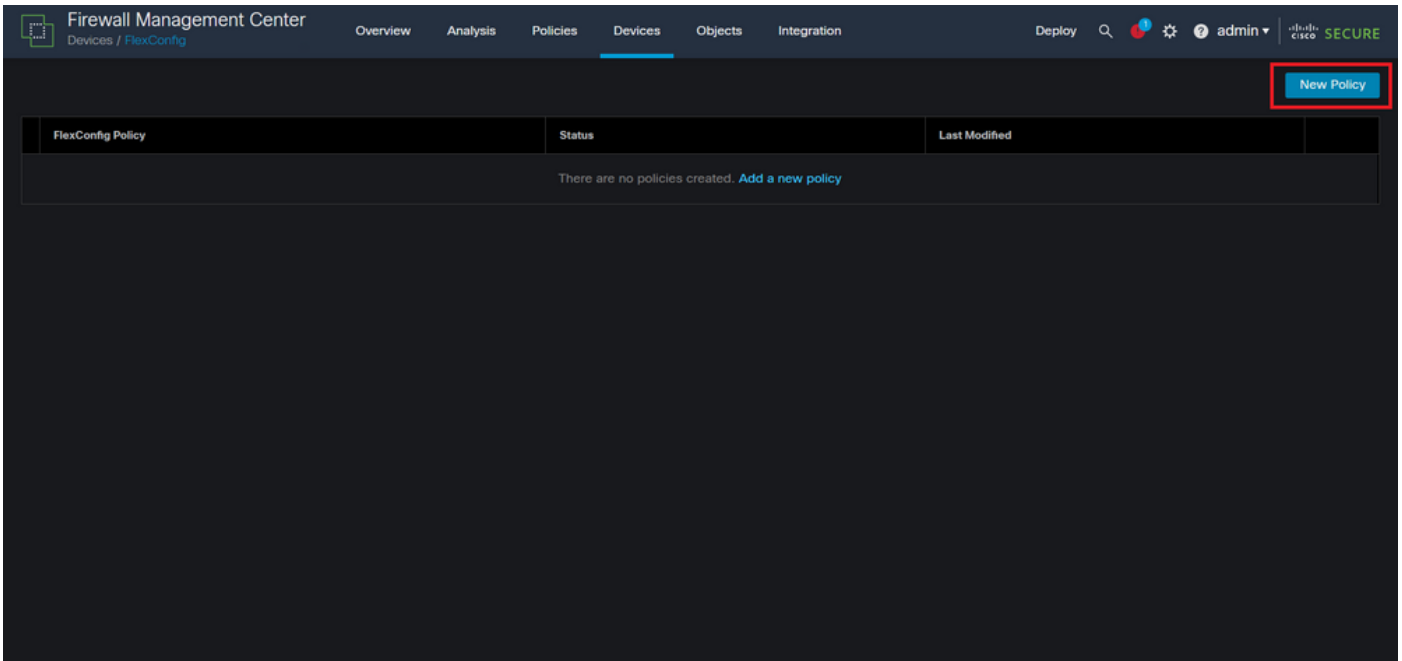


Bild 16. Erstellung von FlexConfig-Richtlinien

Schritt 4.2: Fügen Sie einen Namen für die neue FlexConfig-Richtlinie hinzu, und wählen Sie das FTD aus, das die erstellte Kontrollebenen-ACL anwenden soll.

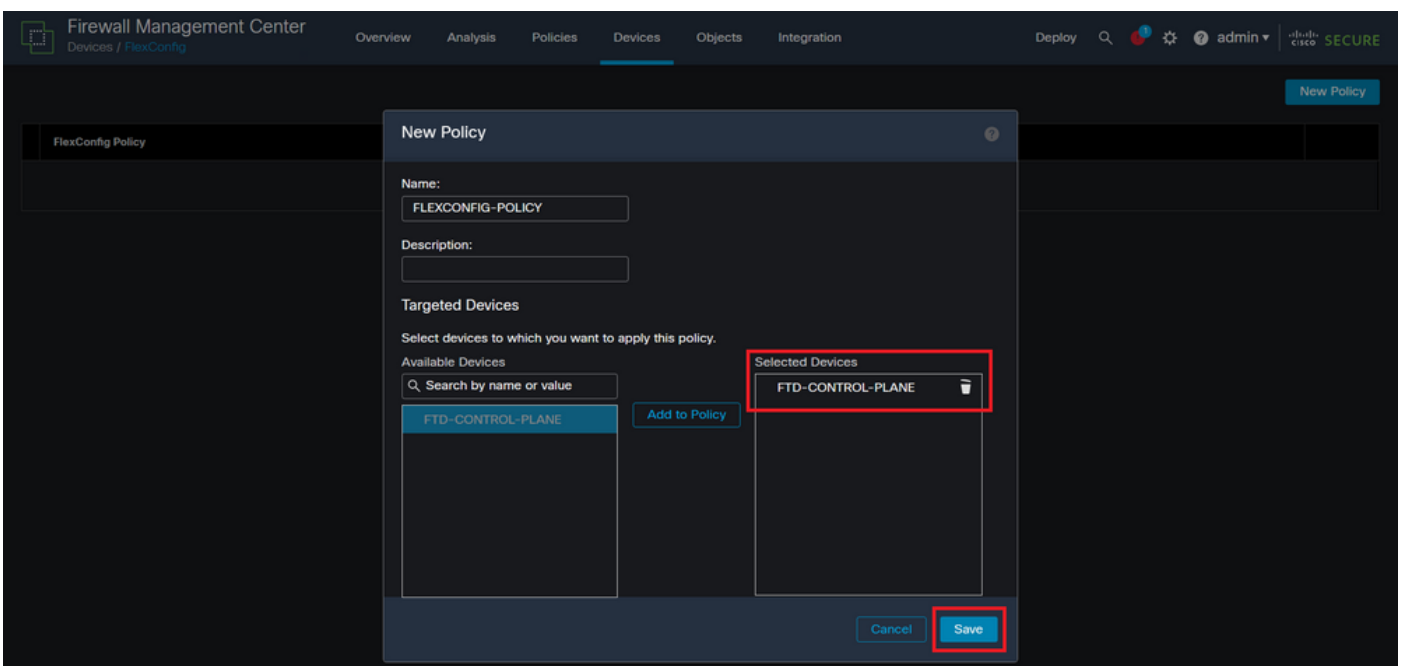


Bild 17. Zuweisung der FlexConfig-Richtlinie für Geräte

Schritt 4.3: Suchen Sie im linken Bereich nach dem FlexConfig-Objekt, das in Schritt 3.2 oben erstellt wurde, und fügen Sie es anschließend der FlexConfig-Richtlinie hinzu. Klicken Sie dazu auf den rechten Pfeil in der Mitte des Fensters, und klicken Sie anschließend auf die Schaltfläche Speichern.

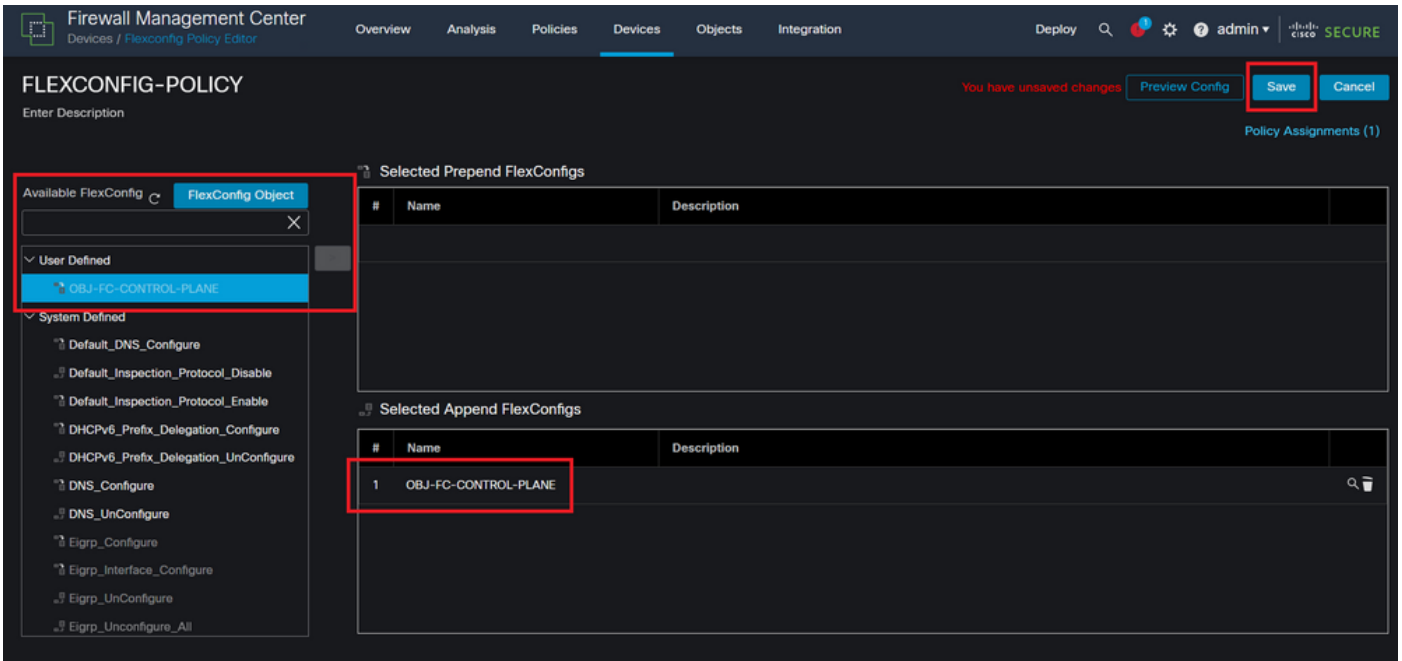


Bild 18. FlexConfig-Richtlinienobjektzuweisung

Schritt 5: Fahren Sie mit der Bereitstellung der Konfigurationsänderung im FTD fort, und navigieren Sie zu Deploy > Advanced Deploy.

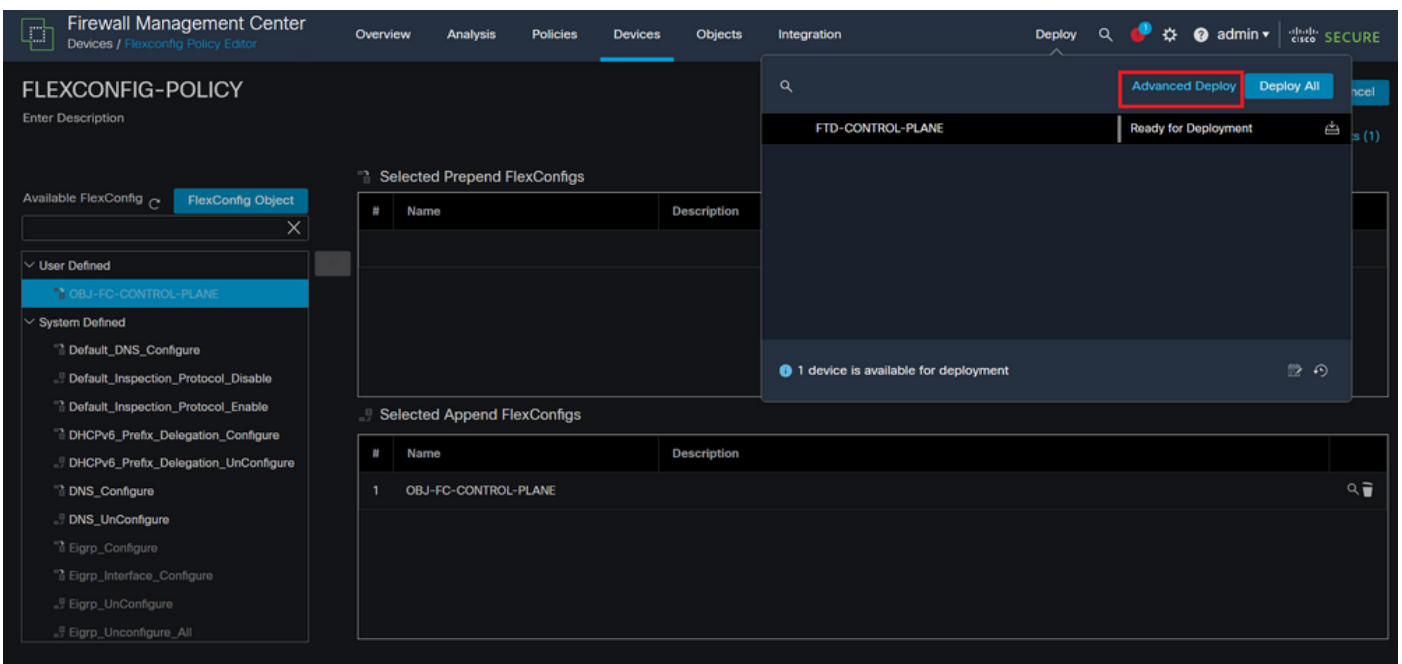


Bild 19. FTD - Erweiterte Bereitstellung

Schritt 5.1: Wählen Sie dann das FTD aus, auf das die FlexConfig-Richtlinie angewendet werden soll. Wenn alles korrekt ist, klicken Sie auf Bereitstellen.

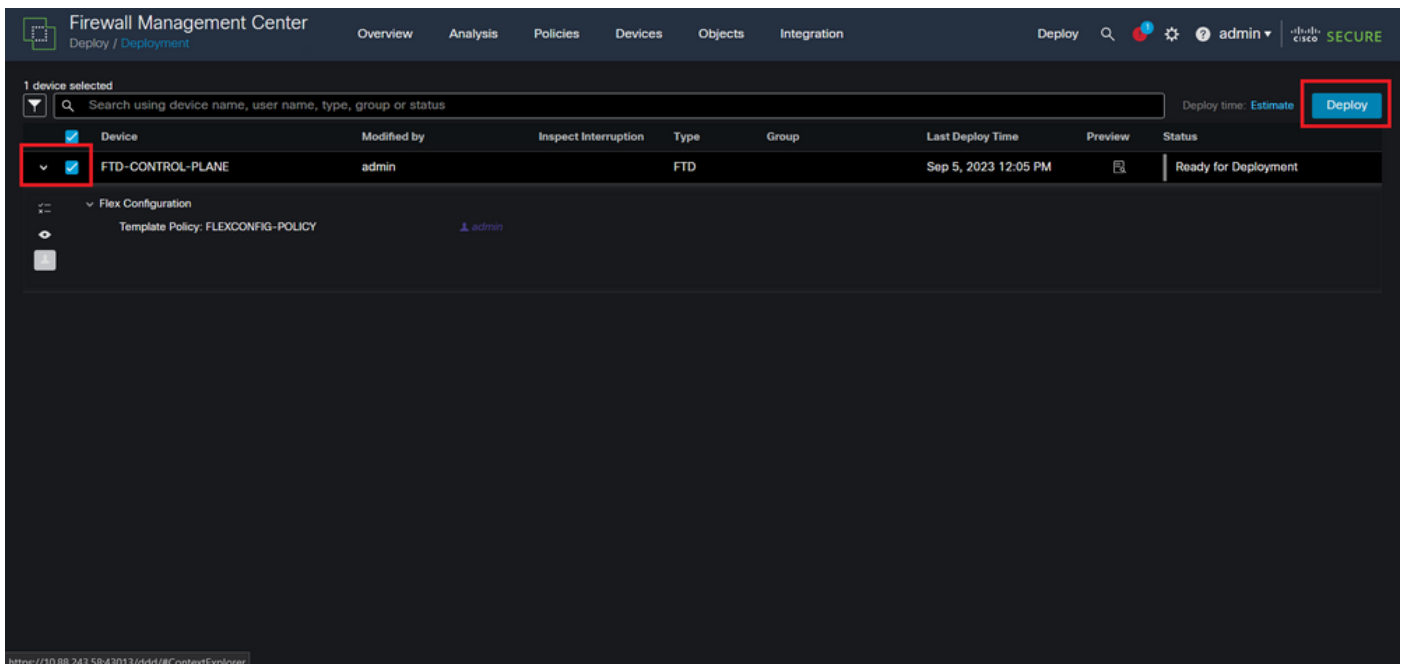


Bild 20. FTD-Bereitstellungsvalidierung

Schritt 5.2: Anschließend wird ein Fenster mit der Bereitstellungsbestätigung angezeigt. Fügen Sie einen Kommentar hinzu, um die Bereitstellung zu verfolgen, und fahren Sie mit der Bereitstellung fort.

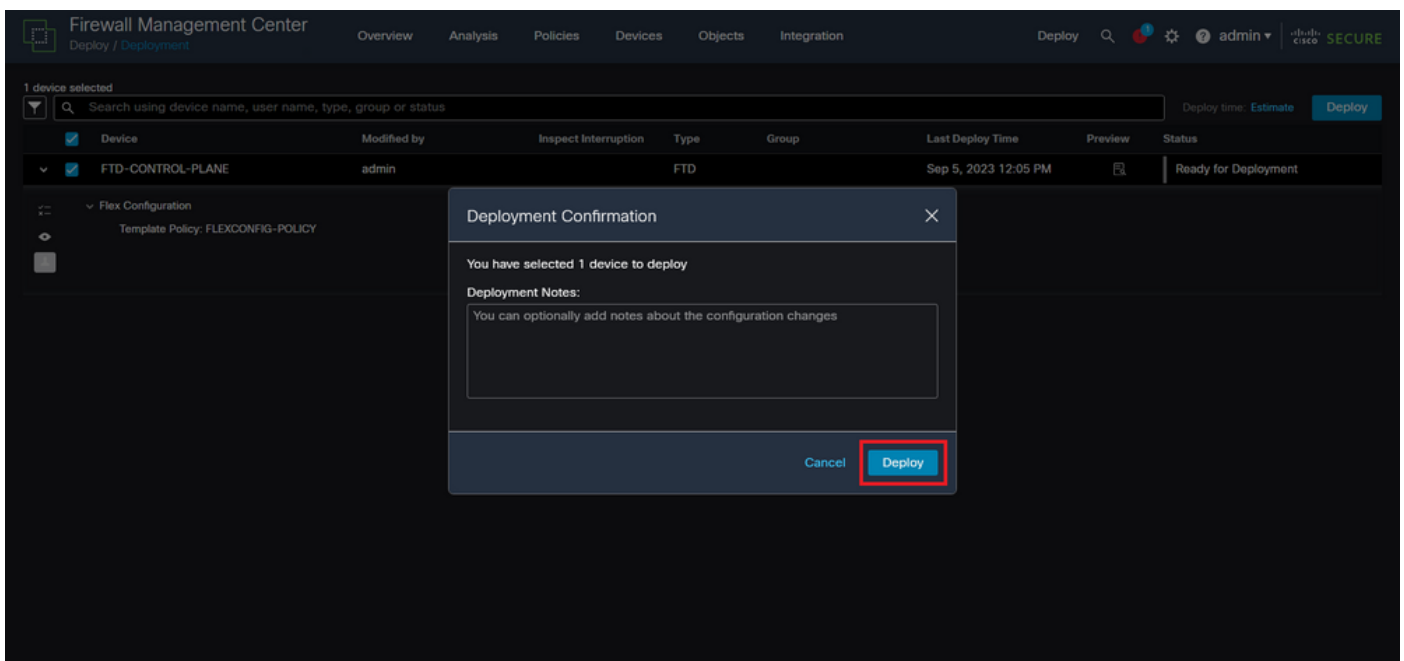


Bild 21. FTD-Bereitstellungskommentare

Schritt 5.3: Bei der Bereitstellung von FlexConfig-Änderungen kann eine Warnmeldung angezeigt werden. Klicken Sie auf Deploy (Bereitstellen), wenn Sie absolut sicher sind, dass die Richtlinienkonfiguration korrekt ist.

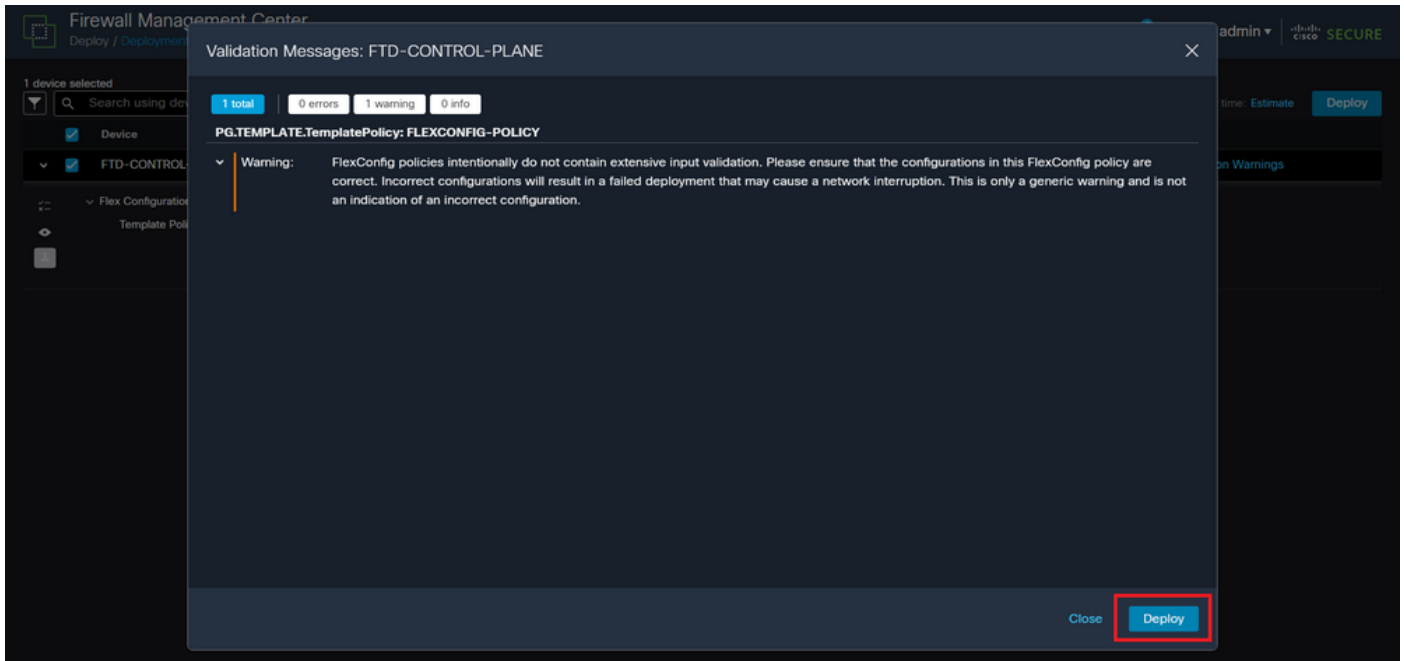


Bild 22. FTD-Bereitstellungs-Flexconfig-Warnung

Schritt 5.4: Bestätigen Sie, dass die Richtlinienbereitstellung für die FTD erfolgreich war.

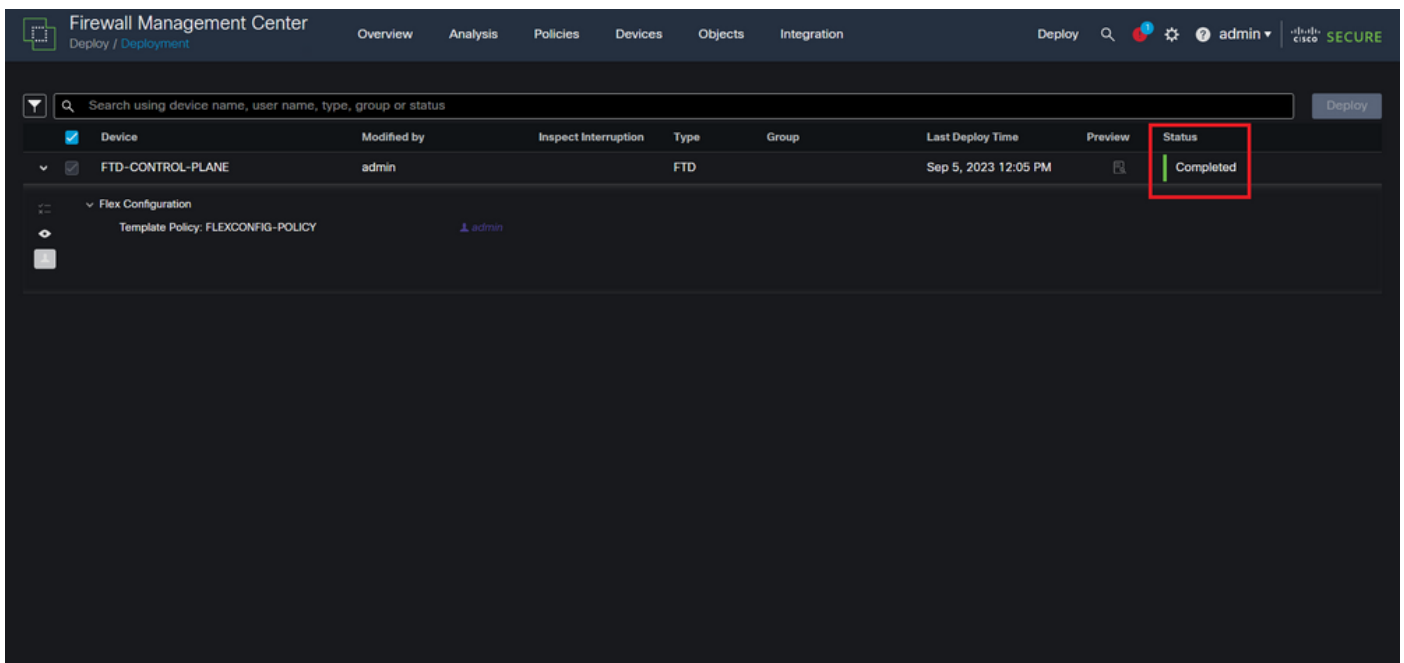


Bild 23. FTD-Bereitstellung erfolgreich

Schritt 6: Wenn Sie eine neue Kontrollebenen-ACL für Ihren FTD erstellen oder eine vorhandene editieren, die aktiv genutzt wird, dann ist es wichtig hervorzuheben, dass die vorgenommenen Konfigurationsänderungen nicht für bereits bestehende Verbindungen zum FTD gelten. Daher müssen Sie die aktiven Verbindungsversuche zum FTD manuell löschen. Stellen Sie dazu die Verbindung mit der CLI des FTD her, und löschen Sie die aktiven Verbindungen wie folgt.

So löschen Sie die aktive Verbindung für eine bestimmte Host-IP-Adresse:

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


So löschen Sie die aktiven Verbindungen für ein ganzes Subnetz:

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

So löschen Sie die aktiven Verbindungen für einen IP-Adressbereich:

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

---

 Hinweis: Es wird dringend empfohlen, das Schlüsselwort "all" am Ende des Befehls clear conn address zu verwenden, um das Löschen der aktiven VPN-Brute-Force-Verbindungsversuche in die sichere Firewall zu erzwingen, vor allem, wenn die Art des VPN-Brute-Force-Angriffs eine Explosion konstanter Verbindungsversuche auslöst.

---

## Konfigurieren einer von FDM verwalteten Kontrollebenen-ACL für FTD

Mit diesem Verfahren müssen Sie in einem FDM eine Kontrollebenen-ACL konfigurieren, um eingehende VPN-Brute-Force-Angriffe auf die externe FTD-Schnittstelle zu blockieren:

Schritt 1: Öffnen Sie die FDM-GUI über HTTPS, und melden Sie sich mit Ihren Anmeldeinformationen an.

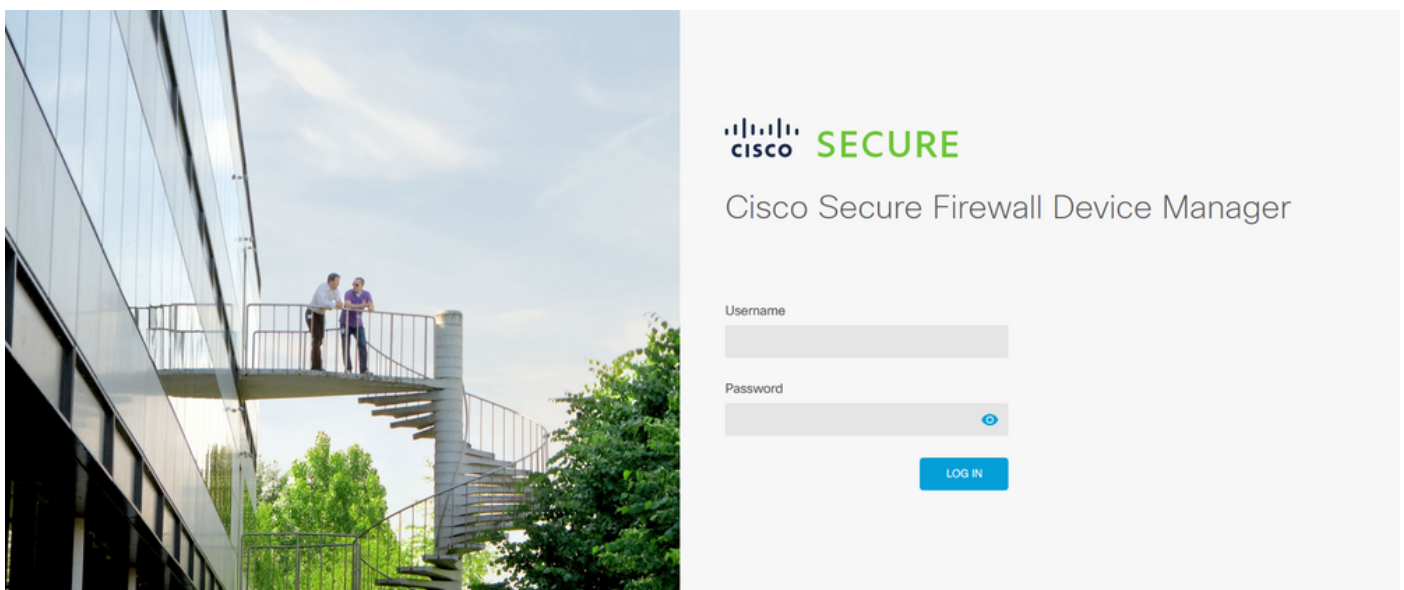


Bild 24. FDM-Anmeldeseite

Schritt 2: Sie müssen ein Objektnetzwerk erstellen. Navigieren Sie dazu zu Objekte:

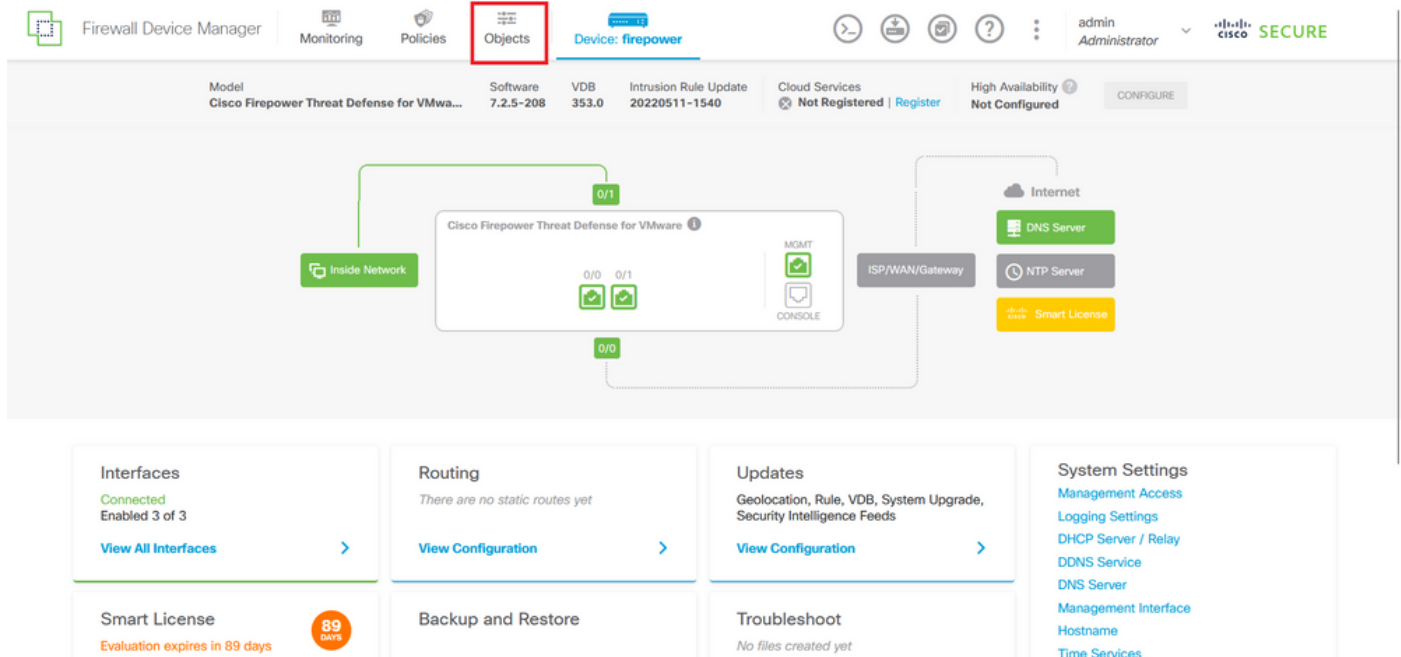


Bild 25. FDM-Haupt-Dashboard

Schritt 2.1: Wählen Sie im linken Bereich "Networks" (Netzwerke) aus, und klicken Sie dann auf die Schaltfläche "+", um ein neues Netzwerkobjekt zu erstellen.

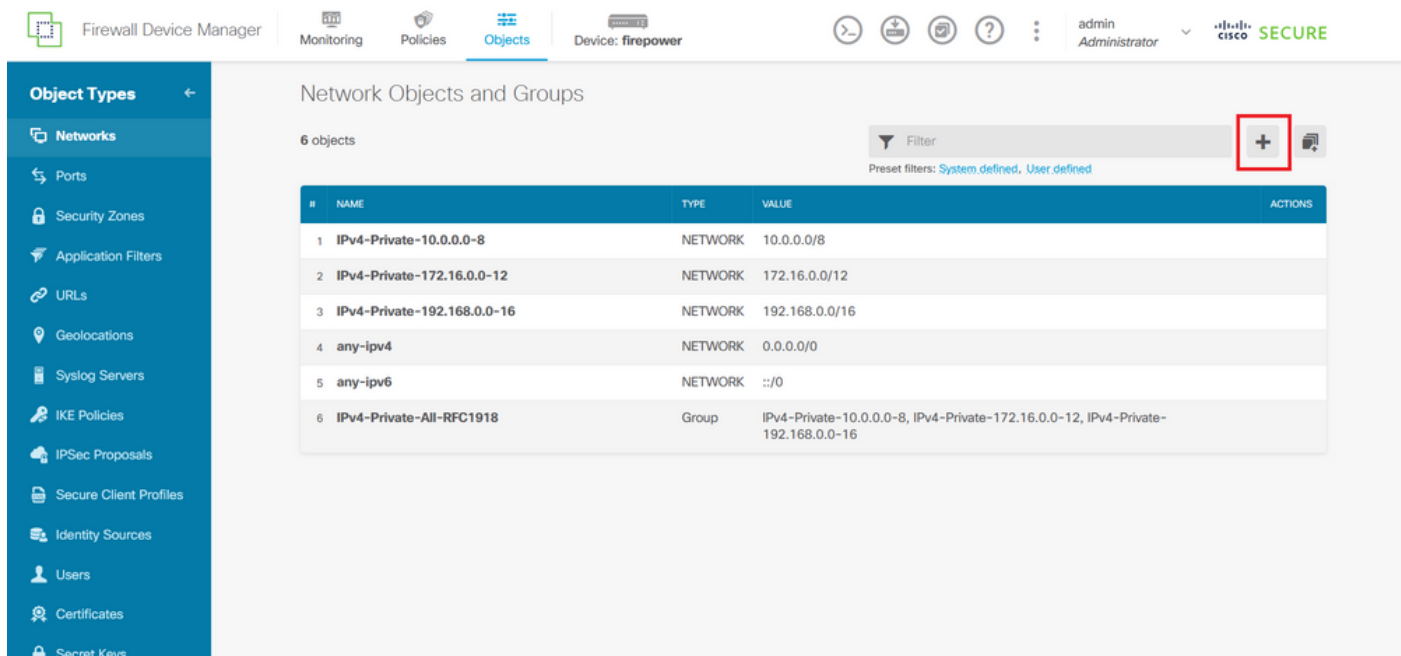


Bild 26. Objekterstellung

Schritt 2.2: Fügen Sie einen Namen für das Netzwerkobjekt hinzu, wählen Sie den Netzwerktyp für das Objekt aus, fügen Sie die IP-Adresse, die Netzwerkadresse oder den IP-Bereich hinzu, um den Datenverkehr abzugleichen, der dem FTD verweigert werden muss. Klicken Sie dann auf die Schaltfläche OK, um das Objektnetzwerk zu vervollständigen.



- In diesem Beispiel soll das konfigurierte Objektnetzwerk Brute-Force-VPN-Angriffe blockieren, die vom Subnetz 192.168.1.0/24 ausgehen.

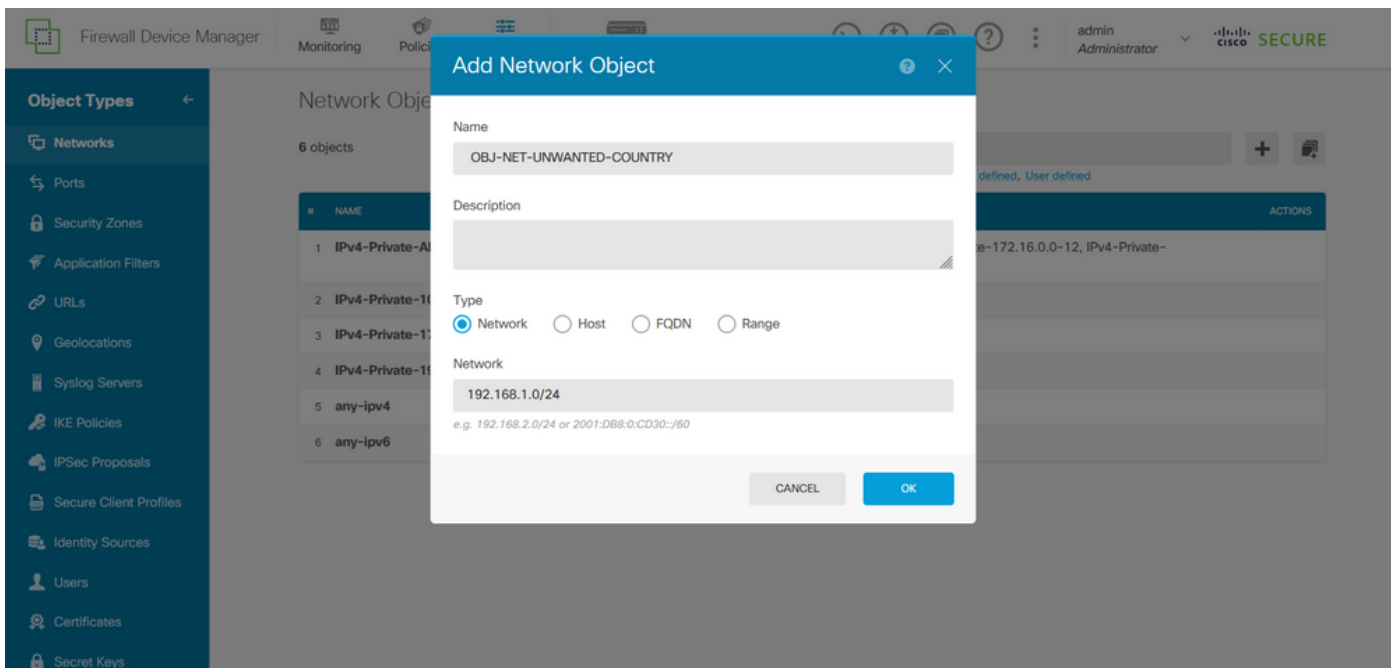


Bild 27. Netzwerkobjekt hinzufügen

Schritt 3: Anschließend müssen Sie eine erweiterte Zugriffskontrollliste erstellen. Navigieren Sie dazu zur Registerkarte Gerät im oberen Menü.

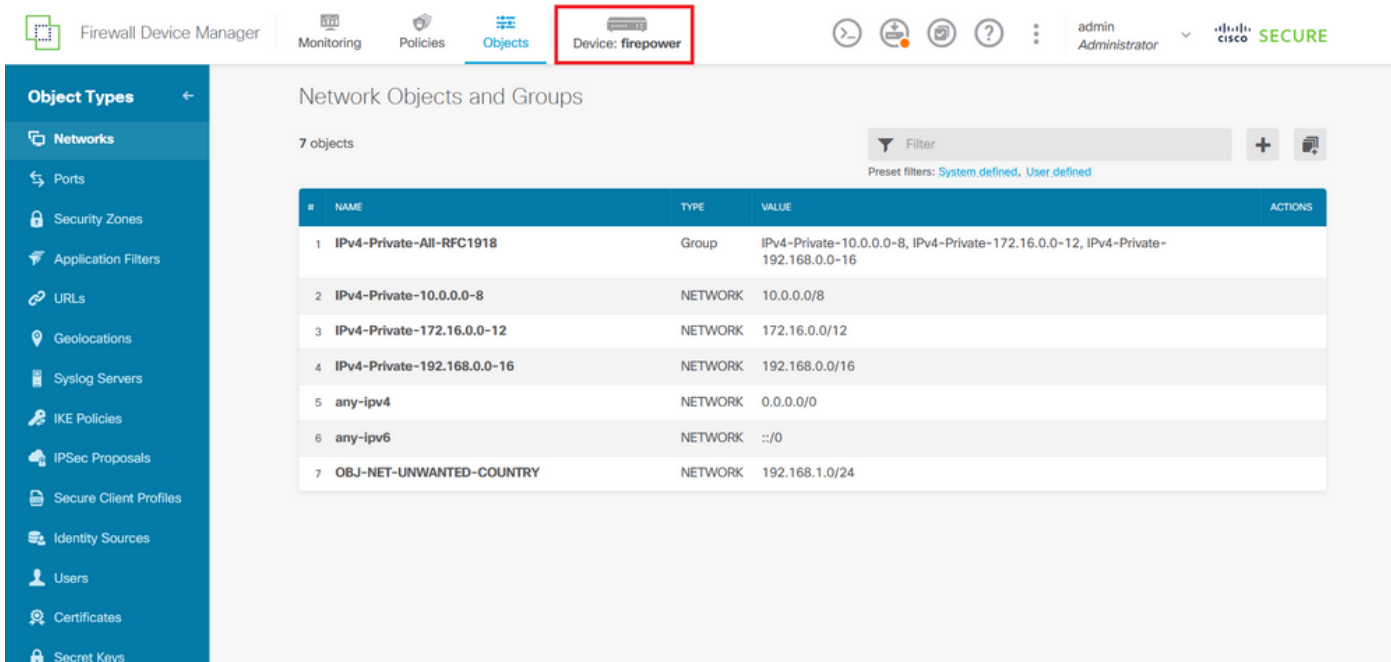


Bild 28. Seite mit Geräteeinstellungen

Schritt 3.1: Blättern Sie nach unten, und wählen Sie im Feld Erweiterte Konfiguration die Option Konfiguration anzeigen aus.

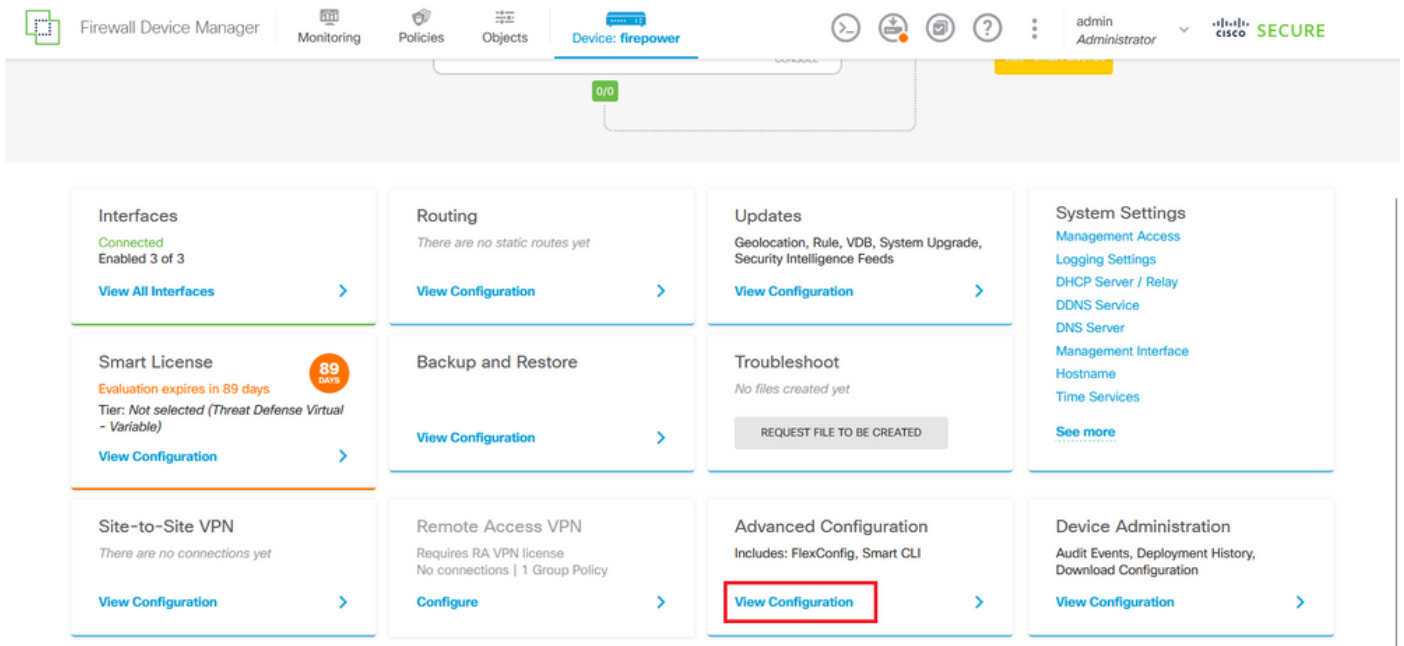


Bild 29. Erweiterte FDM-Konfiguration

Schritt 3.2: Navigieren Sie dann im linken Bereich zu Smart CLI > Objects, und klicken Sie auf CREATE SMART CLI OBJECT (SMART CLI-OBJEKT ERSTELLEN).

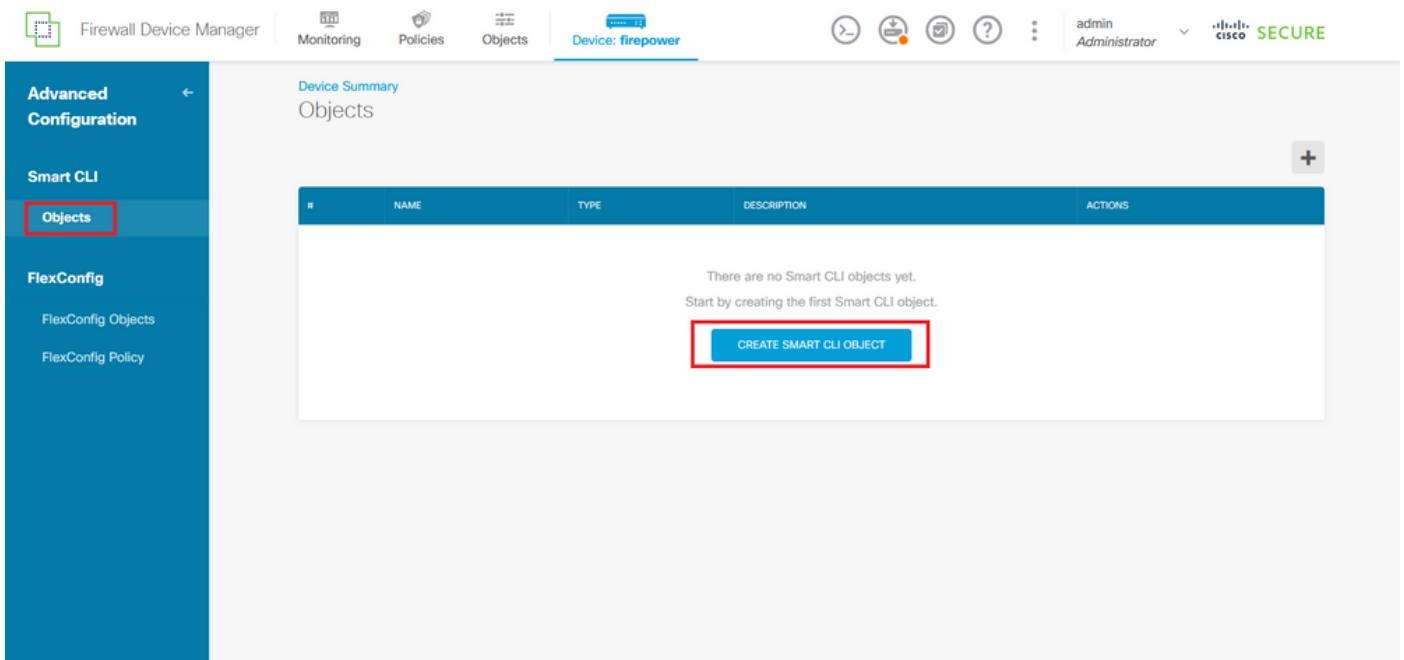


Bild 30. Smart CLI-Objekte

Schritt 3.3: Fügen Sie einen Namen für die zu erstellende erweiterte ACL hinzu, wählen Sie im Dropdown-Menü für die CLI-Vorlage die Option "Extended Access List" aus, und konfigurieren Sie die erforderlichen ACEs mithilfe des im obigen Schritt 2.2 erstellten Netzwerkobjekts. Klicken Sie anschließend auf OK, um die ACL abzuschließen.

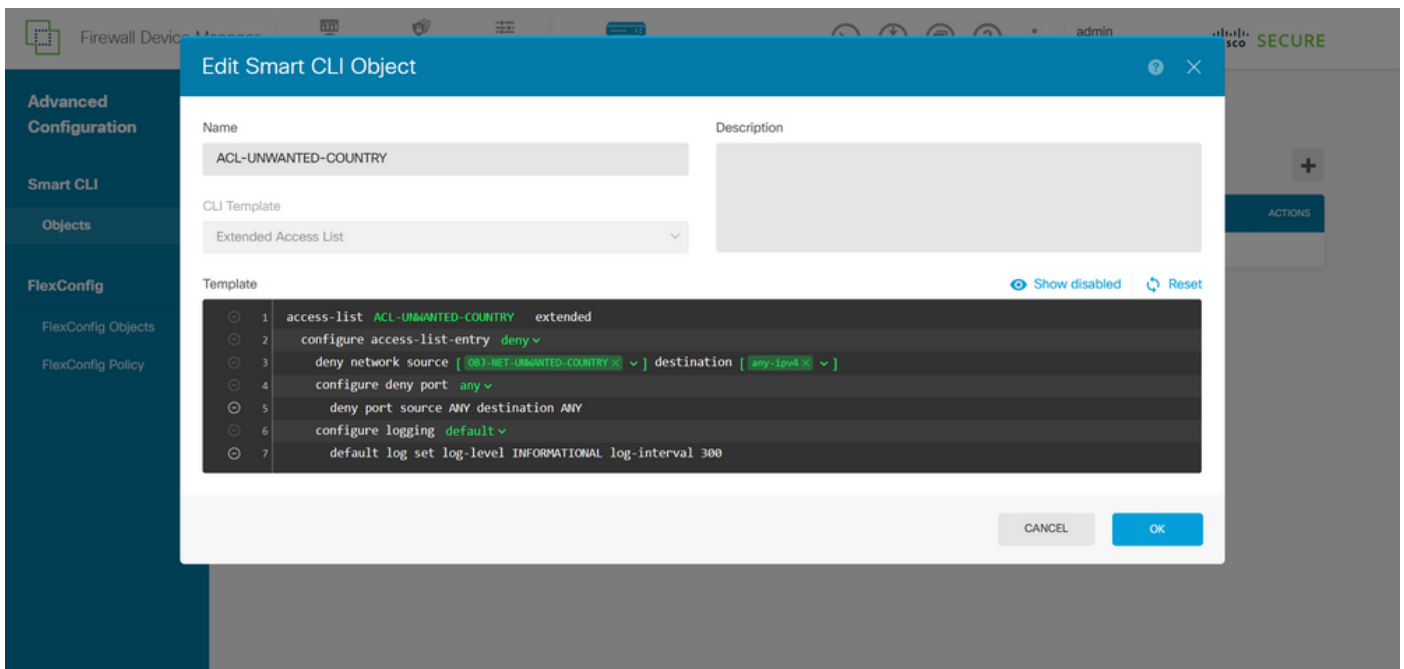



Bild 31. Erstellung erweiterter ACLs

 **Hinweis:** Wenn Sie weitere ACEs für die ACL hinzufügen müssen, können Sie dies tun, indem Sie mit der Maus auf die linke Seite des aktuellen ACE zeigen. Daraufhin werden drei anklickbare Punkte angezeigt. Klicken Sie darauf, und wählen Sie Duplizieren aus, um weitere ACEs hinzuzufügen.

Schritt 4: Anschließend müssen Sie ein FlexConfig-Objekt erstellen. Navigieren Sie dazu zum linken Bereich, wählen Sie FlexConfig > FlexConfig Objects aus, und klicken Sie auf CREATE FLEXCONFIG OBJECT.

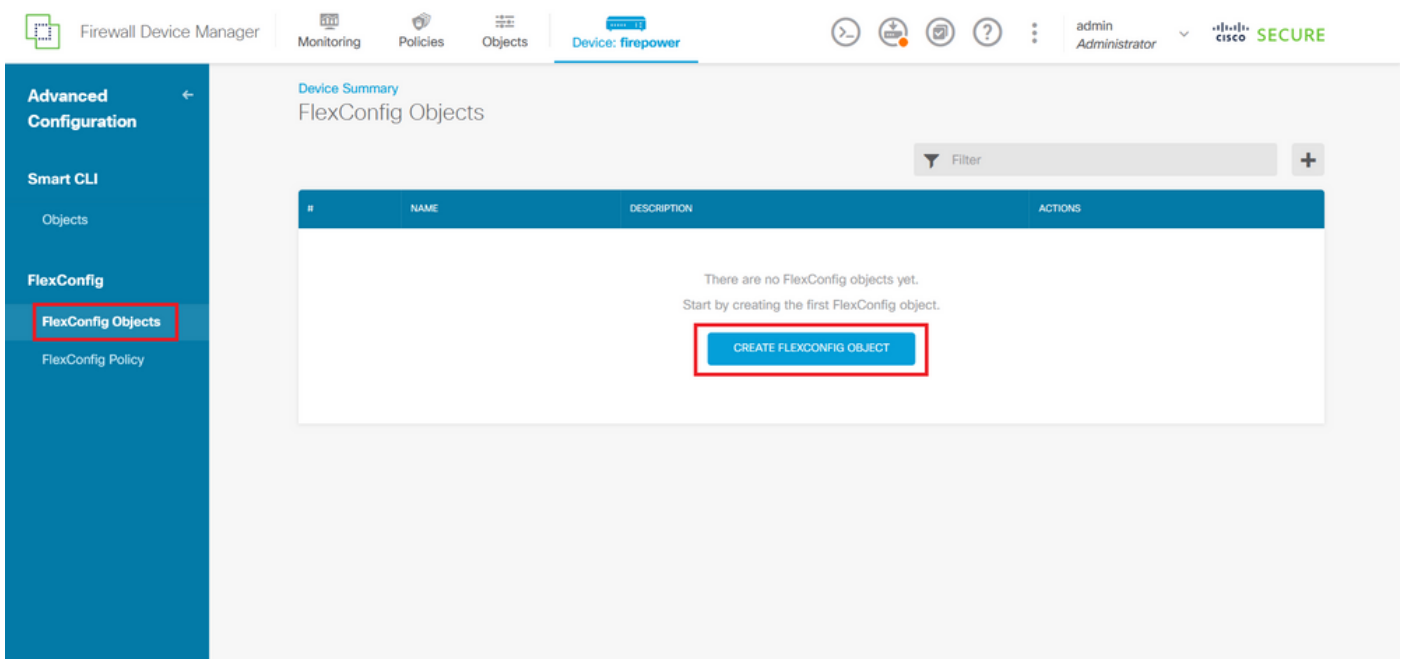


Bild 32. FlexConfig-Objekte

Schritt 4.1: Fügen Sie einen Namen für das FlexConfig-Objekt hinzu, um die Kontrollebenen-ACL

für die externe Schnittstelle wie folgt als eingehend zu erstellen und zu konfigurieren.

## Befehlszeilensyntax

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

Dies wird in das nächste Befehlsbeispiel übersetzt, das die erweiterte ACL verwendet, die in Schritt 3.3 "ACL-UNWANTED-COUNTRY" wie folgt erstellt wurde:

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

So sollte es im FlexConfig-Objektfenster konfiguriert werden. Wählen Sie anschließend die Schaltfläche OK, um das FlexConfig-Objekt abzuschließen.

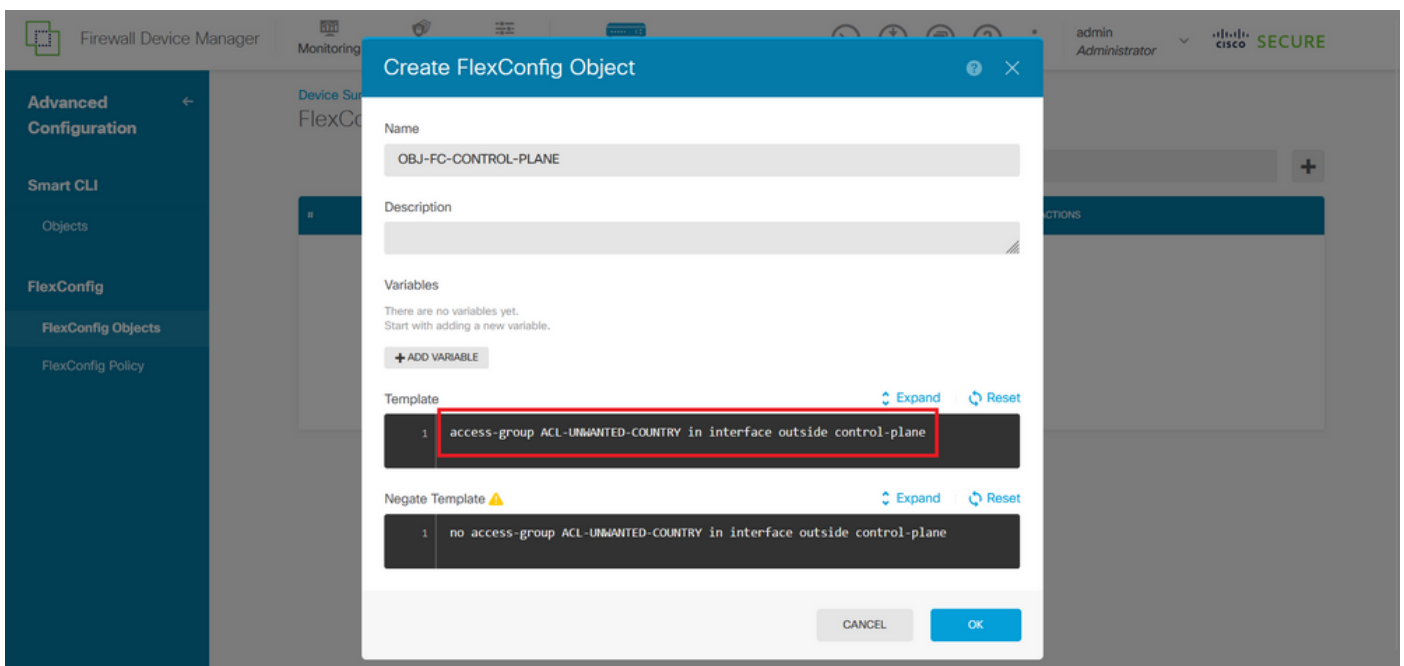


Bild 33. Erstellung von FlexConfig-Objekten

Schritt 5: Fahren Sie mit der Erstellung einer FlexConfig-Richtlinie fort. Navigieren Sie dazu zu Flexconfig > FlexConfig Policy, klicken Sie auf die Schaltfläche "+", und wählen Sie das FlexConfig-Objekt aus, das im obigen Schritt 4.1 erstellt wurde.

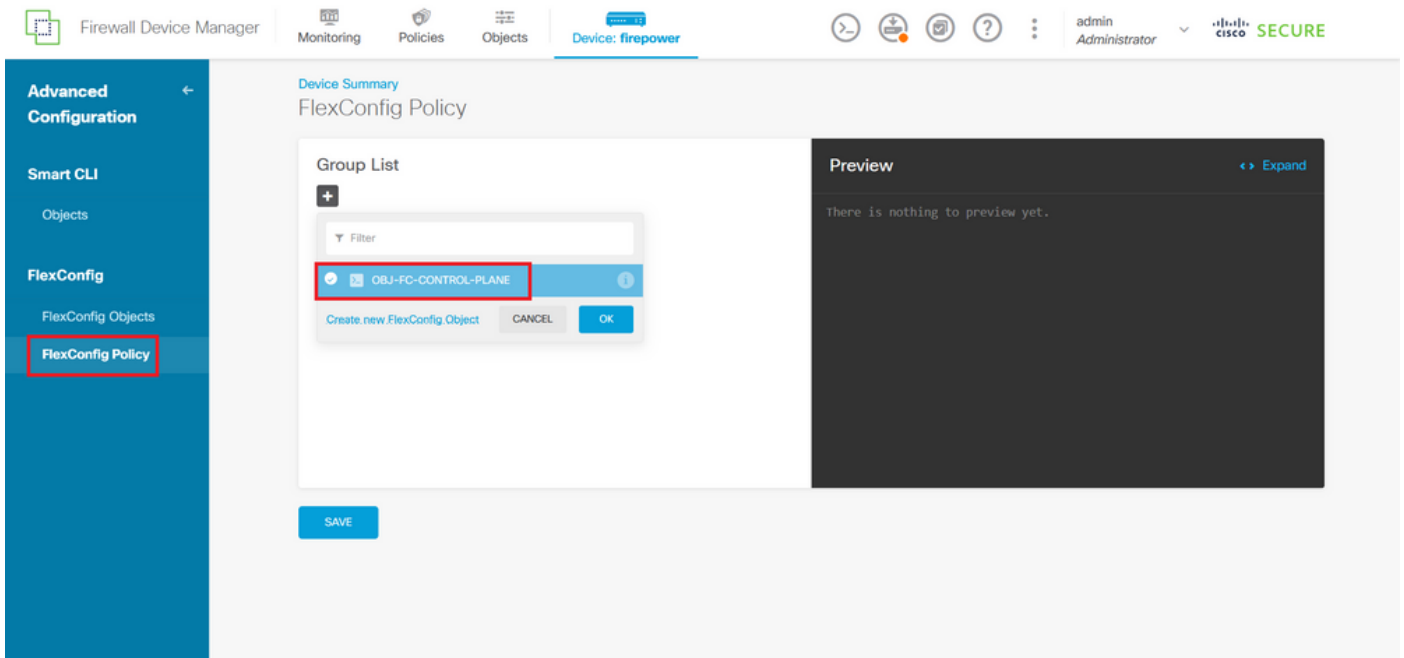


Bild 34. FlexConfig-Richtlinie

Schritt 5.1: Überprüfen Sie, ob in der FlexConfig-Vorschau die richtige Konfiguration für die erstellte Kontrollebenen-ACL angezeigt wird, und klicken Sie auf die Schaltfläche Speichern.

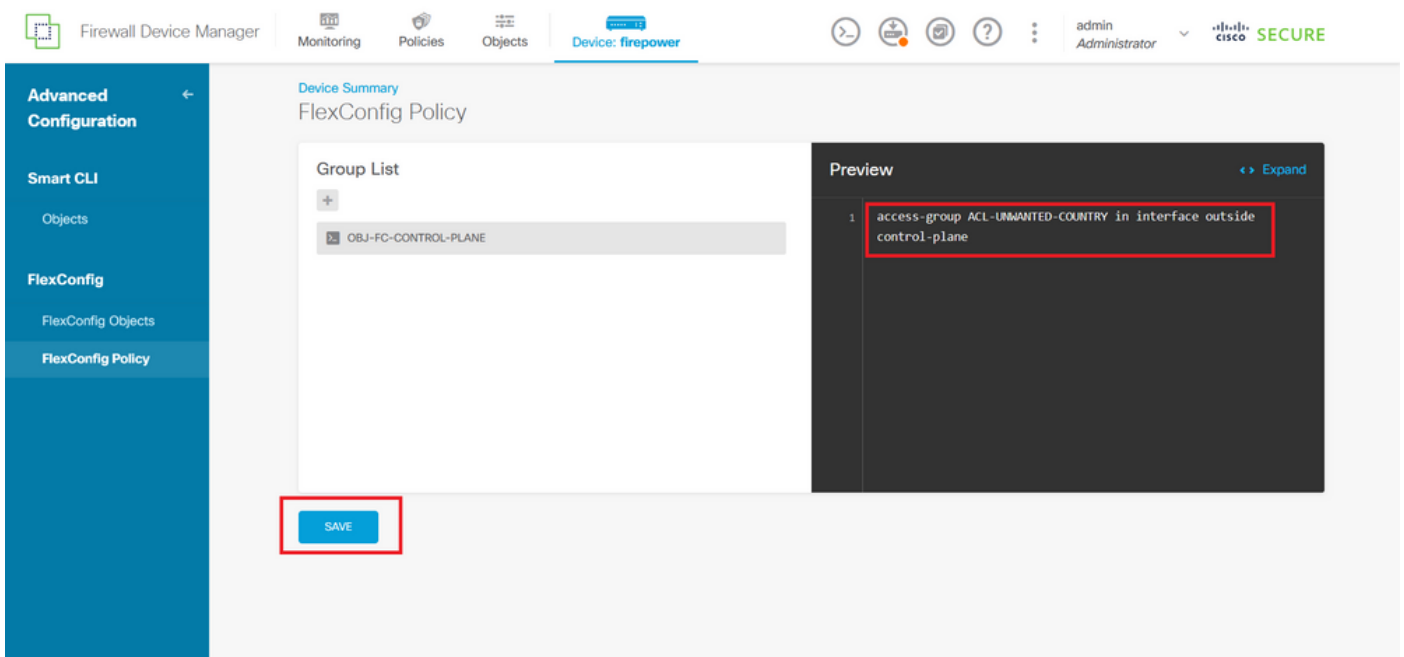


Bild 35. Vorschau der FlexConfig-Richtlinie

Schritt 6: Stellen Sie die Konfigurationsänderungen auf dem FTD bereit, das Sie gegen die VPN-Brute-Force-Angriffe schützen möchten. Klicken Sie dazu im oberen Menü auf die Schaltfläche Deployment (Bereitstellung), überprüfen Sie, ob die bereitzustellenden Konfigurationsänderungen richtig sind, und klicken Sie dann auf DEPLOY NOW (JETZT BEREITSTELLEN).

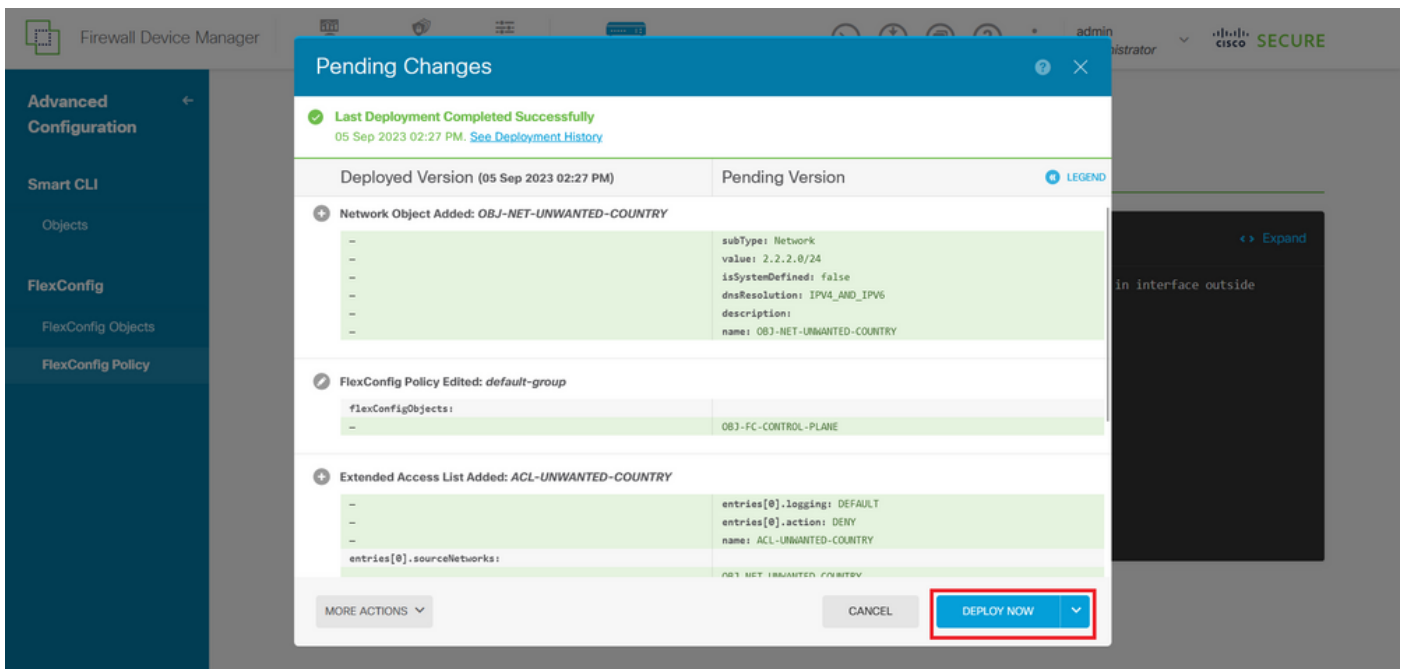


Bild 36. Ausstehende Bereitstellung

### Schritt 6.1: Überprüfen der erfolgreichen Richtlinienbereitstellung

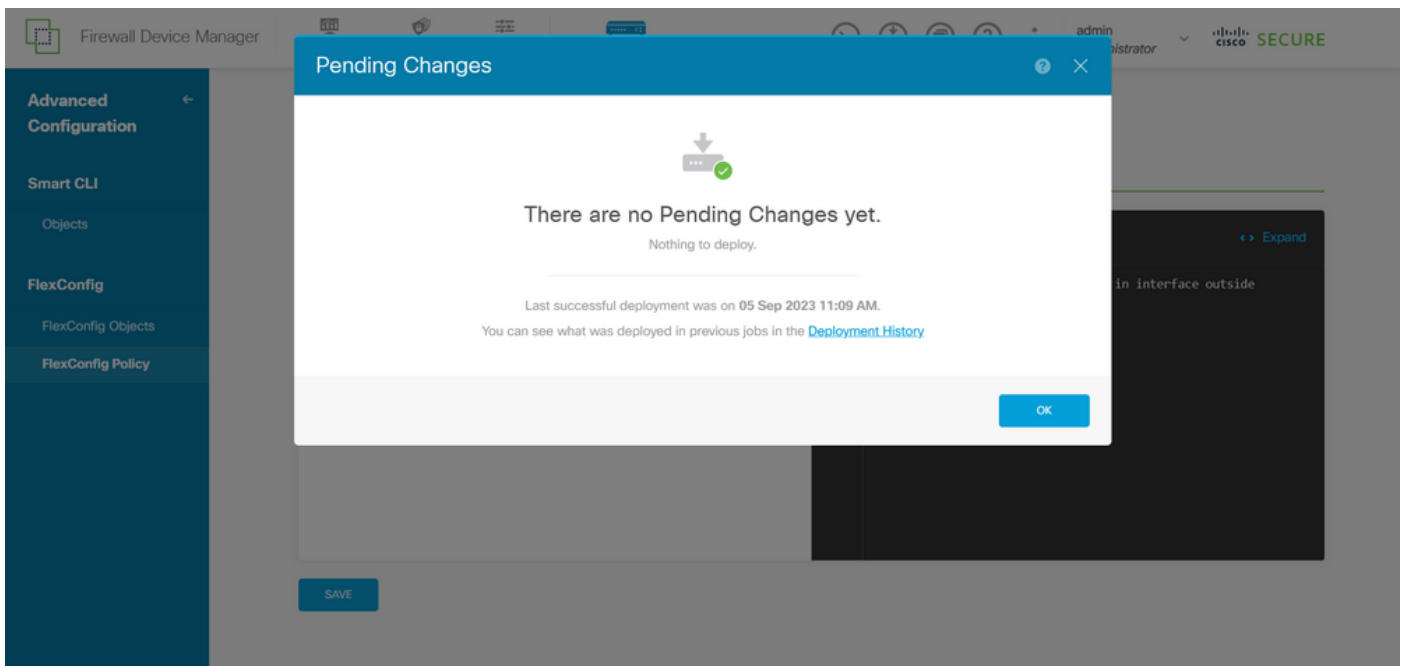


Bild 37. Bereitstellung erfolgreich

Schritt 7. Wenn Sie eine neue Kontrollebenen-ACL für Ihren FTD erstellen oder eine vorhandene editieren, die aktiv genutzt wird, dann ist es wichtig hervorzuheben, dass die vorgenommenen Konfigurationsänderungen nicht für bereits bestehende Verbindungen zum FTD gelten. Daher müssen Sie die aktiven Verbindungsversuche zum FTD manuell löschen. Stellen Sie dazu die Verbindung mit der CLI des FTD her, und löschen Sie die aktiven Verbindungen wie folgt.

So löschen Sie die aktive Verbindung für eine bestimmte Host-IP-Adresse:

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


So löschen Sie die aktiven Verbindungen für ein ganzes Subnetz:

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

So löschen Sie die aktiven Verbindungen für einen IP-Adressbereich:

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

---

 Hinweis: Es wird dringend empfohlen, das Schlüsselwort "all" am Ende des Befehls clear conn address zu verwenden, um das Löschen der aktiven VPN-Brute-Force-Verbindungsversuche in die sichere Firewall zu erzwingen, vor allem, wenn die Art des VPN-Brute-Force-Angriffs eine Explosion konstanter Verbindungsversuche auslöst.

---

### Konfigurieren einer Kontrollebenen-ACL für ASA mit CLI

Mit diesem Verfahren müssen Sie in einer ASA CLI eine Kontrollebenen-ACL konfigurieren, um eingehende VPN-Brute-Force-Angriffe auf die externe Schnittstelle zu blockieren:

Schritt 1: Melden Sie sich über die CLI bei der sicheren Firewall-ASA an, und erhalten Sie wie folgt Zugriff auf das 'configure-Terminal'.

```
asa# configure terminal
```

Schritt 2: Verwenden Sie den nächsten Befehl, um eine erweiterte ACL zu konfigurieren, die eine Host-IP-Adresse oder Netzwerkadresse für den Datenverkehr blockiert, der zur ASA blockiert werden muss.

- In diesem Beispiel erstellen Sie eine neue ACL mit dem Namen "ACL-UNWANTED-COUNTRY". Der konfigurierte ACE-Eintrag blockiert Brute-Force-VPN-Angriffe aus dem Subnetz 192.168.1.0/24.

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

Schritt 3: Verwenden Sie den nächsten Zugriffsgruppenbefehl, um die ACL "ACL-UNWANTED-COUNTRY" als Kontrollebenen-ACL für die externe ASA-Schnittstelle zu konfigurieren.

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

Schritt 4: Wenn Sie eine neue Kontrollebenen-ACL erstellen oder eine vorhandene bearbeiten, die aktiv genutzt wird, ist es wichtig zu betonen, dass die vorgenommenen Konfigurationsänderungen nicht für bereits bestehende Verbindungen mit der ASA gelten. Sie müssen daher die aktiven Verbindungsversuche mit der ASA manuell löschen. Löschen Sie dazu die aktiven Verbindungen wie folgt.

So löschen Sie die aktive Verbindung für eine bestimmte Host-IP-Adresse:

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


So löschen Sie die aktiven Verbindungen für ein ganzes Subnetz:

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

So löschen Sie die aktiven Verbindungen für einen IP-Adressbereich:

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

---

 Hinweis: Es wird dringend empfohlen, das Schlüsselwort "all" am Ende des Befehls clear conn address zu verwenden, um das Löschen der aktiven VPN-Brute-Force-Verbindungsversuche in die sichere Firewall zu erzwingen, vor allem, wenn die Art des VPN-Brute-Force-Angriffs eine Explosion konstanter Verbindungsversuche auslöst.

---

Alternative Konfiguration zum Blockieren von Angriffen für eine sichere Firewall mithilfe des Befehls "shun"

Im Falle einer sofortigen Option, Angriffe für die sichere Firewall zu blockieren, können Sie den Befehl "shun" verwenden. Mit dem Befehl hunccommand können Sie Verbindungen von einem angreifenden Host blockieren.



- Wenn Sie eine IP-Adresse ignorieren, werden alle zukünftigen Verbindungen von der Quell-IP-Adresse gelöscht und protokolliert, bis die Blockierungsfunktion manuell entfernt wird.
- Die Blockierungsfunktion des Befehls `shun` wird angewendet, unabhängig davon, ob aktuell eine Verbindung mit der angegebenen Host-Adresse aktiv ist.
- Wenn Sie die Zieladresse, die Quell- und Zielports und das Protokoll angeben, dann lassen Sie die passende Verbindung fallen und schließen alle zukünftigen Verbindungen von der Quell-IP ab. Adresse; alle zukünftigen Verbindungen werden vermieden, nicht nur solche, die diesen spezifischen Verbindungsparametern entsprechen.
- Sie können nur einen Befehl pro Quell-IP-Adresse haben.
- Da der `shun` command verwendet wird, um Angriffe dynamisch zu blockieren, wird er in der Gerätekonfiguration zur Bedrohungsabwehr nicht angezeigt.
- Wenn eine Schnittstellenkonfiguration entfernt wird, werden alle Nebenstellen, die an diese Schnittstelle angeschlossen sind, ebenfalls entfernt.

- Shun-Befehlssyntax:

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

- Um eine Shun-Funktion zu deaktivieren, verwenden Sie die negative Form dieses Befehls:

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

Um eine Host-IP-Adresse zu vermeiden, gehen Sie für die sichere Firewall wie folgt vor. In diesem Beispiel wird der Befehl "shun" verwendet, um Brute-Force-VPN-Angriffe zu blockieren, die von der Quell-IP-Adresse 192.168.1.10 ausgehen.

### Konfigurationsbeispiel für FTD

Schritt 1: Melden Sie sich über die CLI beim FTD an, und wenden Sie den Befehl `shun` wie folgt an.

```
<#root>
```

```
>
```

```
shun 192.168.1.10
```

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

```
Shun 192.168.1.10 successful
```

Schritt 2: Sie können die folgenden Befehle zum Anzeigen verwenden, um die verworfenen IP-Adressen im FTD zu bestätigen und die Anzahl der verworfenen Treffer pro IP-Adresse zu überwachen:

```
<#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)
```

## Konfigurationsbeispiel für ASA

Schritt 1: Melden Sie sich über die CLI bei der ASA an, und wenden Sie den Befehl shun wie folgt an.

```
<#root>
```

```
asa#
```

```
shun 192.168.1.10
```

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


```
Shun 192.168.1.10 successful
```

Schritt 2: Mit den folgenden Befehlen zum Anzeigen können Sie die Anzahl der gesendeten IP-Adressen in der ASA bestätigen und die Anzahl der gesendeten IP-Adressen pro IP-Adresse überwachen:

```
<#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)
```

---

 Hinweis: Weitere Informationen zum Befehl shun für die sichere Firewall finden Sie in der [Cisco Secure Firewall Threat Defense Command Reference](#)

---

## Überprüfung

So bestätigen Sie, dass die ACL-Konfiguration der Kontrollebene für die sichere Firewall vorhanden ist:

Schritt 1: Melden Sie sich über die CLI bei der sicheren Firewall an, und führen Sie die nächsten Befehle aus, um zu bestätigen, dass die ACL-Konfiguration der Kontrollebene angewendet wurde.

Ausgabebeispiel für von FMC verwaltete FTD:

```
<#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
```

Ausgabebeispiel für von FDM verwaltete FTD:

```
<#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
```

Ausgabebeispiel für 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
```

Schritt 2: Um zu bestätigen, dass die Kontrollebenen-ACL den erforderlichen Datenverkehr blockiert, verwenden Sie den Befehl Packet-Tracer, um eine eingehende TCP 443-Verbindung mit der externen Schnittstelle der sicheren Firewall zu simulieren, und dann den Befehl show access-list <acl-name>. Die Anzahl der ACL-Treffer sollte jedes Mal erhöht werden, wenn eine VPN-Brute-Force-Verbindung mit der sicheren Firewall durch die Kontrollebenen-ACL blockiert wird:

- In diesem Beispiel simuliert der Befehl "Packet-Tracer" eine eingehende TCP-443-Verbindung, die vom Host 192.168.1.10 stammt und an die externe IP-Adresse unserer sicheren Firewall gerichtet ist. Die Ausgabe von "Packet-Tracer" bestätigt, dass der Datenverkehr verworfen wird, und die Ausgabe von "show access-list" zeigt die inkrementellen Trefferzahlen für unsere ACL auf der Kontrollebene an:

## Beispiel für FTD-Ausgabe

```
<#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
```

## Ausgabebeispiel für 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

---

 Hinweis: Wenn eine RAVPN-Lösung wie das Cisco Secure Client VPN in der sicheren Firewall implementiert ist, kann ein echter Verbindungsversuch zur sicheren Firewall durchgeführt werden, um zu bestätigen, dass die ACL auf der Kontrollebene wie erwartet funktioniert, um den erforderlichen Datenverkehr zu blockieren.

---

## Verwandte Fehler

- ENH | Standortbasierte AnyConnect Client-Verbindungen: Cisco Bug-ID [CSCvs65322](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.