

セキュアなファイアウォール脅威対策とASAのためのコントロールプレーンアクセスコントロールポリシーの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[コンフィギュレーション](#)

[FMCによって管理されるFTDのコントロールプレーンACLの設定](#)

[FDMによって管理されるFTDのコントロールプレーンACLの設定](#)

[CLIを使用したASAのコントロールプレーンACLの設定](#)

[「shun」コマンドを使用してセキュアファイアウォールの攻撃をブロックする代替設定](#)

[確認](#)

[関連バグ](#)

はじめに

このドキュメントでは、セキュアファイアウォール脅威対策および適応型セキュリティアプライアンス(ASA)のコントロールプレーンアクセスルールを設定するプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- セキュアファイアウォール脅威対策(FTD)
- Secure Firewall Device Manager(FDM)
- セキュアファイアウォール管理センター(FMC)
- セキュアなファイアウォールASA
- Access Control List (ACL; アクセス コントロール リスト)
- FlexConfig

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Secure Firewall Threat Defenseバージョン7.2.5
- Secure Firewall Manager Centerバージョン7.2.5
- Secure Firewall Device Managerバージョン7.2.5
- セキュアファイアウォールASAバージョン9.18.3

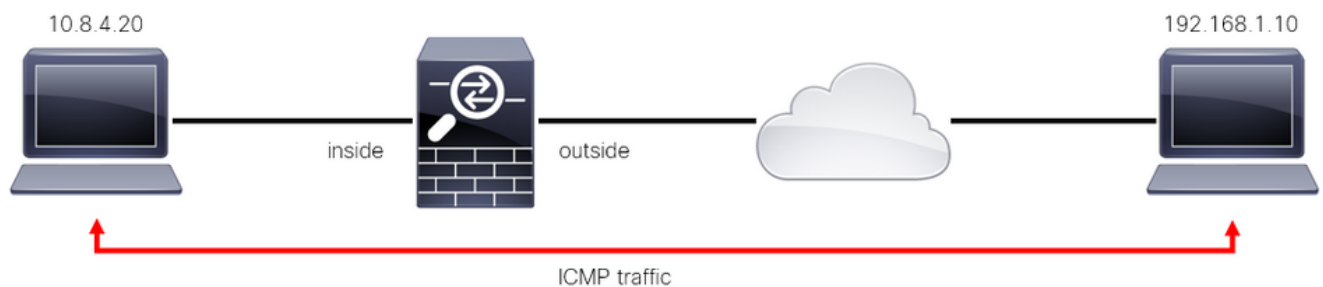
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

通常、トラフィックはファイアウォールを通過し、データインターフェイス間でルーティングされます。状況によっては、セキュアなファイアウォール宛てのトラフィックを拒否することが有益です。シスコのセキュアファイアウォールでは、コントロールプレーンアクセスコントロールリスト(ACL)を使用して、「to-the-box」トラフィックを制限できます。コントロールプレーンACLが役立つ例としては、セキュアファイアウォールへのVPN（サイト間またはリモートアクセスVPN）トンネルを確立できるピアを制御する場合があります。

ファイアウォールの「through-the-box」トラフィックの保護

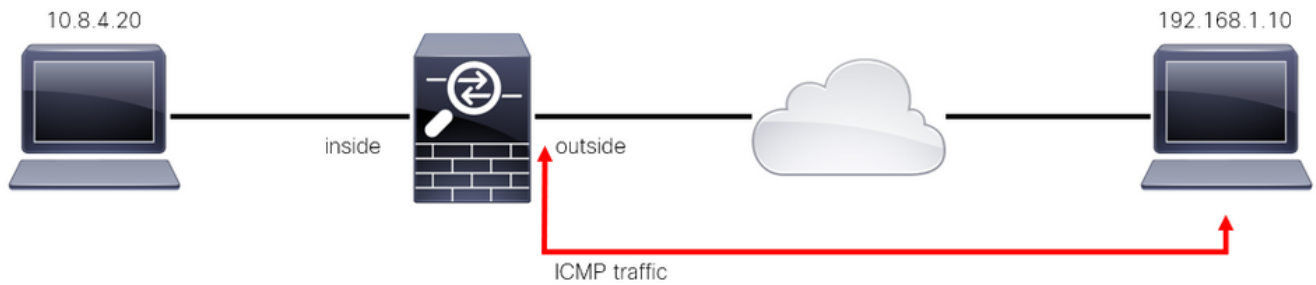
トラフィックは通常、1つのインターフェイス（インバウンド）から別のインターフェイス（アウトバウンド）にファイアウォールを通過します。これは「through-the-box」トラフィックと呼ばれ、アクセスコントロールポリシー(ACP)とプレフィルタルールの両方で管理されます。



画像 1.through-the-boxトラフィックの例

ファイアウォールの「to-the-box」トラフィックの保護

トラフィックがFTDインターフェイス（サイト間またはリモートアクセスVPN）に直接送信される別のケースもあります。これは「to-the-box」トラフィックと呼ばれ、その特定のインターフェイスのコントロールプレーンによって管理されます。



画像 2.To-the-boxトラフィックの例

コントロールプレーンACLに関する重要な考慮事項

- FMC/FTDバージョン7.0以降では、ASAで使用されるのと同じコマンド構文を使用して、FlexConfigを使用してコントロールプレーンACLを設定する必要があります。
- キーワードcontrol-planeがaccess-group設定に追加され、セキュアなファイアウォールインターフェイスに対してトラフィックを「強制」します。コマンドにコントロールプレーンワードが追加されないと、ACLはセキュアファイアウォールを「通過する」トラフィックを制限します。
- コントロールプレーンACLは、セキュアなファイアウォールインターフェイスへのSSH、ICMP、またはTELNET着信を制限しません。これらはプラットフォーム設定ポリシーに従って処理（許可/拒否）され、より高い優先順位を持ちます。
- コントロールプレーンACLはトラフィックをセキュアファイアウォール自体に「制限」しますが、FTDのアクセスコントロールポリシーまたはASAの通常のACLはセキュアファイアウォールを「通過」するトラフィックを制御します。
- 通常のACLとは異なり、ACLの最後には暗黙の「deny」は存在しません。
- このドキュメントの作成時点では、FTDの位置情報機能を使用してFTDへのアクセスを制限することはできません。

設定

次の例では、特定の国からのIPアドレスのセットが、FTD RAVPNへのログインを試みることにより、VPNへのブルートフォースを試みます。これらのVPNの総当たり攻撃からFTDを保護する最良のオプションは、外部FTDインターフェイスへの接続をブロックするようにコントロールプレーンACLを設定することです。

コンフィギュレーション

FMCによって管理されるFTDのコントロールプレーンACLの設定

外部FTDインターフェイスへの着信VPNブルートフォース攻撃をブロックするようにコントロールプレーンACLを設定するには、FMCで次の手順を実行する必要があります。

ステップ 1：HTTPS経由でFMCグラフィックユーザインターフェイス(GUI)を開き、クレデンシャルでログインします。



画像 3.FMCログインページ

ステップ 2：拡張ACLを作成する必要があります。このためには、「オブジェクト」>「オブジェクト管理」に移動します。

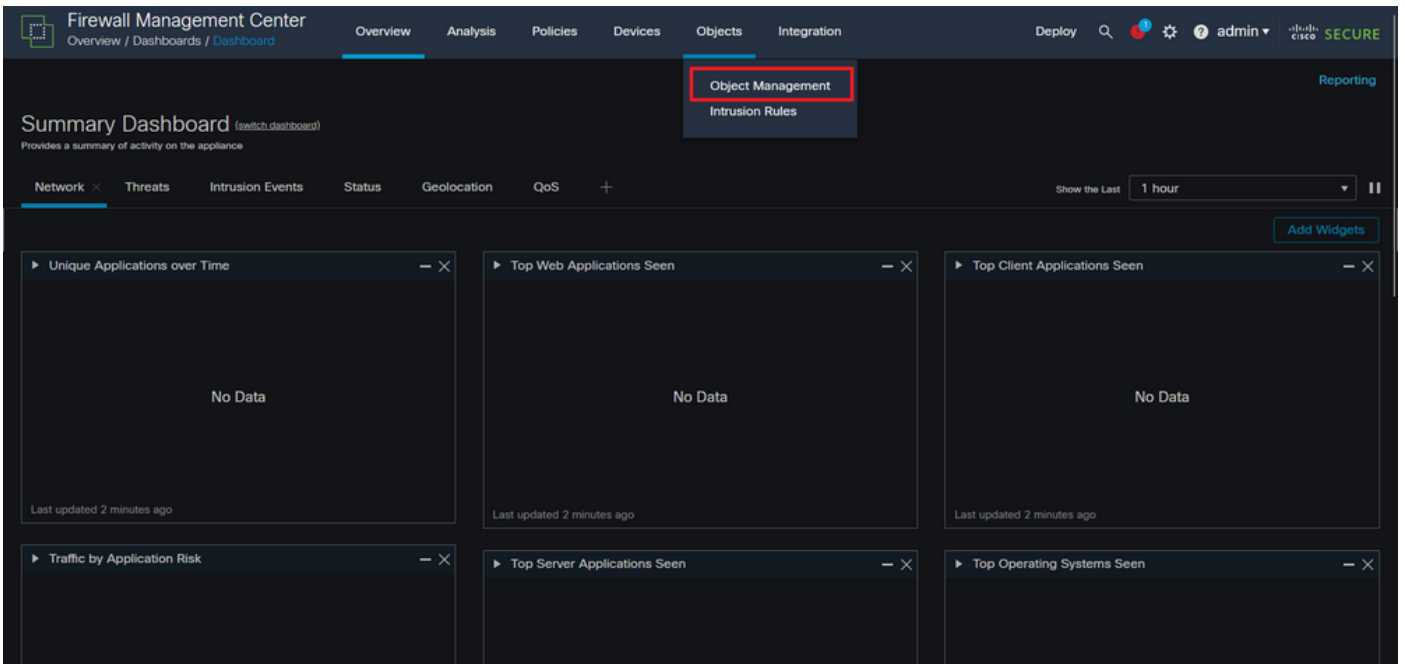


図 4.オブジェクト管理

ステップ 2.1：左側のパネルから、Access List > Extendedの順に移動して、拡張ACLを作成します。

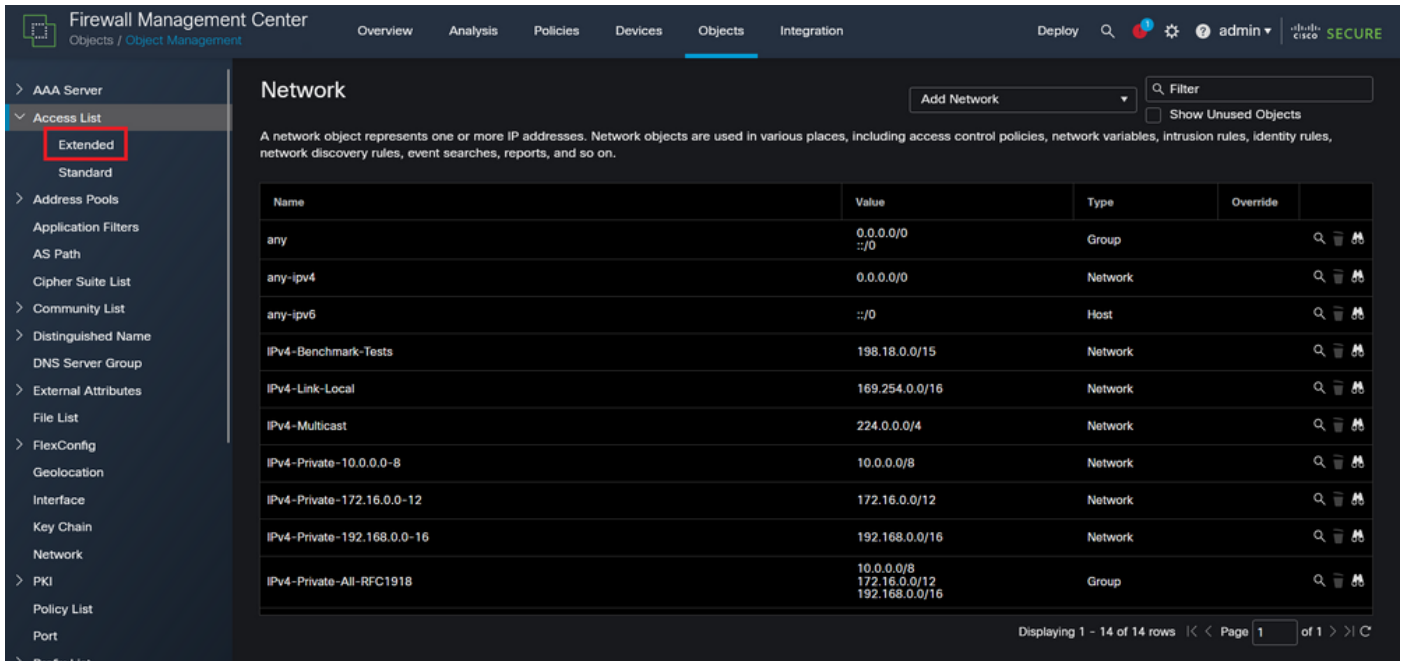


図 5. 拡張ACLメニュー

ステップ 2.2 : 次に、Add Extended Access Listを選択します。

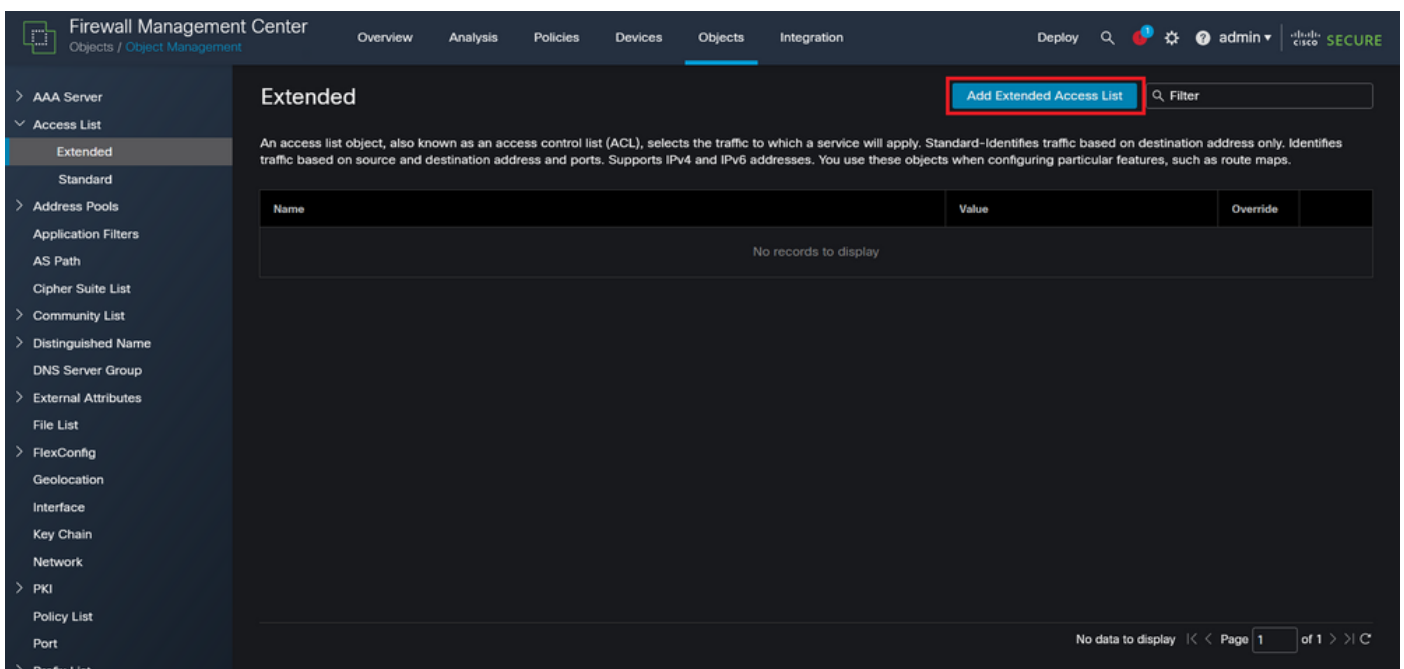


図 6. 拡張ACLの追加

ステップ 2.3 : 拡張ACLの名前を入力し、Addボタンをクリックしてアクセスコントロールエントリ(ACE)を作成します。

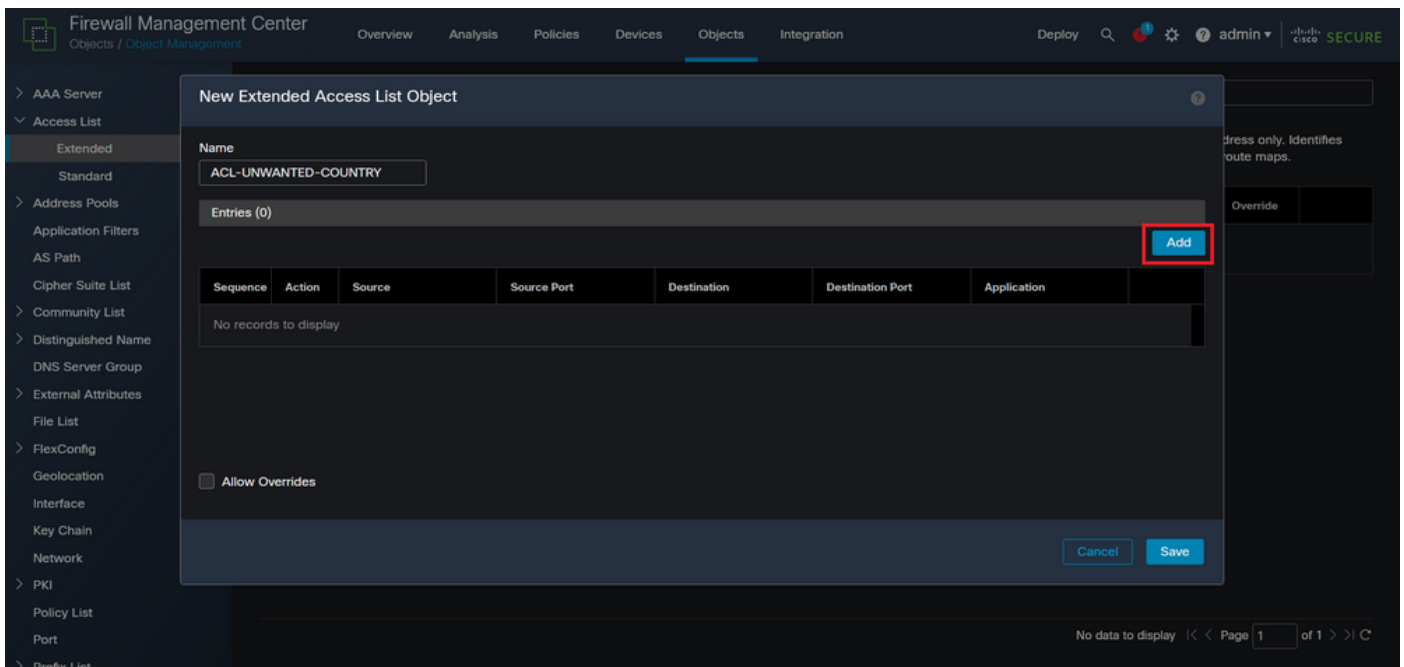


図 7.拡張ACLエントリ

ステップ 2.4 : ACEのアクションをBlockに変更し、FTDに対して拒否する必要があるトラフィックと一致するように送信元ネットワークを追加し、宛先ネットワークをAnyのままにして、AddボタンをクリックしてACEエントリを完了します。

– この例では、設定されたACEエントリにより、192.168.1.0/24サブネットからのVPNブルートフォース攻撃がブロックされます。

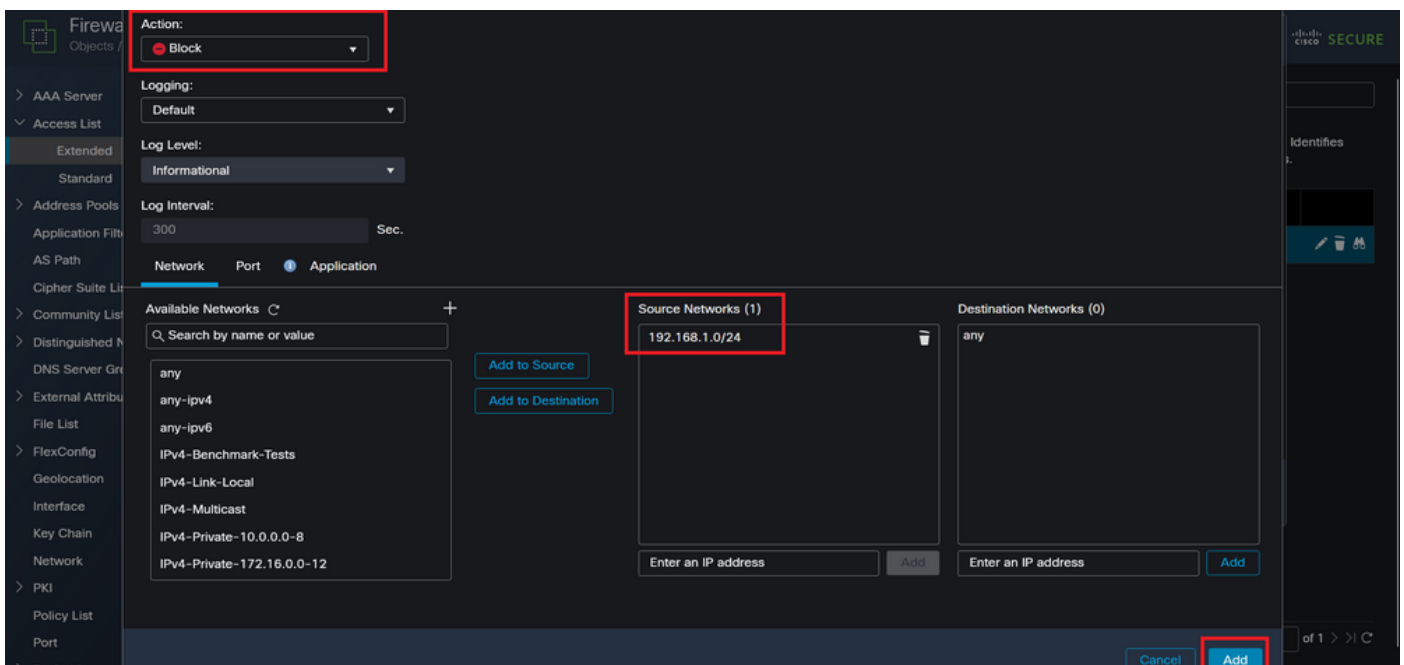


図 8.拒否されたネットワーク

ステップ 2.5 : さらにACEエントリを追加する必要がある場合は、もう一度Addボタンをクリックして、ステップ2.4を繰り返します。その後、Saveボタンをクリックして、ACLの設定を完了します。

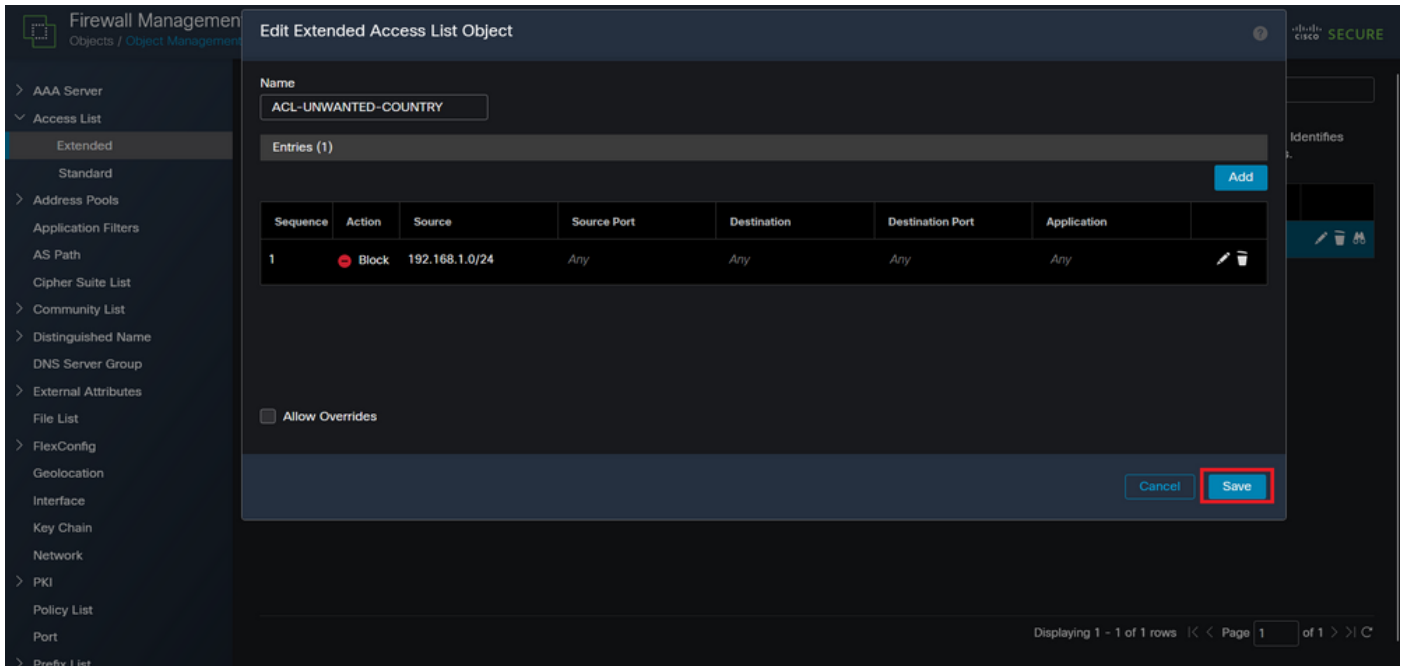


図 9. 完成した拡張ACLエントリ

ステップ 3 : 次に、コントロールプレーンACLを外部FTDインターフェイスに適用するように Flex-Configオブジェクトを設定する必要があります。このためには、左側のパネルに移動し、オプションFlexConfig > FlexConfig Objectを選択します。

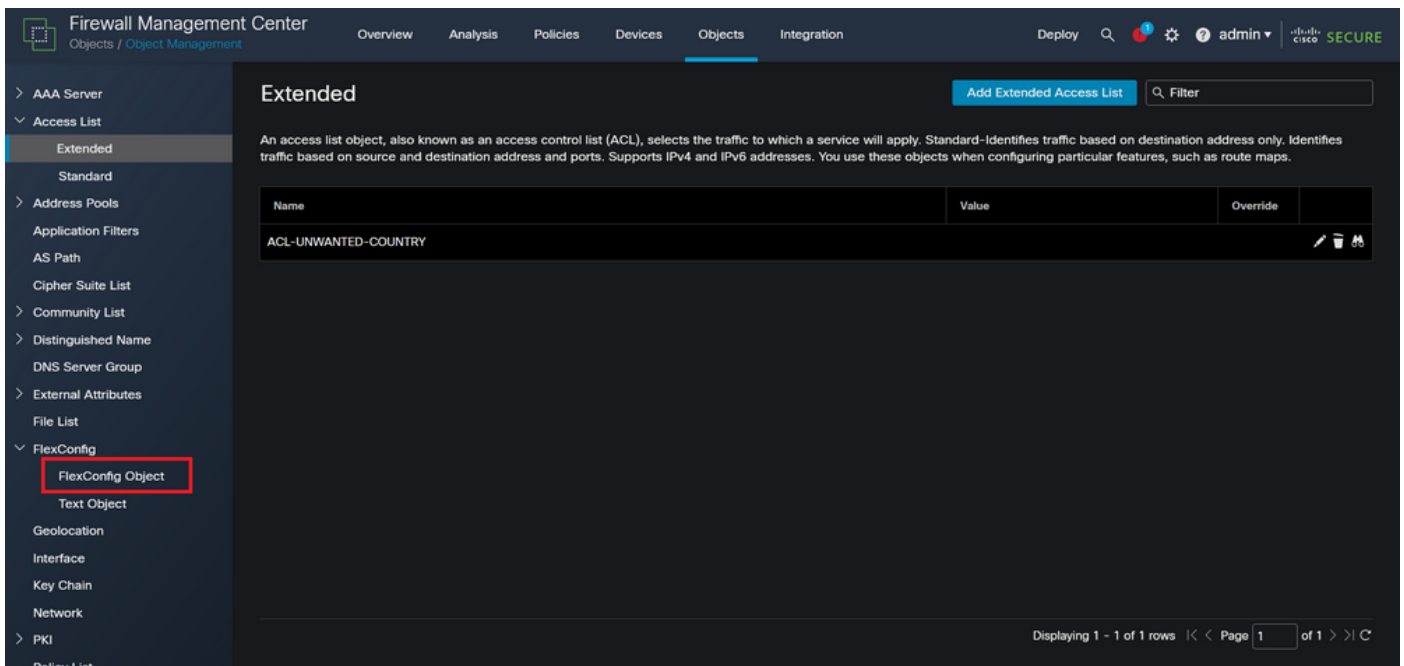


図 10. FlexConfigオブジェクトメニュー

ステップ 3.1 : [FlexConfigオブジェクトの追加]をクリックします。

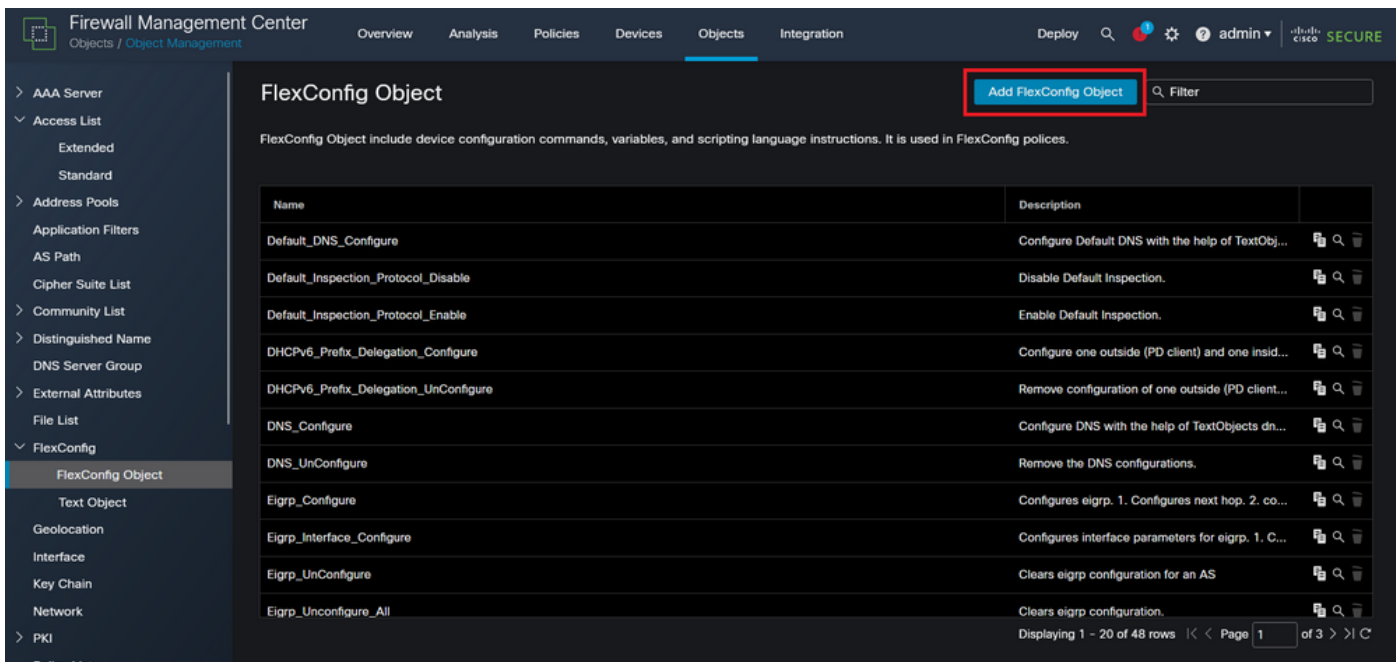


図 11. Flexconfigオブジェクトの追加

ステップ 3.2 : FlexConfigオブジェクトの名前を追加し、ACLポリシーオブジェクトを挿入します。このためには、Insert > Insert Policy Object > Extended ACL Objectの順に選択します。

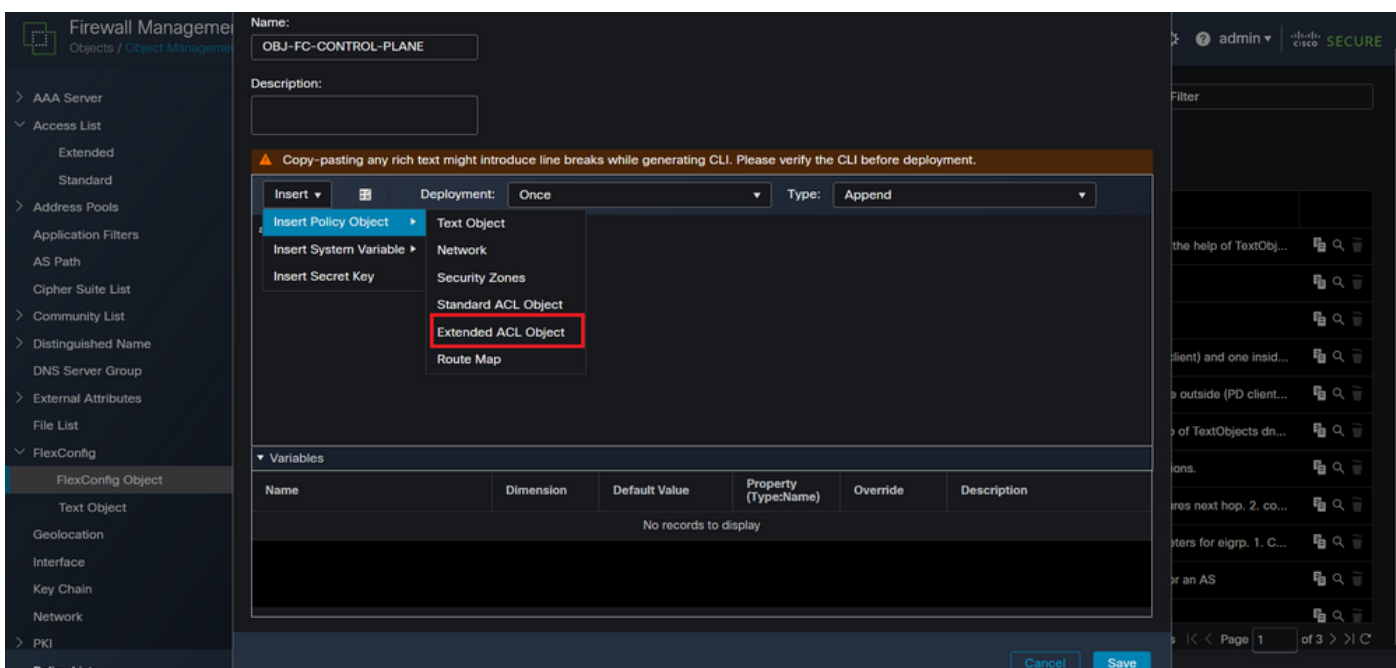


図 12. FlexConfigオブジェクト変数

ステップ 3.3 : ACLオブジェクト変数の名前を追加してから、ステップ2.3で作成した拡張ACLを選択します。その後、Saveボタンをクリックします。

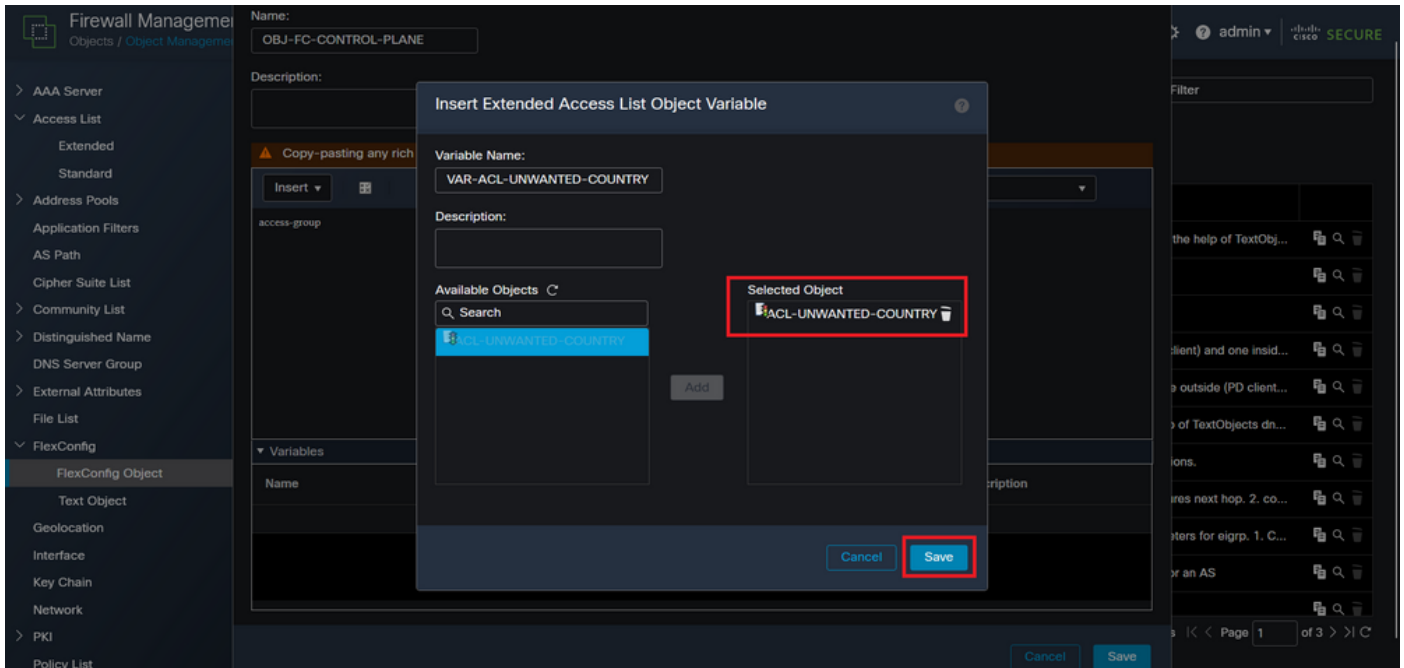


図 13. FlexConfig オブジェクト変数 ACL 割り当て

ステップ 3.4 : 次に、コントロールプレーン ACL を外部インターフェイスのインバウンドとして次のように設定します。

コマンドライン構文 :

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

これは、次のコマンド例に変換されます。この例では、上記のステップ 2.3 で作成した ACL 変数「VAR-ACL-UNWANTED-COUNTRY」を次のように使用しています。

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

FlexConfig オブジェクトウィンドウで設定する方法は次のとおりです。その後、Save ボタンを選択して FlexConfig オブジェクトを完了します。

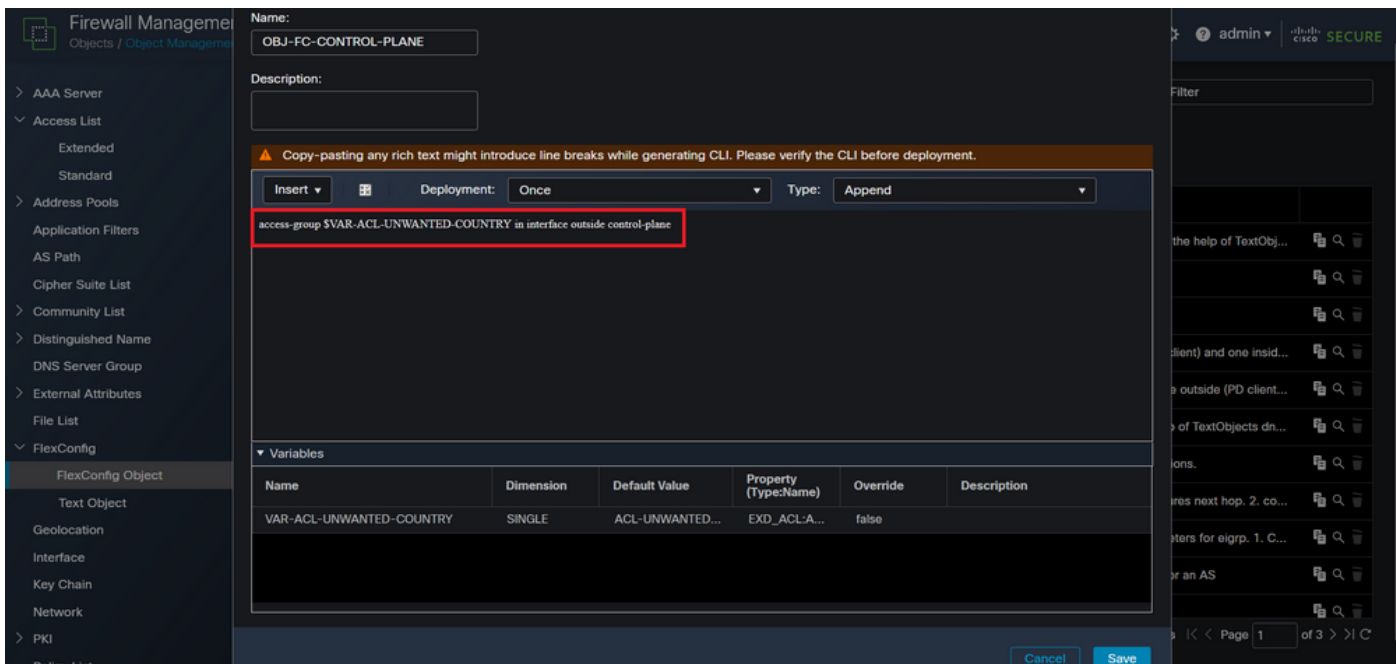


図 14. Flexconfig Object complete コマンドライン

ステップ 4 : FlexConfig オブジェクトの設定を FTD に適用する必要があります。そのためには、Devices > FlexConfig の順に選択します。

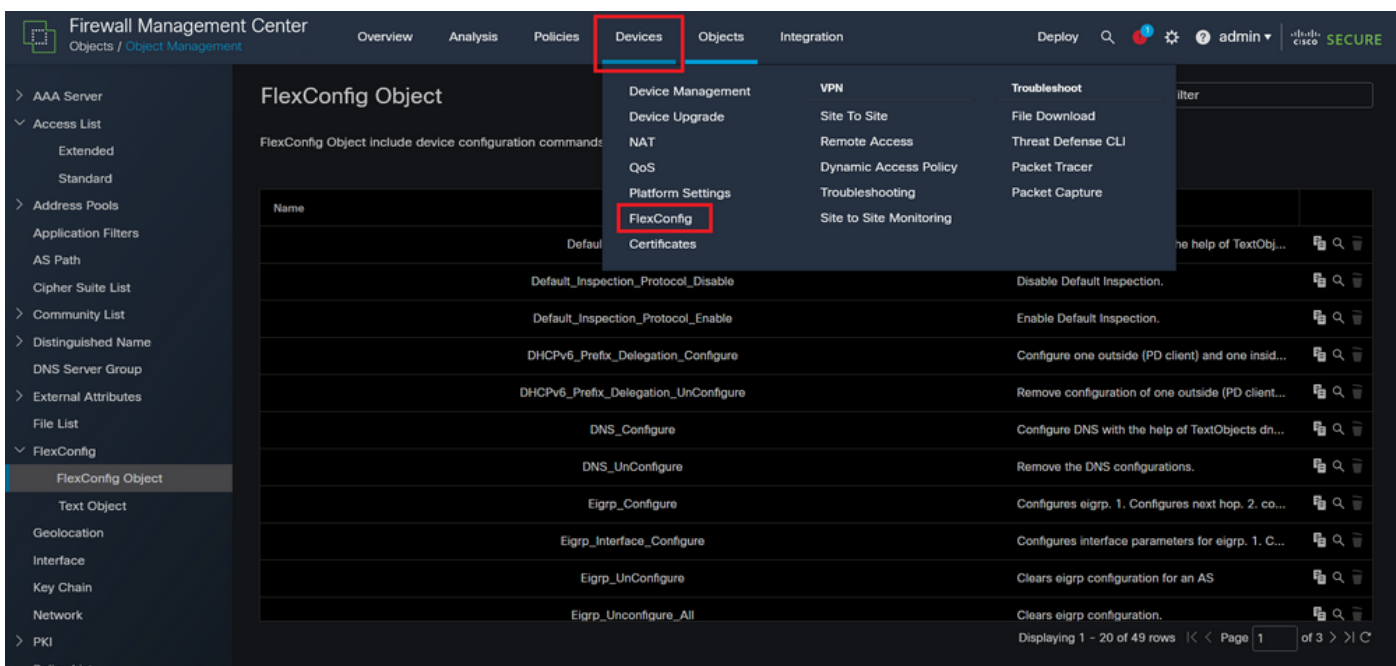


図 15. FlexConfig Policy メニュー

ステップ 4.1 : 次に、FTD 用に作成された FlexConfig がいない場合は New Policy をクリックするか、既存の FlexConfig ポリシーを編集します。

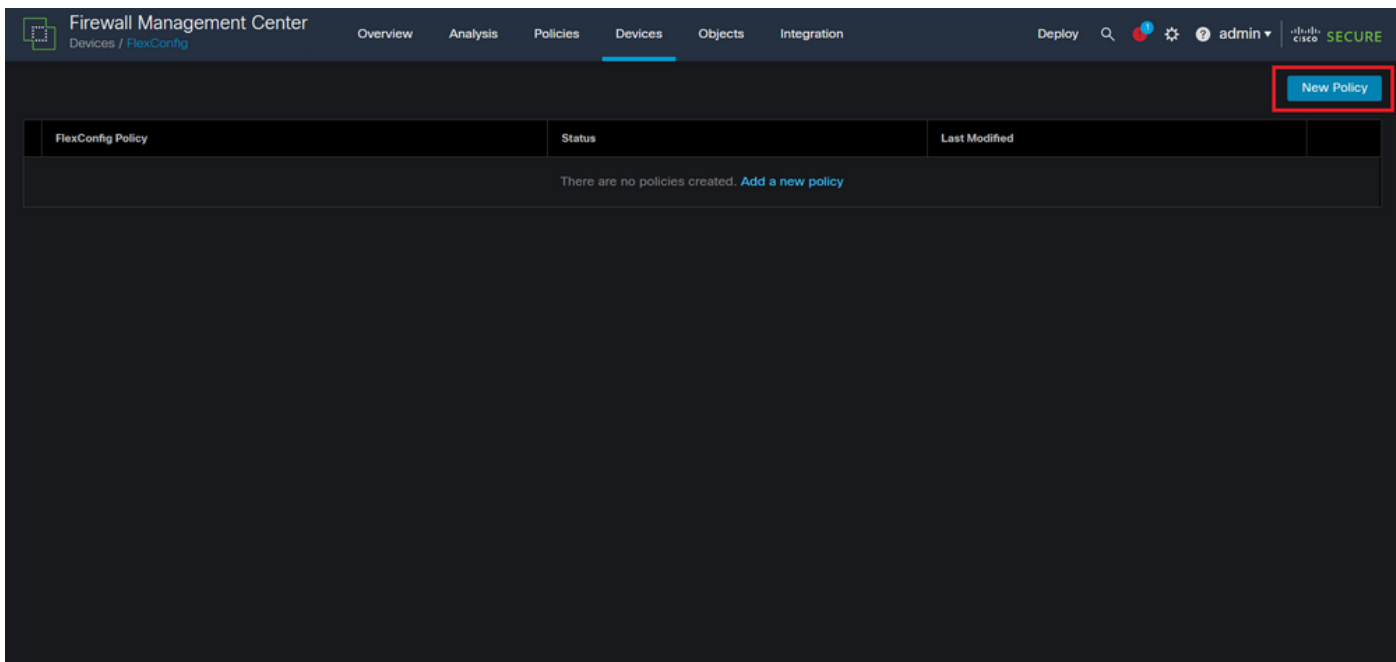


図 16.FlexConfigポリシーの作成

ステップ 4.2 : 新しいFlexConfigポリシーの名前を追加し、作成したコントロールプレーンACLを適用するFTDを選択します。

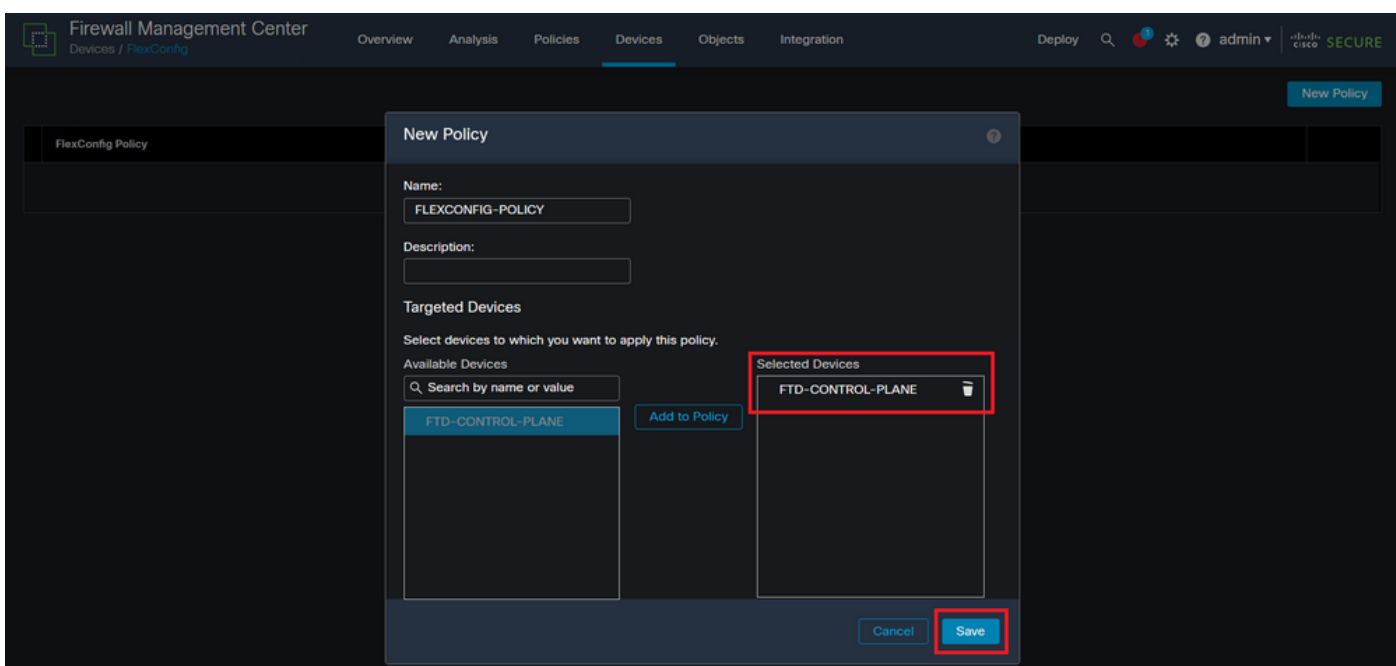


図 17.FlexConfigポリシーデバイスの割り当て

ステップ 4.3 : 左側のパネルで、上記のステップ3.2で作成したFlexConfigオブジェクトを検索し、ウィンドウの中央にある右矢印をクリックしてFlexConfigポリシーに追加します。その後、「Save」ボタンをクリックします。

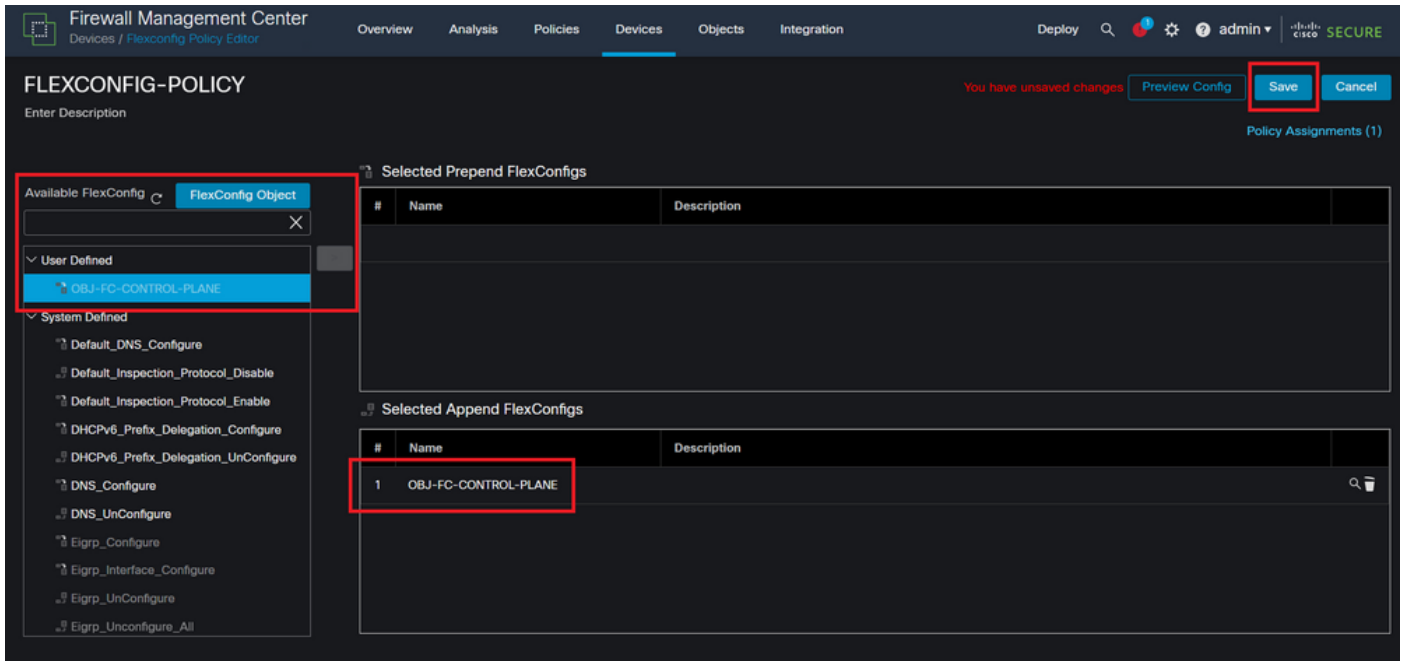


図 18. FlexConfig ポリシー オブジェクト の 割り 当て

ステップ 5： 設定 変更 を FTD に 展 開 す る た め 、 Deploy > Advanced Deploy の 順 に 移 動 し ます 。

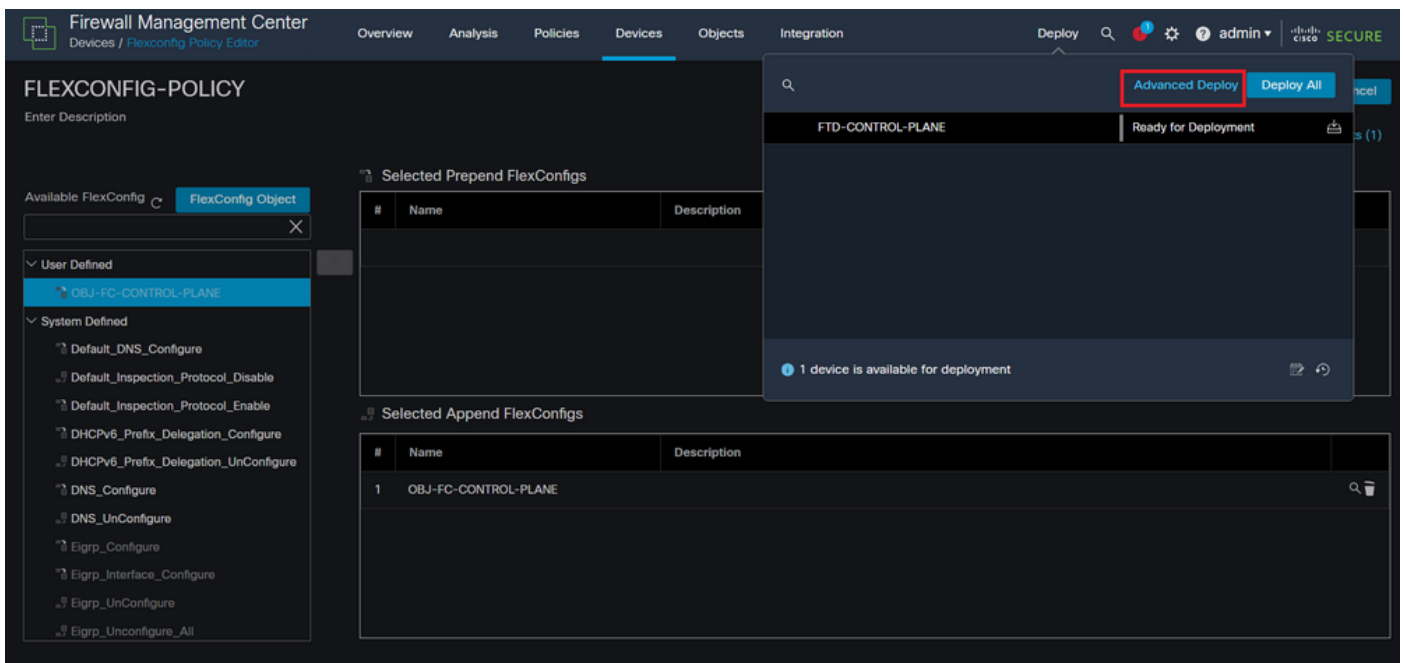


図 19. FTD の 高 度 な 導 入

ステップ 5.1： 次 に 、 FlexConfig ポリシー を 適 用 す る FTD を 選 択 し ます 。 す べ て が 正 し い 場 合 は 、 「 配 置 」 を ク リ ッ ク し ます 。

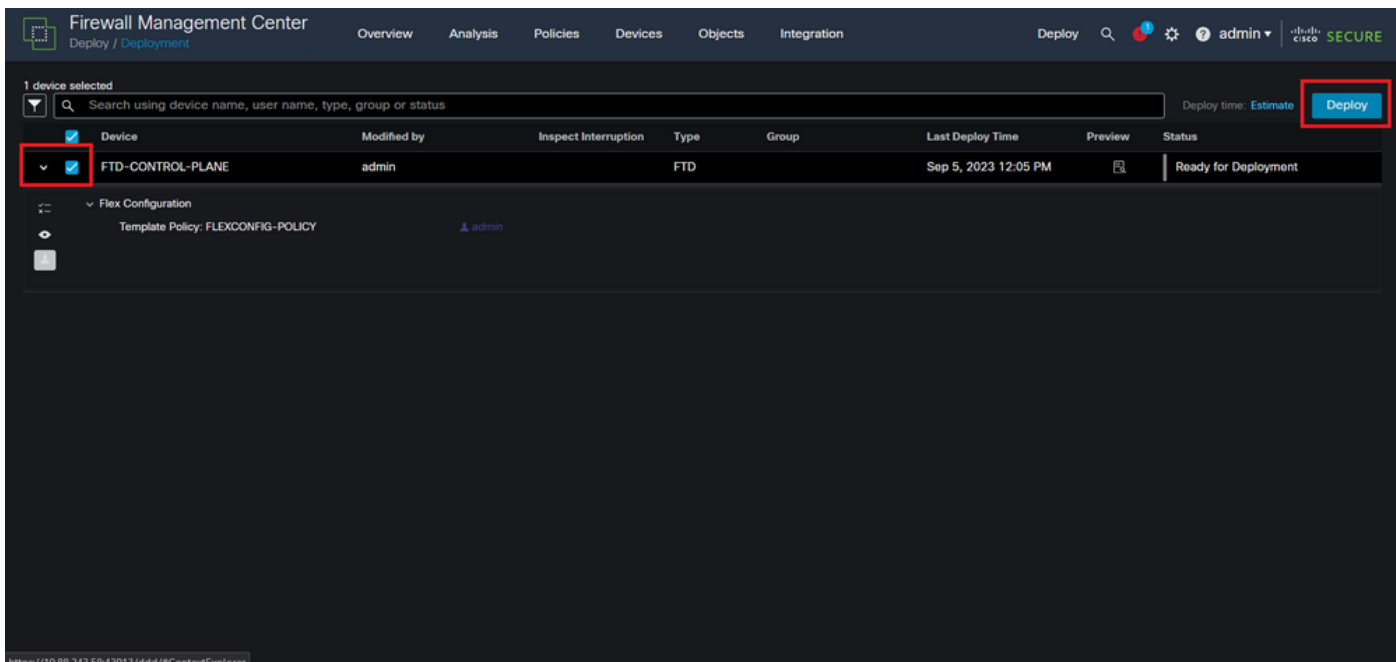


図 20.FTD導入の検証

ステップ 5.2 : その後、「配備の確認」ウィンドウが表示され、配備を追跡するためのコメントを追加して「配備」に進みます。

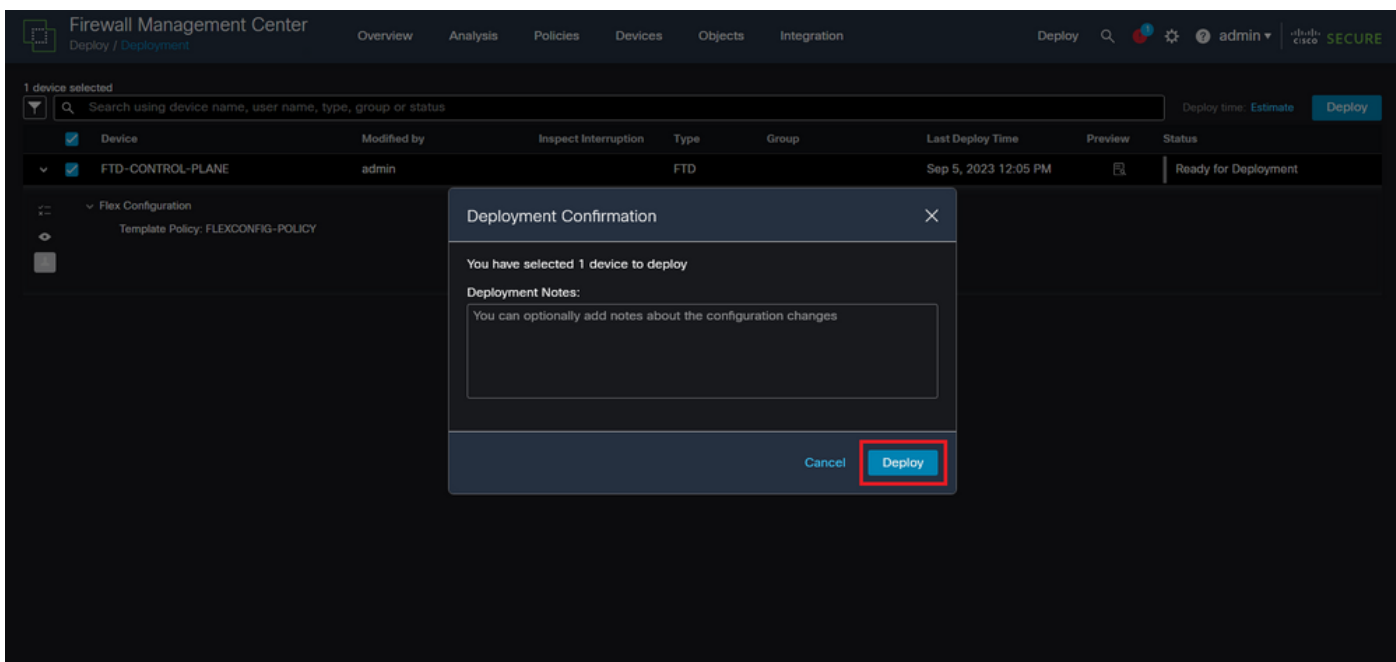


図 21.FTD導入に関するコメント

ステップ 5.3 : FlexConfigの変更を導入するときに警告メッセージが表示される場合があります。ポリシー設定が正しいことが完全に確認できている場合にのみ、Deployをクリックします。

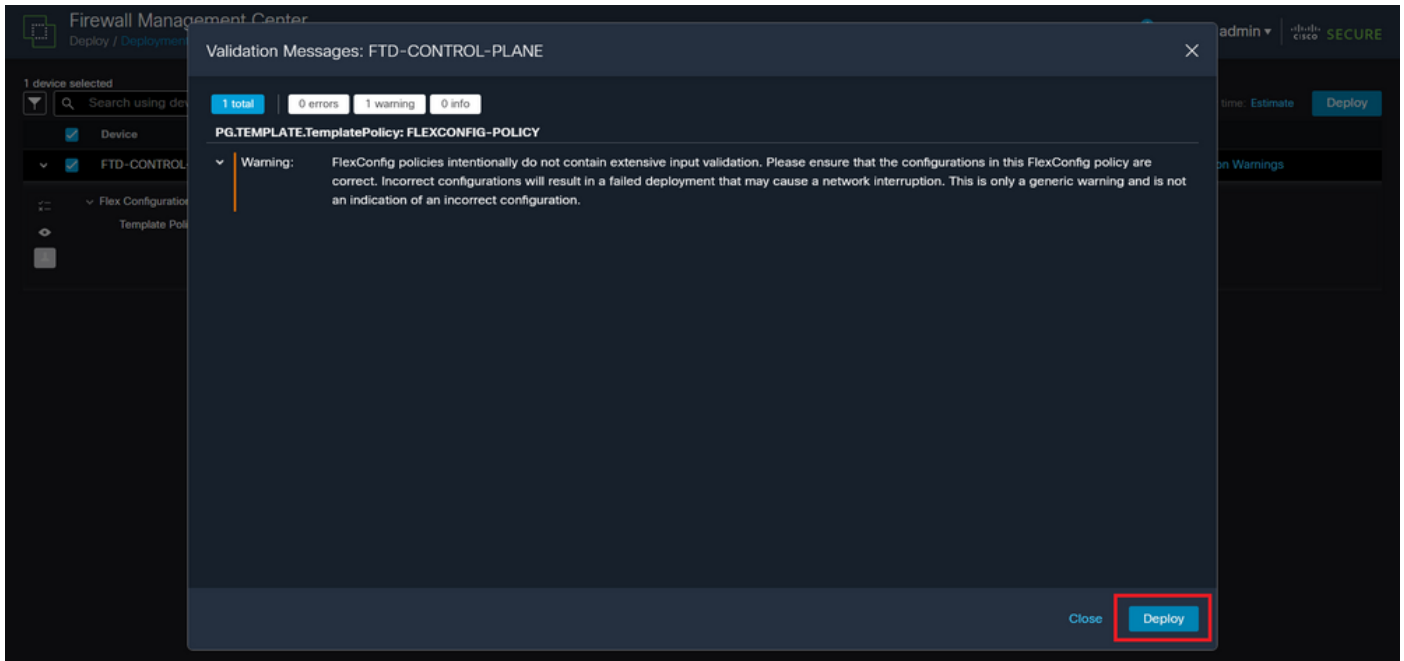


図 22.FTD展開Flexconfigの警告

ステップ 5.4 : FTDのポリシー展開が正常に行われたことを確認します。

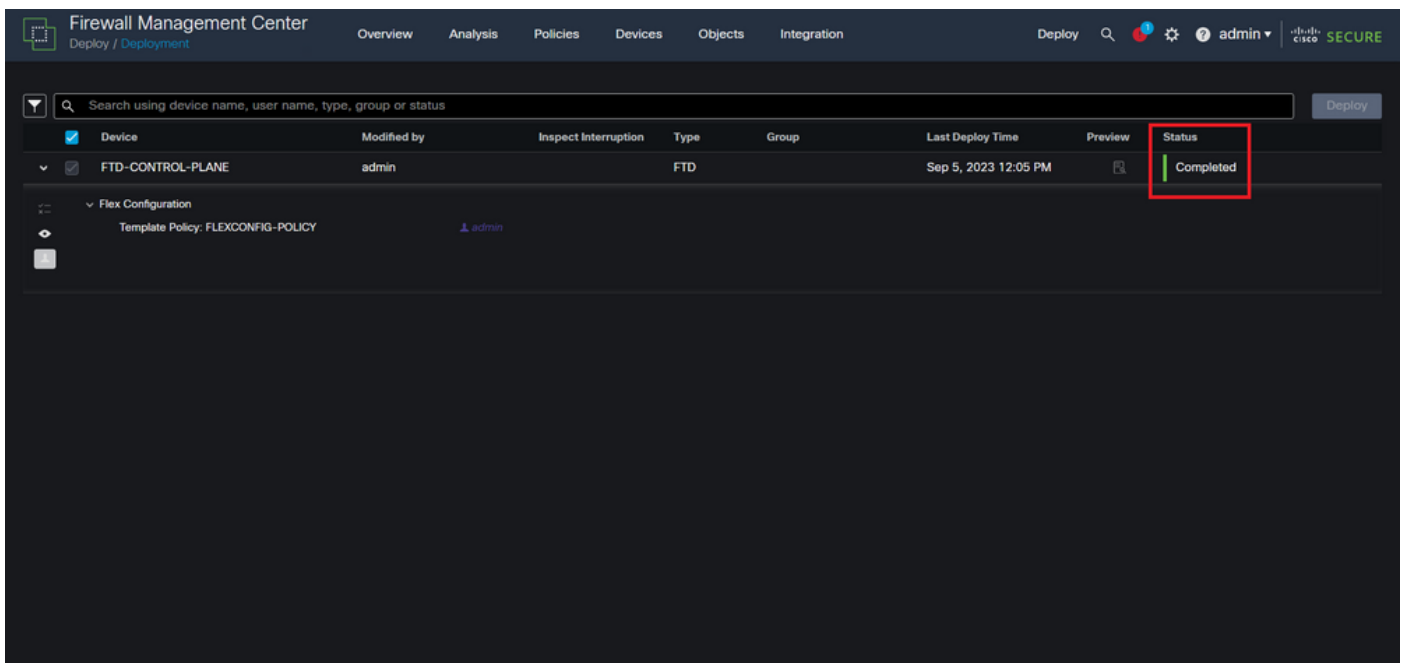


図 23.FTDの導入に成功

手順 6 : FTD用に新しいコントロールプレーンACLを作成する場合、またはアクティブに使用されている既存のコントロールプレーンACLを編集する場合は、加えられた設定変更がFTDへの確立済みの接続に適用されないことを強調することが重要です。したがって、FTDへのアクティブな接続試行を手動でクリアする必要があります。そのためには、次のようにFTDのCLIに接続し、アクティブな接続をクリアします。

特定のホストIPアドレスのアクティブな接続をクリアするには、次の手順を実行します。


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

サブネットワーク全体のアクティブな接続をクリアするには、次の手順を実行します。

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

特定の範囲のIPアドレスに対するアクティブな接続をクリアするには、次の手順を実行します。

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

 注：clear conn addressコマンドの最後にキーワード「all」を使用して、アクティブなVPN総当たり攻撃によるセキュアなファイアウォールへの接続試行を強制的にクリアすることを強く推奨します。これは主に、VPN総当たり攻撃の性質によって絶え間ない接続試行の爆発が発生している場合に行われます。

FDMによって管理されるFTDのコントロールプレーンACLの設定

外部FTDインターフェイスへの着信VPNブルートフォース攻撃をブロックするようにコントロールプレーンACLを設定するためにFDMで実行する必要がある手順を次に示します。

ステップ 1：HTTPS経由でFDM GUIを開き、クレデンシャルでログインします。

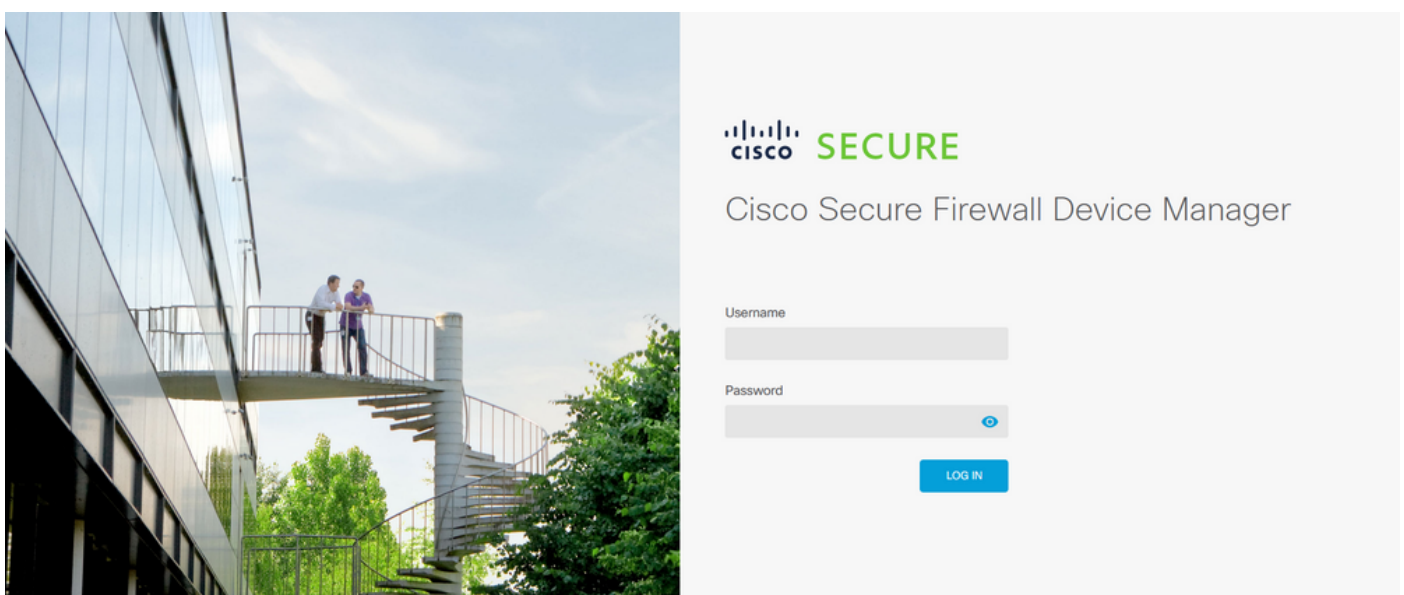


図 24.FDMログイン・ ページ

ステップ 2 : オブジェクトネットワークを作成する必要があります。この場合は、次のオブジェクトに移動します。

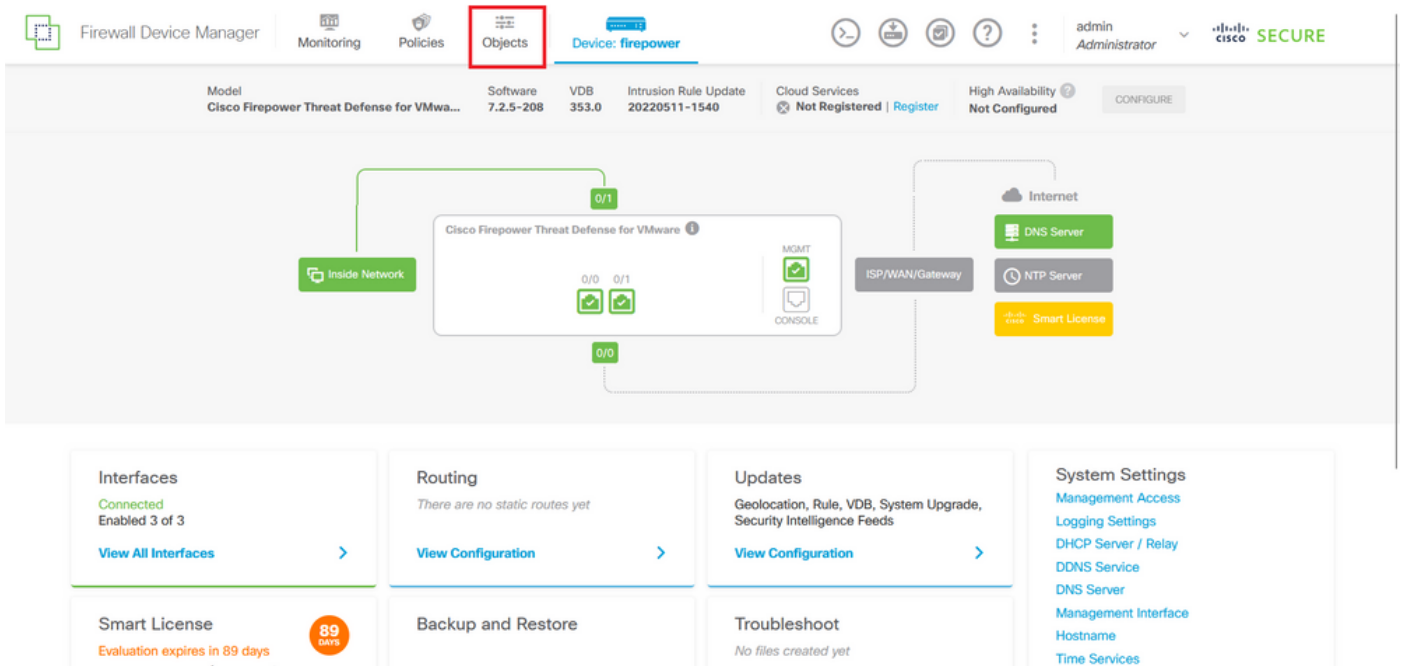


図 25.FDMメイン・ ダッシュボード

ステップ 2.1 : 左側のパネルからNetworksを選択し、「+」ボタンをクリックして新しいネットワークオブジェクトを作成します。

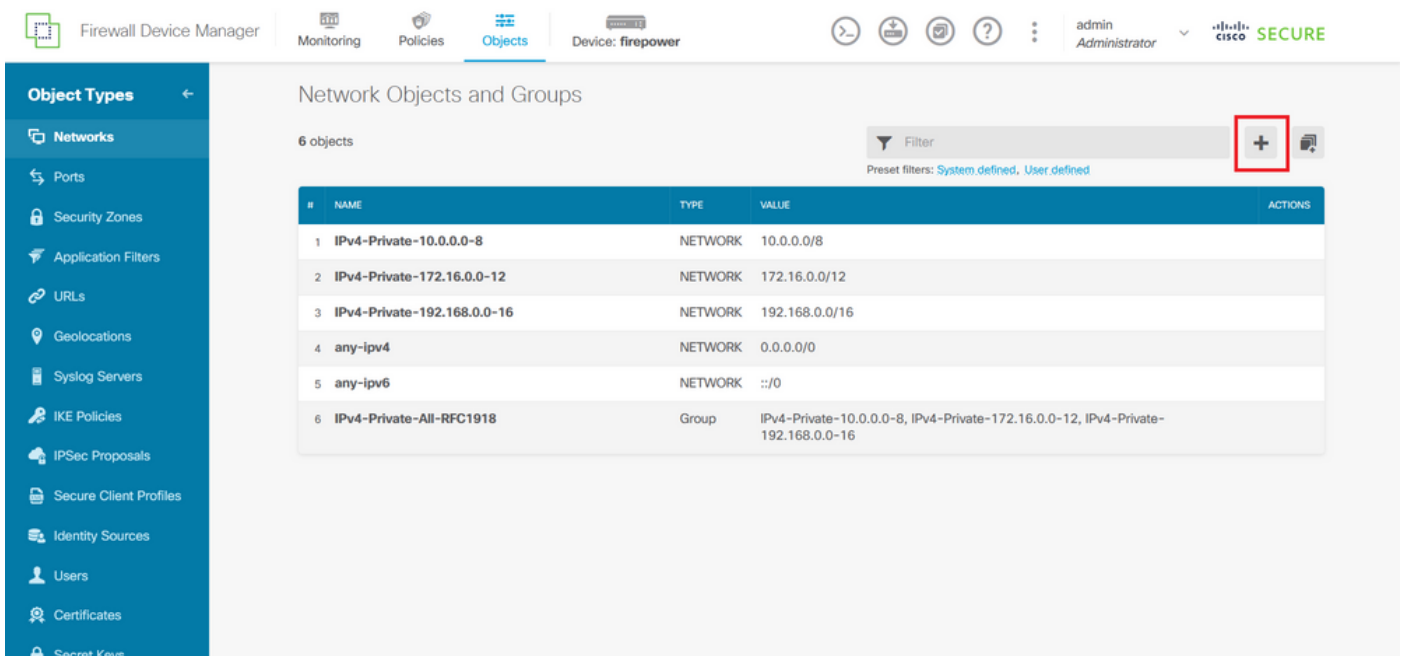


図 26.オブジェクトの作成

ステップ 2.2 : ネットワークオブジェクトの名前を追加し、オブジェクトのネットワークタイプを選択し、FTDに対して拒否する必要があるトラフィックに一致するIPアドレス、ネットワークアドレス、またはIPの範囲を追加します。次に、[OK]ボタンをクリックしてオブジェクトネット

ワークを完了します。

- この例で設定するオブジェクトネットワークは、192.168.1.0/24サブネットからのVPNブルートフォース攻撃をブロックすることを目的としています。

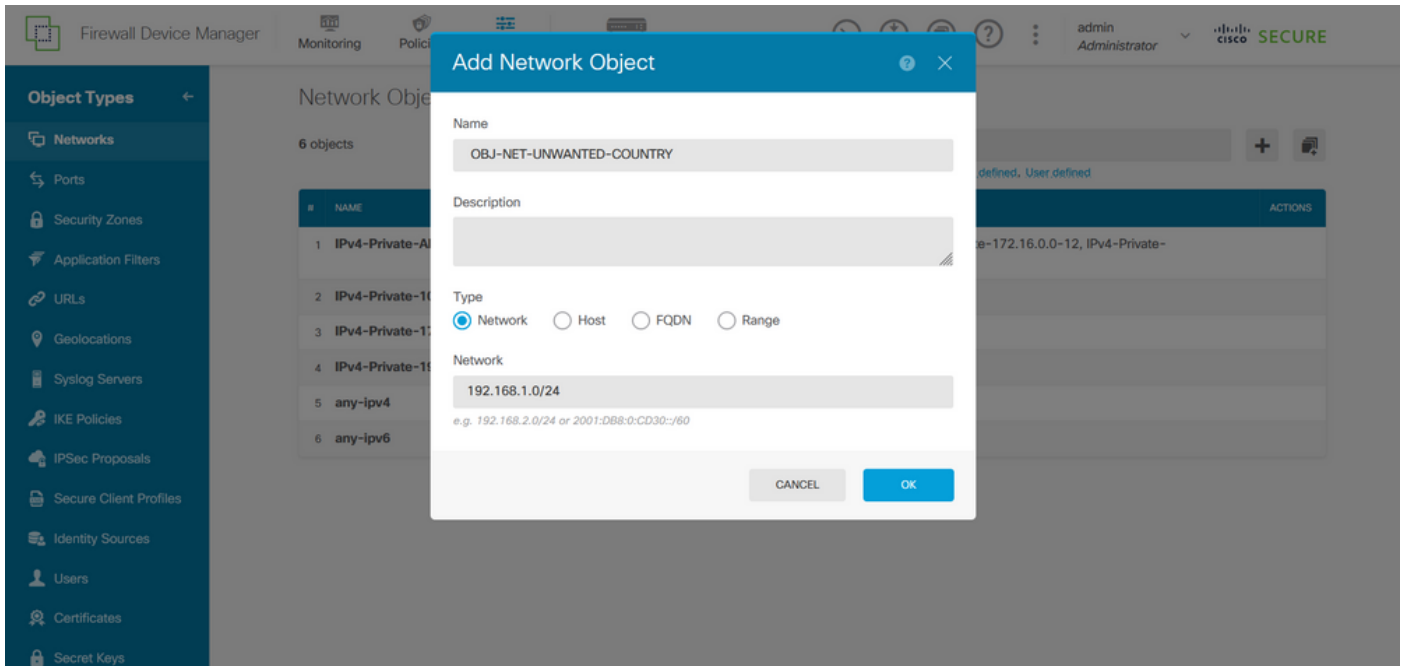


図 27. ネットワークオブジェクトの追加

ステップ 3：次に、拡張ACLを作成する必要があります。それには、トップメニューのDeviceタブに移動します。

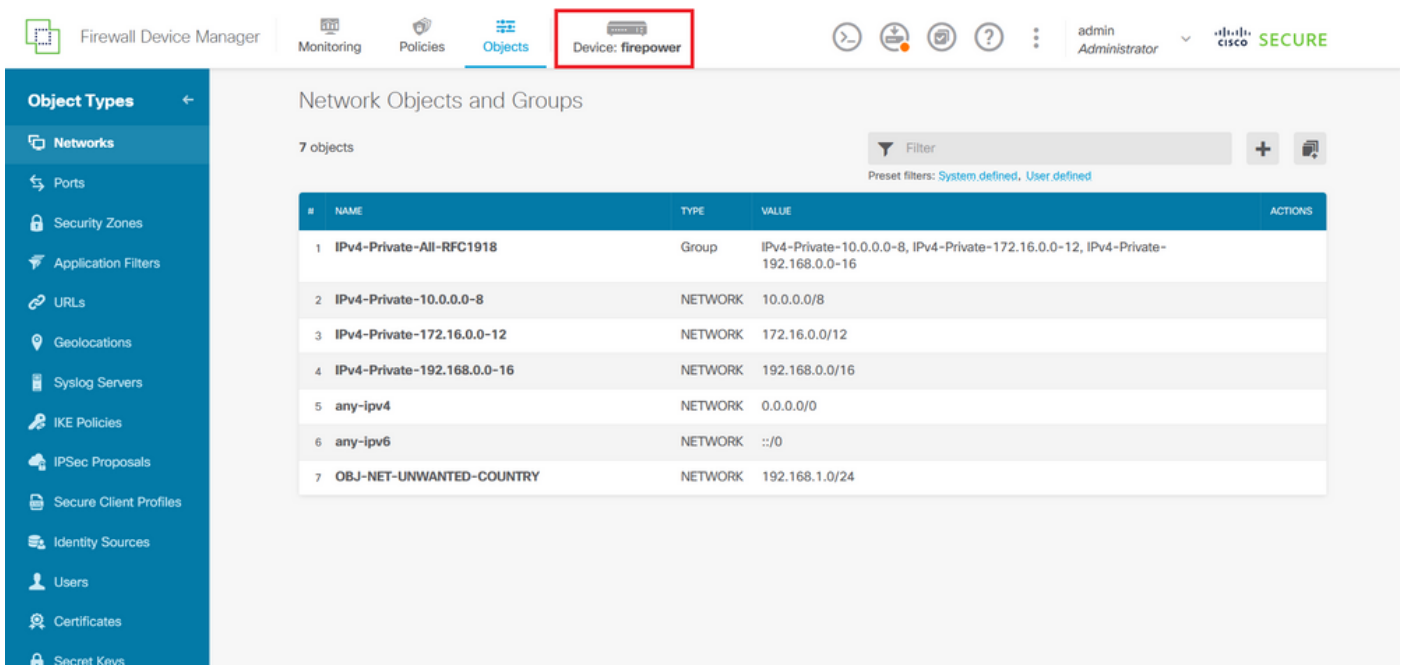


図 28. デバイス設定ページ

ステップ 3.1：下にスクロールして、次のようにAdvanced Configurationの画面でView Configurationを選択します。

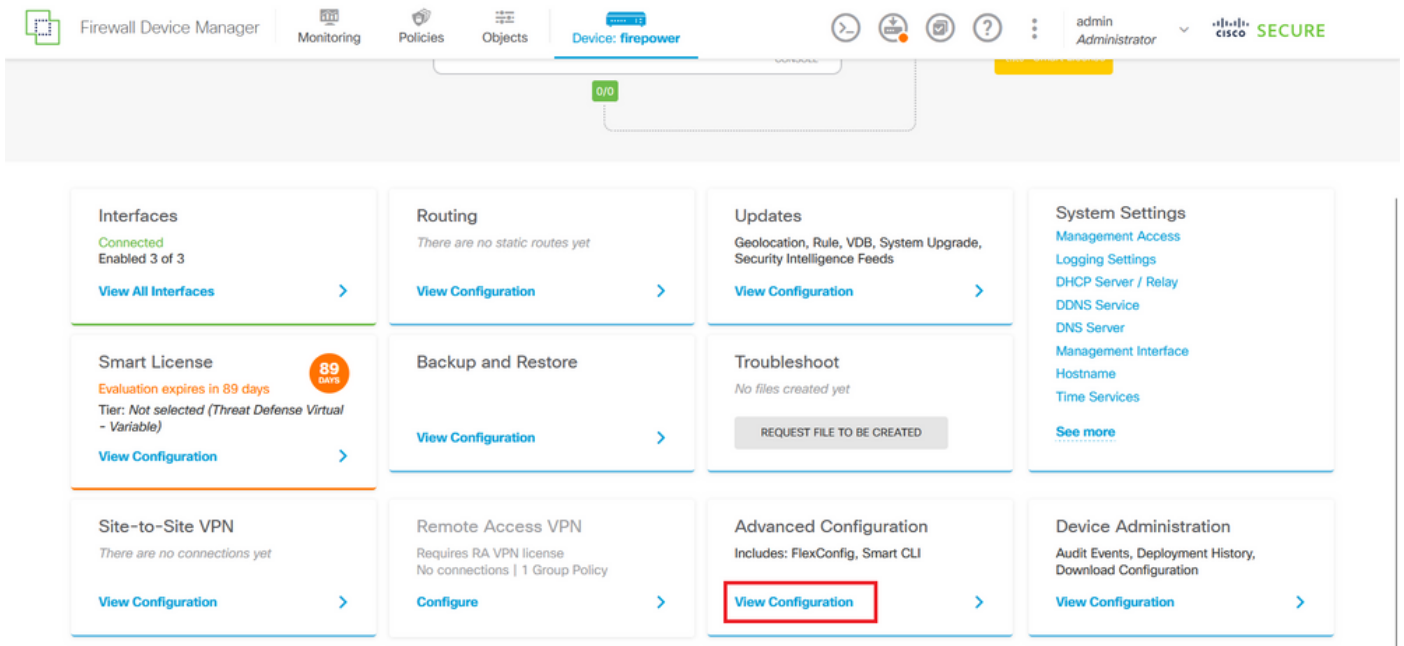


図 29.FDMの詳細設定

ステップ 3.2 : 次に、左側のパネルから Smart CLI > Objects に移動し、CREATE SMART CLI OBJECT をクリックします。

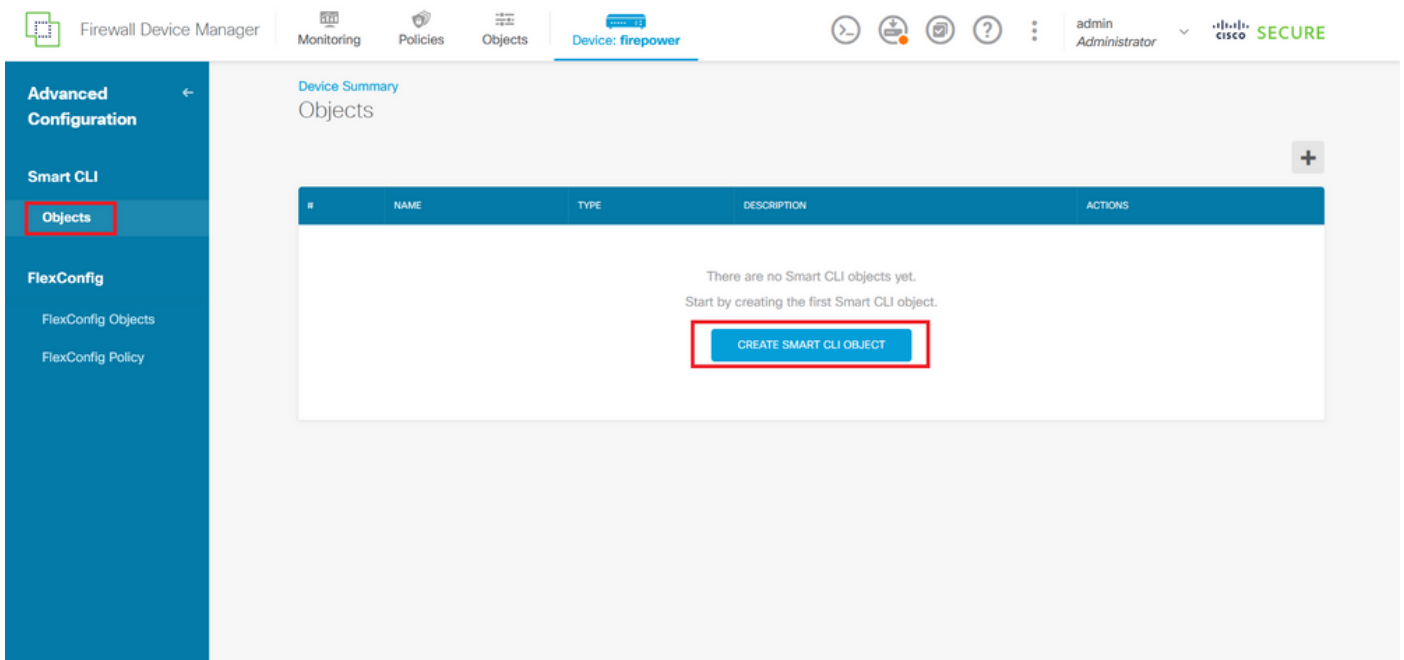


図 30.スマートCLIオブジェクト

ステップ 3.3 : 作成する拡張ACLの名前を追加し、CLIテンプレートのドロップダウンメニューから Extended Access List を選択し、上記のステップ 2.2 で作成したネットワークオブジェクトを使用して必要な ACE を設定し、OK ボタンをクリックして ACL を完成させます。

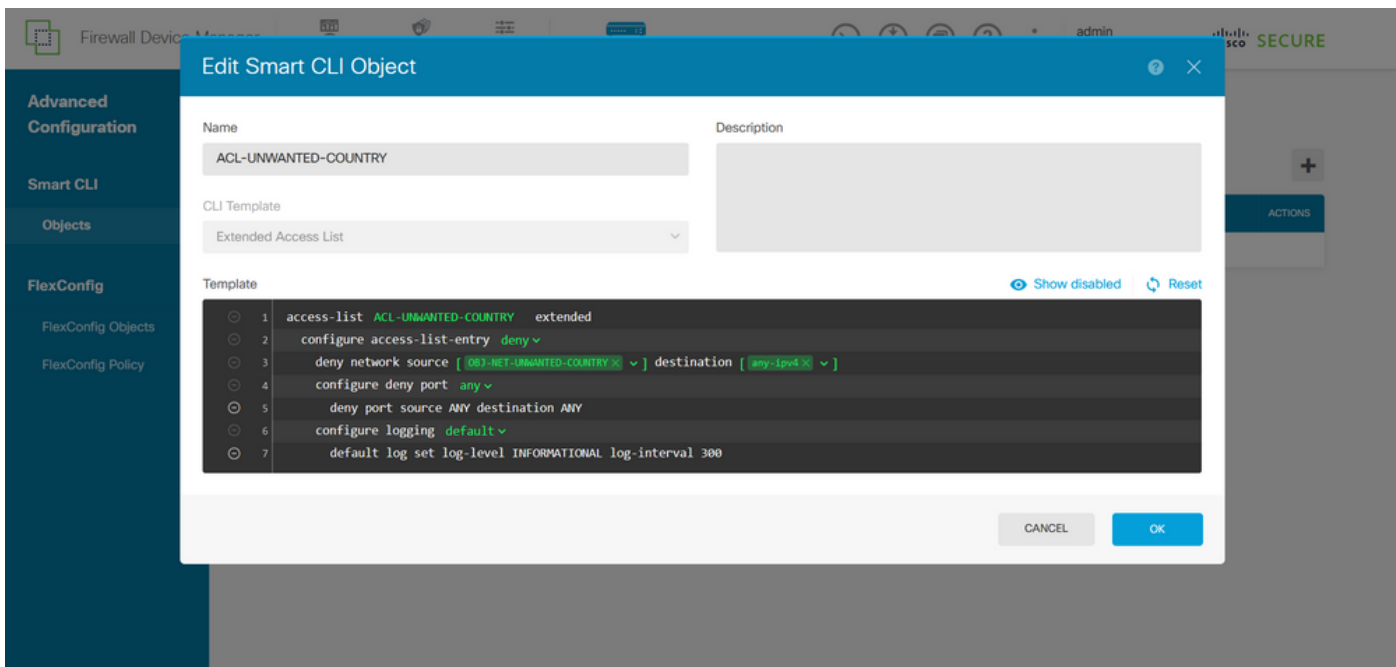



図 31.拡張ACLの作成

 注：ACLにさらにACEを追加する必要がある場合は、現在のACEの左側にマウスを置くと、クリック可能な3つのドットが表示されます。それらをクリックし、Duplicateを選択してACEを追加します。

ステップ 4：次に、FlexConfigオブジェクトを作成する必要があります。これには、左側のパネルに移動し、FlexConfig > FlexConfig Objectsを選択し、CREATE FLEXCONFIG OBJECTをクリックします。

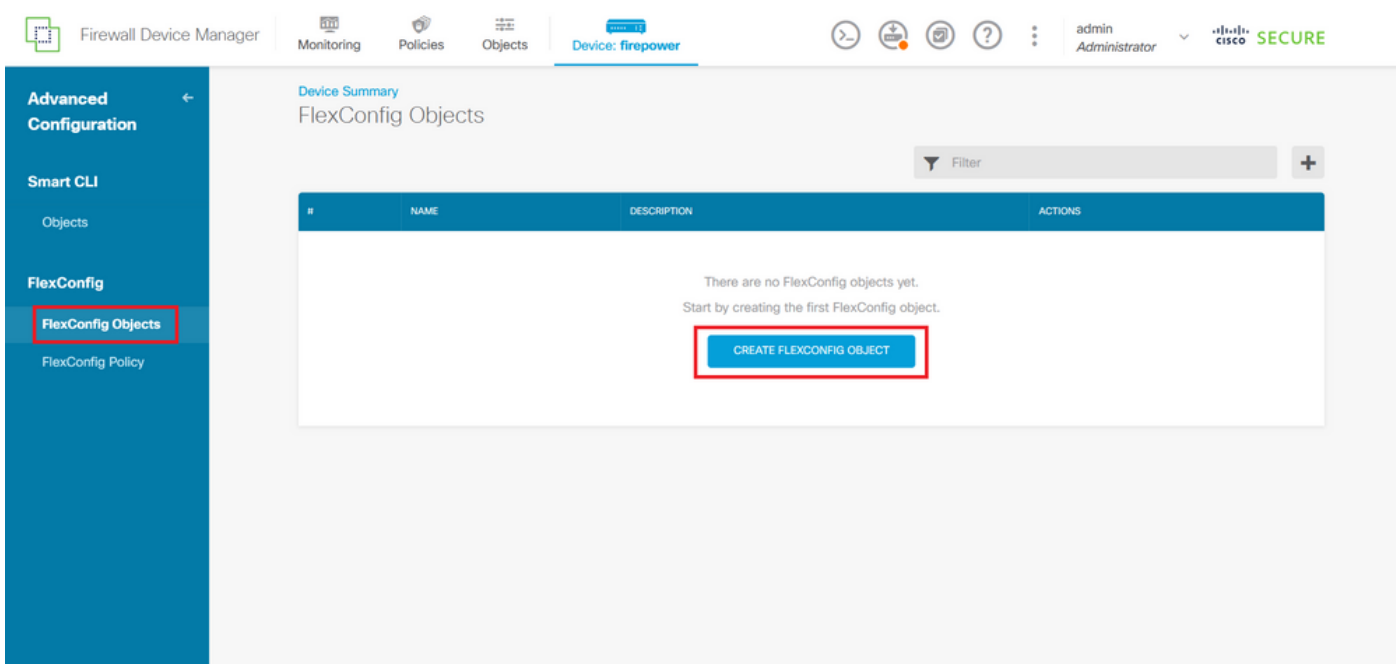


図 32.FlexConfigオブジェクト

ステップ 4.1：コントロールプレーンACLを作成し、外部インターフェイスのインバウンドとして設定するには、FlexConfigオブジェクトの名前を次のように追加します。

コマンドライン構文：

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

これは、次のコマンド例に変換されます。この例では、上記のステップ3.3で作成した拡張ACL「ACL-UNWANTED-COUNTRY」を次のように使用しています。

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

FlexConfigオブジェクトウィンドウでこのように設定する必要があります。その後、OKボタンを選択してFlexConfigオブジェクトを完了します。

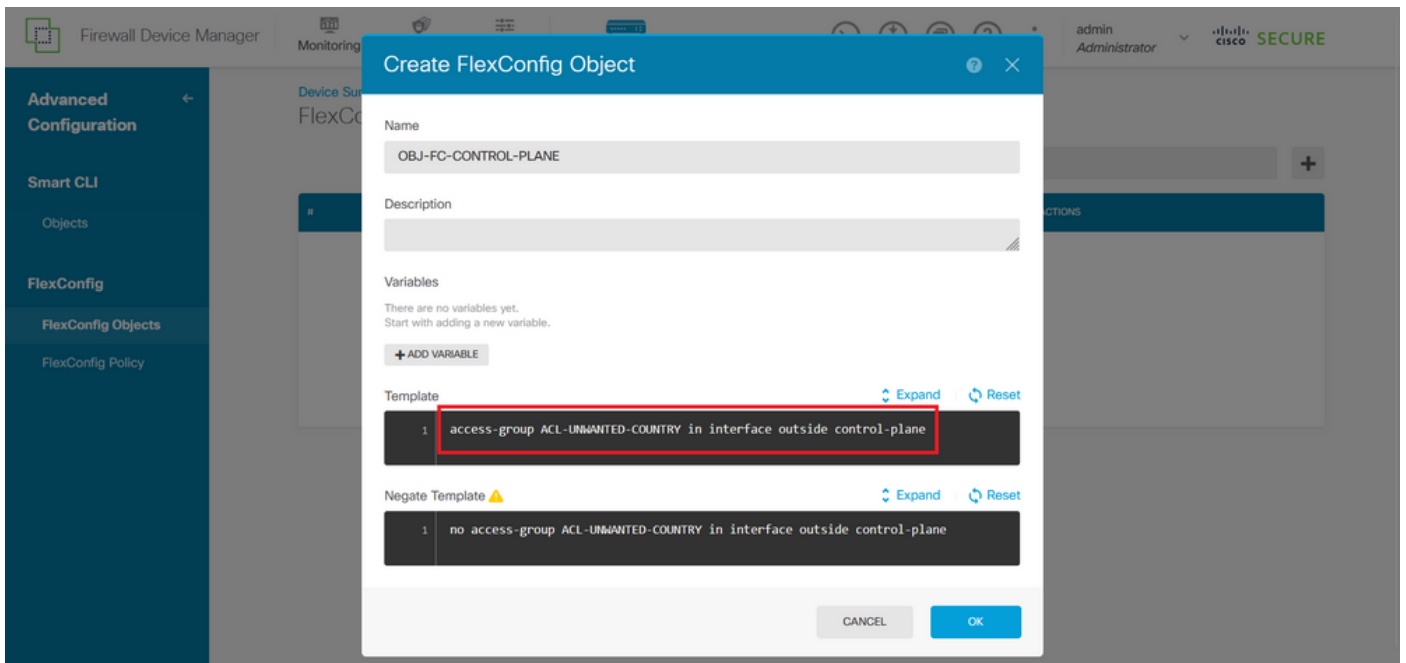


図 33. FlexConfigオブジェクトの作成

ステップ 5：FlexConfigポリシーの作成に進み、Flexconfig > FlexConfig Policyに移動し、「+」ボタンをクリックして、上記のステップ4.1で作成したFlexConfigオブジェクトを選択します。

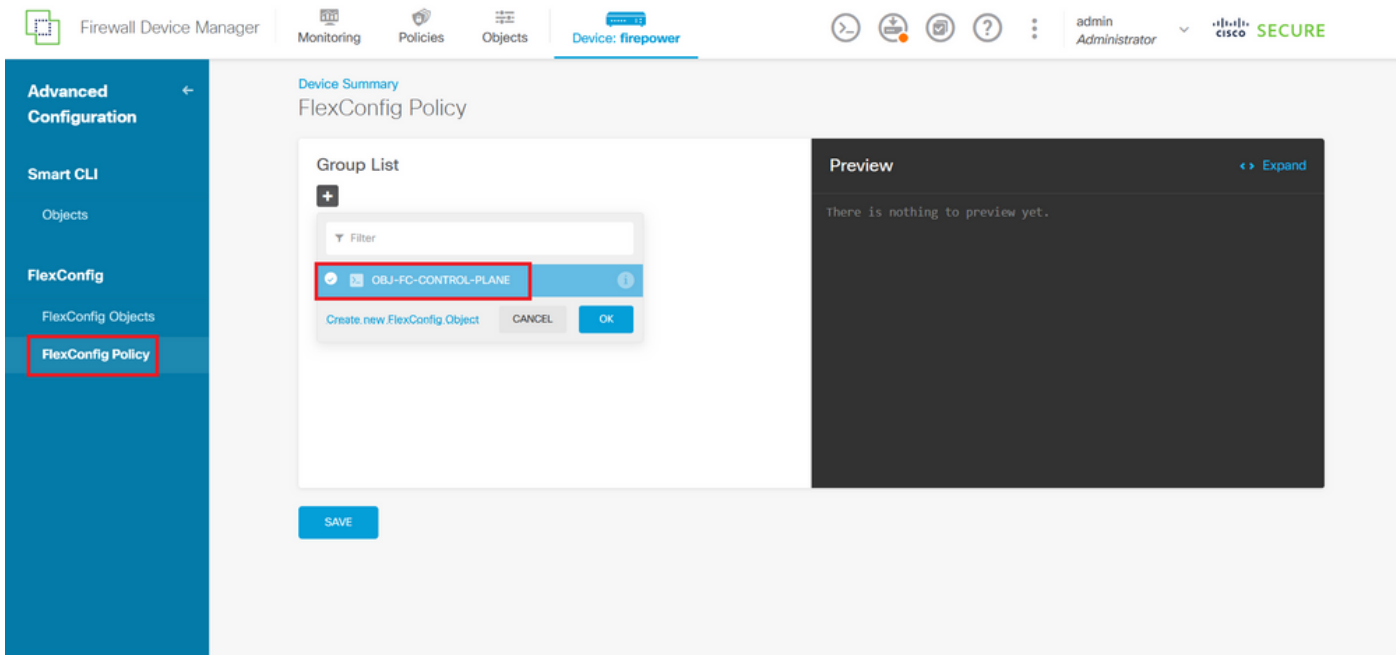


図 34. FlexConfigポリシー

ステップ 5.1 : FlexConfigプレビューに、作成されたコントロールプレーンACLの正しい設定が表示されていることを確認し、Saveボタンをクリックします。

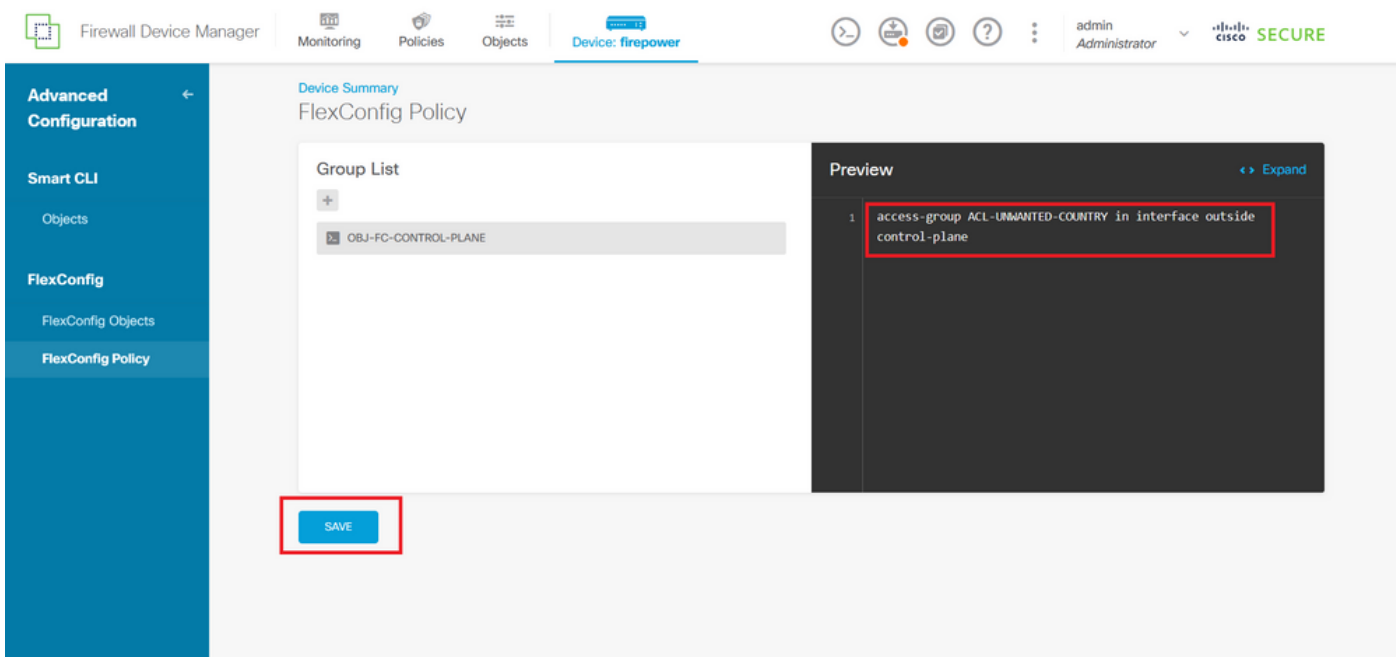


図 35. FlexConfigポリシープレビュー

手順 6 : VPN総当たり攻撃から保護したいFTDに設定変更を展開します。それには、トップメニューのDeploymentボタンをクリックし、展開する設定変更が正しいことを確認して、DEPLOY NOWをクリックします。

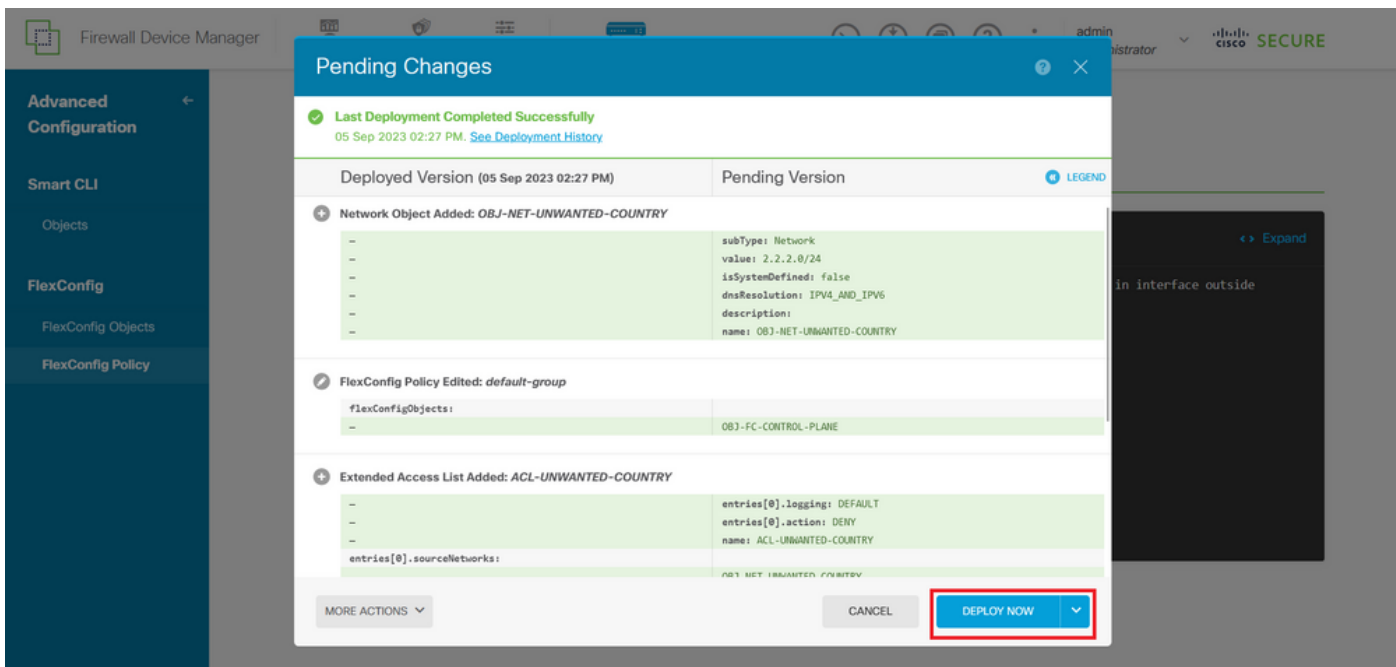


図 36.保留中の展開

ステップ 6.1 : ポリシーの展開が正常に行われたことを検証します。

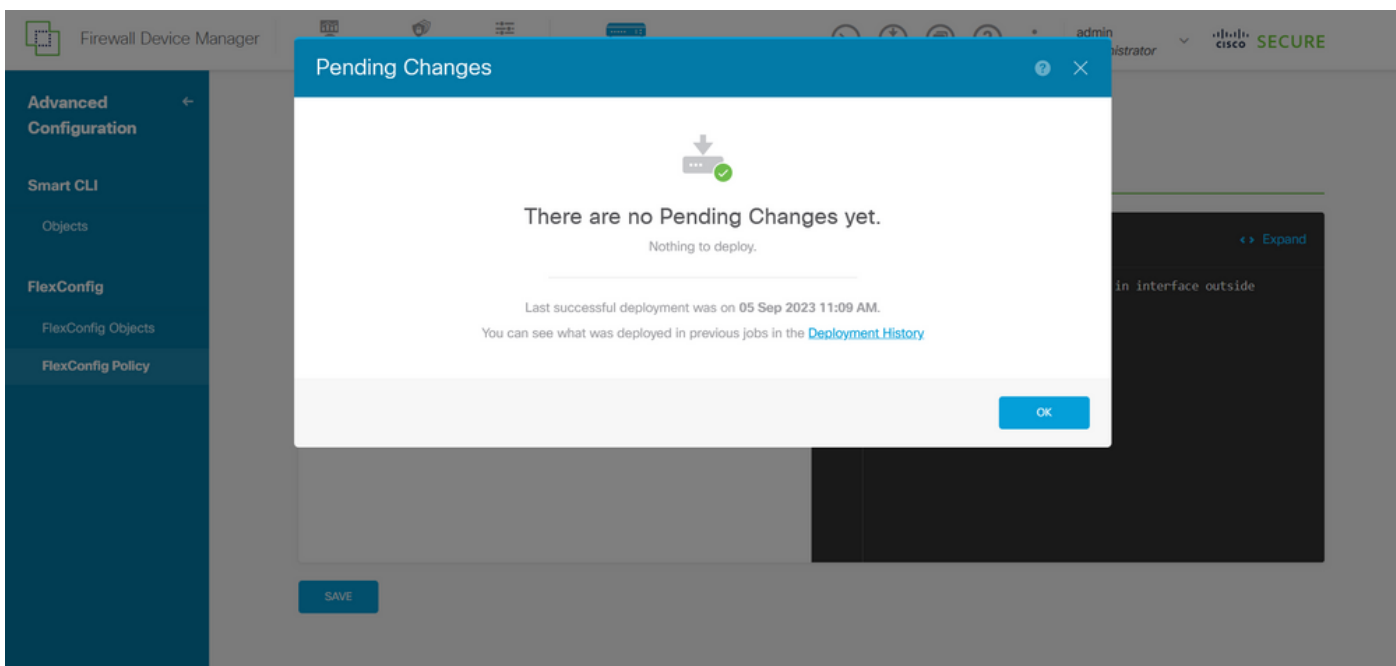


図 37.展開が成功しました

手順 7 : FTD用に新しいコントロールプレーンACLを作成する場合、またはアクティブに使用されている既存のコントロールプレーンACLを編集する場合は、加えられた設定変更がFTDへの確立済みの接続に適用されないことを強調することが重要です。したがって、FTDへのアクティブな接続試行を手動でクリアする必要があります。そのためには、次のようにFTDのCLIに接続し、アクティブな接続をクリアします。

特定のホストIPアドレスのアクティブな接続をクリアするには、次の手順を実行します。


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

サブネットワーク全体のアクティブな接続をクリアするには、次の手順を実行します。

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

特定の範囲のIPアドレスに対するアクティブな接続をクリアするには、次の手順を実行します。

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

 注：clear conn addressコマンドの最後にキーワード「all」を使用して、アクティブなVPN総当たり攻撃によるセキュアなファイアウォールへの接続試行を強制的にクリアすることを強く推奨します。これは主に、VPN総当たり攻撃の性質によって絶え間ない接続試行の爆発が発生している場合に行われます。

CLIを使用したASAのコントロールプレーンACLの設定

外部インターフェイスへの着信VPNブルートフォース攻撃をブロックするようにコントロールプレーンACLを設定するには、ASA CLIで次の手順を実行する必要があります。

ステップ 1：CLIを介してセキュアファイアウォールASAにログインし、次のように「configure terminal」にアクセスします。

```
asa# configure terminal
```

ステップ 2：次のコマンドを使用して、ASAに対してブロックする必要があるトラフィックのホストIPアドレスまたはネットワークアドレスをブロックするように拡張ACLを設定します。

– この例では、「ACL-UNWANTED-COUNTRY」という名前の新しいACLを作成し、設定したACEエントリによって、192.168.1.0/24サブネットからのVPNブルートフォース攻撃をブロックします。

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

ステップ 3： 次のaccess-groupコマンドを使用して、「ACL-UNWANTED-COUNTRY」ACLを外部ASAインターフェイスのコントロールプレーンACLとして設定します。

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

ステップ 4： 新しいコントロールプレーンACLを作成する場合、またはアクティブに使用されている既存のコントロールプレーンACLを編集する場合は、加えられた設定変更がASAへの既存の接続に適用されないことを強調することが重要です。そのため、ASAへのアクティブな接続試行を手動でクリアする必要があります。このため、次のようにアクティブな接続をクリアします。

特定のホストIPアドレスのアクティブな接続をクリアするには、次の手順を実行します。


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

サブネットネットワーク全体のアクティブな接続をクリアするには、次の手順を実行します。

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

特定の範囲のIPアドレスに対するアクティブな接続をクリアするには、次の手順を実行します。

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

 注： clear conn addressコマンドの最後にキーワード「all」を使用して、アクティブなVPN総当たり攻撃によるセキュアなファイアウォールへの接続試行を強制的にクリアすることを強く推奨します。これは主に、VPN総当たり攻撃の性質によって絶え間ない接続試行の爆発が発生している場合に行われます。

「shun」コマンドを使用してセキュアファイアウォールの攻撃をブロックする代替設定

セキュアなファイアウォールに対する攻撃を即時にブロックするオプションがある場合は、「shun」コマンドを使用できます。huncommandコマンドを使用すると、攻撃ホストからの接続をブロックできます。

- IPアドレスを回避すると、送信元IPアドレスからの以降のすべての接続はドロップされ、ブロッ

キング機能が手動で削除されるまでログに記録されます。

- huncommandのblocking関数は、指定されたホストアドレスとの接続が現在アクティブであるかどうかにかかわらず適用されます。

-宛先アドレス、送信元ポートと宛先ポート、およびプロトコルを指定した場合、一致する接続をドロップし、送信元IPからの以降のすべての接続を回避します

アドレス。これらの特定の接続パラメータに一致するものだけでなく、将来のすべての接続が排除されます。

-送信元IPアドレスごとにonescuncommandのみを指定できます。

- hushuncommandは攻撃を動的にブロックするために使用されるため、脅威防御デバイスの設定には表示されません。

- インターフェイス設定が削除されると、そのインターフェイスに接続されているすべてのshunも削除されます。

- Shunコマンド構文：

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

- 回避を無効にするには、このコマンドのno形式を使用します。

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

ホストIPアドレスを回避するには、セキュアファイアウォールで次の手順を実行します。この例では、「shun」コマンドを使用して、送信元IPアドレス192.168.1.10からのVPNブルートフォースアタックをブロックしています。

FTDの設定例

ステップ 1：CLIを使用してFTDにログインし、次のようにshunコマンドを適用します。

```
<#root>
```

```
>
```

```
shun 192.168.1.10
```

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

```
Shun 192.168.1.10 successful
```

ステップ 2： 次のshowコマンドを使用して、FTD内の排除IPアドレスを確認し、IPアドレスごとの排除ヒットカウントをモニタできます。

```
<#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の設定例

ステップ 1： CLIを使用してASAにログインし、次のようにshunコマンドを適用します。

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

Shun 192.168.1.10 successful
```

ステップ 2： 次のshowコマンドを使用して、ASAの排除IPアドレスを確認し、IPアドレスごとの排除ヒットカウントをモニタできます。

```
<#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：secure firewall shunコマンドの詳細については、『[Cisco Secure Firewall Threat Defense Command Reference](#)』を参照してください

確認

コントロールプレーンACL設定がセキュアファイアウォールに対して設定されていることを確認するには、次の手順を実行します。

ステップ 1：CLIを介してセキュアファイアウォールにログインし、次のコマンドを実行して、コントロールプレーンACL設定が適用されていることを確認します。

FMCによって管理されるFTDの出力例を次に示します。

```
<#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によって管理されるFTDの出力例を次に示します：

```
<#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の出力例：

<#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
```

ステップ 2：コントロールプレーンACLが必要なトラフィックをブロックしていることを確認するには、packet-tracerコマンドを使用して、セキュアファイアウォールの外部インターフェイスへの着信TCP 443接続をシミュレートします。次に、show access-list <acl-name>コマンドを使用します。VPNのブルートフォース接続がコントロールプレーンACLによってブロックされるたびに、ACLのヒットカウントが増加します。

– この例では、packet-tracerコマンドにより、ホスト192.168.1.10から送信され、セキュアファイアウォールの外部IPアドレスに宛てられた着信TCP 443接続がシミュレートされます。「packet-tracer」の出力はトラフィックがドロップされていることを示し、「show access-list」の出力はコントロールプレーンACLのヒットカウントの増分を示します。

FTDの出力例

<#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の出力例

<#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 : Cisco Secure Client VPNなどのRAVPNソリューションがセキュアファイアウォールに実装されている場合は、セキュアファイアウォールへの実際の接続を実行して、コントロールプレーンACLが期待どおりに動作して必要なトラフィックをブロックしていることを確認できます。

関連バグ

- ENH | 位置情報ベースのAnyConnectクライアント接続 : Cisco Bug ID [CSCvs65322](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。