# Configurer le contrôle d'accès au plan de contrôle pour Secure FTD et ASA

## Table des matières


- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Trafic prêt à l'emploi de pare-feu sécurisé
  - Trafic prêt à l'emploi du pare-feu sécurisé
  - Considérations importantes concernant les ACL du plan de contrôle
- Configurer
  - Configurations
    - Configurer une liste de contrôle d'accès du plan de contrôle pour FTD géré par FMC
    - [VIDEO] Configurer une liste de contrôle d'accès du plan de contrôle pour FTD géré par FMC
    - Configurer une liste de contrôle d'accès du plan de contrôle pour FTD géré par FDM
    - Configurer une ACL du plan de contrôle pour ASA à l'aide de CLI
    - Configuration alternative pour bloquer les attaques pour le pare-feu sécurisé exécutant Shun
    - Exemple de configuration pour FTD
    - Exemple de configuration pour ASA
- Vérifier
  - Exemple de résultats pour ASA
- Bogues associés
- Informations connexes


## Introduction

Ce document décrit le processus de configuration des règles d'accès au plan de contrôle pour Secure Firewall Threat Defense et Adaptive Security Appliance (ASA).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protection pare-feu contre les menaces (FTD)
- Gestionnaire de périphériques de pare-feu sécurisé (FDM)
- Centre de gestion du pare-feu sécurisé (FMC)
- Pare-feu sécurisé ASA
- Liste de contrôle d'accès (ACL)
- FlexConfig

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Protection pare-feu sécurisée contre les menaces, version 7.2.5
- Secure Firewall Manager Center version 7.2.5
- Gestionnaire de périphériques Secure Firewall Version 7.2.5
- Pare-feu sécurisé ASA version 9.18.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

## Informations générales

Le trafic traverse généralement un pare-feu et est acheminé entre des interfaces de données ; dans certaines circonstances, il est préférable de refuser le trafic destiné au pare-feu sécurisé. Le pare-feu sécurisé Cisco peut utiliser une liste de contrôle d'accès (ACL) du plan de contrôle pour restreindre le trafic prêt à l'emploi. Un exemple de cas où une liste de contrôle d'accès de plan de contrôle peut être utile pour contrôler quels homologues peuvent établir un tunnel VPN (site à site ou accès à distance VPN) vers le pare-feu sécurisé.

Trafic prêt à l'emploi de pare-feu sécurisé

Le trafic traverse normalement les pare-feu d'une interface (entrante) à une autre (sortante), c'est ce qu'on appelle le trafic « tout-en-un » et qui est géré à la fois par les règles de préfiltrage et les règles de contrôle d'accès (ACP).

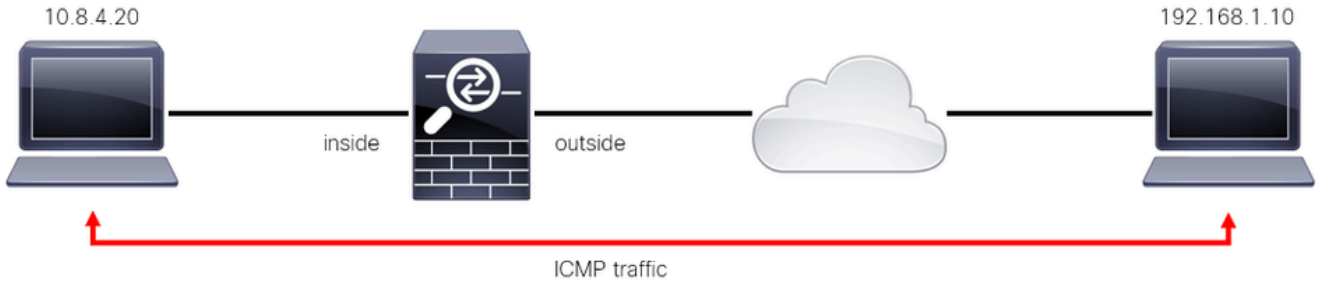



Image 1. Exemple de trafic prêt à l'emploi

Trafic prêt à l'emploi du pare-feu sécurisé

Il existe d'autres cas où le trafic est directement destiné à une interface FTD (VPN de site à site ou d'accès à distance), ce trafic est appelé trafic prêt à l'emploi et est géré par le plan de contrôle de cette interface spécifique.

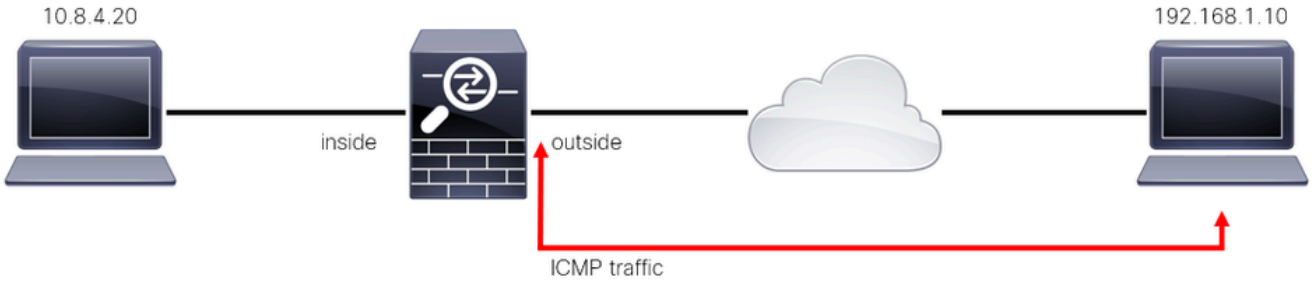



Image 2. Exemple de trafic prêt à l'emploi

Considérations importantes concernant les ACL du plan de contrôle

- À partir de la version 7.0 de FMC/FTD, une liste de contrôle d'accès de plan de contrôle doit être configurée à l'aide de FlexConfig, en utilisant la même syntaxe de commande que celle utilisée sur l'ASA.
- Le plan de contrôle de mot clé est ajouté à la configuration du groupe d'accès, qui applique le trafic à l'interface du pare-feu sécurisé. Sans le mot de plan de contrôle ajouté à la commande, la liste de contrôle d'accès restreindrait le trafic à travers le pare-feu sécurisé.
- Une liste de contrôle d'accès du plan de contrôle ne restreint pas les connexions entrantes SSH, ICMP ou TELNET à une interface de pare-feu sécurisée. Elles sont traitées (autorisées/refusées) conformément aux stratégies des paramètres de la plate-forme et ont une priorité plus élevée.
- Une liste de contrôle d'accès du plan de contrôle restreint le trafic au pare-feu sécurisé lui-

même, tandis que la politique de contrôle d'accès pour le FTD ou les listes de contrôle d'accès normales pour l'ASA contrôle le trafic à travers le pare-feu sécurisé.
- Contrairement à une liste de contrôle d’accès normale, il n’y a pas de « deny » implicite à la fin de la liste.
- La fonctionnalité de recherche de groupe d'objets (OGS) ne fonctionne pas sur les ACL du plan de contrôle, voir l'ID de bogue Cisco CSCwi5818.
- Au moment de la création de ce document, la fonction de géolocalisation FTD ne peut pas être utilisée pour restreindre l'accès au FTD.

# Configurer

Dans l'exemple suivant, un ensemble d'adresses IP d'un pays donné tente de forcer via un VPN le réseau en essayant de se connecter au RAVPN FTD. La meilleure option pour protéger le FTD contre ces attaques de force brute VPN est de configurer une ACL de plan de contrôle pour bloquer ces connexions à l'interface FTD externe.

## Configurations

Configurer une liste de contrôle d'accès du plan de contrôle pour FTD géré par FMC

Voici la procédure que vous devez suivre dans un FMC pour configurer une ACL de plan de contrôle pour bloquer les attaques en force entrantes de VPN vers une interface FTD externe :

Étape 1. Ouvrez l’interface utilisateur graphique FMC via HTTPS et connectez-vous avec vos informations d’identification :

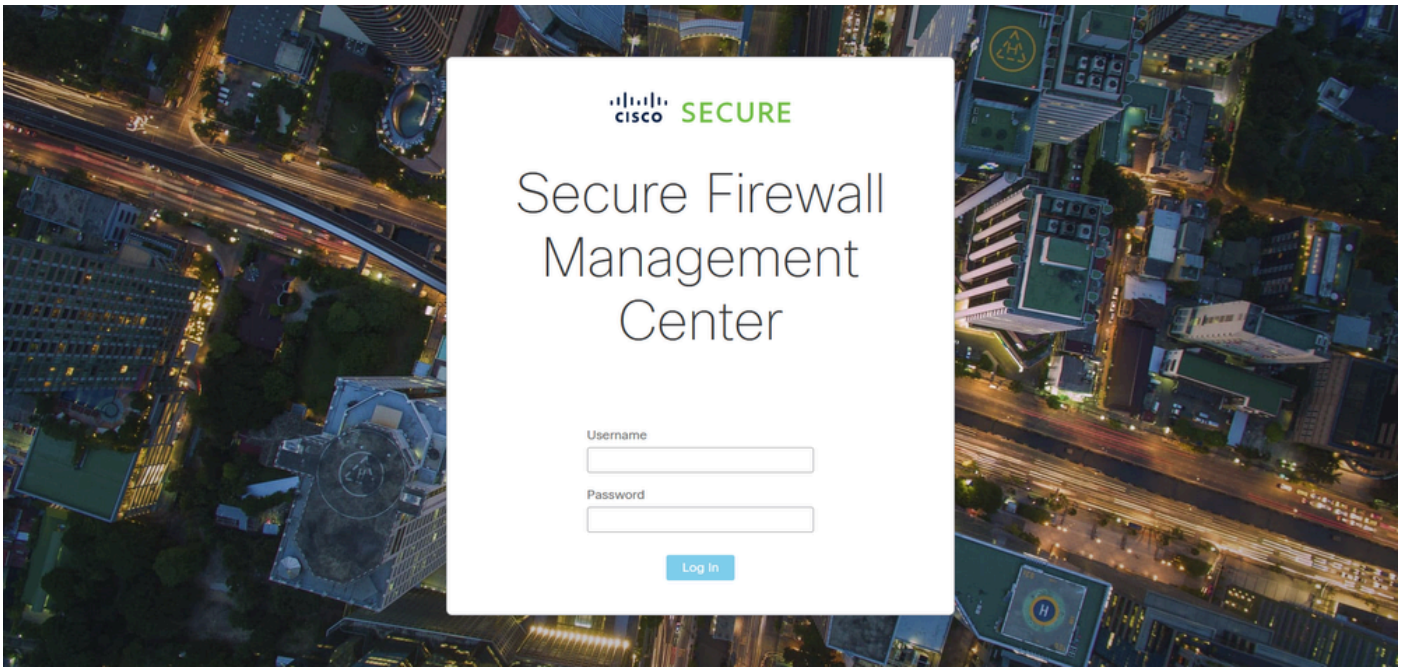



Image 3. Page de connexion FMC

Étape 2. Vous devez créer une liste de contrôle d'accès étendue. Pour cela, accédez à Objets > Gestion des objets :

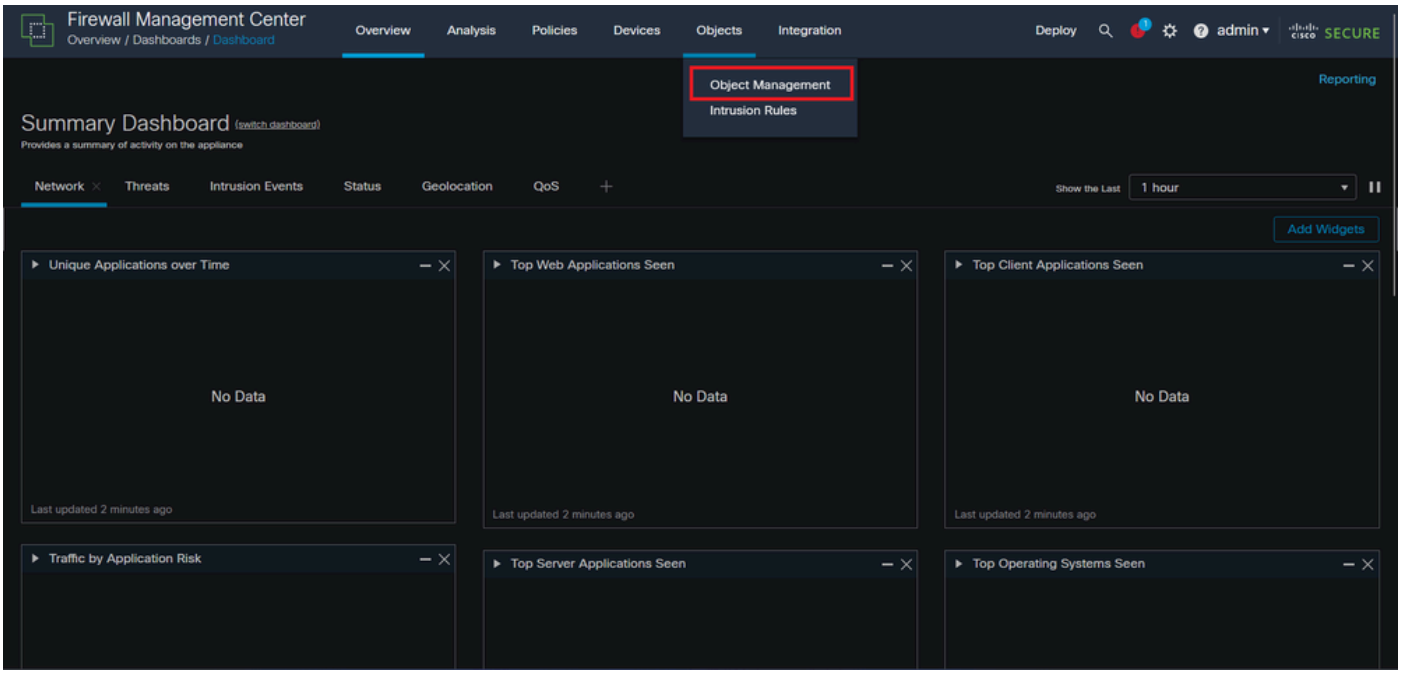



Image 4. Gestion des objets

Étape 2.1. Dans le volet de gauche, accédez à Access List > Extended pour créer une liste de contrôle d'accès étendue :

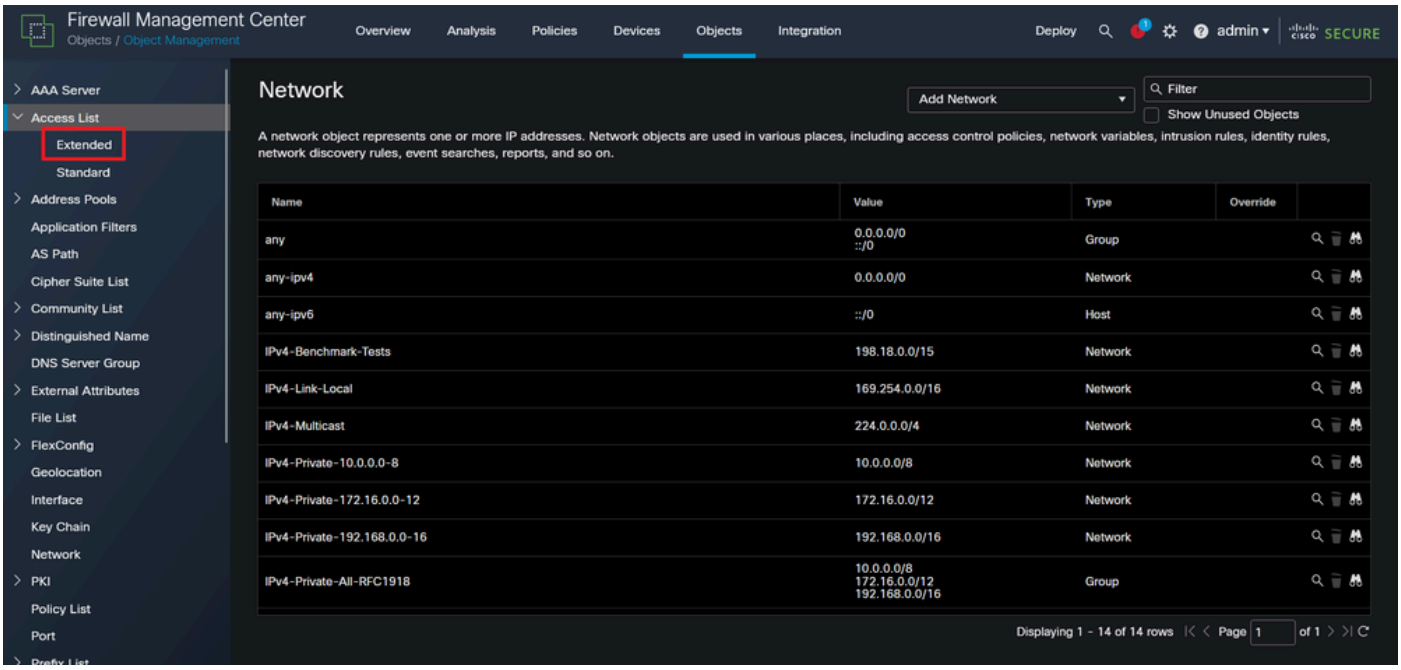



Image 5. Menu ACL étendue

Étape 2.2. Sélectionnez Add Extended Access List :

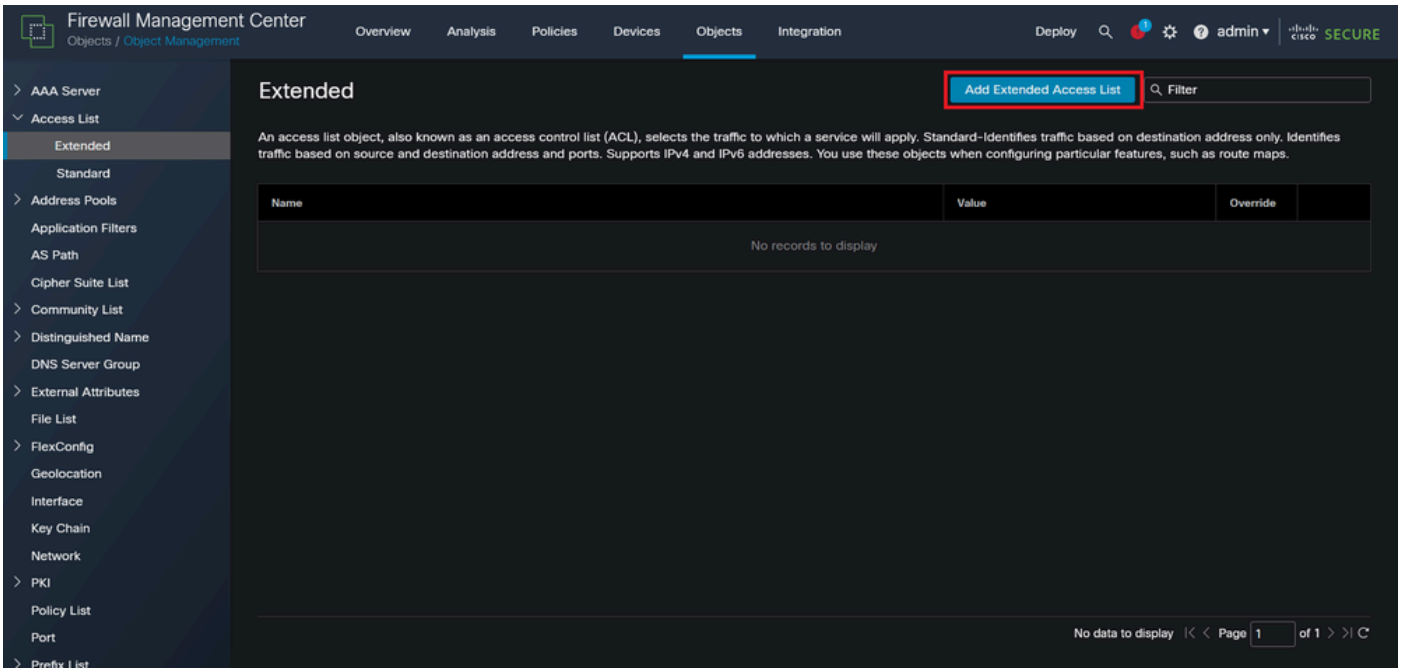



Image 6. Ajouter une liste de contrôle d'accès étendue

Étape 2.3. Tapez un nom pour la liste de contrôle d'accès étendue, puis cliquez sur le bouton Ajouter pour créer une entrée de contrôle d'accès :

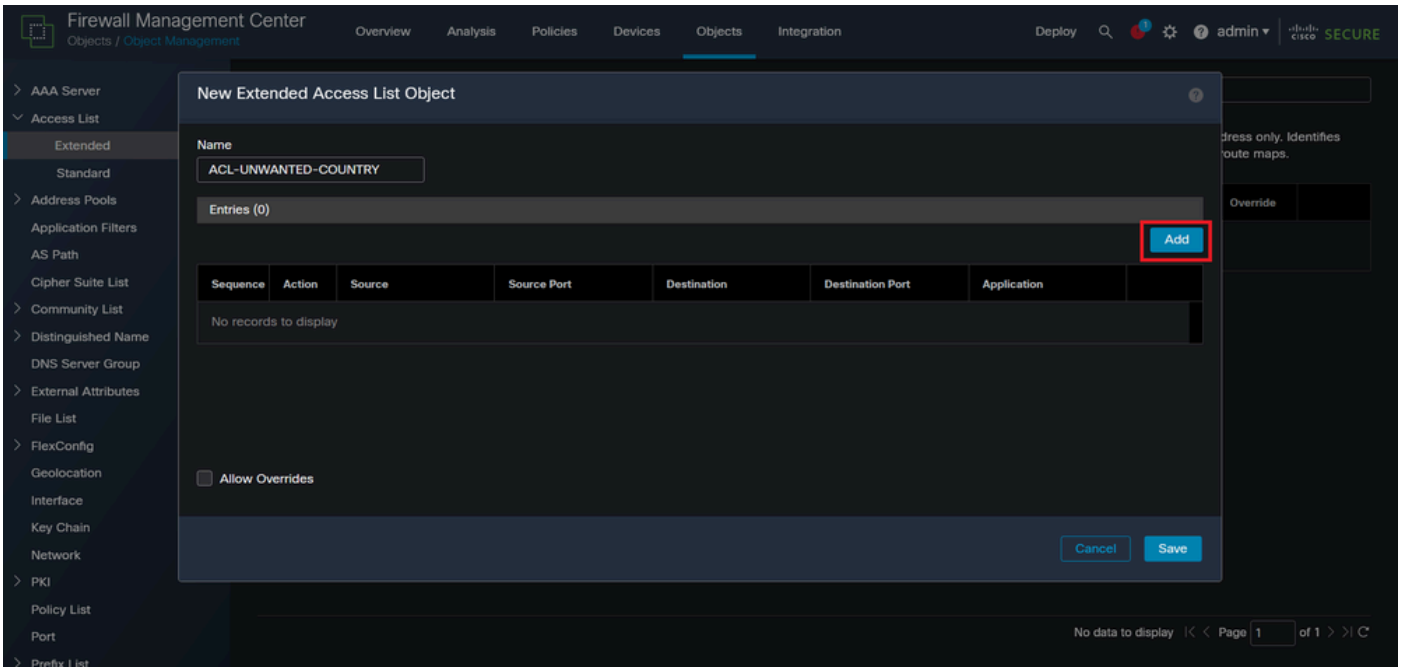



Image 7. Entrées ACL étendues

Étape 2.4. Modifiez l'action ACE en Block, et ajoutez le réseau source pour qu'il corresponde au trafic qui doit être refusé au FTD, conservez le réseau de destination comme Any, et cliquez sur le bouton Add pour terminer l'entrée ACE.

Dans cet exemple, l'entrée ACE configurée bloque les attaques de force brute VPN provenant du sous-réseau 192.168.1.0/24 :

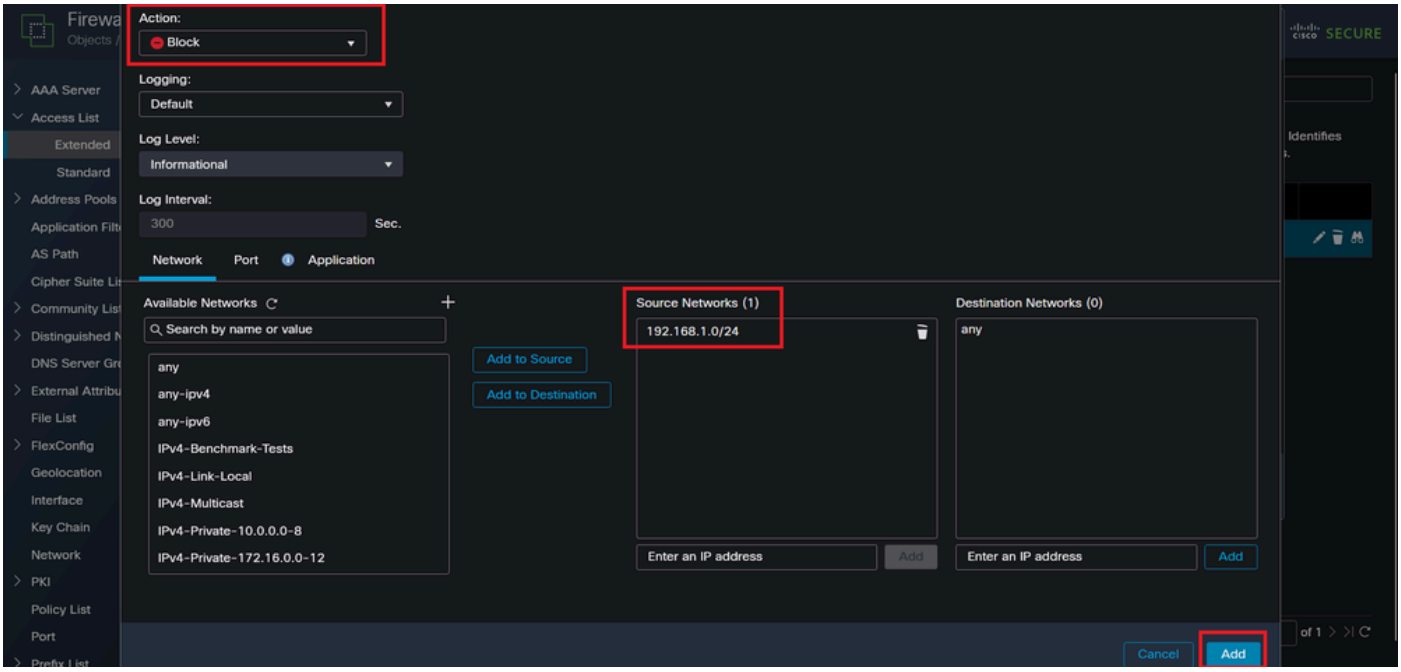



Image 8. Réseaux refusés

Étape 2.5. Si vous devez ajouter d’autres entrées ACE, cliquez de nouveau sur le bouton Add et

répétez l'étape 2.4. Ensuite, cliquez sur le bouton Save pour terminer la configuration de la liste de contrôle d'accès :

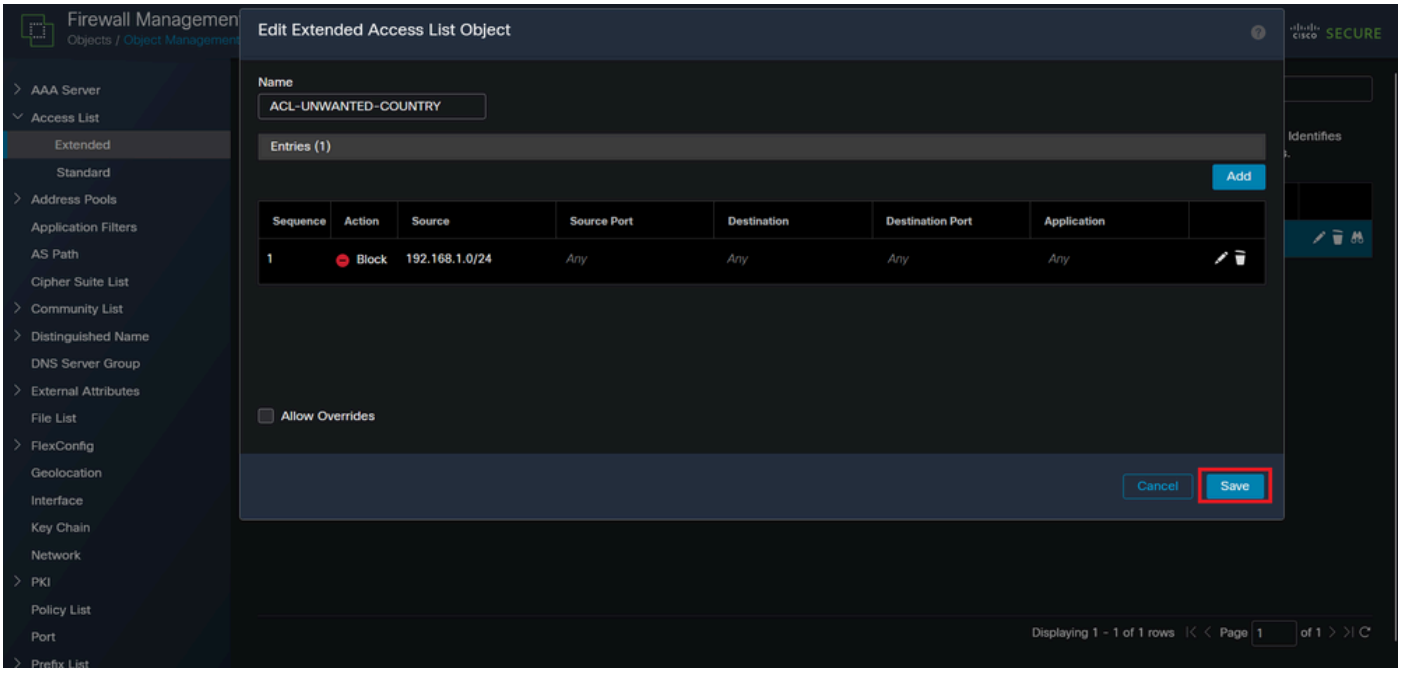



Image 9. Entrées ACL étendues terminées

Étape 3. Vous devez ensuite configurer un objet Flex-Config pour appliquer la liste de contrôle d'accès du plan de contrôle à l'interface FTD externe. Accédez au panneau de gauche et sélectionnez l'option FlexConfig > FlexConfig Object.

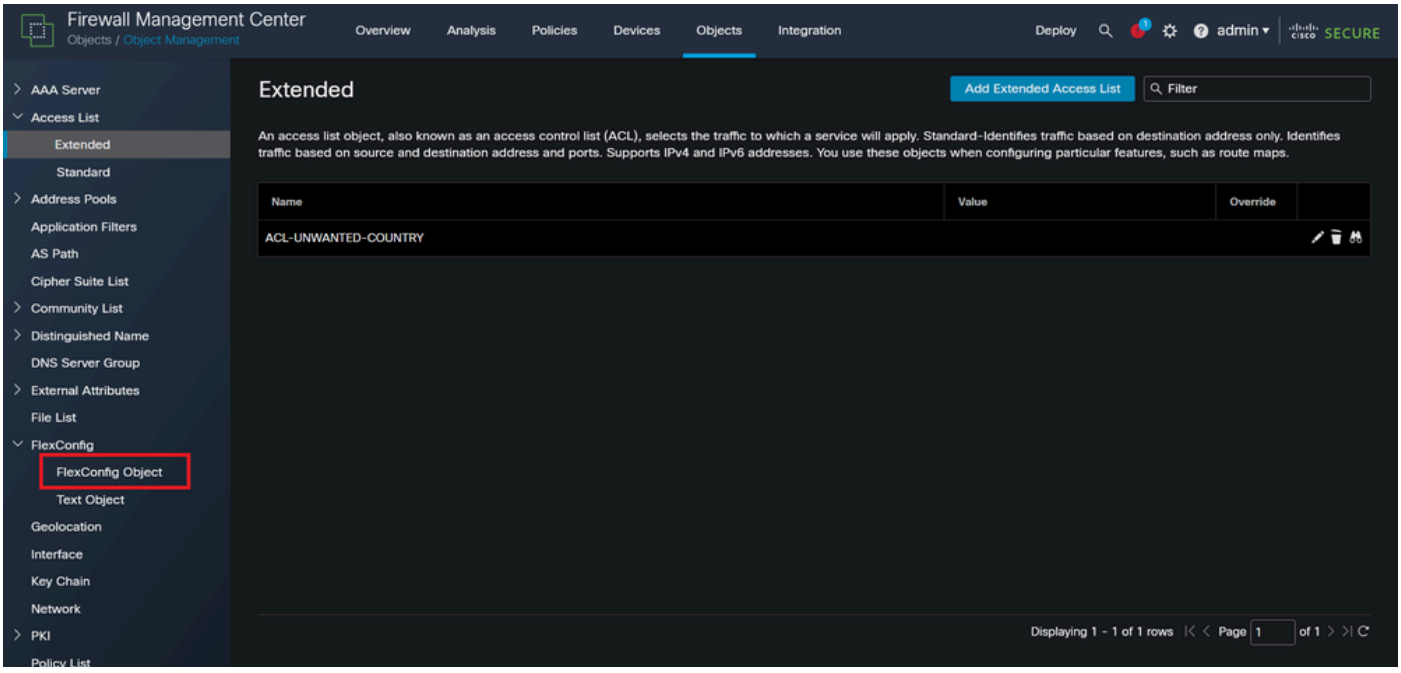



Image 10. Menu Objet FlexConfig

Étape 3.1. Cliquez sur Add FlexConfig Object :

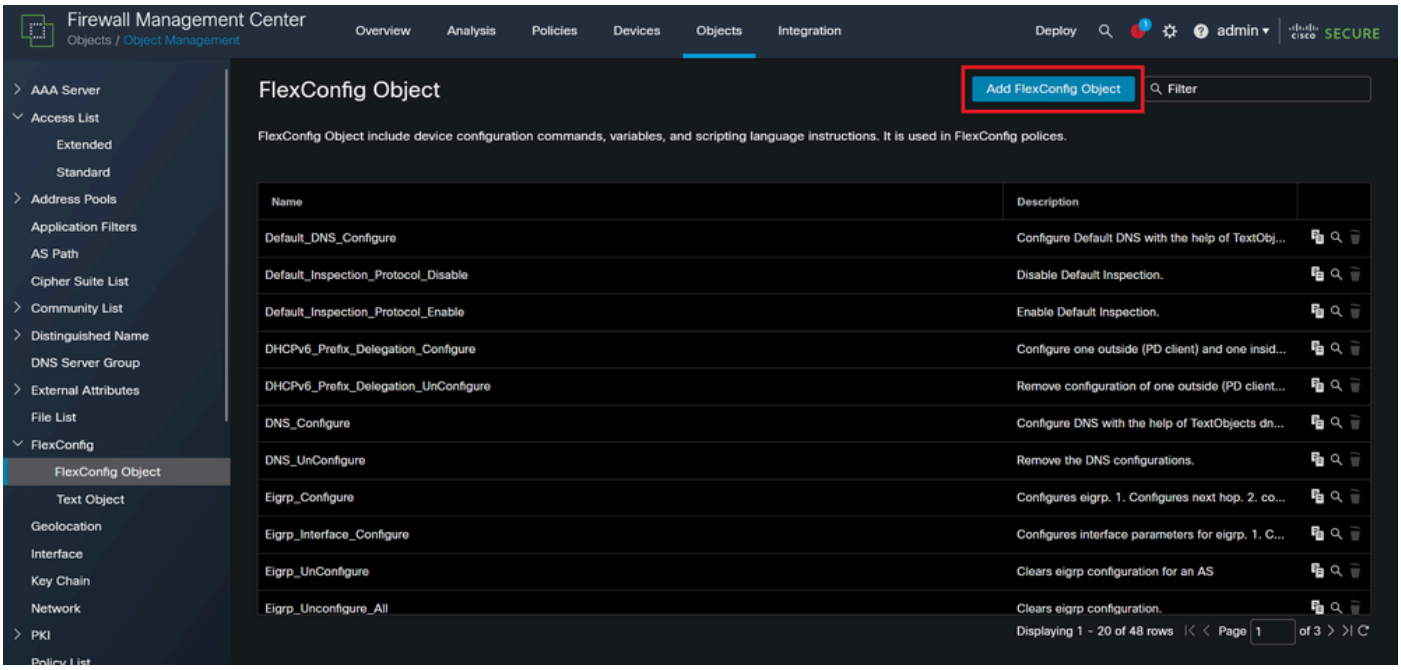



Image 11. Ajouter un objet Flexconfig

Étape 3.2. Ajoutez un nom pour l'objet FlexConfig et insérez un objet de stratégie de liste de contrôle d'accès. Sélectionnez Insert > Insert Policy Object > Extended ACL Object :

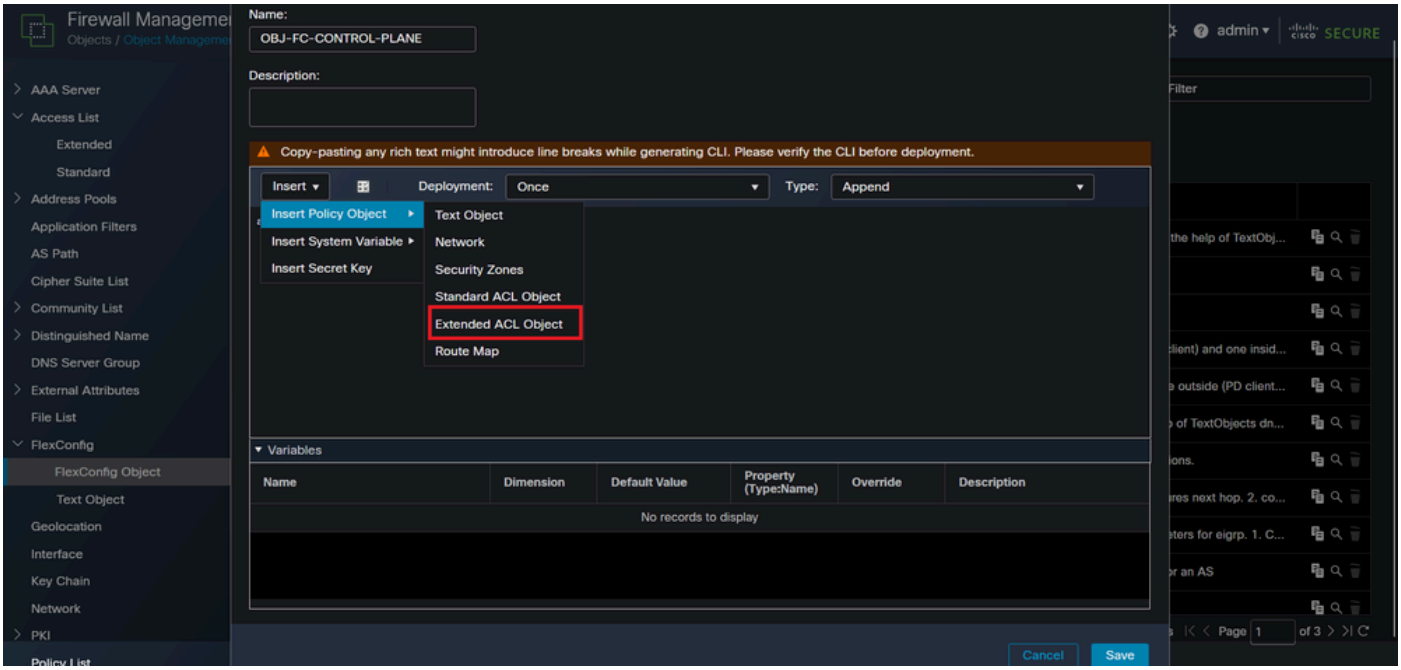



Image 12. Variable objet FlexConfig

Étape 3.3. Ajoutez un nom pour la variable d'objet ACL et sélectionnez la liste de contrôle d'accès étendue créée à l'étape 2.3, cliquez sur le bouton Enregistrer :

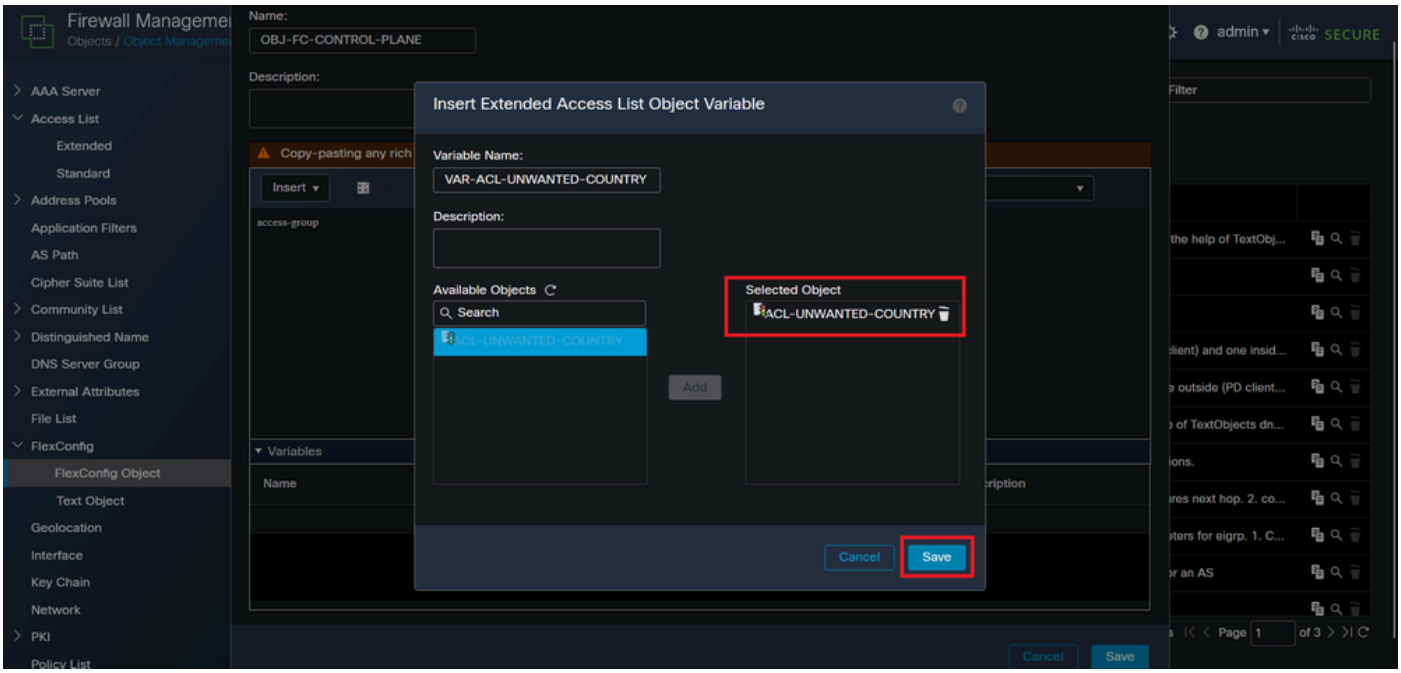



Image 13. Attribution de la variable objet FlexConfig

Étape 3.4. Configurez la liste de contrôle d'accès du plan de contrôle comme entrante pour l'interface externe.

Syntaxe de ligne de commande :

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

Cela se traduit par l'exemple de commande suivant, qui utilise la variable ACL créée à l'étape 2.3 VAR-ACL-UNWANTED-COUNTRY :

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

C'est comme cela que vous devez configurer la fenêtre d'objet FlexConfig, après cela, sélectionnez le bouton Save pour compléter l'objet FlexConfig :

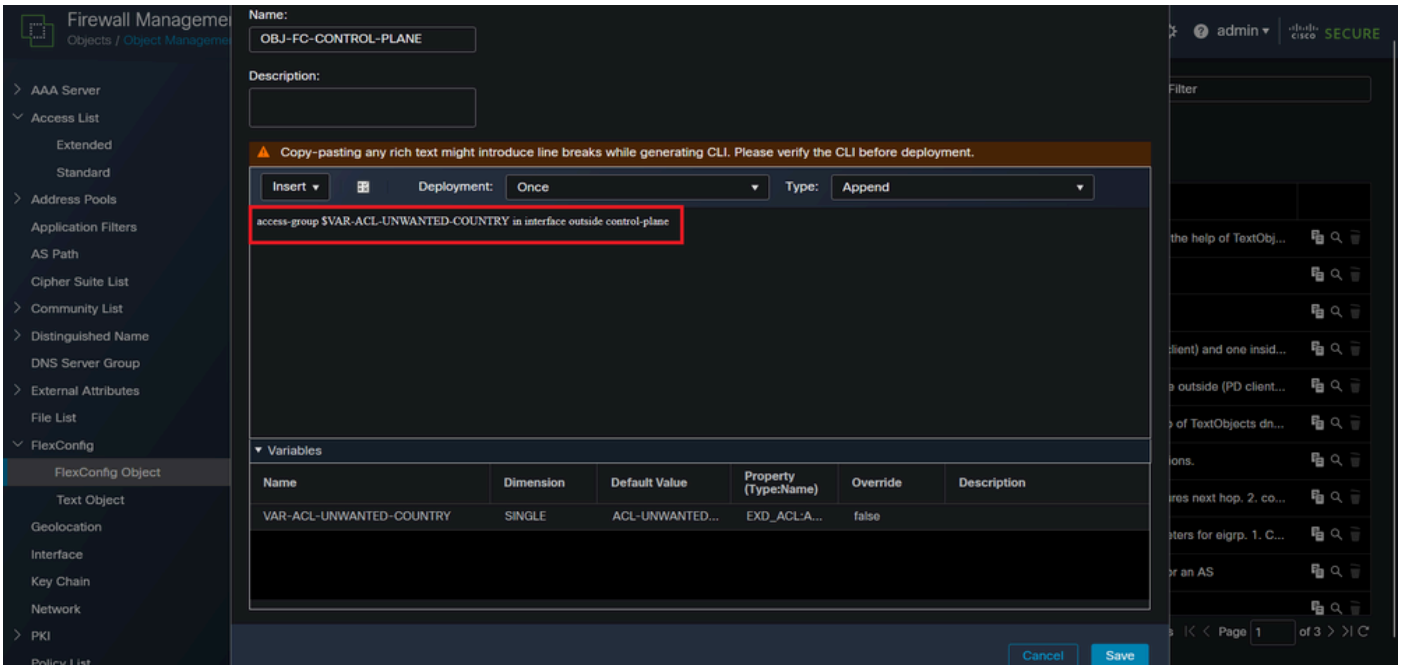



Image 14. Ligne de commande complète de l'objet Flexconfig

Remarque : il est fortement recommandé de configurer la liste de contrôle d'accès du plan de contrôle uniquement pour les interfaces recevant des sessions VPN d'accès à distance entrantes dans le pare-feu sécurisé, comme l'interface externe.

Étape 4. Vous devez appliquer la configuration de l'objet FlexConfig au FTD, accédez à Périphériques > FlexConfig :

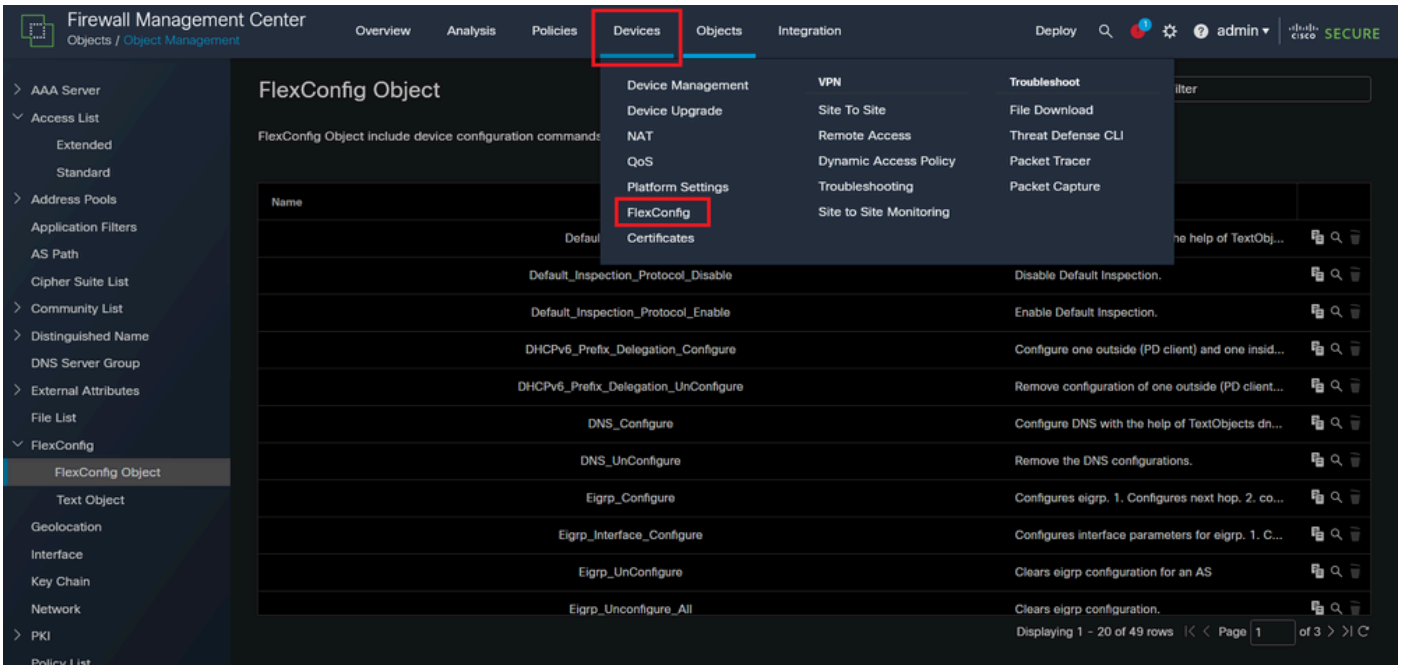



Image 15. Menu FlexConfig Policy

Étape 4.1. Cliquez sur New Policy (Nouvelle stratégie), si aucun FlexConfig n'a déjà été créé pour

votre FTD, modifiez la stratégie FlexConfig existante :

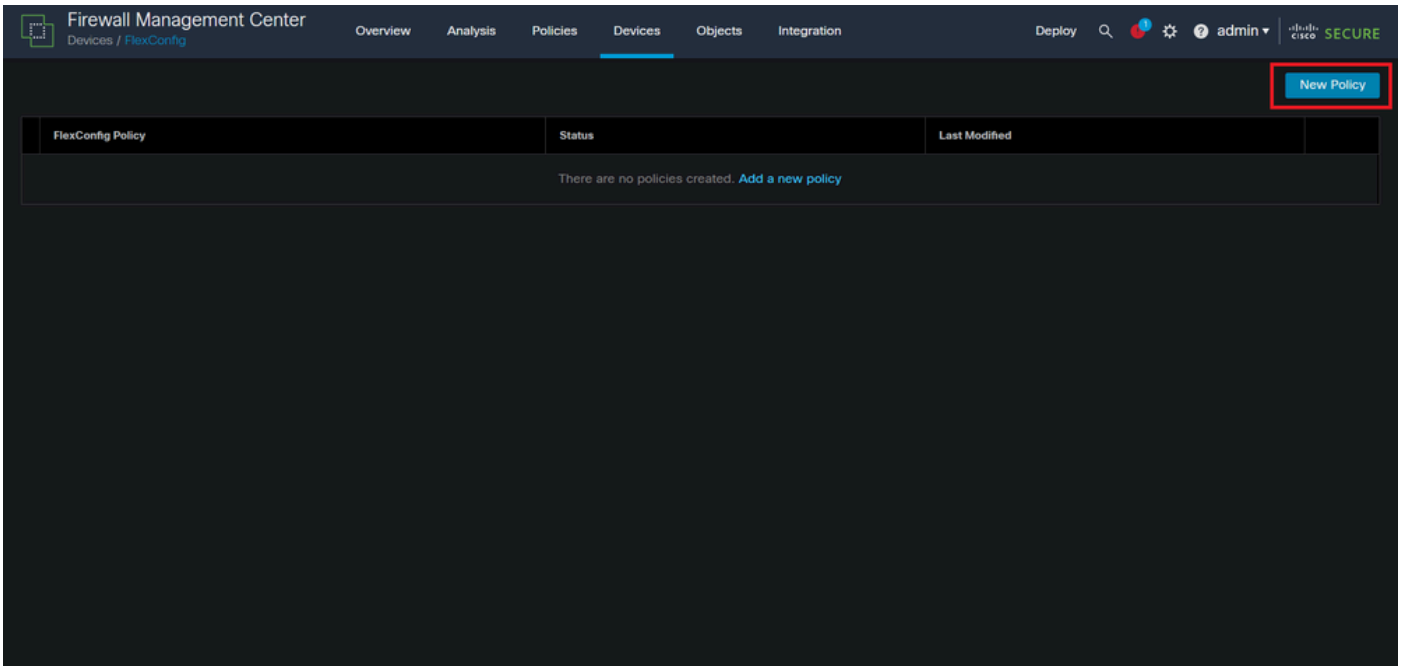



Image 16. Création de la stratégie FlexConfig

Étape 4.2. Ajoutez un nom pour la nouvelle stratégie FlexConfig et sélectionnez le FTD que vous souhaitez appliquer la liste de contrôle d'accès du plan de contrôle créée :

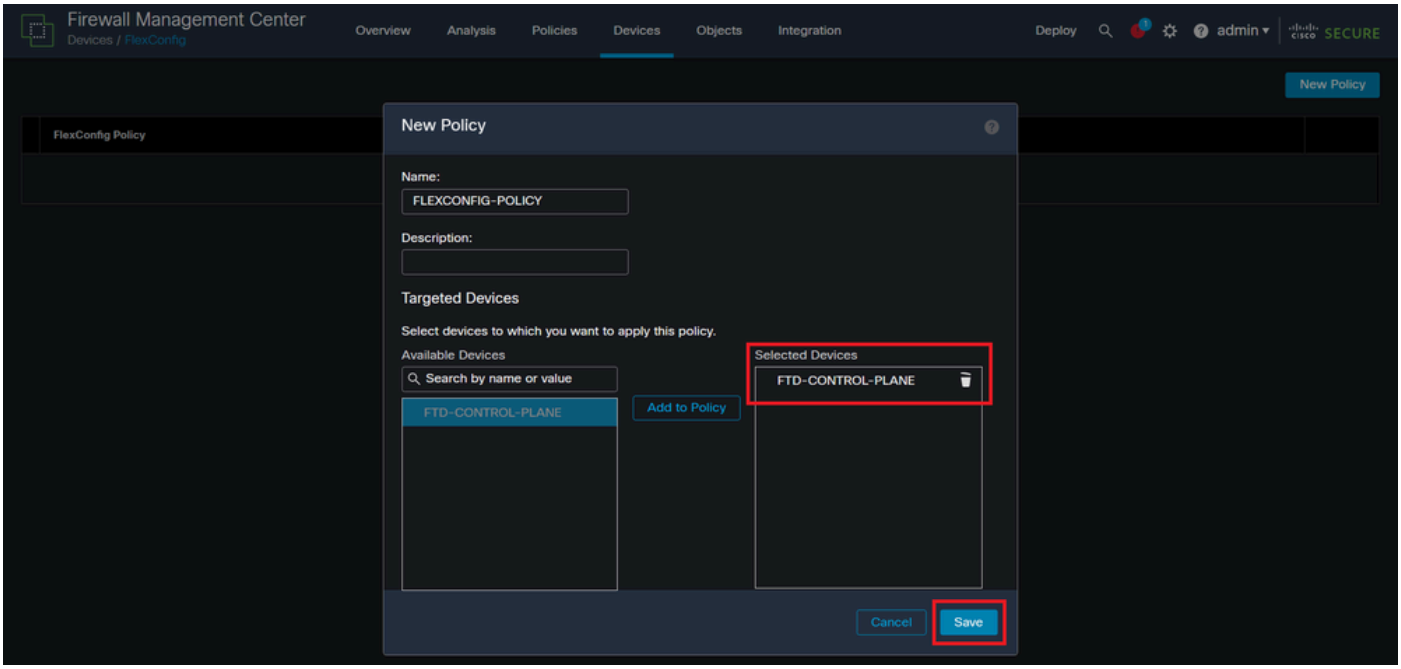



Image 17. Affectation de périphérique FlexConfig Policy

Étape 4.3. Dans le volet gauche, recherchez l'objet FlexConfig créé à l'étape 3.2, puis ajoutez-le à la stratégie FlexConfig en cliquant sur la flèche droite située au milieu de la fenêtre. Cliquez ensuite sur le bouton Save (Enregistrer) :

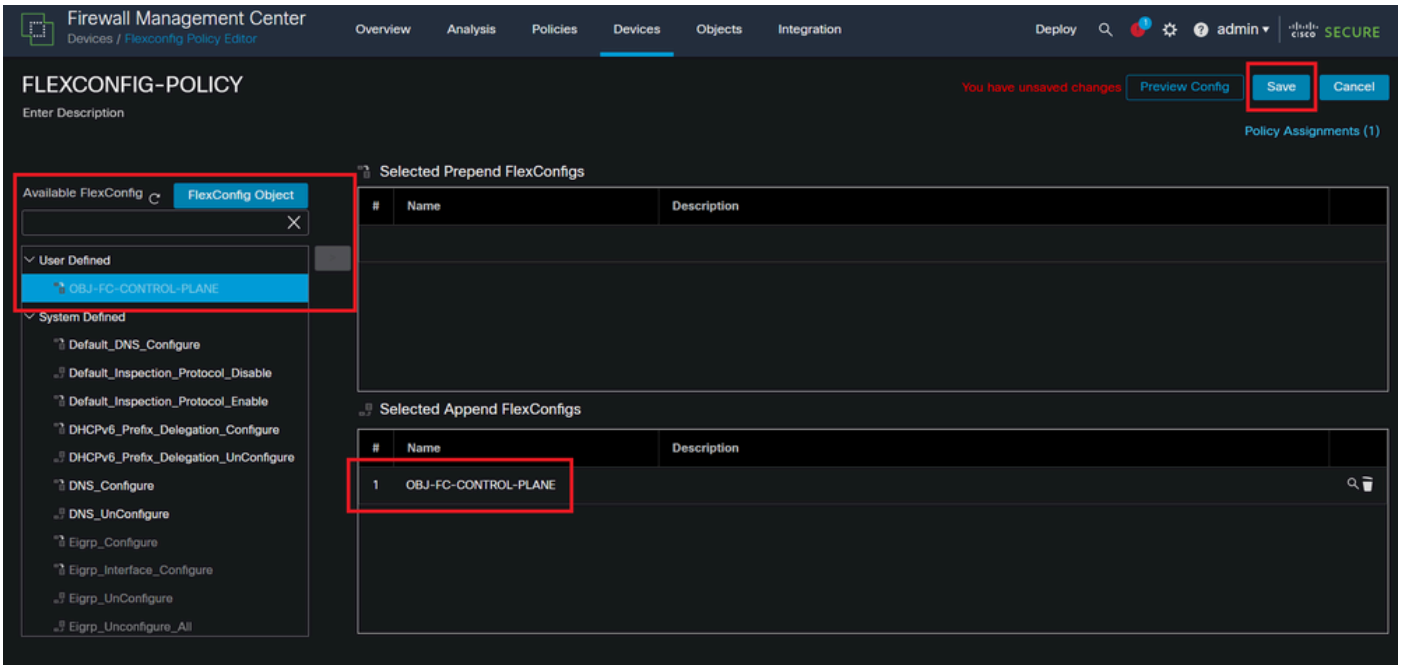



Image 18. Attribution d'objet de stratégie FlexConfig

Étape 5. Procédez au déploiement de la modification de configuration sur le FTD en naviguant jusqu'à Déployer > Déploiement avancé :

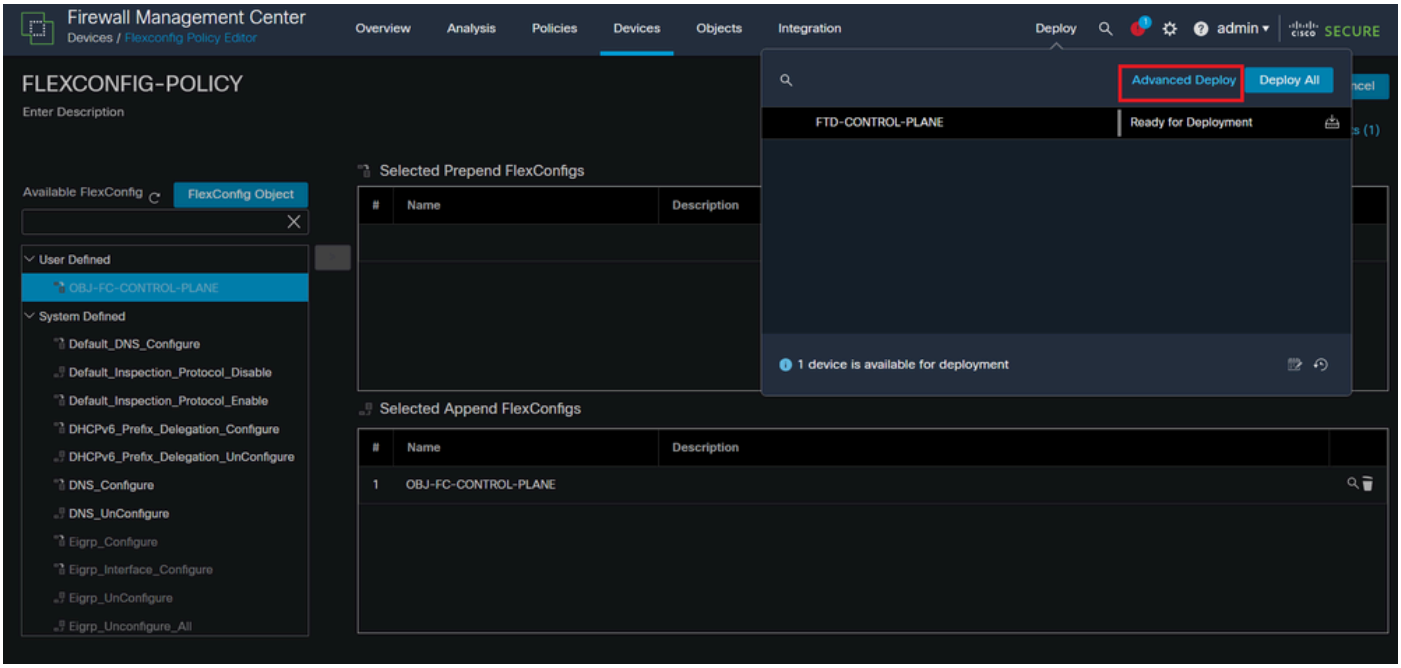



Image 19. Déploiement avancé FTD

Étape 5.1. Sélectionnez le FTD auquel vous souhaitez appliquer la stratégie FlexConfig. Si tout est correct, cliquez sur Déployer :

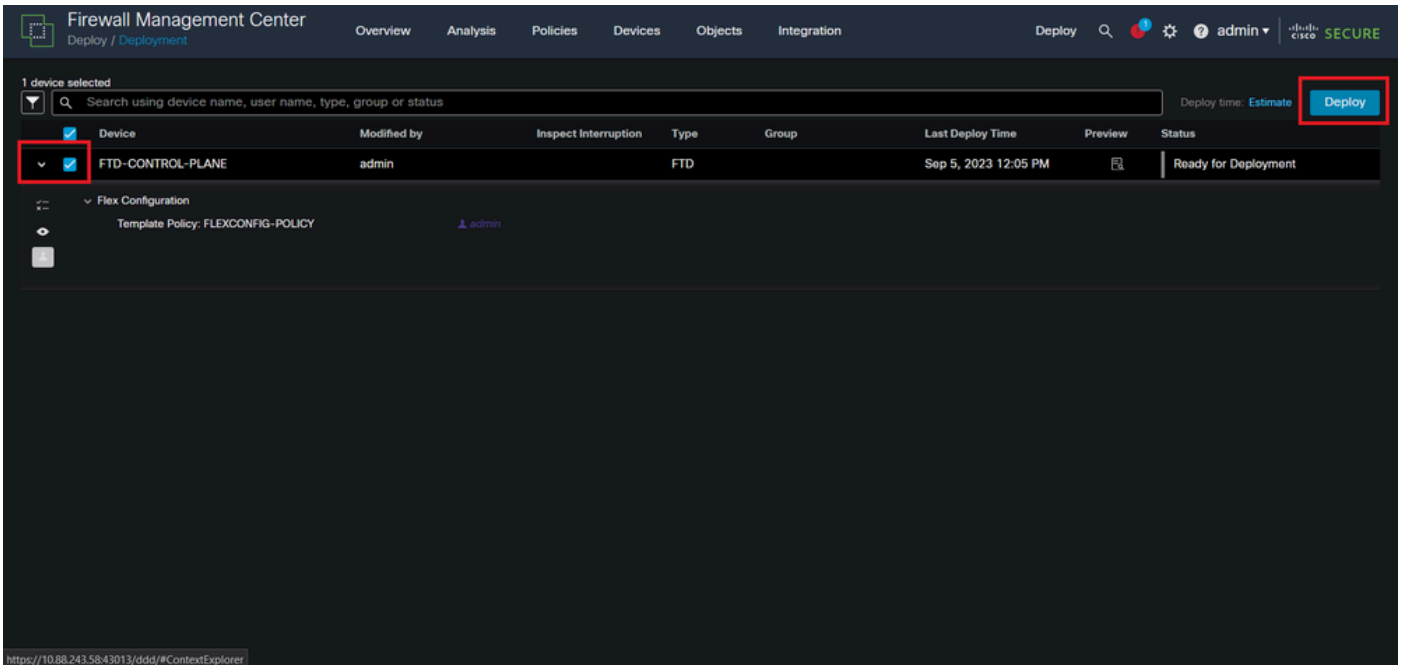



Image 20. Validation du déploiement FTD

Étape 5.2. Ensuite, une fenêtre de confirmation du déploiement s'affiche. Ajoutez un commentaire pour suivre le déploiement et passez à l'étape Déployer :

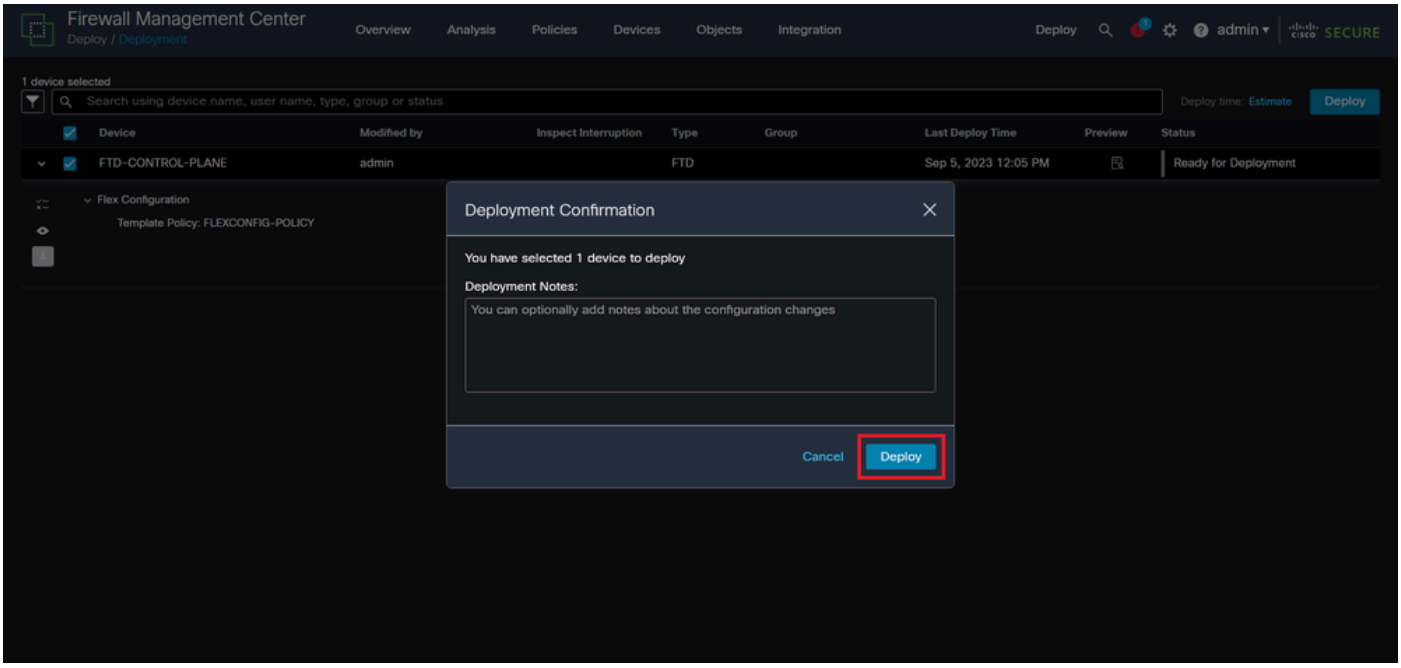



Image 21. Commentaires sur le déploiement FTD

Étape 5.3. Un message d'avertissement peut apparaître lors du déploiement des modifications FlexConfig. Cliquez sur Déployer uniquement si vous êtes entièrement certain que la configuration de la stratégie est correcte :

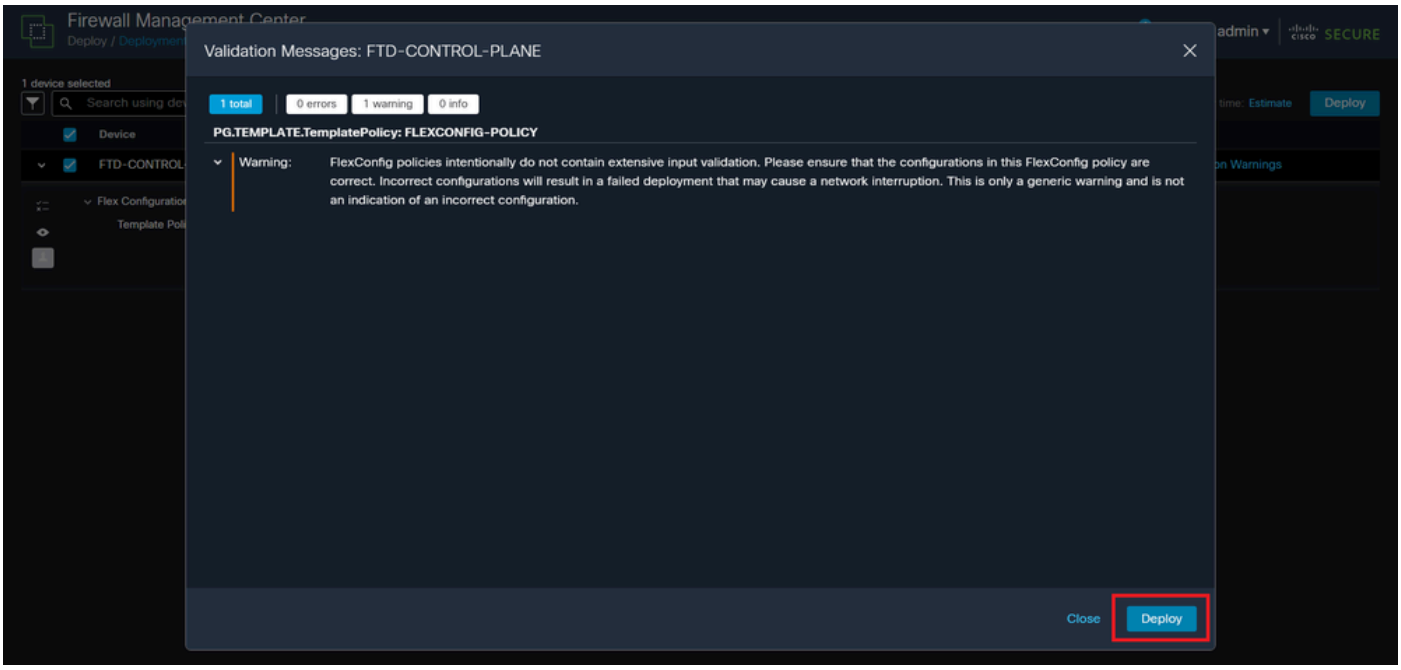



Image 22. Avertissement FTD Deployment Flexconfig

Étape 5.4. Confirmez que le déploiement de la stratégie a réussi pour le FTD :

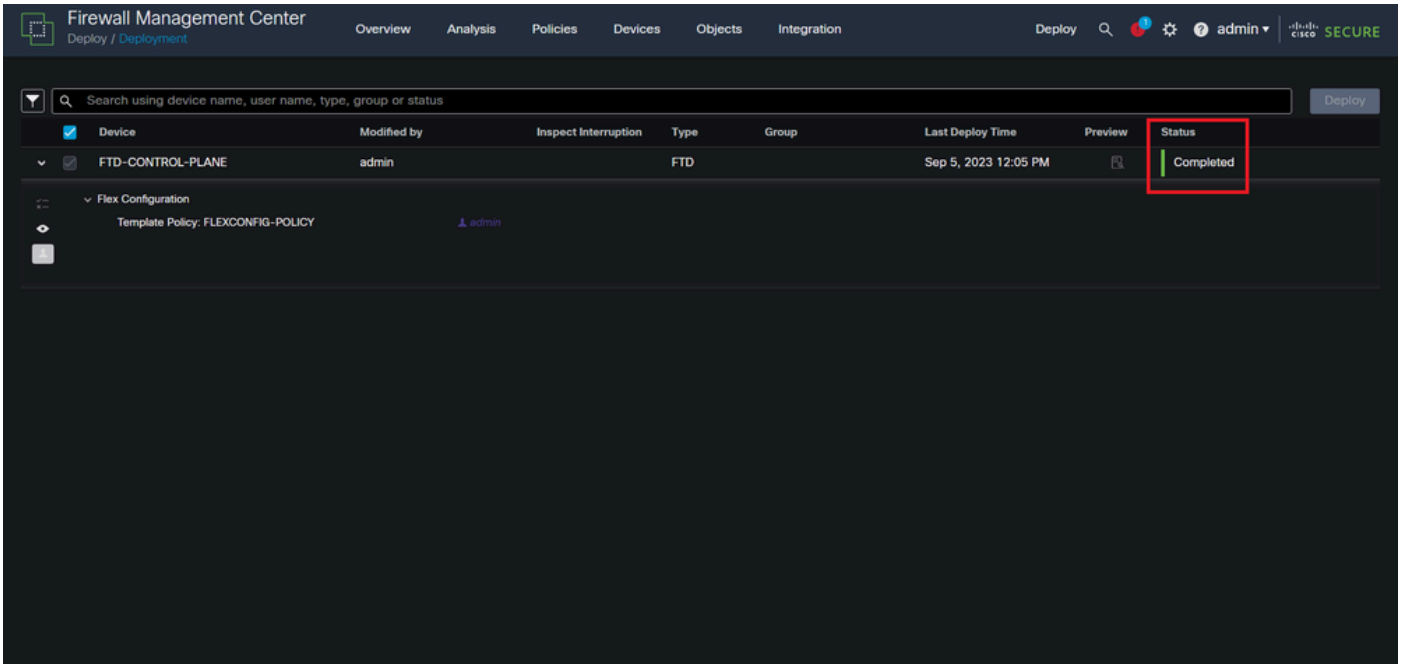



Image 23. Déploiement FTD réussi

Étape 6. Si vous créez une nouvelle liste de contrôle d'accès de plan de contrôle pour votre FTD ou si vous avez modifié une liste existante qui est en cours d'utilisation, il est important de mettre en évidence les modifications apportées à la configuration. Elles ne s'appliquent pas aux connexions déjà établies au FTD. Vous devez effacer manuellement les tentatives de connexion active au FTD, vous connecter à l'interface de ligne de commande du FTD et effacer les connexions actives.

Pour effacer la connexion active d'une adresse IP d'hôte spécifique :

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

Pour effacer les connexions actives d’un réseau de sous-réseau entier :

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

Pour effacer les connexions actives d'une plage d'adresses IP :

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

---

Remarque : il est vivement recommandé d'utiliser le mot clé all à la fin de la commande clear conn address pour forcer la suppression des tentatives de connexion VPN en force brute au pare-feu sécurisé. C'est principalement quand la nature de l'attaque en force brute VPN est de lancer une explosion de tentatives de connexion constantes.

---

[VIDEO] Configurer une liste de contrôle d'accès du plan de contrôle pour FTD géré par FMC

Configurer une liste de contrôle d'accès du plan de contrôle pour FTD géré par FDM

Voici la procédure que vous devez suivre avec un FDM pour configurer une ACL de plan de contrôle pour bloquer les attaques en force entrantes de VPN vers l'interface FTD externe :

Étape 1. Ouvrez l'interface utilisateur graphique de FDM via HTTPS et connectez-vous avec vos informations d'identification :

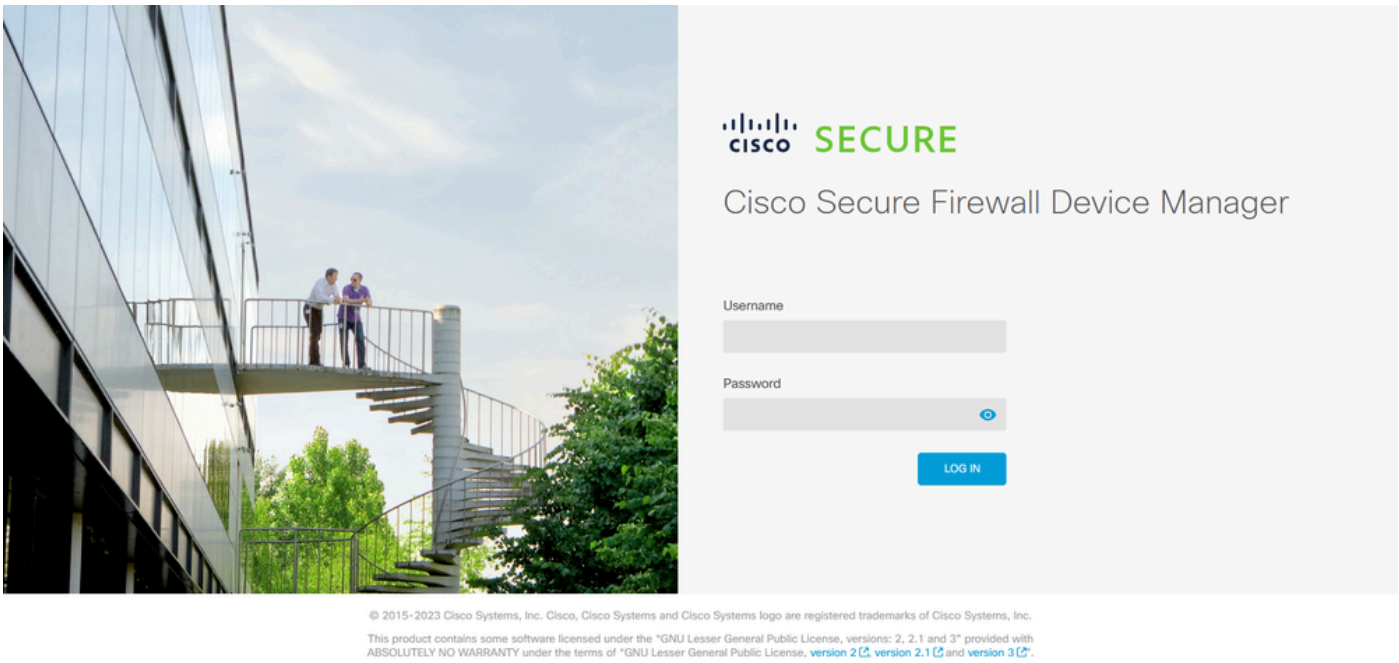



Image 24. Page de connexion de FDM

Étape 2. Vous devez créer un réseau d'objets. Accédez à Objets :

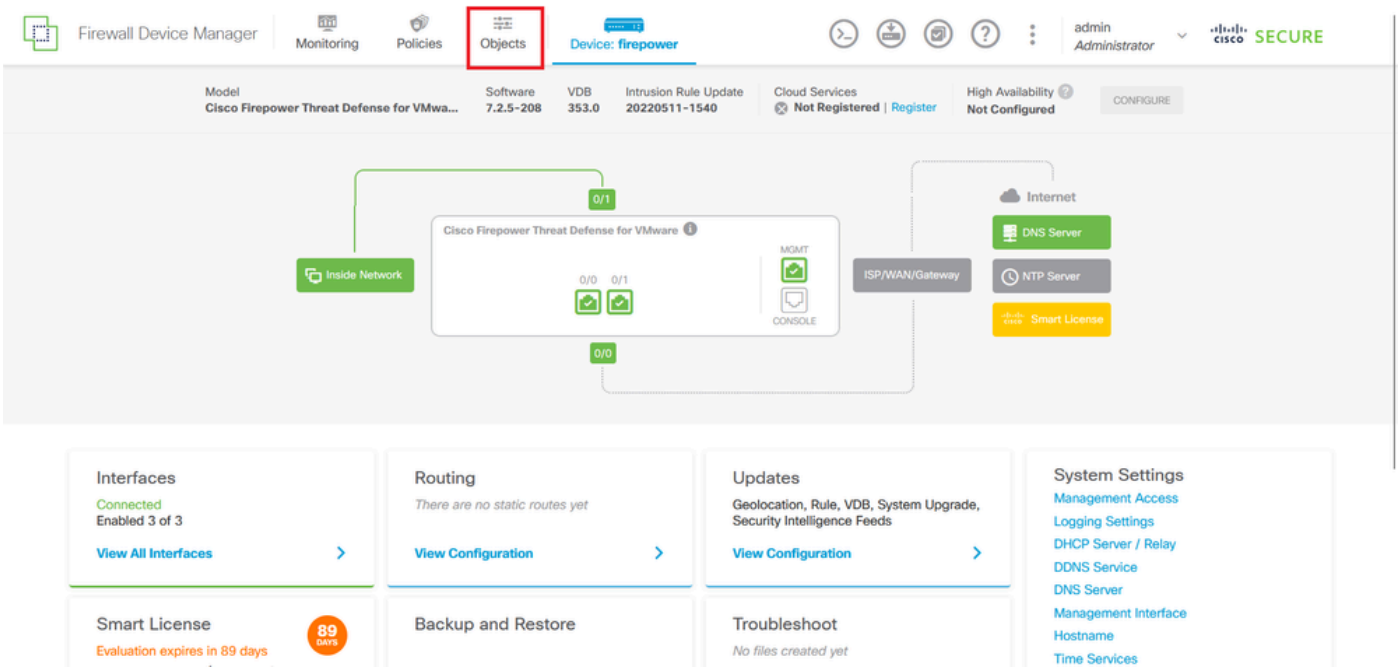



Image 25. Tableau de bord principal FDM

Étape 2.1. Dans le volet de gauche, sélectionnez Réseaux, puis cliquez sur le bouton « + » pour créer un nouvel objet réseau :

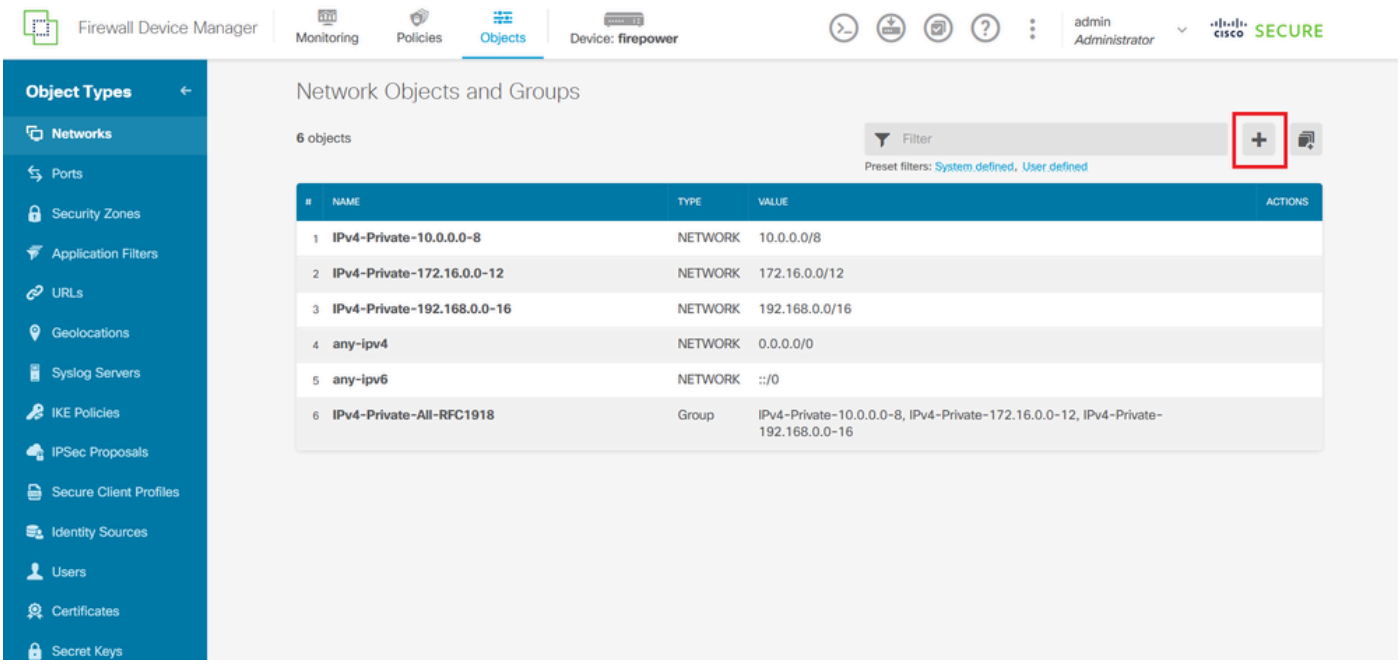



Image 26. Création d'objets

Étape 2.2. Ajoutez un nom pour l'objet réseau, sélectionnez le type de réseau de l'objet, ajoutez l'adresse IP, l'adresse réseau ou la plage d'adresses IP correspondant au trafic qui doit être refusé au FTD. Cliquez ensuite sur le bouton Ok pour terminer le réseau d'objets.

Dans cet exemple, le réseau objet configuré est destiné à bloquer les attaques en force VPN provenant du sous-réseau 192.168.1.0/24 :

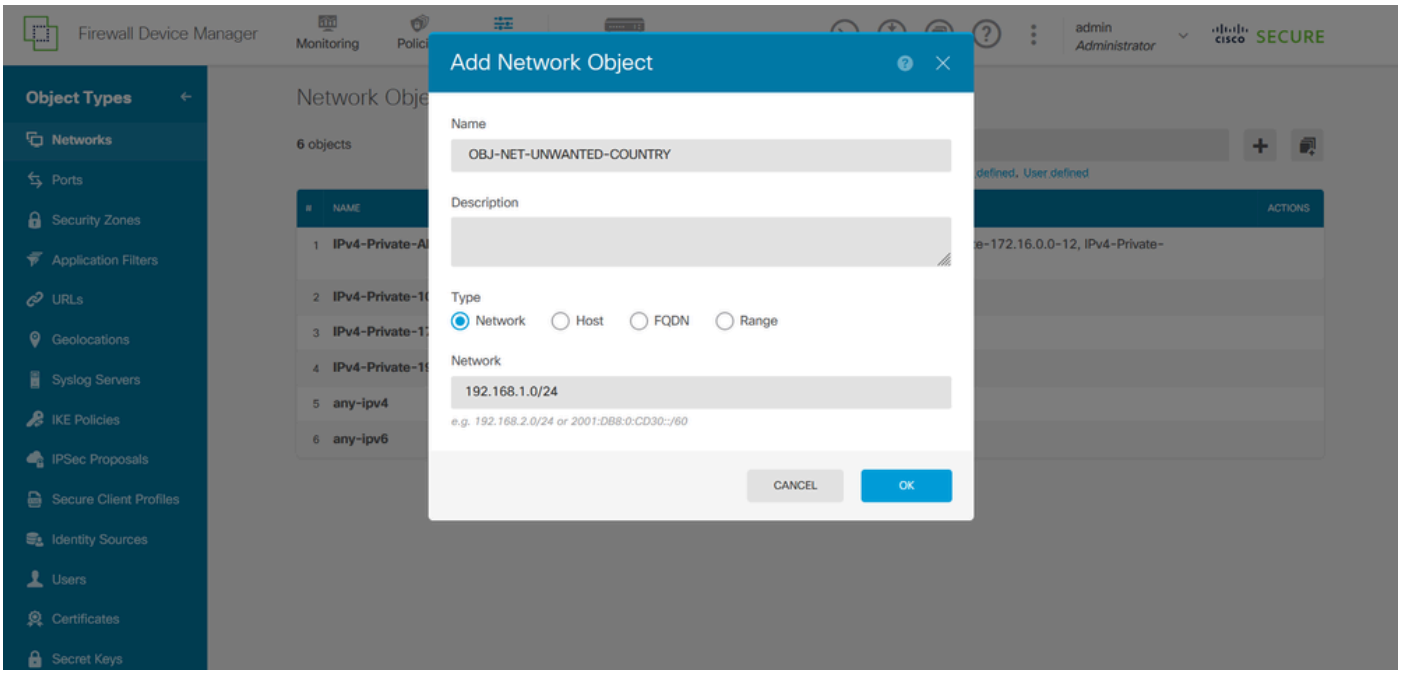



Image 27. Ajouter un objet réseau

Étape 3. Ensuite, vous devez créer une liste de contrôle d'accès étendue, puis accéder à l'onglet

Device du menu supérieur :

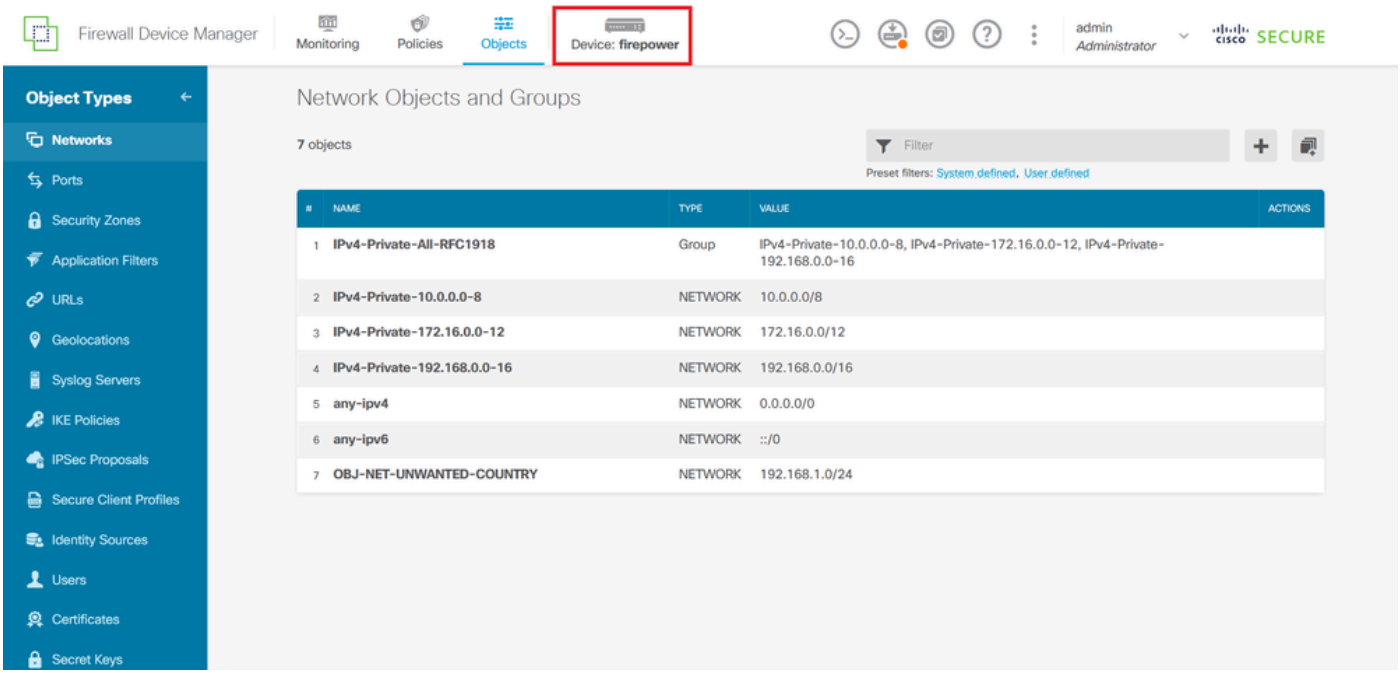



Image 28. Page Paramètres du périphérique

Étape 3.1. Faites défiler la page vers le bas et sélectionnez View Configuration dans le carré Advanced Configuration, comme illustré dans l'image :

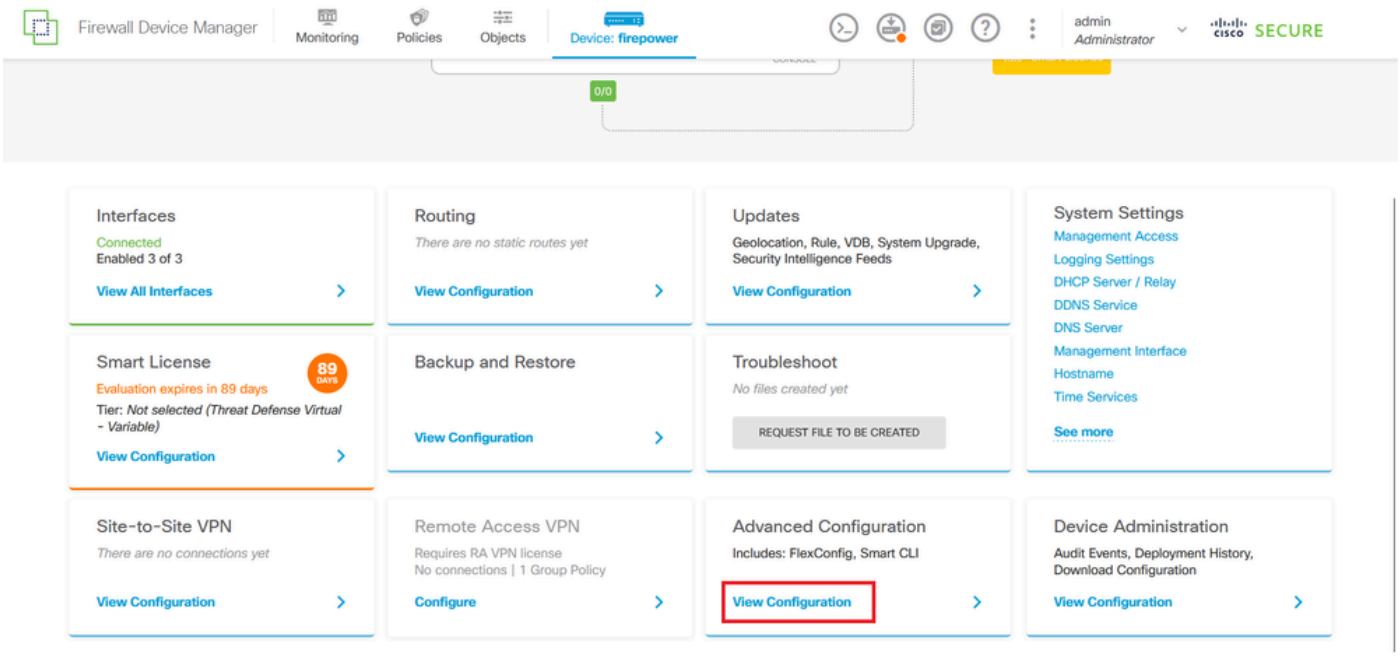



Image 29. Configuration avancée de FDM

Étape 3.2. Dans le volet de gauche, accédez à Smart CLI > Objects et cliquez sur CREATE SMART CLI OBJECT.

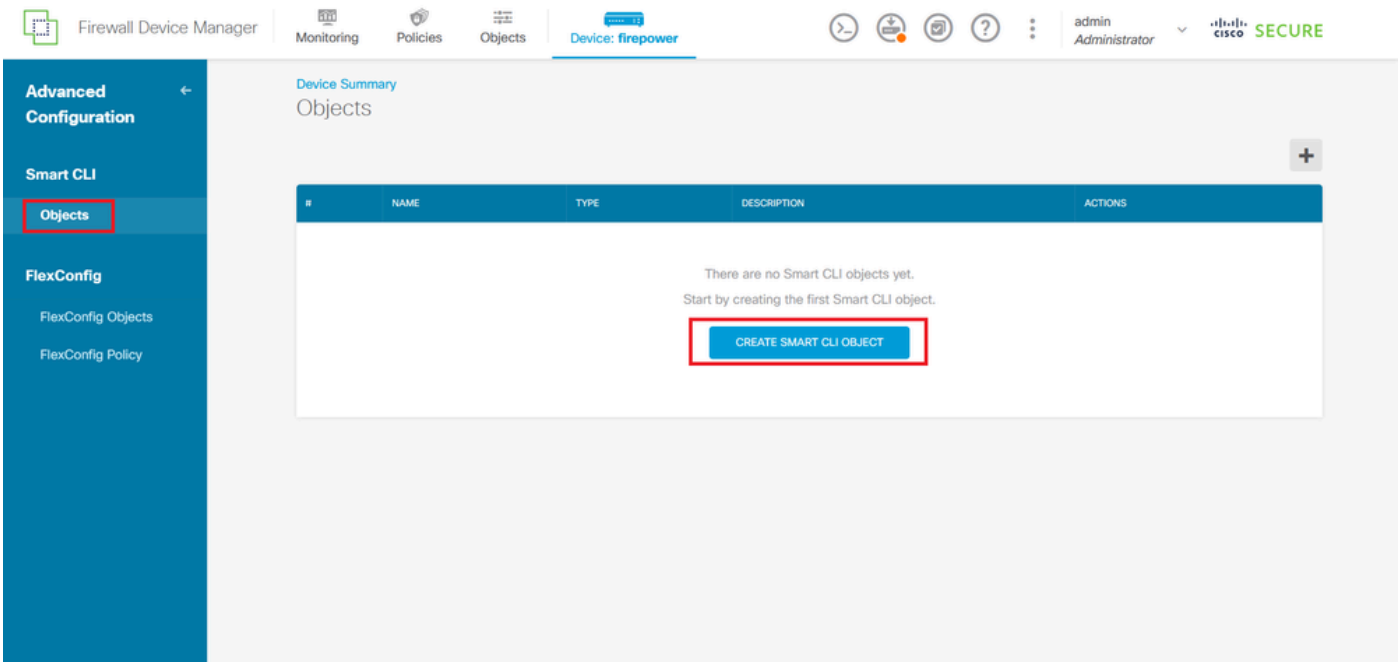



Image 30. Objets Smart CLI

Étape 3.3. Ajoutez un nom pour la liste de contrôle d'accès étendue. Pour créer une liste de contrôle d'accès étendue, sélectionnez-la dans le menu déroulant du modèle CLI, puis configurez les entrées de contrôle d'accès requises à l'aide de l'objet réseau créé à l'étape 2.2. Cliquez ensuite sur le bouton OK pour compléter la liste de contrôle d'accès :

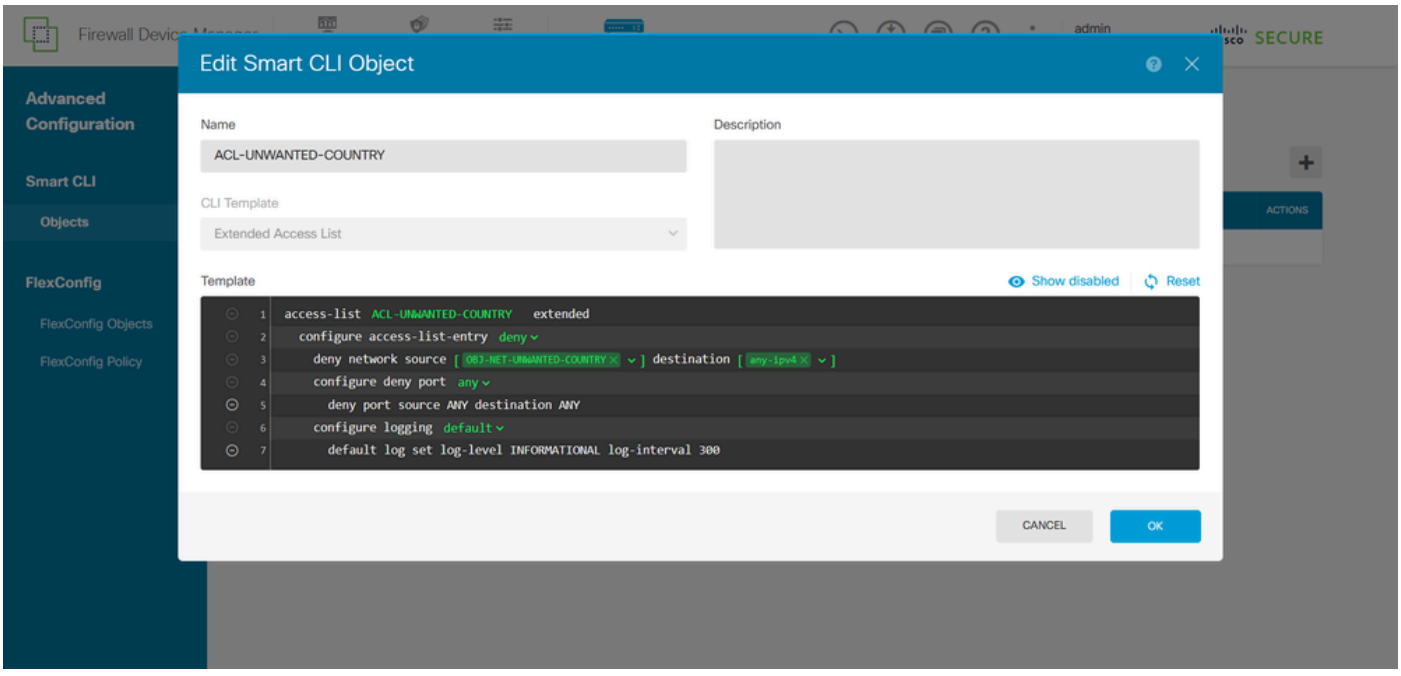



Image 31. Création de liste de contrôle d'accès étendue

Remarque : si vous devez ajouter d'autres ACE pour la liste de contrôle d'accès, vous pouvez le faire en plaçant le curseur de la souris sur la gauche de l'ACE actuelle ; alors trois points cliquables n'apparaissent pas. Cliquez sur ceci et sélectionnez Duplicate pour ajouter

d'autres ACE.

Étape 4. Ensuite, vous devez créer un objet FlexConfig, naviguer vers le panneau de gauche et sélectionner FlexConfig > FlexConfig Objects, puis cliquez sur CREATE FLEXCONFIG OBJECT:

,

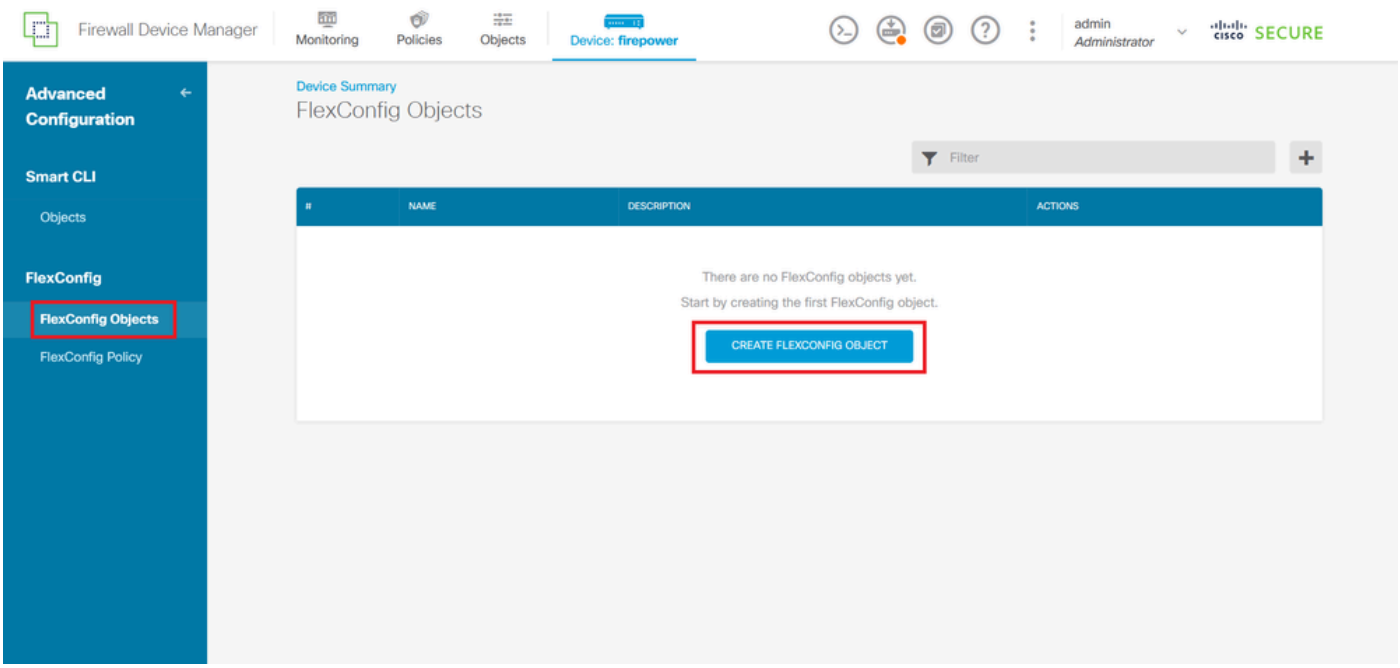



Image 32. Objets FlexConfig

Étape 4.1. Ajoutez un nom pour l'objet FlexConfig afin de créer et de configurer la liste de contrôle d'accès du plan de contrôle comme étant entrante pour l'interface externe.

Syntaxe de ligne de commande :

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

Cela se traduit par l'exemple de commande suivant, qui utilise la liste de contrôle d'accès étendue créée à l'étape 3.3 ACL-UNWANTED-COUNTRY :

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

C'est ainsi qu'il peut être configuré dans la fenêtre d'objet FlexConfig. Cliquez sur le bouton OK

pour terminer l'objet FlexConfig :

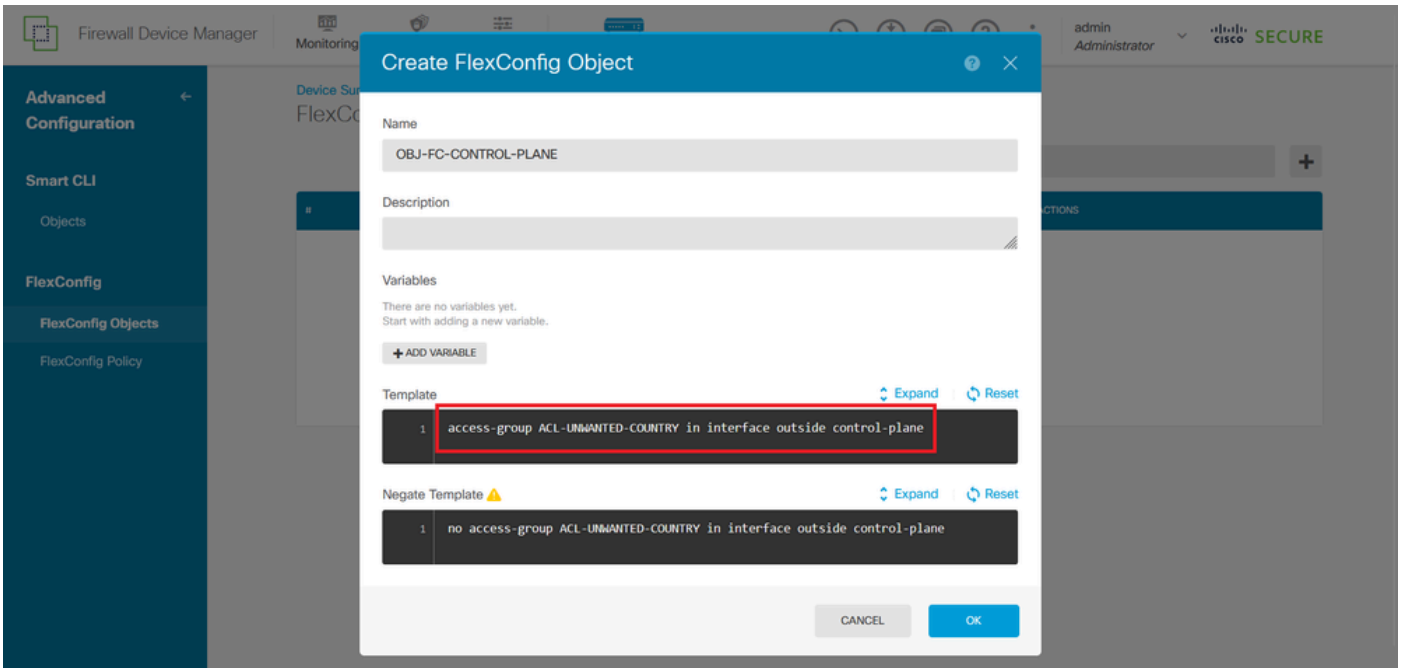



Image 33. Création d'un objet FlexConfig

Remarque : il est fortement recommandé de configurer la liste de contrôle d'accès du plan de contrôle uniquement pour les interfaces recevant des sessions VPN d'accès à distance entrantes dans le pare-feu sécurisé, comme l'interface externe.

Étape 5. Créez une stratégie FlexConfig. Accédez à Flexconfig > FlexConfig Policy, cliquez sur le bouton "+" et sélectionnez l'objet FlexConfig qui a été créé à l'étape 4.1 :

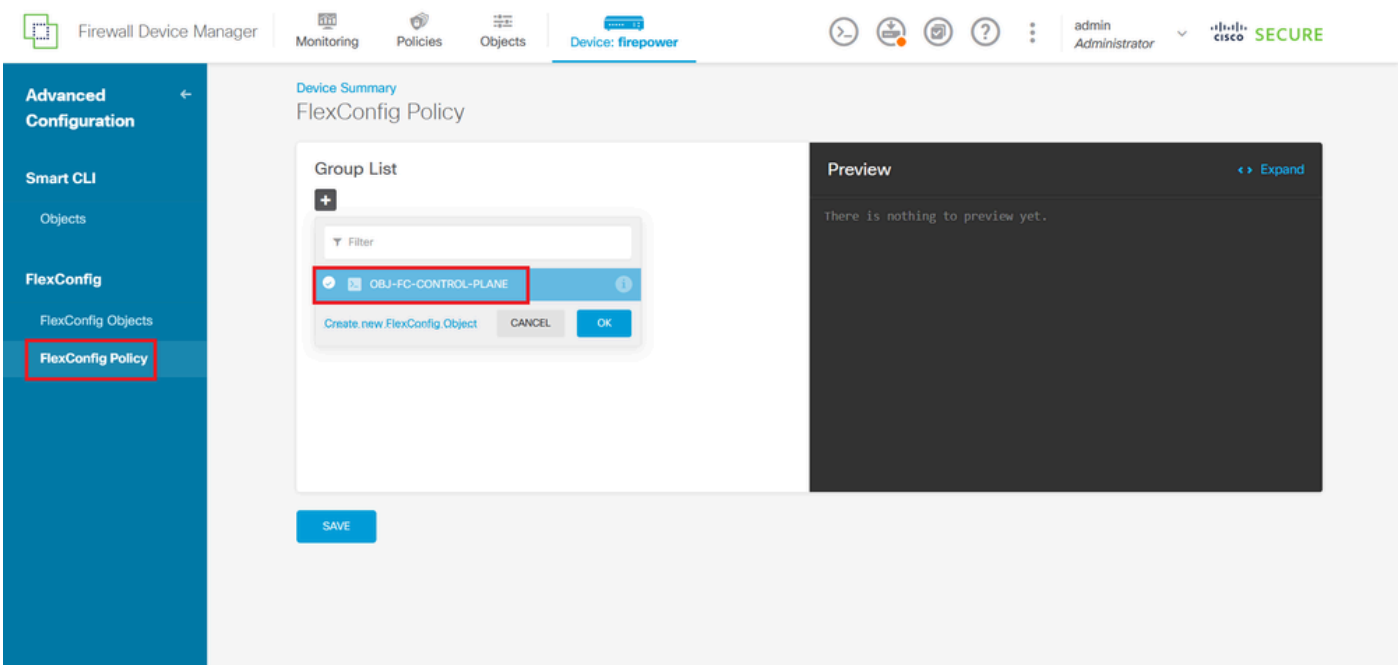


Image 34. Politique FlexConfig

Étape 5.1 : validation de l'aperçu FlexConfig affiche la configuration correcte pour la liste de contrôle d'accès du plan de contrôle créée et cliquez sur le bouton Enregistrer :

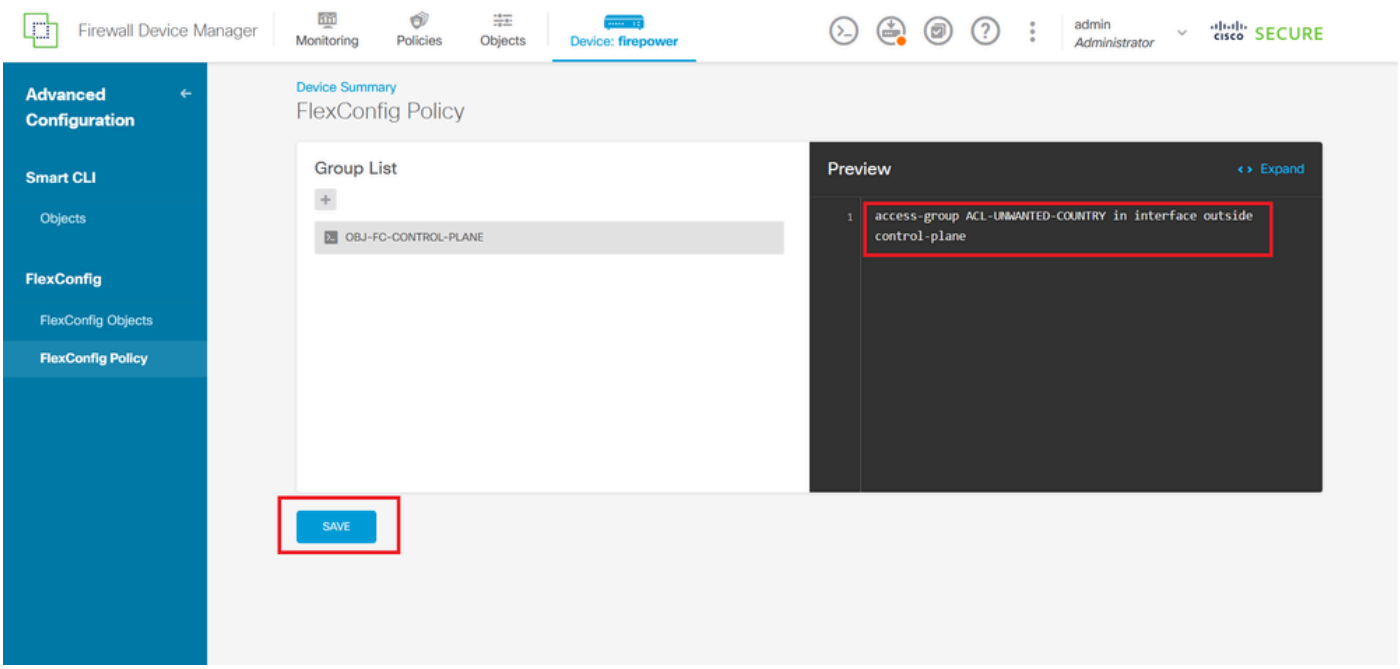



Image 35. Aperçu de la stratégie FlexConfig

Étape 6. Déployez les modifications de configuration sur le FTD que vous souhaitez protéger contre les attaques en force du VPN. Cliquez ensuite sur le bouton Deployment dans le menu supérieur et validez que les modifications de configuration à déployer sont correctes, puis cliquez sur DEPLOY NOW :

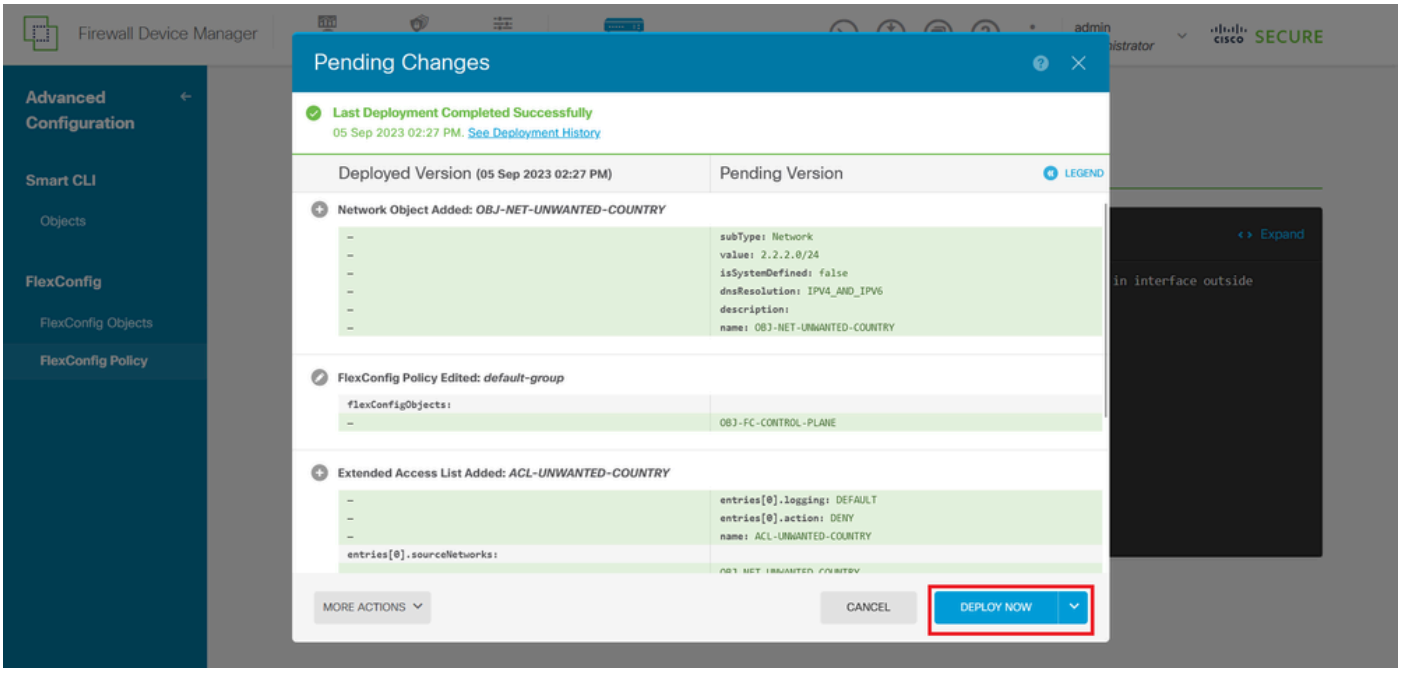


Image 36. Déploiement en attente

Étape 6.1. Validez le déploiement de la stratégie :

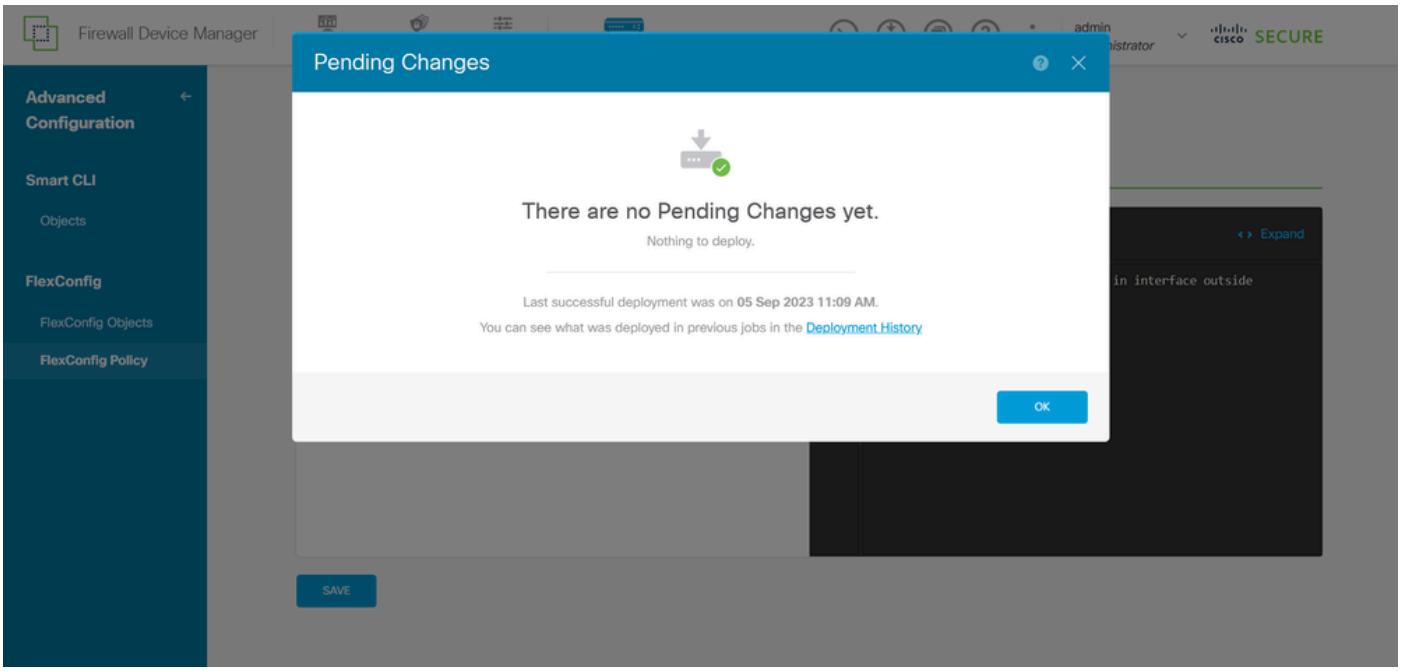



Image 37. Déploiement réussi

Étape 7. Si vous créez une nouvelle liste de contrôle d'accès de plan de contrôle pour votre FTD ou si vous avez modifié une liste existante qui est activement utilisée, il est important de mettre en évidence les modifications apportées à la configuration. Elles ne s'appliquent pas aux connexions déjà établies au FTD. Vous devez effacer manuellement les tentatives de connexion active au FTD, vous connecter à l'interface de ligne de commande du FTD et effacer les connexions actives.

Pour effacer la connexion active d'une adresse IP d'hôte spécifique :

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

Pour effacer les connexions actives d’un réseau de sous-réseau entier :

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

Pour effacer les connexions actives d'une plage d'adresses IP :

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

Remarque : il est vivement recommandé d'utiliser le mot clé all à la fin de la commande clear conn address pour forcer la suppression des tentatives de connexion VPN en force brute au pare-feu sécurisé. C'est principalement quand la nature de l'attaque en force brute VPN est de lancer une explosion de tentatives de connexion constantes.

Configurer une ACL du plan de contrôle pour ASA à l'aide de CLI

Voici la procédure à suivre avec une CLI ASA, c'est-à-dire configurer une ACL de plan de contrôle pour bloquer les attaques en force entrantes VPN vers l'interface externe :

Étape 1 : connectez-vous au pare-feu sécurisé ASA via l'interface de ligne de commande et accédez à la commande configure terminal.

```
asa# configure terminal
```

Étape 2. Exécutez la commande suivante pour configurer une liste de contrôle d'accès étendue, qui bloque une adresse IP hôte ou une adresse réseau pour le trafic qui doit être bloqué vers l'ASA.

Dans cet exemple, vous créez une nouvelle liste de contrôle d'accès appelée ACL-UNWANTED-COUNTRY et l'entrée ACE configurée bloque les attaques en force VPN provenant du sous-réseau 192.168.1.0/24 :

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

Étape 3. Exécutez la commande suivante access-group pour configurer la liste de contrôle d'accès ACL-UNWANTED-COUNTRY en tant que liste de contrôle d'accès du plan de contrôle pour l'interface ASA externe :

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

Remarque : il est fortement recommandé de configurer la liste de contrôle d'accès du plan de contrôle uniquement pour les interfaces recevant des sessions VPN d'accès à distance

entrantes dans le pare-feu sécurisé, comme l'interface externe.

Étape 4. Si vous créez une nouvelle liste de contrôle d’accès de plan de contrôle ou si vous avez modifié une liste existante qui est activement utilisée, il est important de mettre en évidence les modifications apportées à la configuration. Ceux-ci ne s'appliquent pas aux connexions déjà établies à l'ASA, vous devez effacer manuellement les tentatives de connexion active à l'ASA et effacer les connexions actives.

Pour effacer la connexion active d'une adresse IP d'hôte spécifique :

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

Pour effacer les connexions actives d’un réseau de sous-réseau entier :

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

Pour effacer les connexions actives d'une plage d'adresses IP :

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

Remarque : il est vivement recommandé d'utiliser le mot clé all à la fin de la commande clear conn address pour forcer la suppression des tentatives de connexion VPN en force brute au pare-feu sécurisé. C'est principalement quand la nature de l'attaque en force brute VPN est de lancer une explosion de tentatives de connexion constantes.

Configuration alternative pour bloquer les attaques pour le pare-feu sécurisé exécutant Shun

Pour les attaques de blocage immédiates pour le pare-feu sécurisé, vous pouvez exécuter la commande shun. La commande shun vous permet de bloquer les connexions à partir d'un hôte attaquant, consultez plus de détails sur la commande shun :

- Une fois que vous fermez une adresse IP, toutes les connexions futures à partir de l'adresse IP source sont abandonnées et consignées jusqu'à ce que vous supprimiez manuellement la fonction de blocage.
- La fonction blocking de la commande shun est appliquée si une connexion avec l'adresse

hôte spécifiée est actuellement active.
- Si vous spécifiez l'adresse de destination, les ports source et de destination, ainsi que le protocole, vous supprimez la connexion correspondante et placez un shun sur toutes les connexions futures à partir de l'adresse IP source. Toutes les connexions futures sont rejetées, pas seulement celles qui correspondent à ces paramètres de connexion spécifiques.
- Vous ne pouvez avoir qu'une seule commande shun par adresse IP source.
- La commande shun étant utilisée pour bloquer les attaques de manière dynamique, elle n'est pas affichée dans la configuration du périphérique de défense contre les menaces.
- Chaque fois qu'une configuration d'interface est supprimée, tous les shuns qui sont reliés à cette interface sont également supprimés.

Syntaxe de la commande Shun :

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

Pour désactiver un shun, exécutez la forme no de cette commande :

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

Pour désactiver une adresse IP d'hôte, passez à cet exemple pour le pare-feu sécurisé. Dans cet exemple, la commande shun est utilisée pour bloquer les attaques de force brute VPN provenant de l'adresse IP source 192.168.1.10.

Exemple de configuration pour FTD

Étape 1. Connectez-vous au FTD via l'interface de ligne de commande et exécutez la commande shun :

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

```
Shun 192.168.1.10 successful
```

Étape 2. Vous pouvez exécuter les commandes show pour confirmer les adresses IP de shun dans le FTD et pour surveiller le nombre d'occurrences de shun par adresse 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)
```

Exemple de configuration pour ASA

Étape 1. Connectez-vous à l'ASA via l'interface de ligne de commande et appliquez la commande shun :

<#root>

```
asa#

 shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf



Shun 192.168.1.10 successful
```

Étape 2. Vous pouvez exécuter les commandes show pour confirmer les adresses IP de shun dans l'ASA et pour surveiller le nombre de succès de shun par adresse 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)
```

Remarque : Pour plus d'informations sur la commande secure firewall shun, référez-vous à Référence des commandes Cisco Secure Firewall Threat Defense.

# Vérifier

Pour confirmer que la configuration de la liste de contrôle d'accès du plan de contrôle est en place pour le pare-feu sécurisé, procédez comme suit :

Étape 1 : connectez-vous au pare-feu sécurisé via l'interface de ligne de commande et exécutez les commandes suivantes pour confirmer que la configuration de la liste de contrôle d'accès du plan de contrôle est appliquée.

Exemple de résultat pour le FTD géré par 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
```

Exemple de résultat pour le FTD géré par 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
```

Exemple de résultat pour 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
```

Étape 2. Pour confirmer que la liste de contrôle d'accès du plan de contrôle bloque le trafic requis, exécutez la commande packet-tracer pour simuler une connexion TCP 443 entrante à l'interface externe du pare-feu sécurisé. Ensuite, exécutez la commande show access-list <acl-name> , le nombre d'occurrences de la liste de contrôle d'accès peut être incrémenté chaque fois qu'une connexion VPN en force brute au pare-feu sécurisé est bloquée par la liste de contrôle d'accès du plan de contrôle.

Dans cet exemple, la commande packet-tracer simule une connexion TCP 443 entrante provenant de l'hôte 192.168.1.10 et destinée à l'adresse IP externe du pare-feu sécurisé. La sortie packet-tracer confirme que le trafic est abandonné et la sortie show access-list affiche les incréments du nombre de succès pour la liste de contrôle d'accès du plan de contrôle en place :

Exemple de résultat pour 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

## Exemple de résultats pour 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
```

Remarque : si une solution RAVPN telle que Cisco Secure Client VPN est implémentée dans le pare-feu sécurisé, une tentative de connexion réelle au pare-feu sécurisé peut alors être effectuée pour confirmer que la liste de contrôle d'accès du plan de contrôle fonctionne comme prévu pour bloquer le trafic requis.

## Bogues associés

- ENH | Connexions AnyConnect Client basées sur la géolocalisation : ID de bogue Cisco CSCvs65322
- DOC : La recherche de groupes d'objets ASA/FTD ne prend pas en charge les ACL du plan de contrôle : ID de bogue Cisco CSCwi58818

## Informations connexes

- Configurer des stratégies basées sur la géolocalisation pour un VPN d'accès à distance sur la défense pare-feu sécurisée
- Atténuer les attaques par pulvérisation de mot de passe sur le pare-feu sécurisé VPN distant
- Guide de référence des technologies VPN Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.