Configurer les politiques de contrôle d'accès au plan de contrôle pour Secure Firewall Threat Defense et ASA

Table des matières

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 version 7.2.5
- Secure Firewall Manager Center version 7.2.5
- Secure Firewall Device Manager 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. Par exemple, lorsqu'une liste de contrôle d'accès du plan de contrôle peut être utile, il est possible de 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 du 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 il est géré à la fois par les politiques de contrôle d'accès (ACP) et les règles de pré-filtrage.

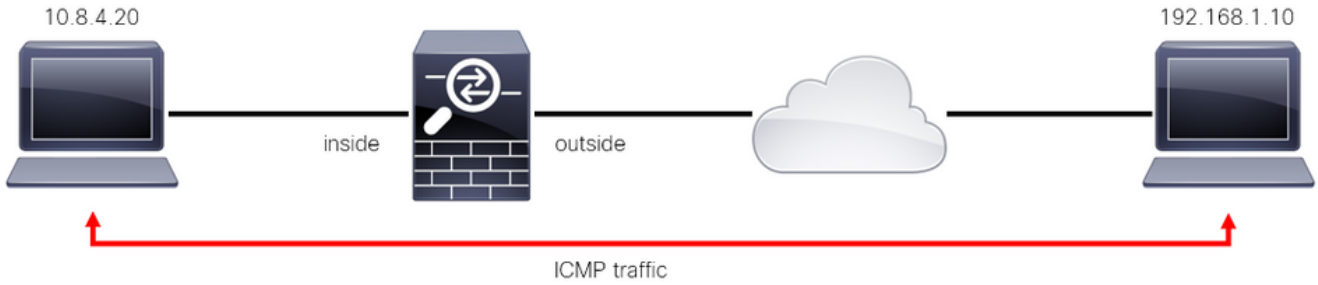

Image 1. Exemple de trafic prêt à l'emploi

Trafic prêt à l'emploi du pare-feu sécurisé

Dans d'autres cas, le trafic est directement destiné à une interface FTD (VPN de site à site ou d'accès à distance). Il s'agit du trafic « prêt à l'emploi », géré par le plan de contrôle de cette interface spécifique.

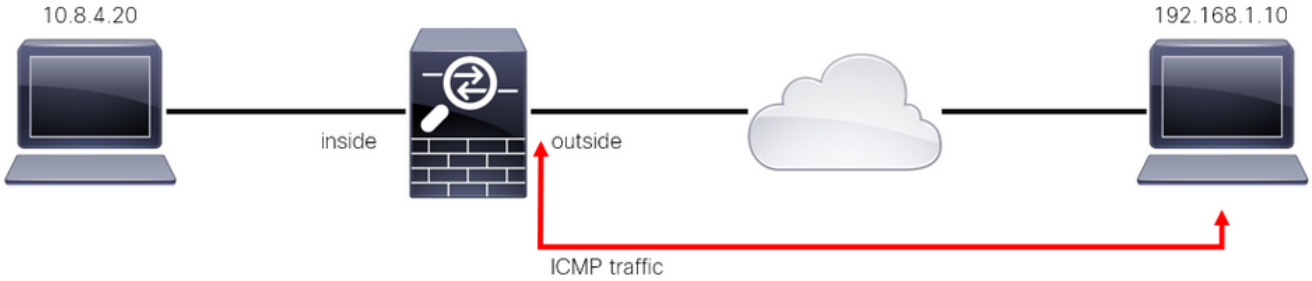

Image 2. Exemple de trafic prêt à l'emploi

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 du 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 mot clé control-plane est ajouté à la configuration access-group, qui appliquera le trafic 'vers' l'interface de pare-feu sécurisée. 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 'vers' le pare-feu sécurisé lui-même, alors 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.
- Au moment de la création de ce document, la fonction de géolocalisation du 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 le VPN dans 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 l'interface FTD externe :

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

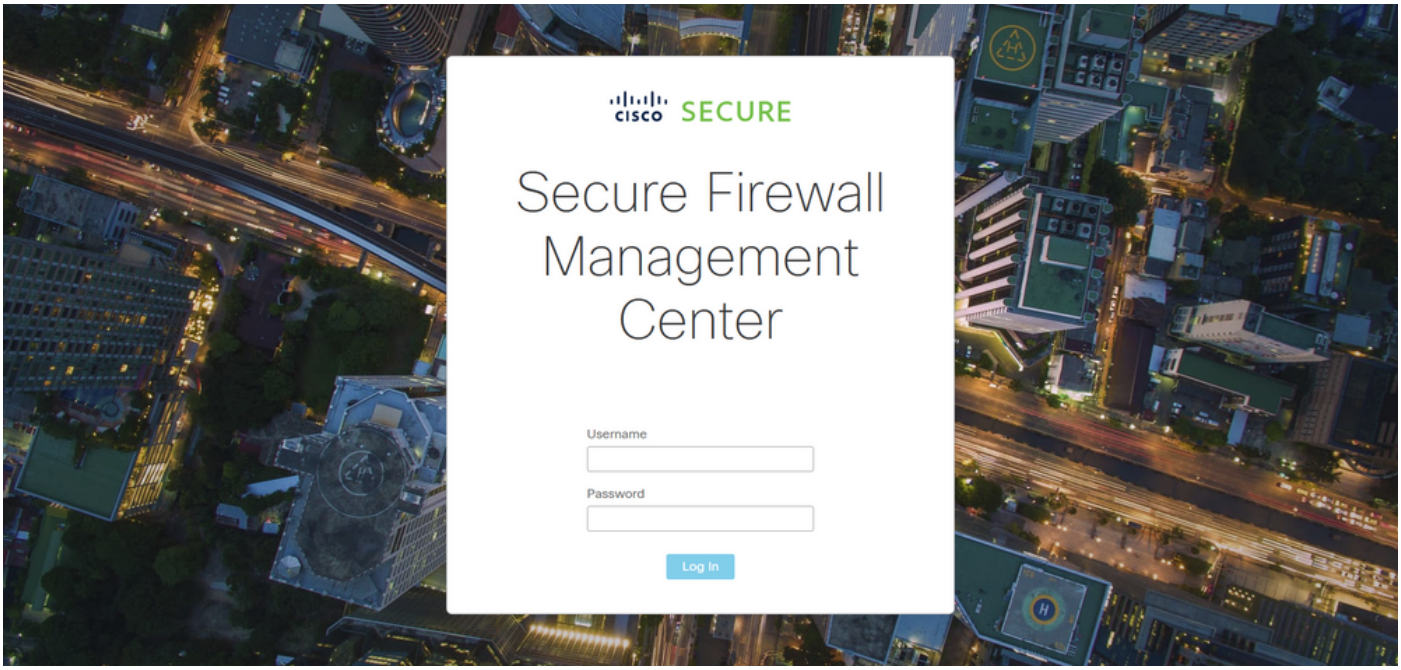

Image 3. Page de connexion FMC

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

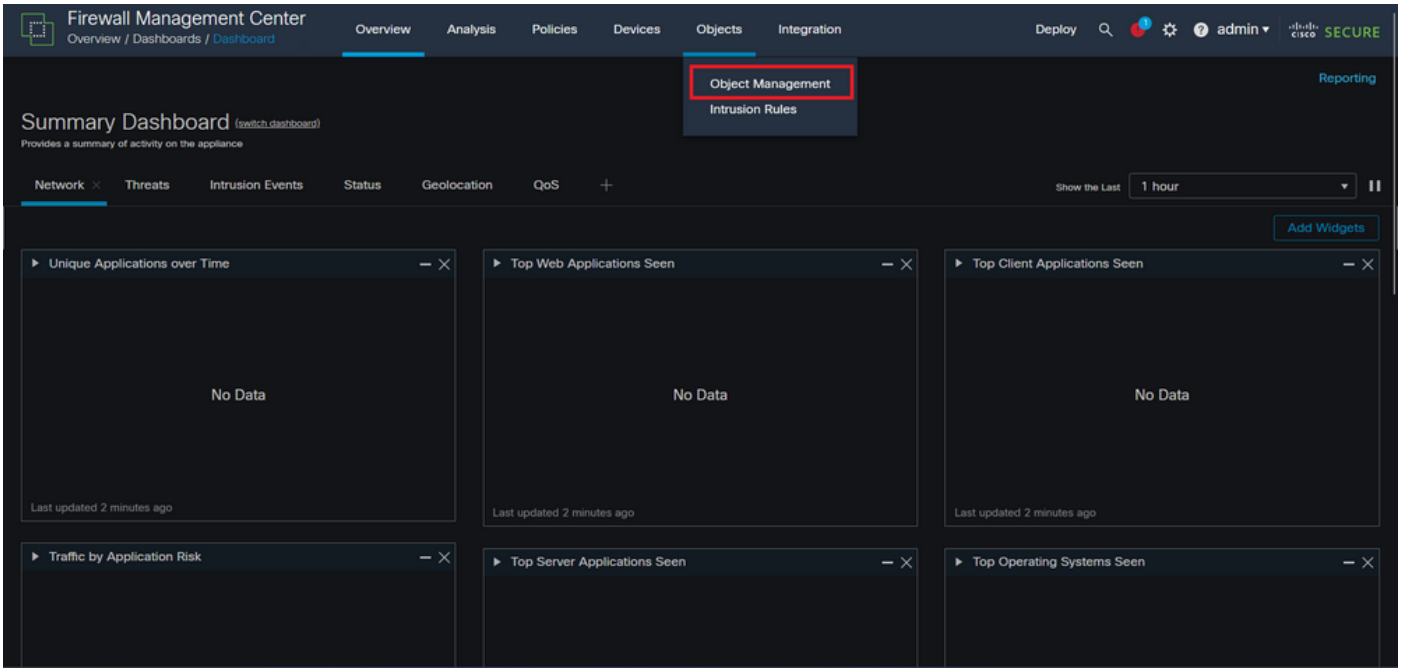

Image 4. Gestion des objets

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

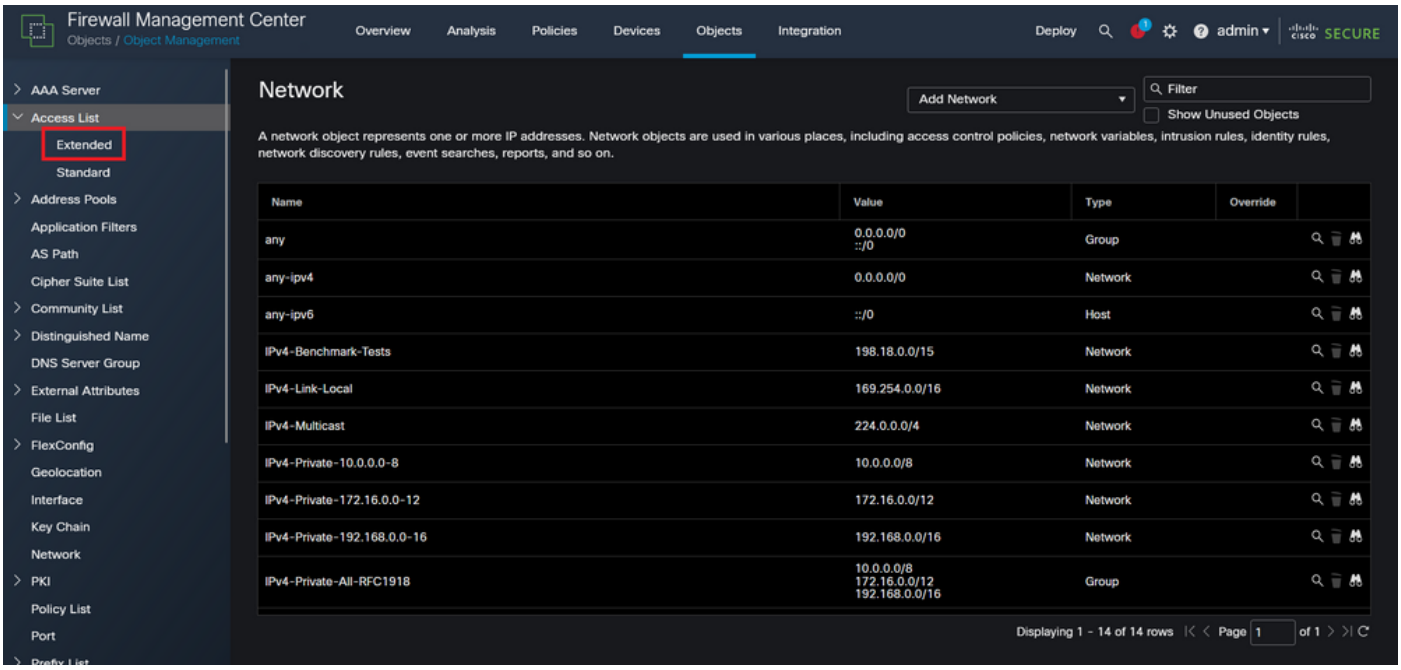

Image 5. Menu ACL étendue

Étape 2.2. Sélectionnez ensuite Ajouter une liste d'accès étendue.

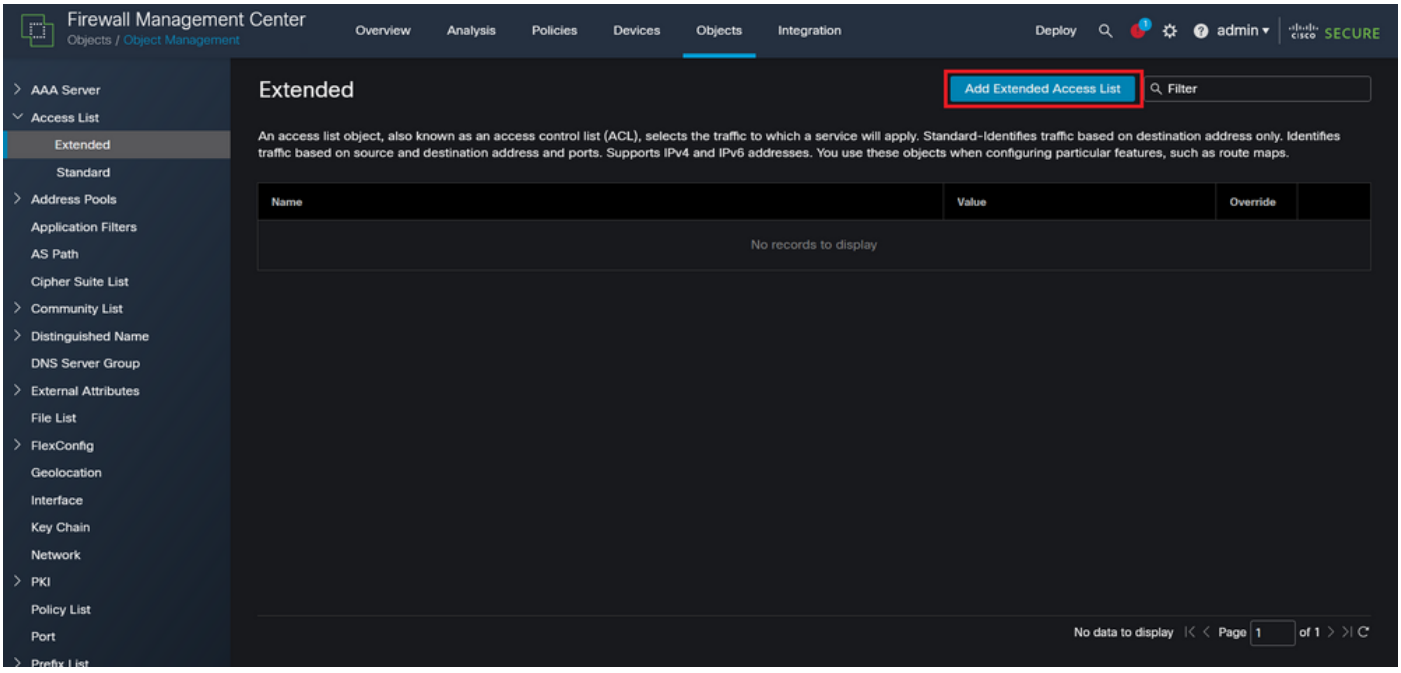

Image 6. Ajouter une liste de contrôle étendue

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 :

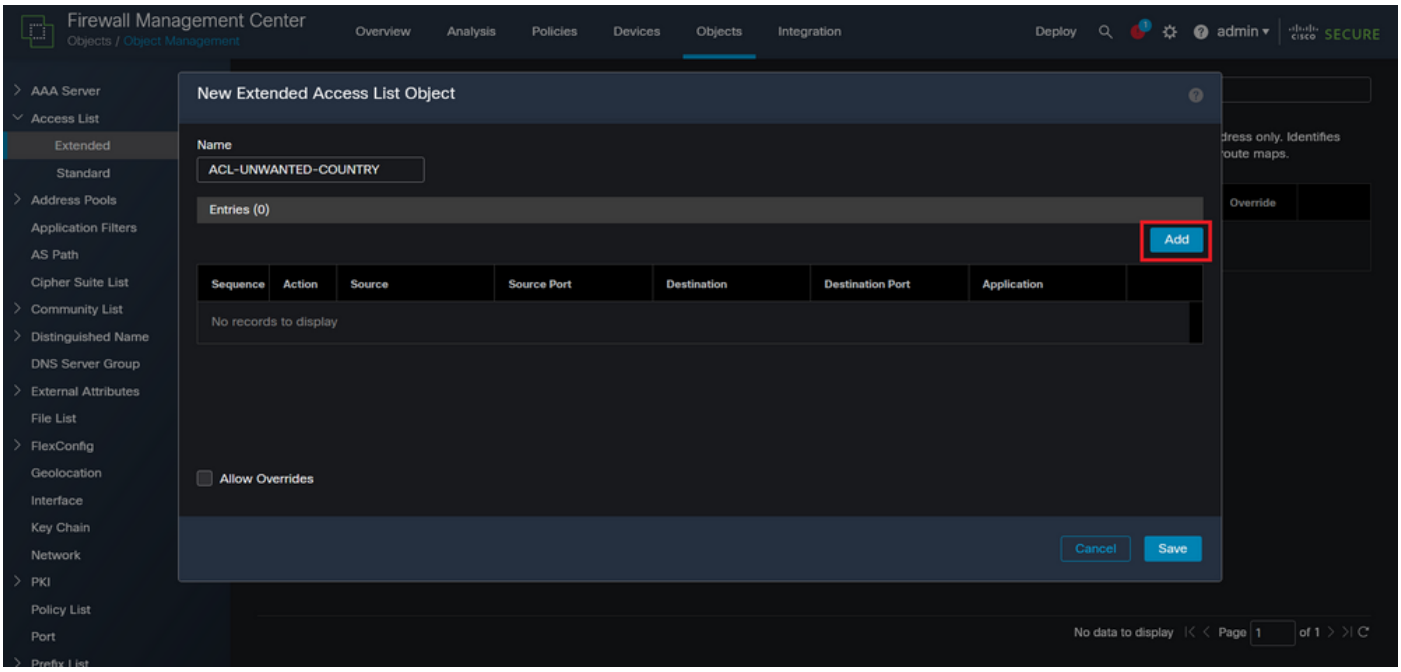

Image 7. Entrées ACL étendues

Étape 2.4. Remplacez l'action ACE par Block (Bloquer), puis ajoutez le réseau source pour qu'il corresponde au trafic devant être refusé au FTD, conservez le réseau de destination sur Any (Tous) et cliquez sur le bouton Add (Ajouter) pour terminer l'entrée ACE :

- Dans cet exemple, l'entrée ACE configurée bloquera les attaques en force de VPN provenant du sous-réseau 192.168.1.0/24.

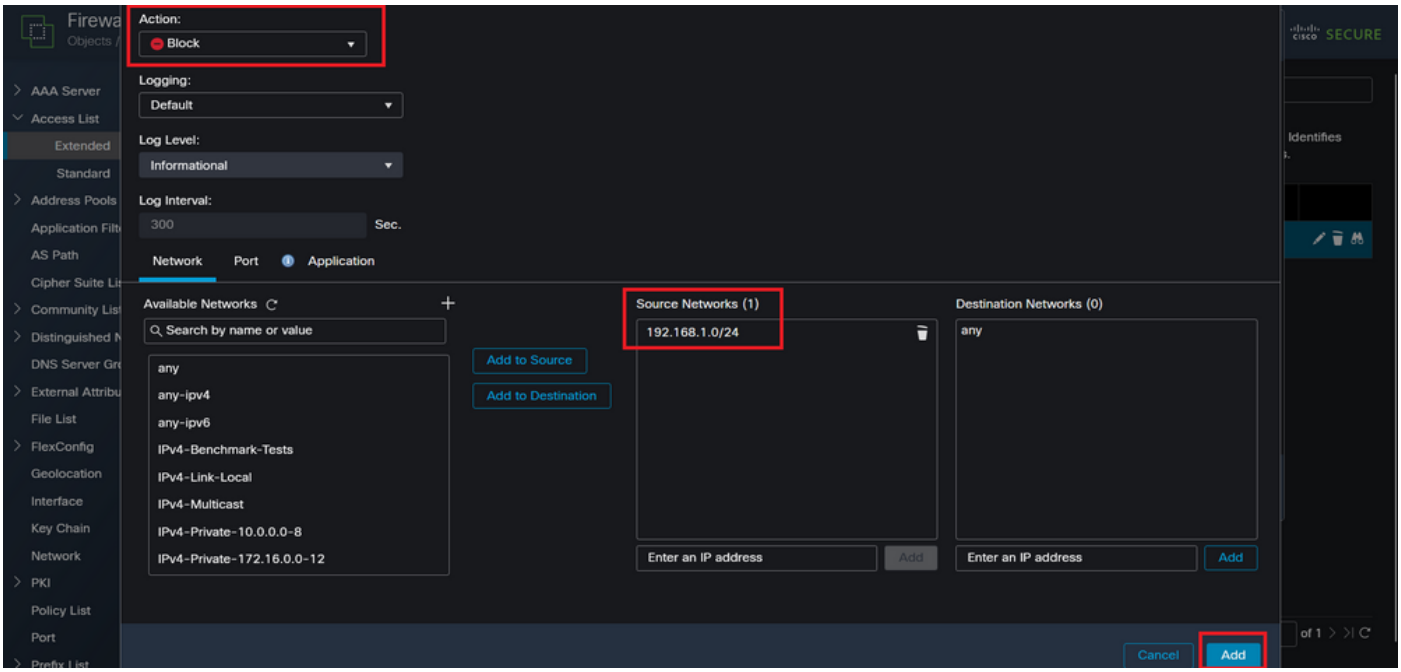

Image 8. Réseaux refusés

Étape 2.5. Si vous devez ajouter d'autres entrées ACE, cliquez à nouveau sur le bouton Add et répétez l'étape 2.4. Ensuite, cliquez sur le bouton Save (Enregistrer) pour terminer la configuration de la liste de contrôle d’accès.

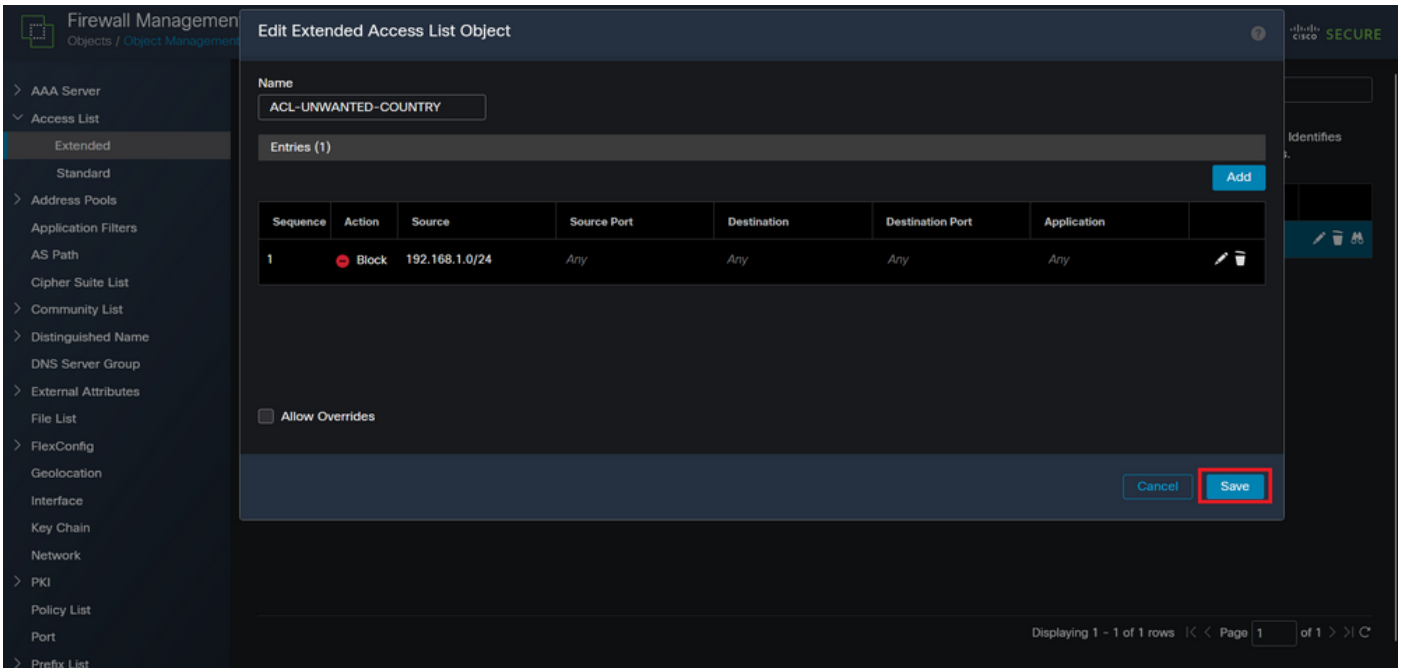

Image 9. Entrées ACL étendues terminées

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. Pour cela, accédez au panneau de gauche et sélectionnez l'option FlexConfig > FlexConfig Object.

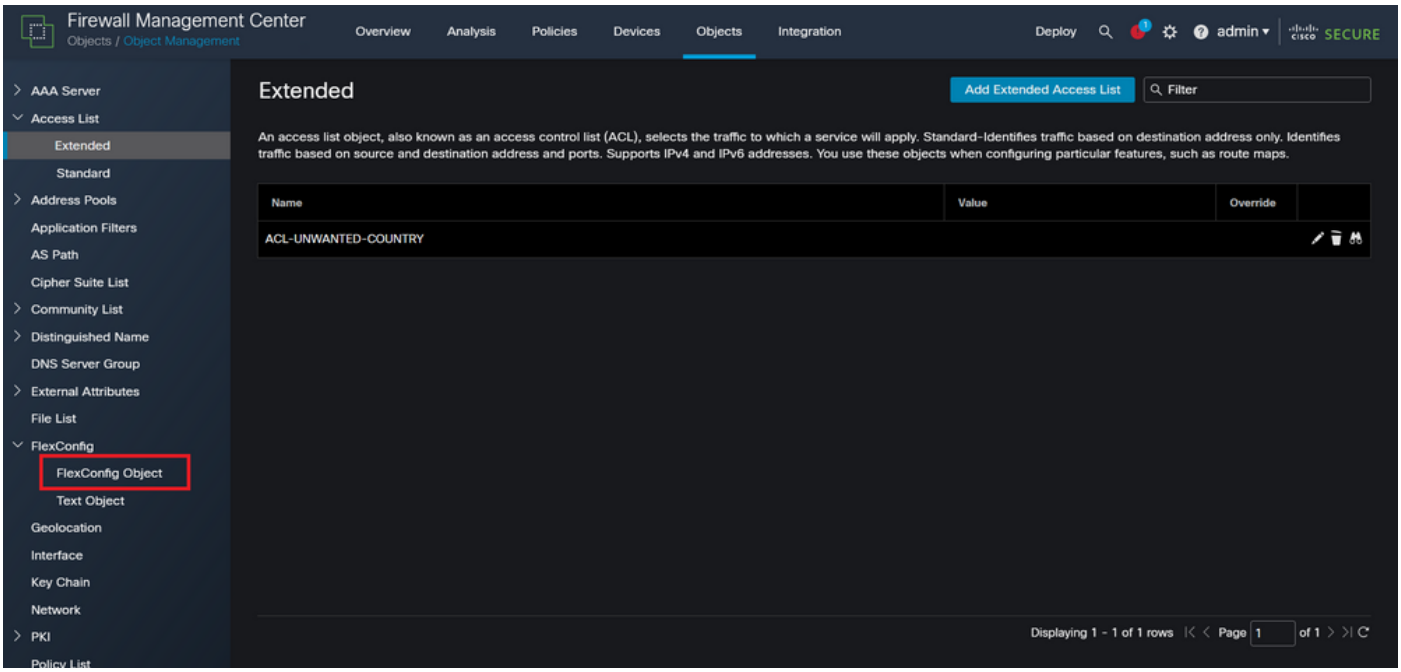

Image 10. Menu Objet FlexConfig

Étape 3.1. Cliquez sur Ajouter un objet FlexConfig.

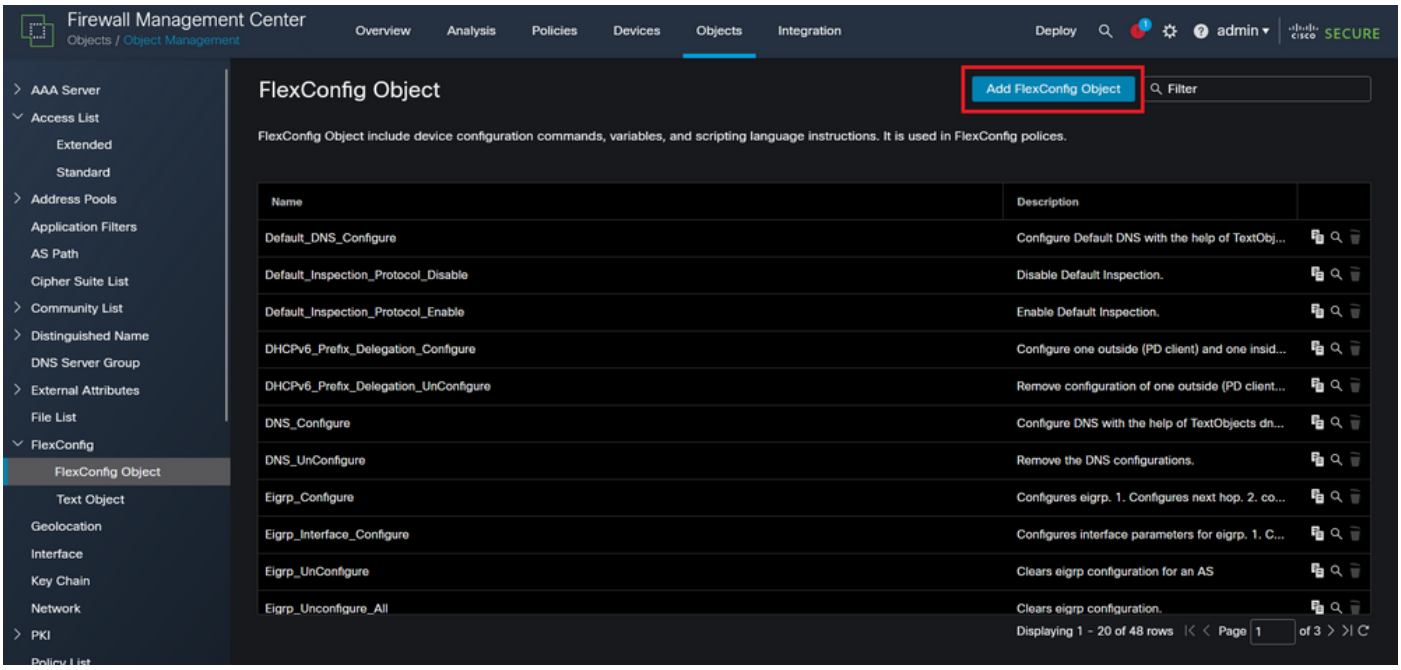

Image 11. Ajouter un objet Flexconfig

Étape 3.2. Ajoutez un nom pour l'objet FlexConfig, puis insérez un objet de stratégie ACL. Pour cela, sélectionnez Insert > Insert Policy Object > Extended ACL Object.

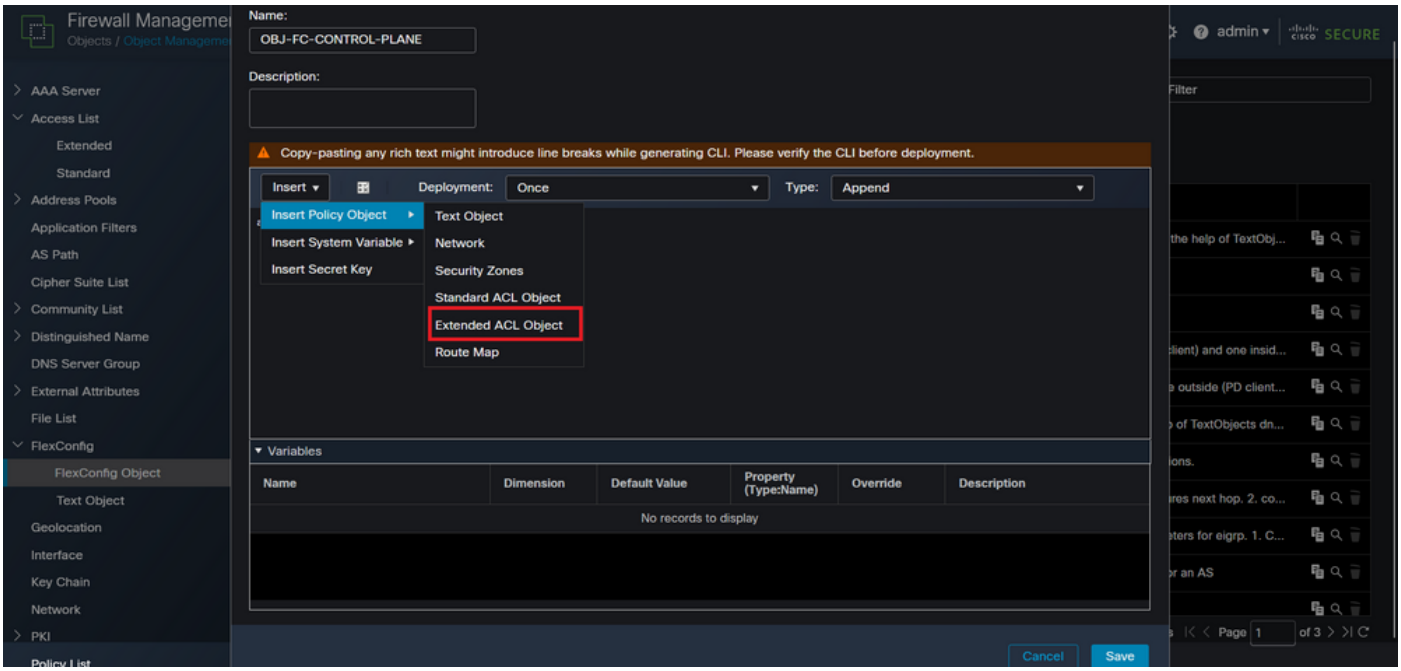

Image 12. Variable objet FlexConfig

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

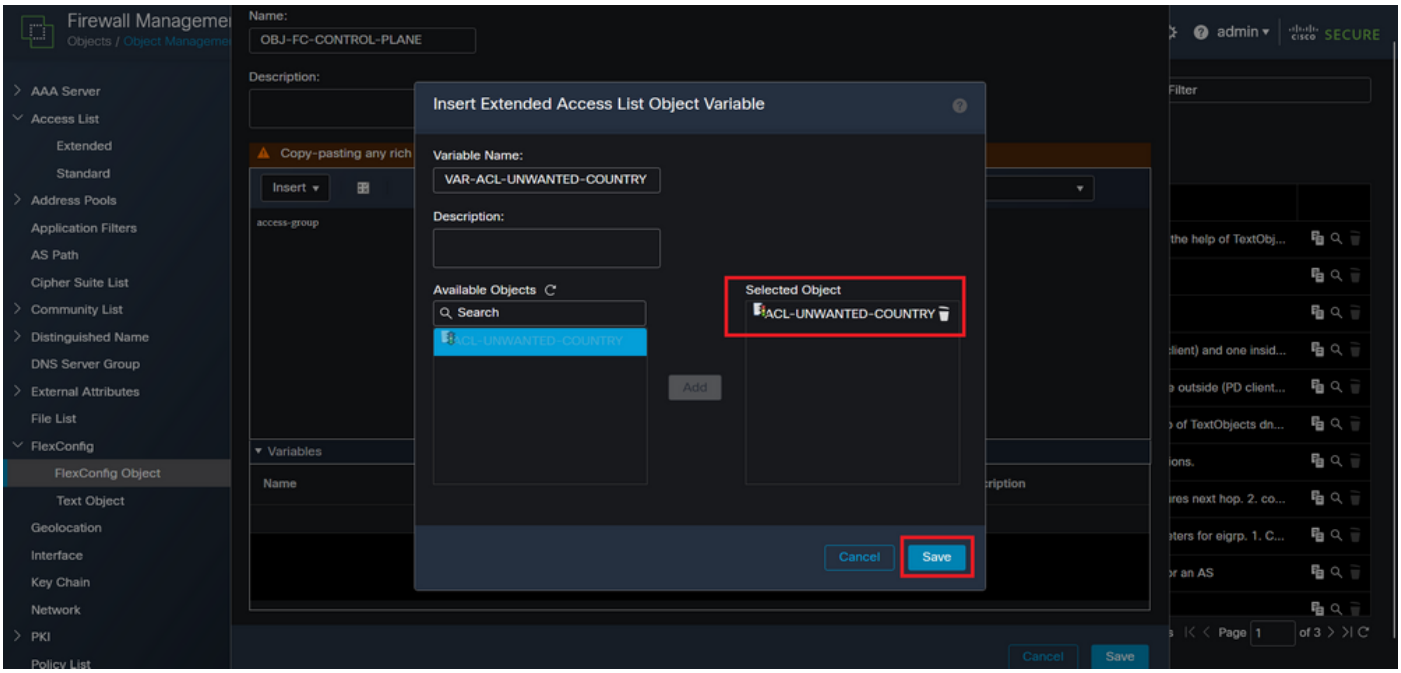

Image 13. FlexConfig, variable d'objet attribution ACL

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

Syntaxe de ligne de commande :

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

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

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

C'est ainsi qu'il doit être configuré dans la fenêtre d'objet FlexConfig, après quoi, sélectionnez le bouton Enregistrer pour terminer l'objet FlexConfig.

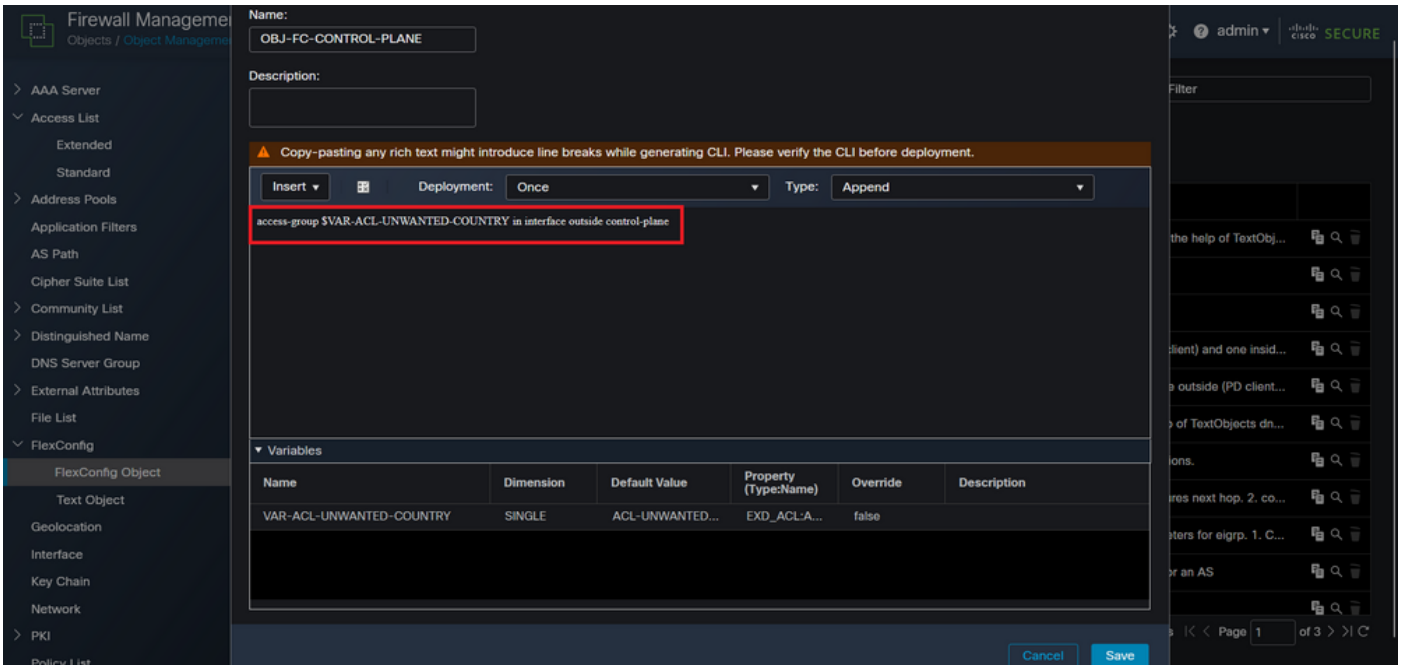

Image 14. Flexconfig, objet ligne de commande complète

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

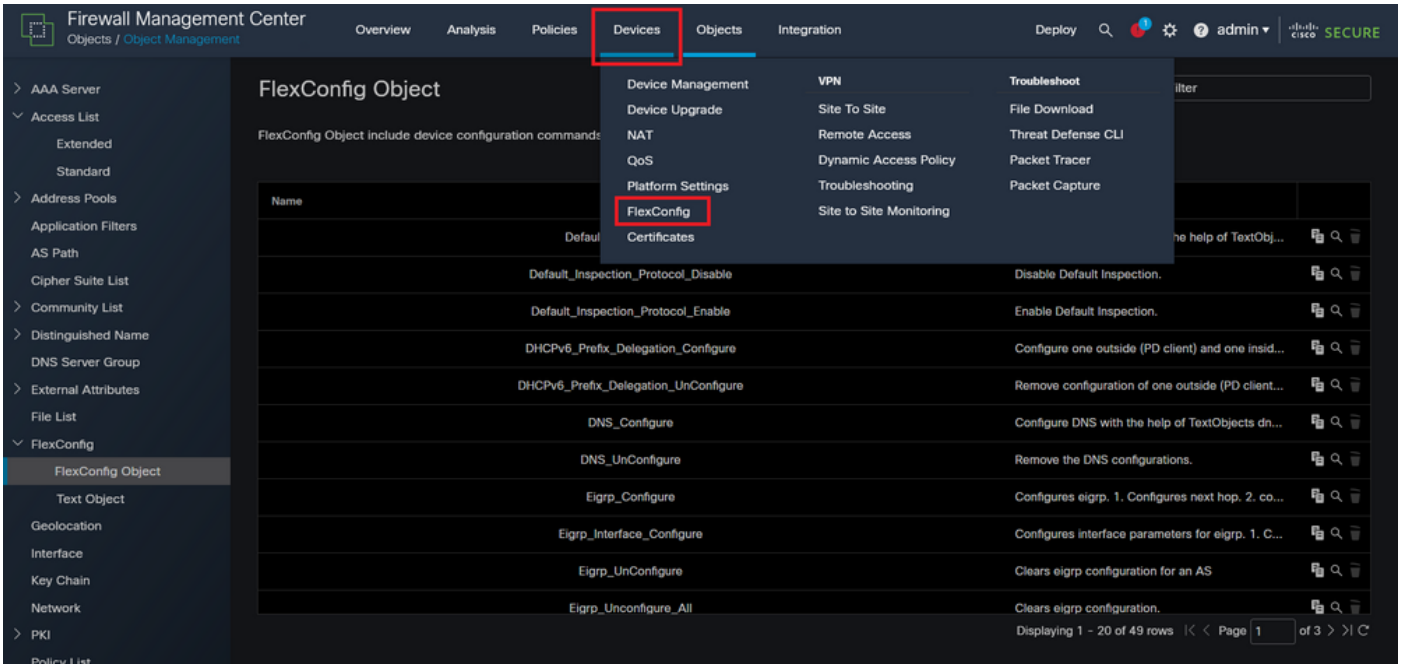

Image 15. Menu FlexConfig Policy

Étape 4.1. Cliquez ensuite sur New Policy (Nouvelle stratégie) si aucun FlexConfig n'a déjà été créé pour votre FTD, ou modifiez la stratégie FlexConfig existante.

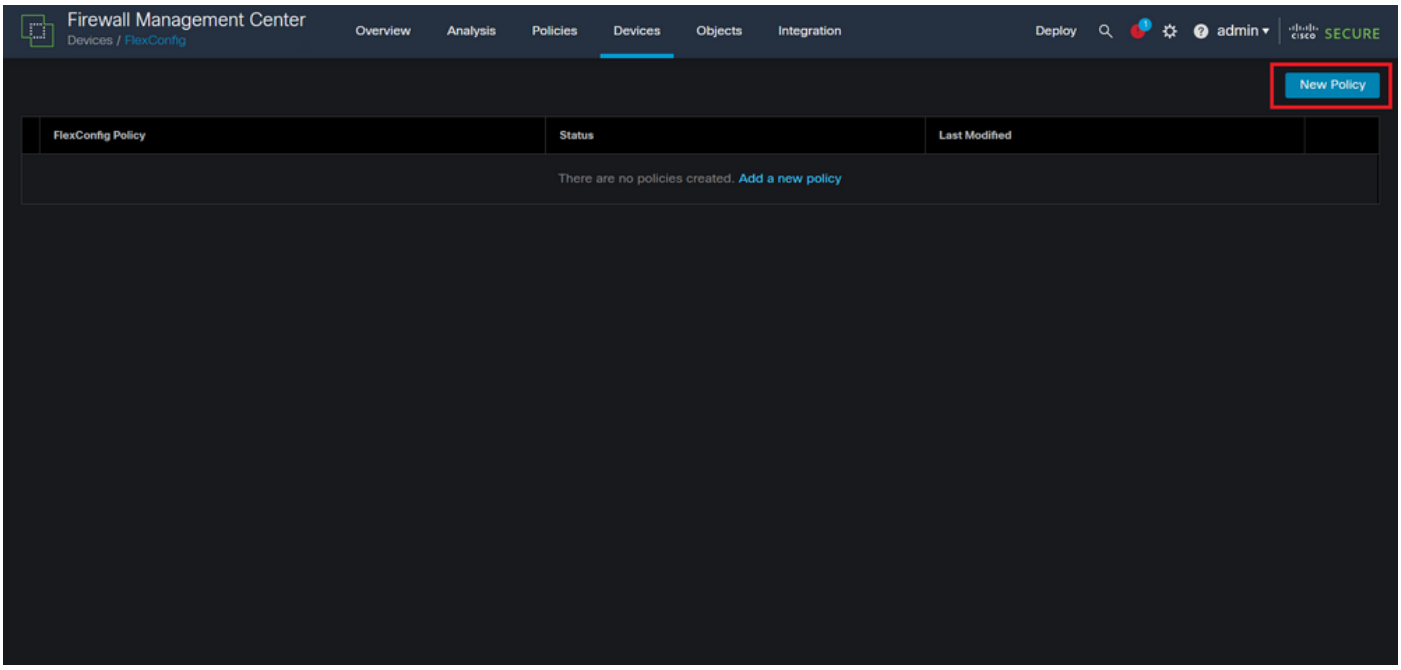

Image 16. Création de stratégie FlexConfig

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

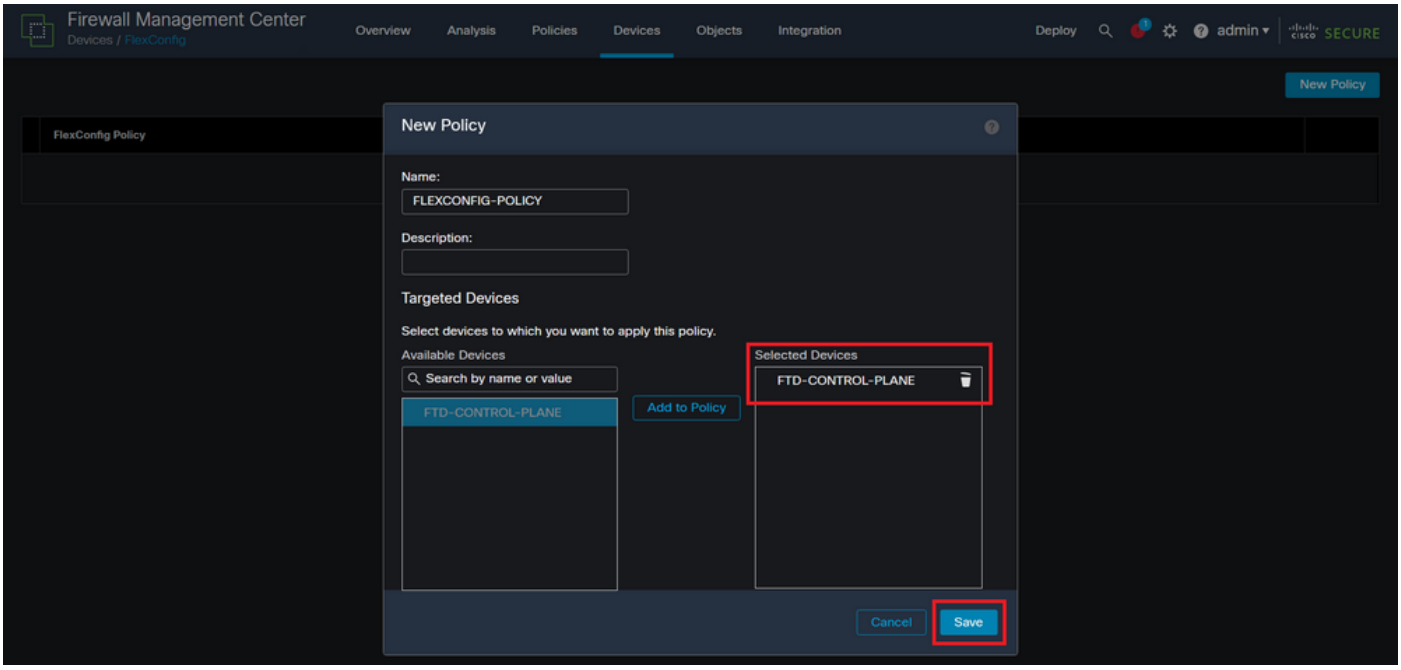

Image 17. Affectation de périphérique FlexConfig Policy

Étape 4.3. Dans le volet de gauche, recherchez l'objet FlexConfig créé à l'étape 3.2 ci-dessus, puis ajoutez-le à la stratégie FlexConfig en cliquant sur la flèche droite située au milieu de la fenêtre. Ensuite, cliquez sur le bouton Enregistrer.

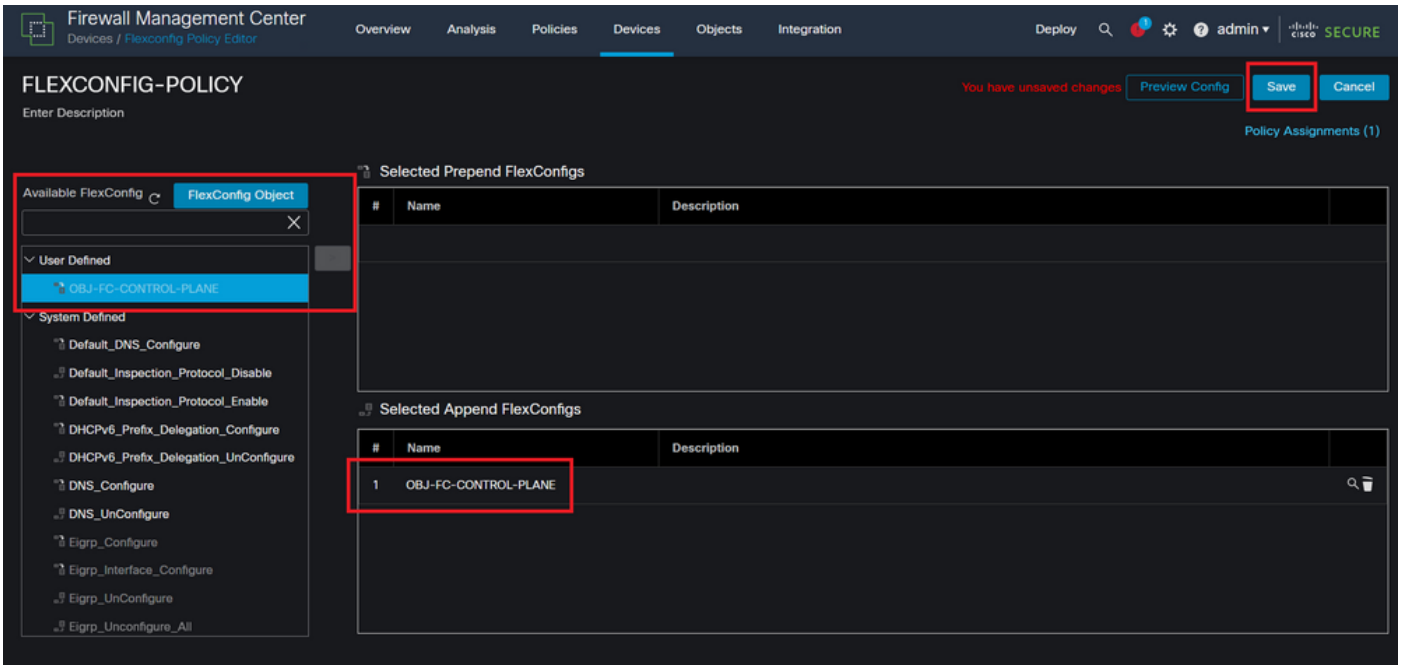

Image 18. Attribution d'objet Stratégie FlexConfig

Étape 5. Poursuivez le déploiement de la modification de configuration sur le FTD. Pour cela, accédez à Déployer > Déploiement avancé.

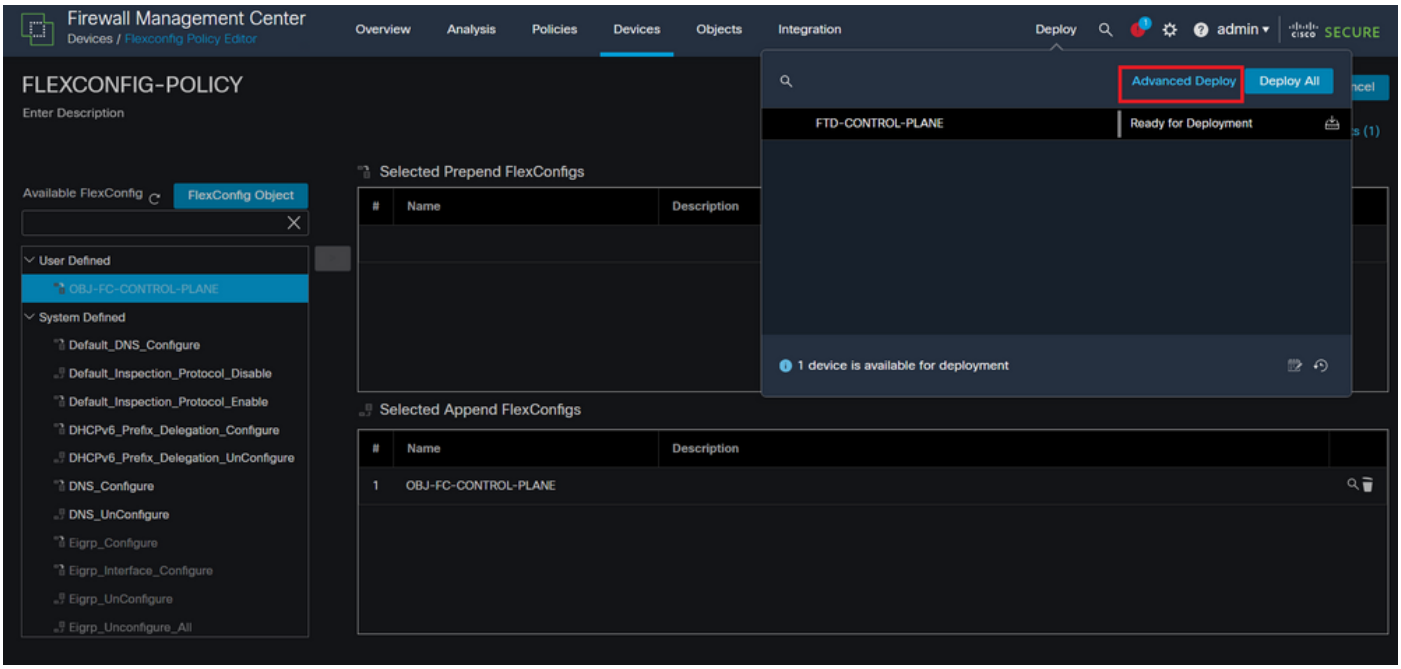

Image 19. Déploiement avancé FTD

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

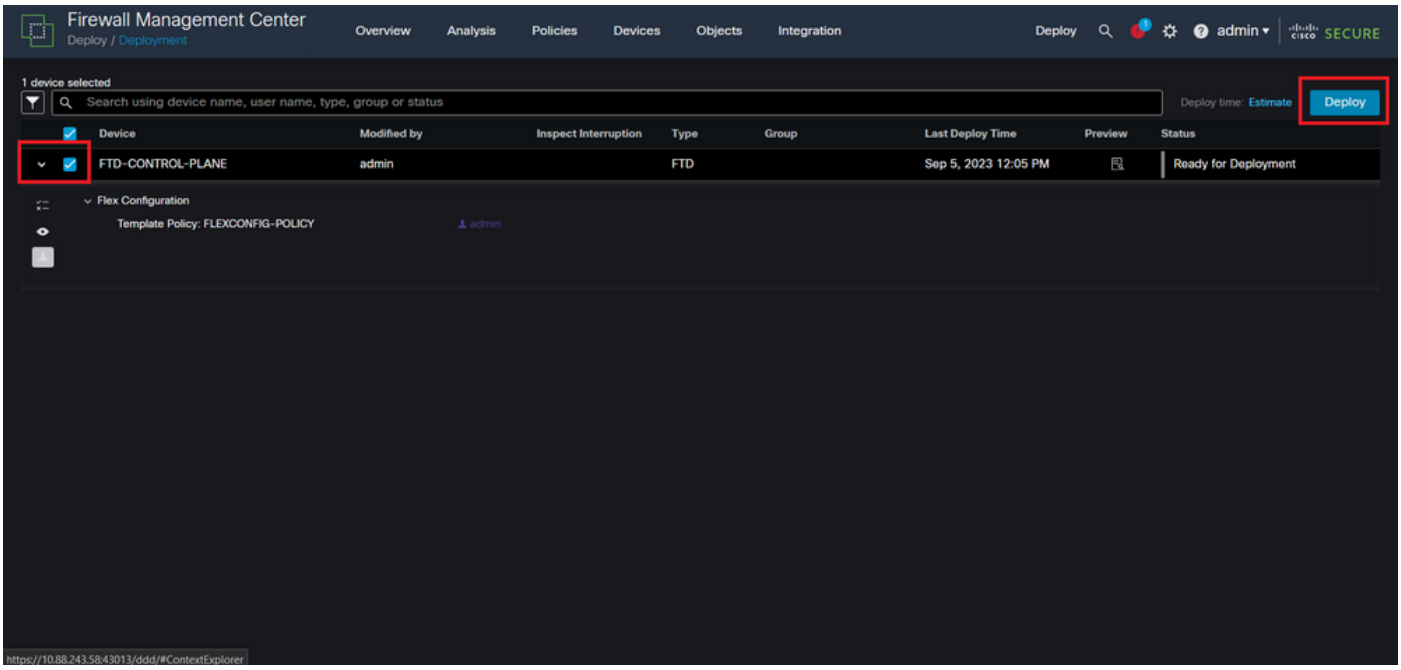

Image 20. Validation du déploiement FTD

Étape 5.2. Ensuite, une fenêtre de confirmation du déploiement s'affiche, ajoute un commentaire pour suivre le déploiement et passe à Déployer.

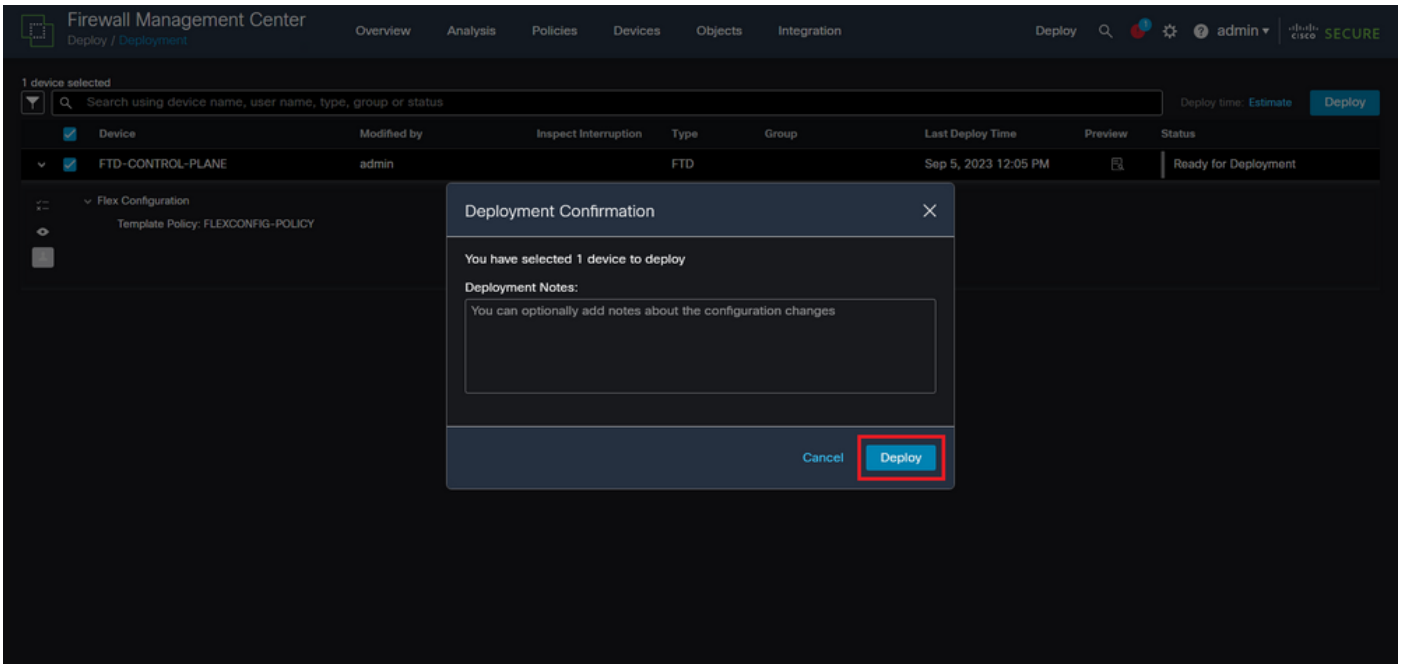

Image 21. Commentaires sur le déploiement FTD

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

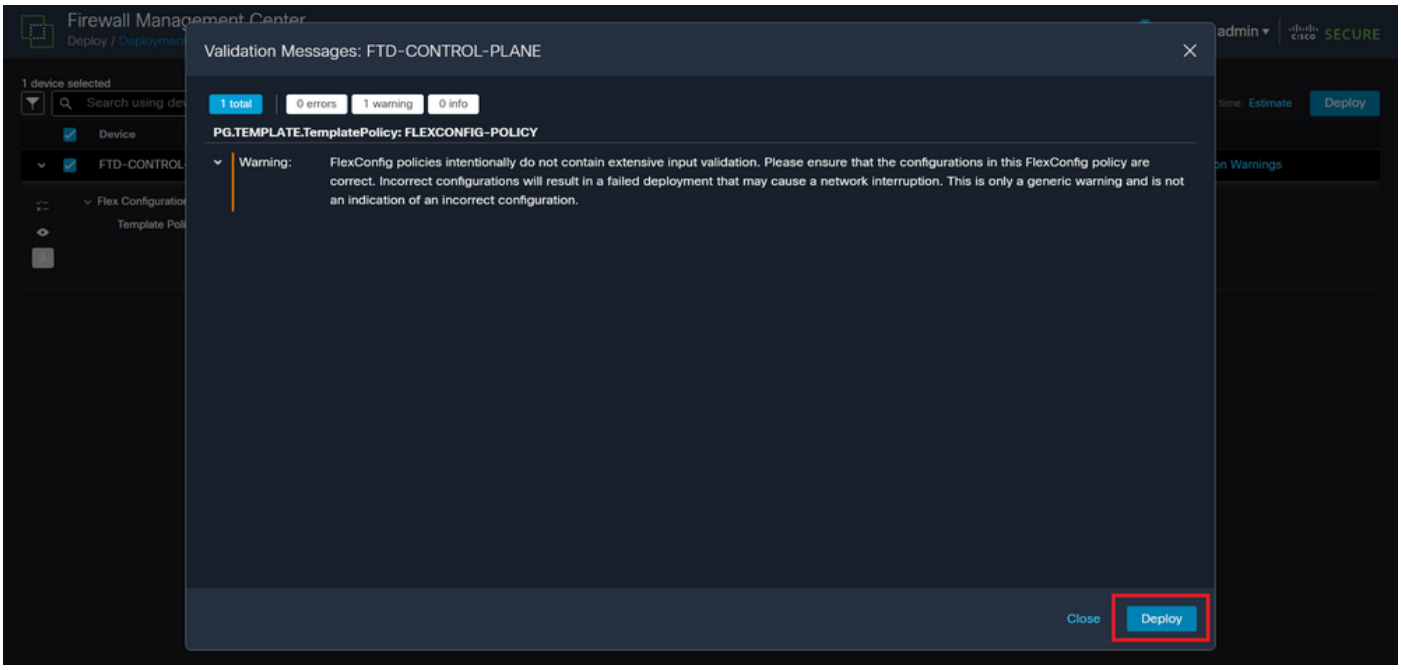

Image 22. Avertissement FTD Deployment Flexconfig

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

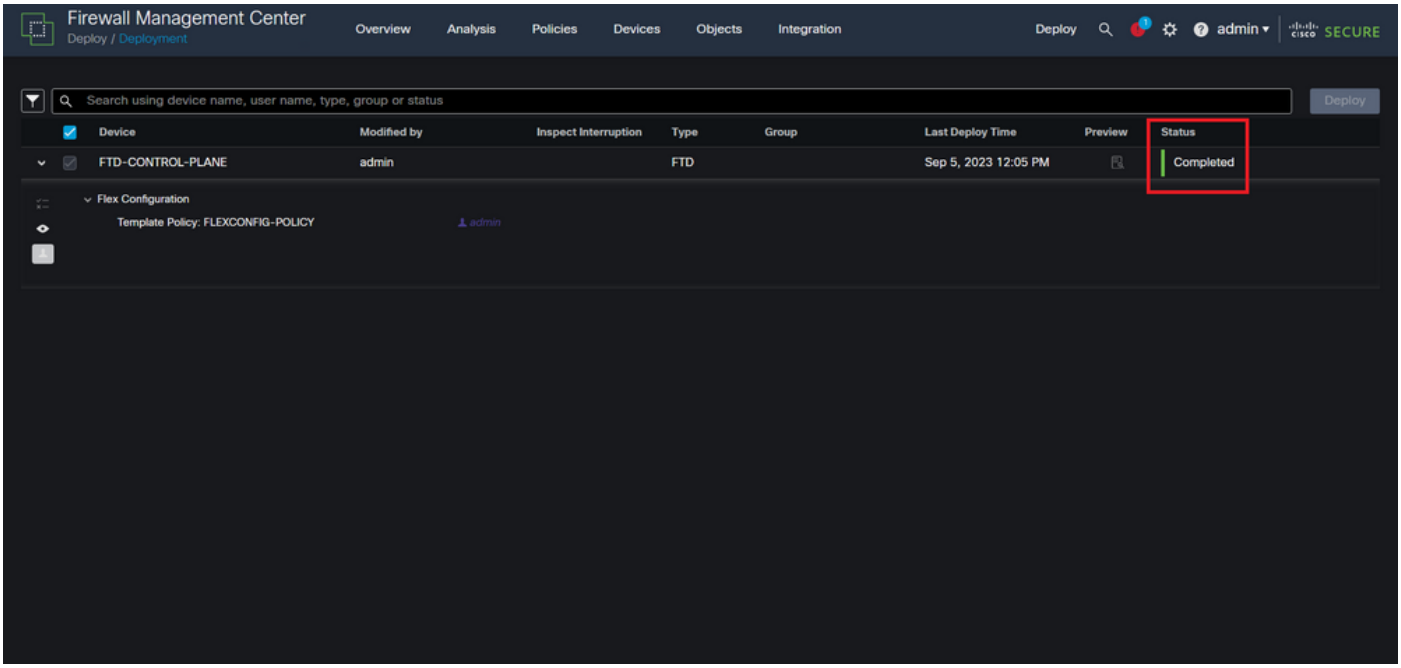

Image 23. Déploiement FTD réussi

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 en cours d'utilisation, il est important de souligner que les modifications de configuration apportées ne s'appliquent pas aux connexions déjà établies au FTD. Par conséquent, vous devez effacer manuellement les tentatives de connexion actives au FTD. Pour cela, connectez-vous à l'interface de ligne de commande du FTD et effacez les connexions actives comme suit.

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 fortement recommandé d'utiliser le mot clé « all » à la fin de la commande clear conn address pour forcer l'effacement des tentatives de connexion en force brute VPN actives vers le pare-feu sécurisé, principalement lorsque la nature de l'attaque en force brute VPN lance une rafale de tentatives de connexion constantes.

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

Voici la procédure que vous devez suivre dans 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.

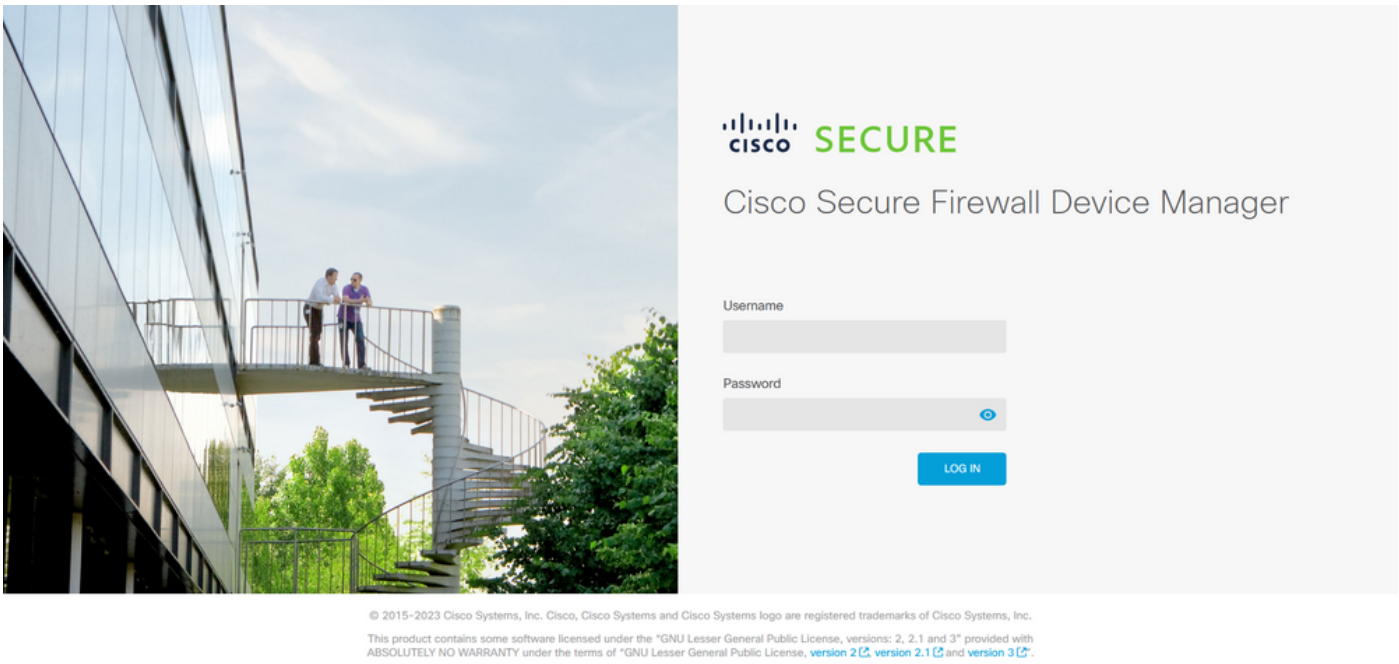

Image 24. Page Connexion à FDM

Étape 2. Vous devez créer un réseau d'objets. Pour cela, accédez à Objets :

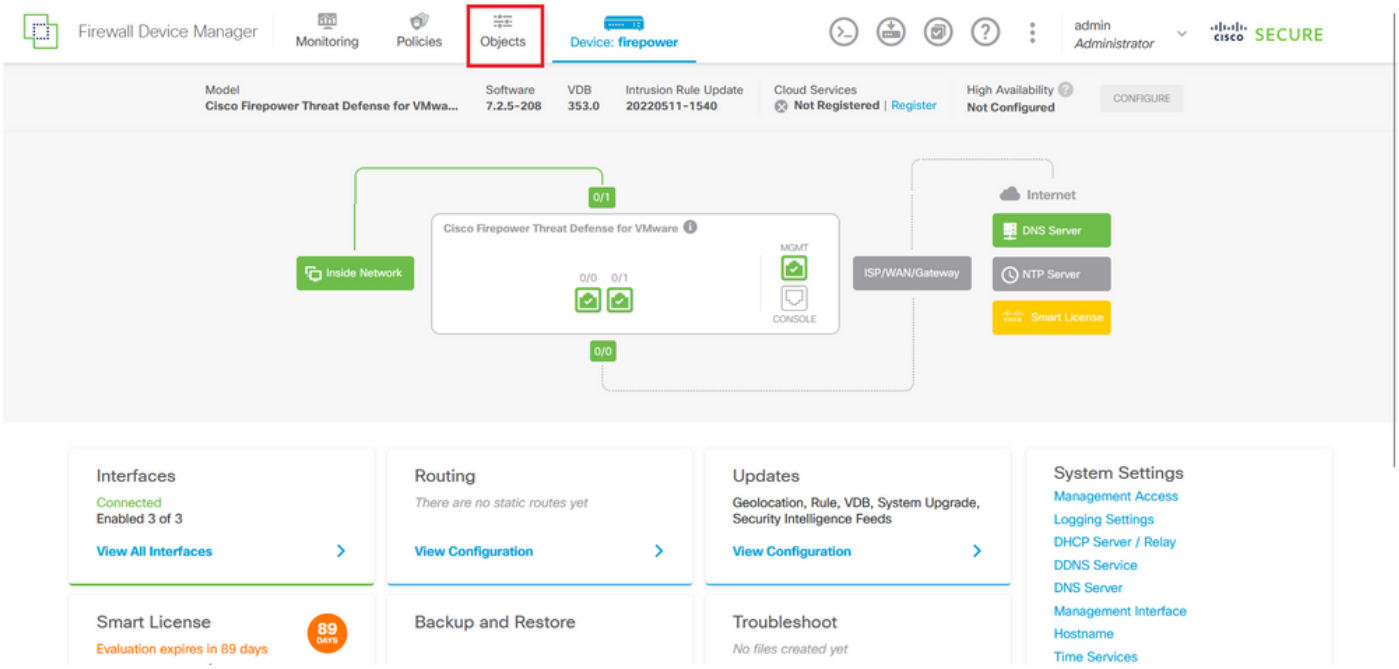

Image 25. Tableau de bord principal FDM

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

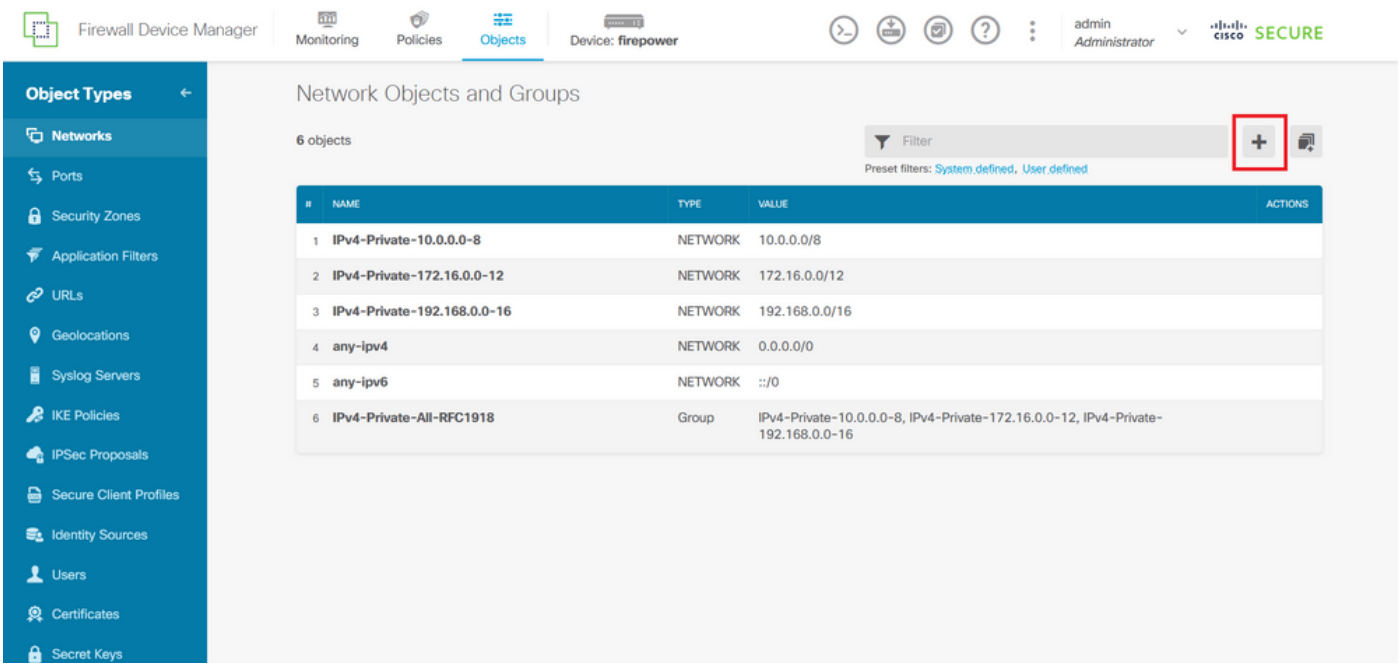

Image 26. Création d'objets

Étape 2.2. Ajoutez un nom pour l'objet réseau, sélectionnez le type de réseau pour l'objet, ajoutez l'adresse IP, l'adresse réseau ou la plage d'adresses IP pour faire correspondre le 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 de VPN provenant du sous-réseau 192.168.1.0/24.

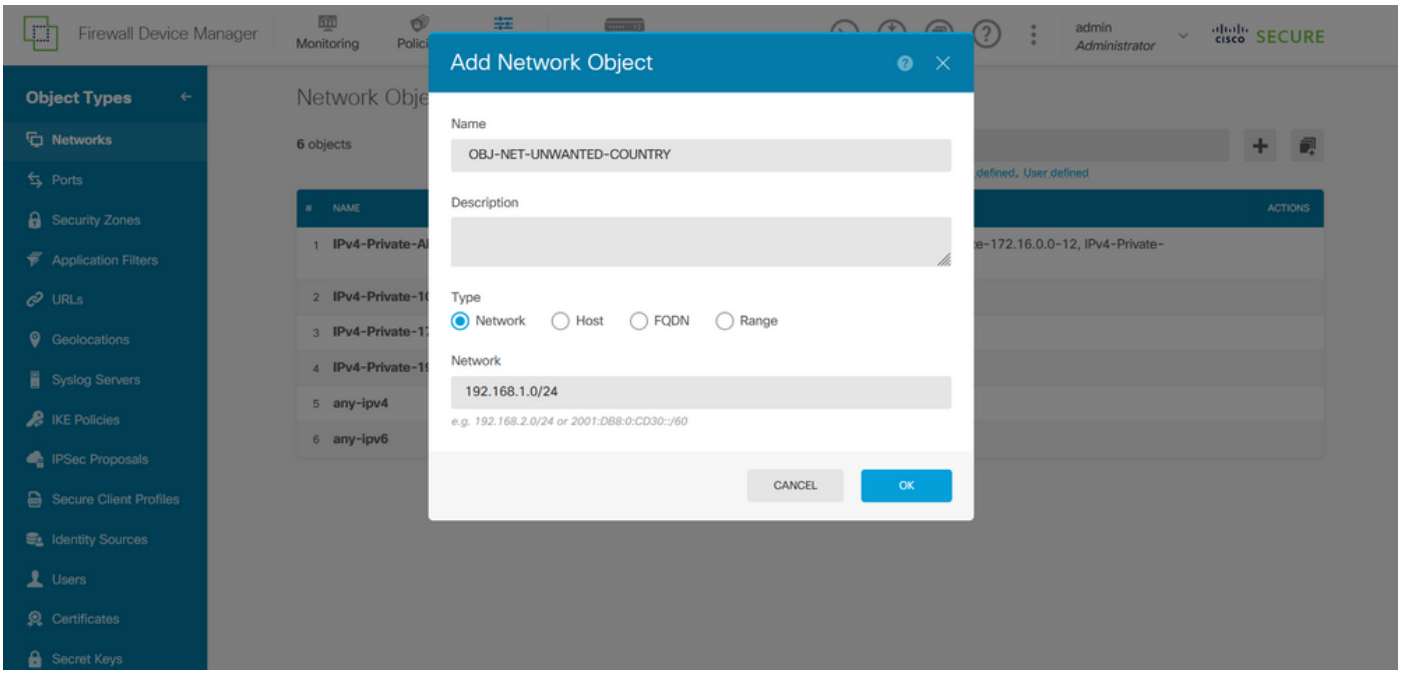

Image 27. Ajouter un objet réseau

Étape 3. Ensuite, vous devez créer une liste de contrôle d'accès étendue. Pour cela, accédez à l'onglet Device du menu supérieur.

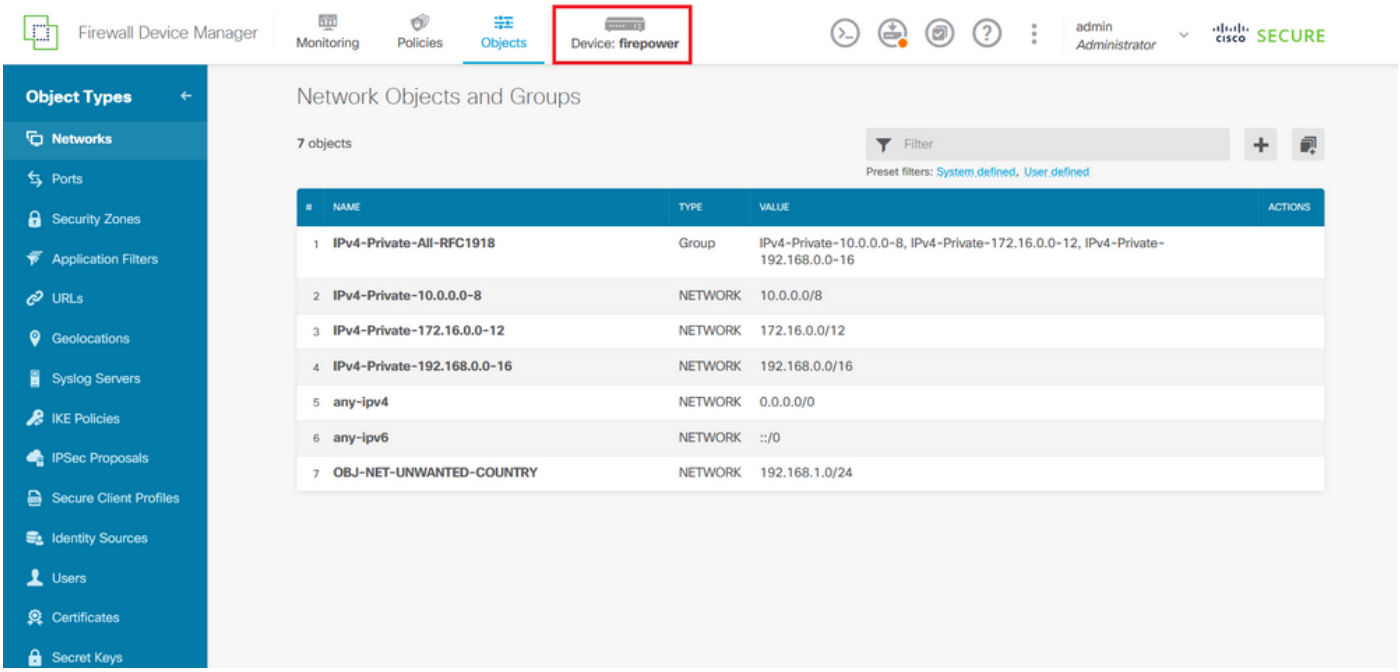

Image 28. Page Paramètres du périphérique

Étape 3.1. Faites défiler vers le bas et sélectionnez Afficher la configuration dans le carré Configuration avancée comme suit.

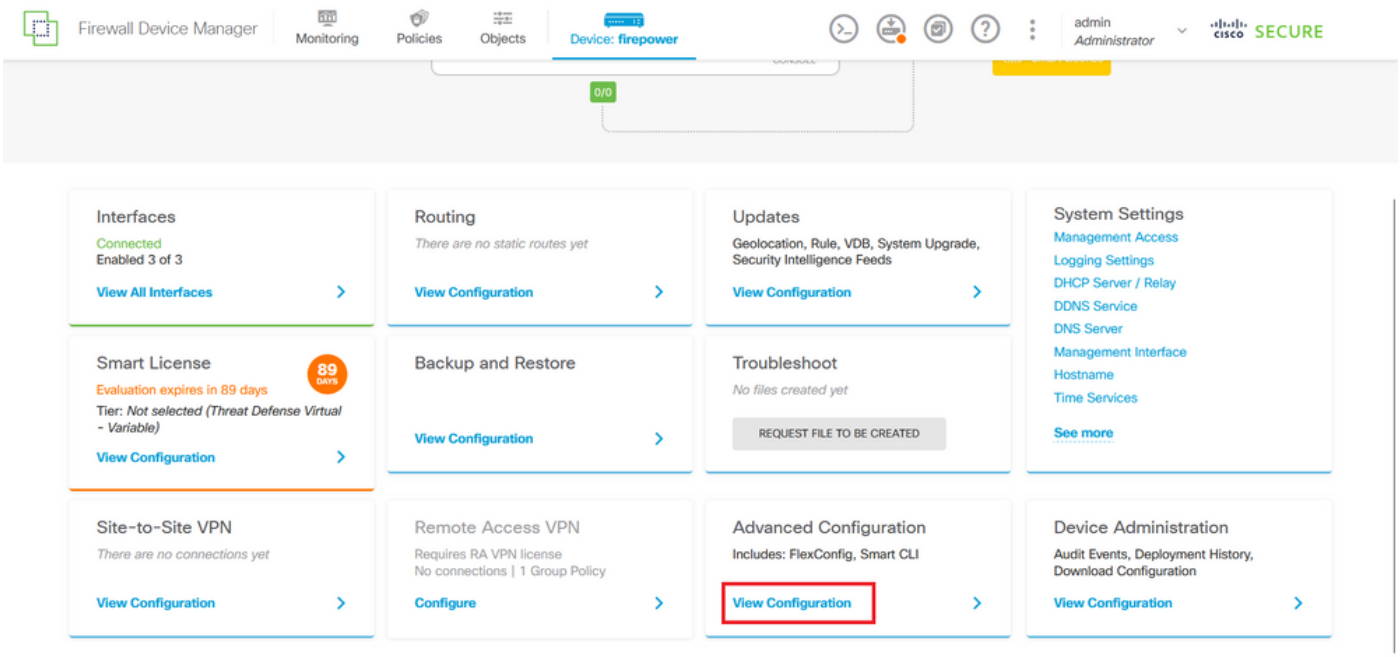

Image 29. Configuration avancée de FDM

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

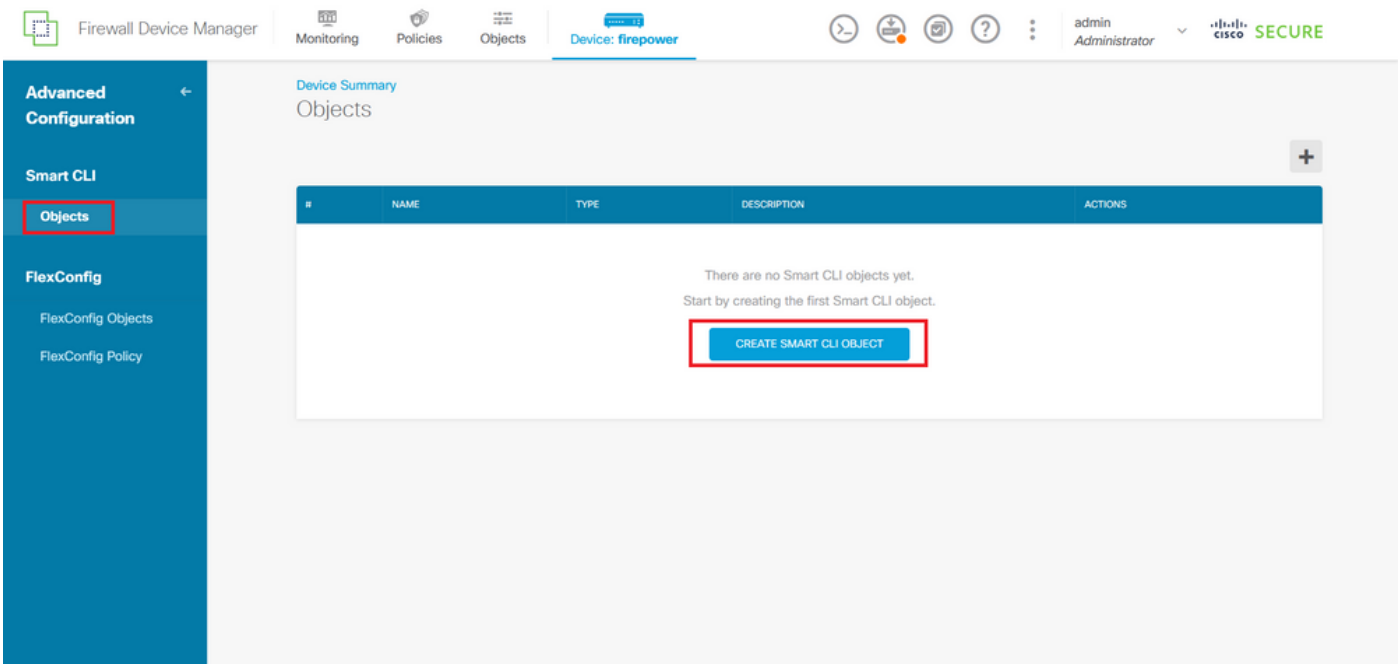

Image 30. Objets Smart CLI

Étape 3.3. Ajoutez un nom à la liste de contrôle d'accès étendue à créer, sélectionnez Liste d'accès étendue dans le menu déroulant du modèle CLI, puis configurez les ACE requises à l'aide de l'objet réseau créé à l'étape 2.2 ci-dessus, puis cliquez sur le bouton OK pour terminer la liste de contrôle d'accès.

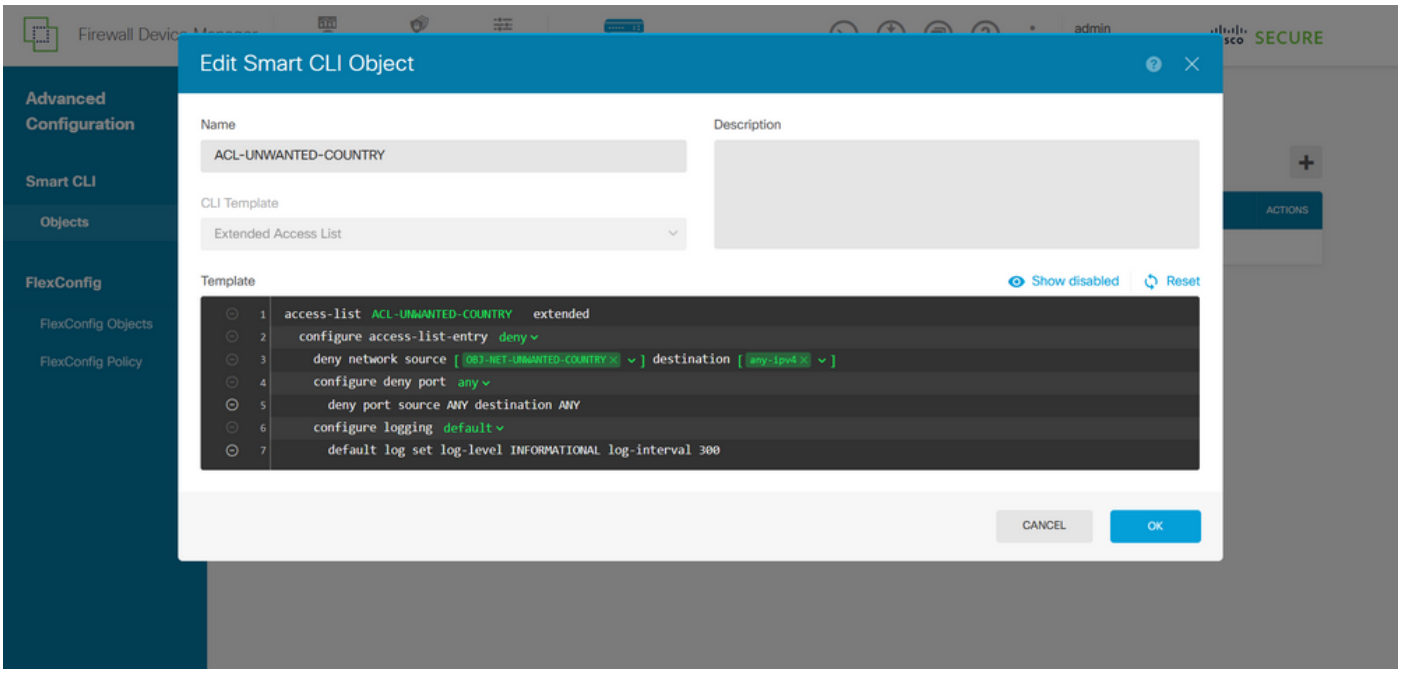

Image 31. Création ACL étendue

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 ; trois points cliquables s'affichent alors. Cliquez dessus et sélectionnez Dupliquer pour ajouter d'autres ACE.

Étape 4. Ensuite, vous devez créer un objet FlexConfig, pour cela, naviguez vers le panneau de gauche et sélectionnez FlexConfig > Objets FlexConfig, puis cliquez sur CREATE FLEXCONFIG OBJECT.

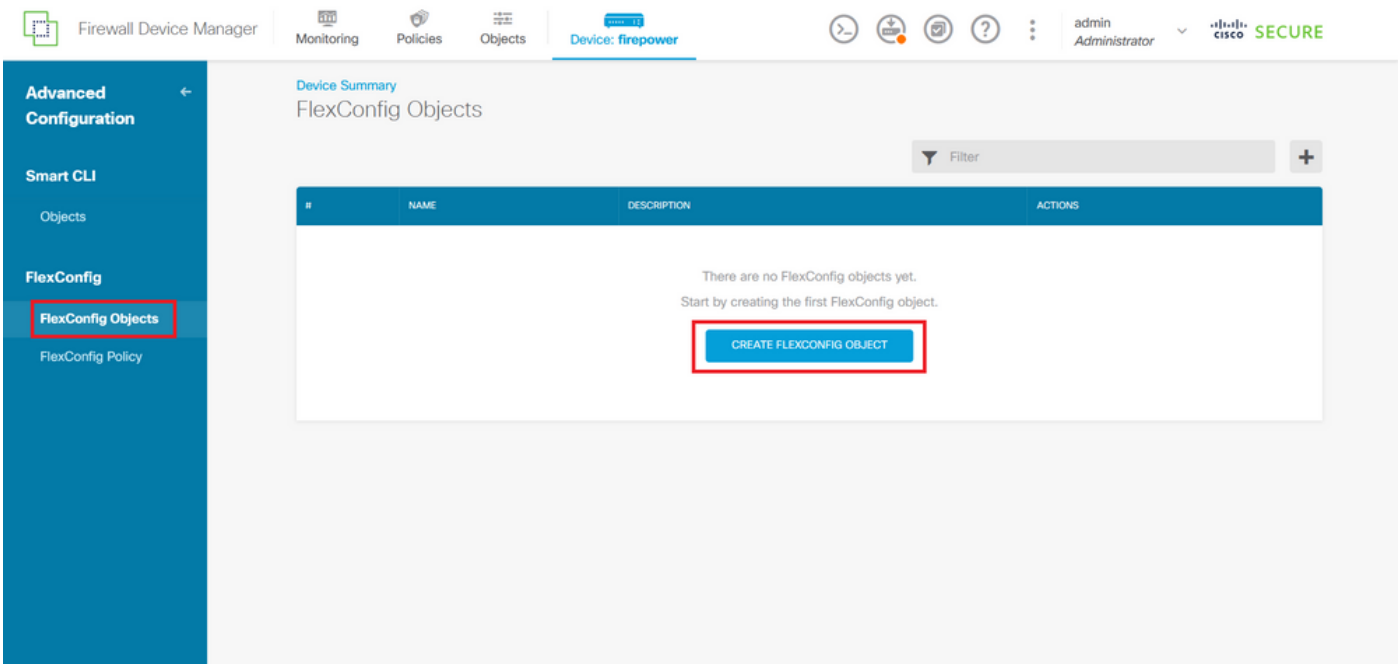

Image 32. Objets FlexConfig

Étape 4.1. Ajoutez un nom à l'objet FlexConfig pour créer et configurer la liste de contrôle d'accès

du plan de contrôle comme entrant pour l'interface externe comme suit.

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 ci-dessus « ACL-UNWANTED-COUNTRY » comme suit :

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

C'est ainsi qu'il doit être configuré dans la fenêtre d'objet FlexConfig, après quoi, sélectionnez le bouton OK pour terminer l'objet FlexConfig.

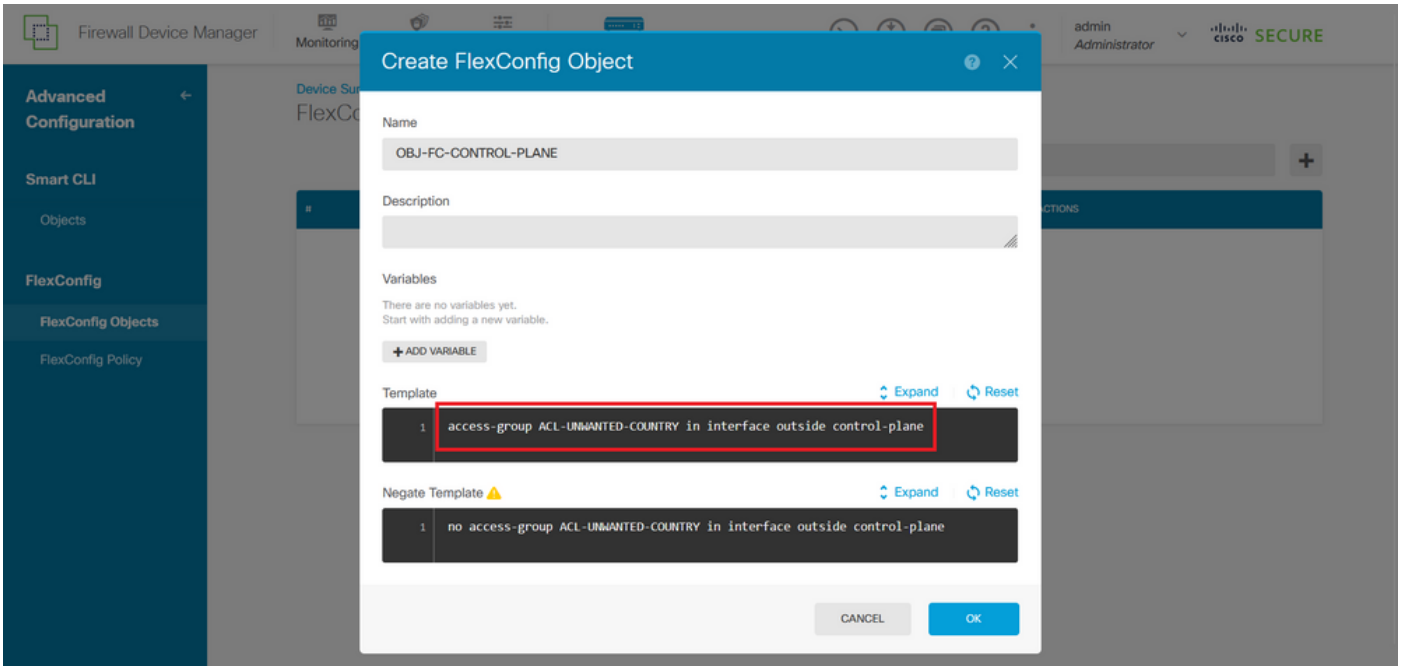

Image 33. Création d'objet FlexConfig

Étape 5. Continuez à créer une politique FlexConfig, pour cela, accédez à Flexconfig > FlexConfig Policy, cliquez sur le bouton '+', et sélectionnez l'objet FlexConfig qui a été créé à l'étape 4.1 ci-dessus.

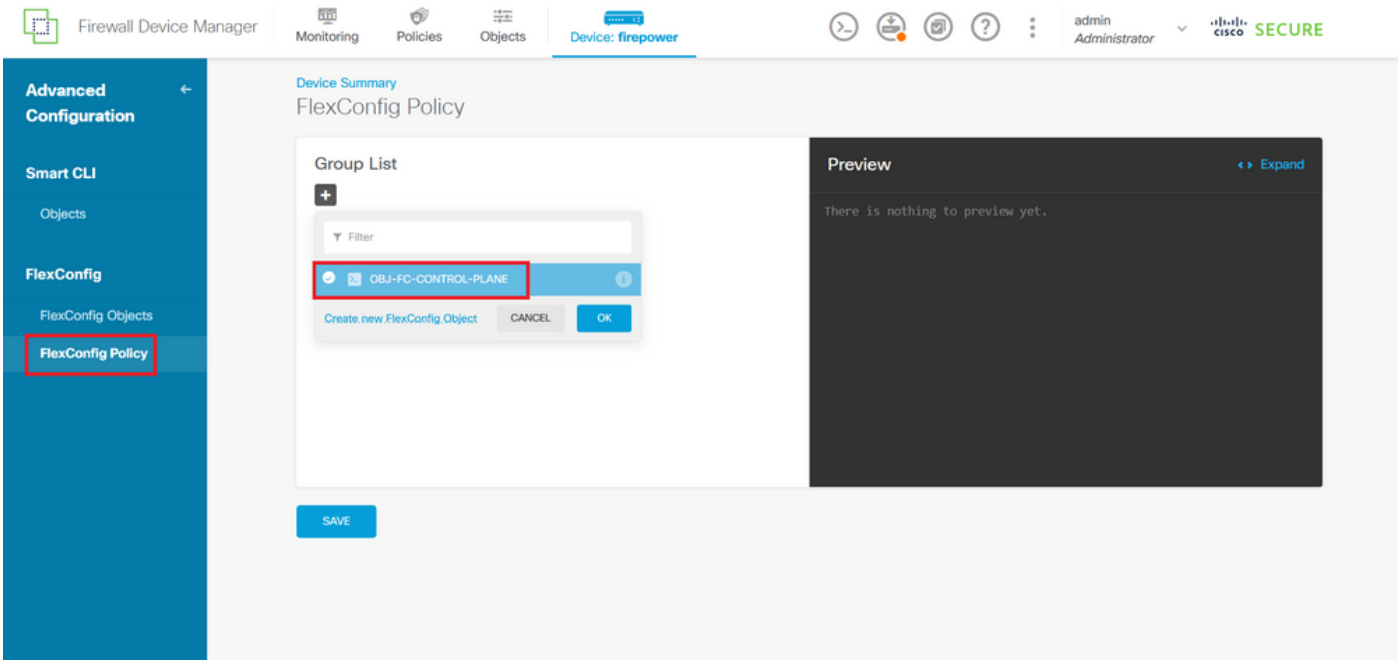

Image 34. Politique FlexConfig

Étape 5.1. Vérifiez que l'aperçu de FlexConfig affiche la configuration correcte pour la liste de contrôle d'accès du plan de contrôle créée et cliquez sur le bouton Save (Enregistrer).

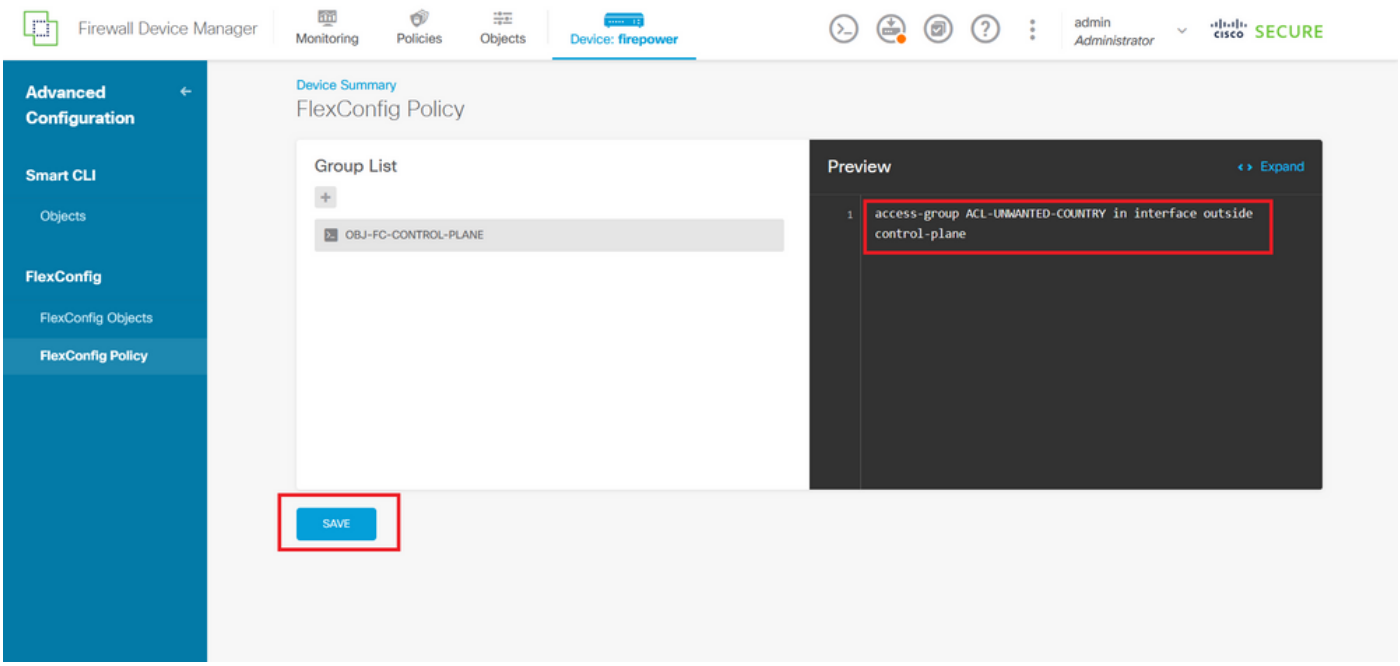

Image 35. Aperçu de la stratégie FlexConfig

Étape 6. Déployez les modifications de configuration sur le FTD que vous souhaitez protéger contre les attaques en force VPN. Pour cela, cliquez sur le bouton Déploiement dans le menu supérieur, vérifiez que les modifications de configuration à déployer sont correctes, puis cliquez sur DÉPLOYER MAINTENANT.

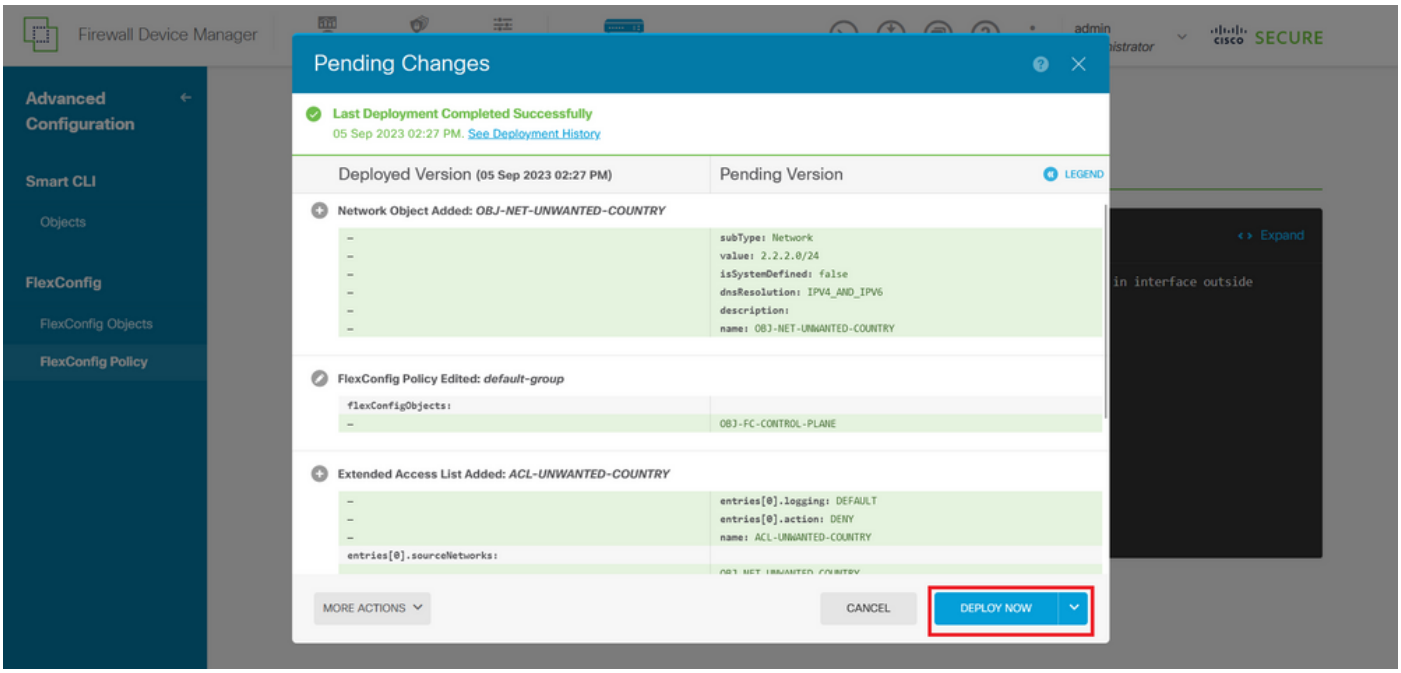

Image 36. Déploiement en attente

Étape 6.1. Vérifiez que le déploiement de la stratégie a réussi.

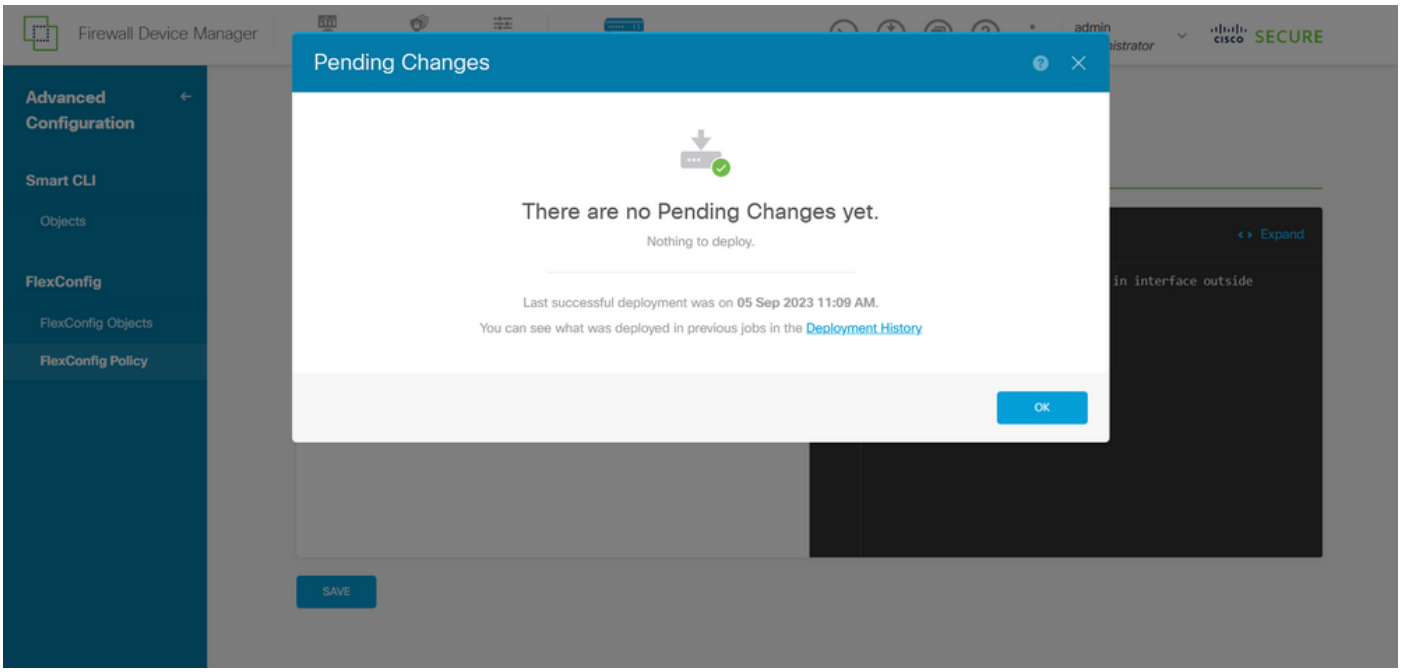

Image 37. Déploiement réussi

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 en cours d'utilisation, il est important de souligner que les modifications de configuration apportées ne s'appliquent pas aux connexions déjà établies au FTD. Par conséquent, vous devez effacer manuellement les tentatives de connexion actives au FTD. Pour cela, connectez-vous à l'interface de ligne de commande du FTD et effacez les connexions actives comme suit.

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 fortement recommandé d'utiliser le mot clé « all » à la fin de la commande clear conn address pour forcer l'effacement des tentatives de connexion en force brute VPN actives vers le pare-feu sécurisé, principalement lorsque la nature de l'attaque en force brute VPN lance une rafale de tentatives de connexion constantes.

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

Voici la procédure à suivre dans une interface de ligne de commande ASA pour configurer une liste de contrôle d'accès du plan de contrôle pour bloquer les attaques en force entrantes du VPN vers l'interface externe :

Étape 1. Connectez-vous au pare-feu sécurisé ASA via l'interface de ligne de commande et accédez au « terminal de configuration » comme suit.

```
asa# configure terminal
```

Étape 2. Utilisez la commande suivante pour configurer une liste de contrôle d'accès étendue afin de bloquer 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 brute 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. Utilisez la commande next 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
```

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, alors il est important de souligner que les modifications de configuration apportées ne s'appliquent pas aux connexions déjà établies à l'ASA, par conséquent, vous devez effacer manuellement les tentatives de connexion active à l'ASA. Pour cela, effacez les connexions actives comme suit.

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 fortement recommandé d'utiliser le mot clé « all » à la fin de la commande clear conn address pour forcer l'effacement des tentatives de connexion en force brute VPN actives vers le pare-feu sécurisé, principalement lorsque la nature de l'attaque en force brute VPN lance une rafale de tentatives de connexion constantes.

Configuration alternative pour bloquer les attaques du pare-feu sécurisé à l'aide de la commande « shun »

En cas d'option immédiate de blocage des attaques pour le pare-feu sécurisé, vous pouvez alors

utiliser la commande « shun ». La commande hunvous permet de bloquer les connexions d'un hôte attaquant.

- Une fois l'adresse IP désactivée, toutes les connexions futures à partir de l'adresse IP source sont abandonnées et consignées jusqu'à ce que la fonction de blocage soit supprimée manuellement.

- La fonction de blocage de la commande hunest appliquée qu'une connexion avec l'adresse hôte spécifiée soit active ou non.

- Si vous spécifiez l'adresse de destination, les ports source et de destination, ainsi que le protocole, vous supprimez la connexion correspondante et vous placez un shun sur toutes les futures connexions à partir de l'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 hunpar adresse IP source.

- Comme la commande hunest 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, utilisez la forme no de cette commande :

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

Pour désactiver une adresse IP d'hôte, procédez comme suit 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 appliquez la commande shun comme suit.

```
<#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 utiliser les commandes show suivantes 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 comme suit.

```
<#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 utiliser les commandes show suivantes pour confirmer les adresses IP de shun dans l'ASA et pour surveiller le nombre d'occurrences 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, consultez le document Cisco Secure Firewall Threat Defense Command Reference

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, utilisez la commande packet-tracer pour simuler une connexion TCP 443 entrante à l'interface externe du pare-feu sécurisé, puis utilisez la commande show access-list <acl-name> , le nombre d'occurrences de la liste de contrôle d'accès doit s'incrémenter 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 de notre pare-feu sécurisé. Le résultat « packet-tracer » confirme que le trafic est abandonné et le résultat « show access-list »

affiche les incréments du nombre de succès pour notre ACL de 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 résultat 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 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

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.