Calculer le nombre d'éléments de liste d'accès à l'aide de FMC CLI

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Calcul du nombre d'éléments de liste d'accès (ACE) à l'aide de FMC CLI

Impact d'un ACE élevé

Choix du moment d'activation de la recherche de groupe d'objets (OGS)

Activation de la recherche de groupes d'objets

Vérifier

Informations connexes

Introduction

Ce document décrit comment trouver quelle règle de votre stratégie de contrôle d'accès s'étend au nombre d'éléments de la liste d'accès.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de la technologie Firepower
- Connaissances sur la configuration des politiques de contrôle d’accès sur FMC

Composants utilisés

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

- Cisco Secure Firewall Management Center (FMC)
- Cisco Firepower Threat Defense (FTD)

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

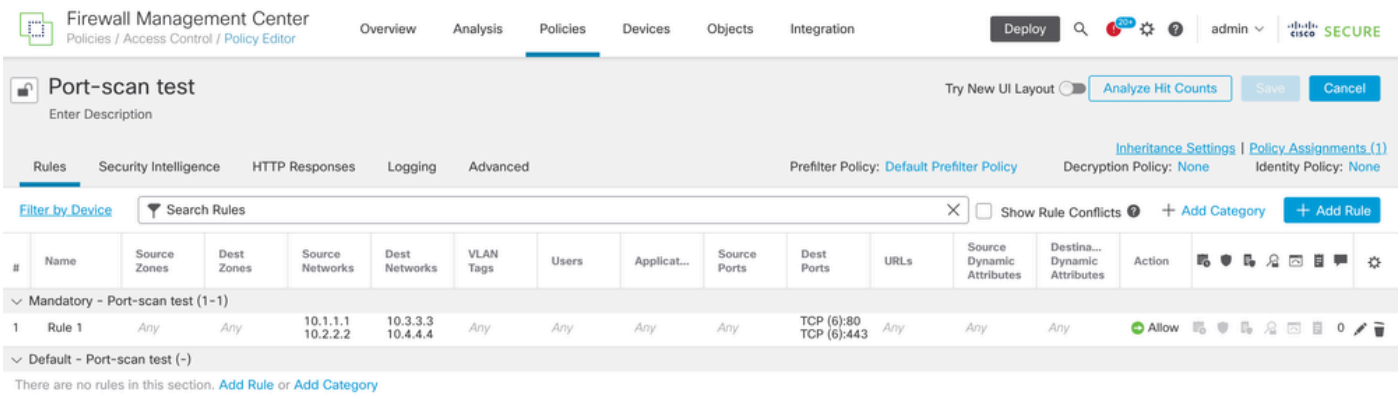
Une règle de contrôle d'accès est créée à l'aide d'une ou de plusieurs combinaisons de ces paramètres :

- Adresse IP (source et destination)
- Ports (source et destination)
- URL (catégories fournies par le système et URL personnalisées)
- Détecteurs d'applications
- Réseaux locaux virtuels (VLAN)
- Zones

En fonction de la combinaison des paramètres utilisés dans la règle d'accès, l'extension de la règle change sur le capteur. Ce document met en évidence diverses combinaisons de règles sur le FMC et leurs extensions respectives associées sur les capteurs.

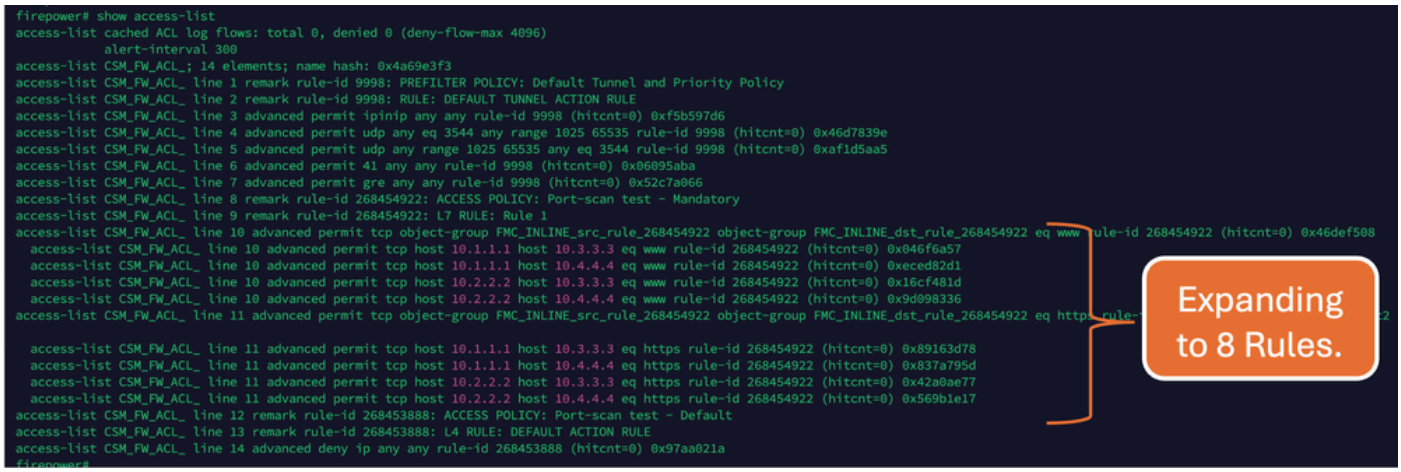
Calcul du nombre d'éléments de liste d'accès (ACE) à l'aide de FMC CLI

Examinez la configuration d'une règle d'accès à partir du FMC, comme illustré dans l'image :



Configuration des règles dans la stratégie de contrôle d'accès

Si vous voyez cette règle dans l'interface de ligne de commande du FTD, vous remarquerez qu'elle a été étendue à 8 règles.



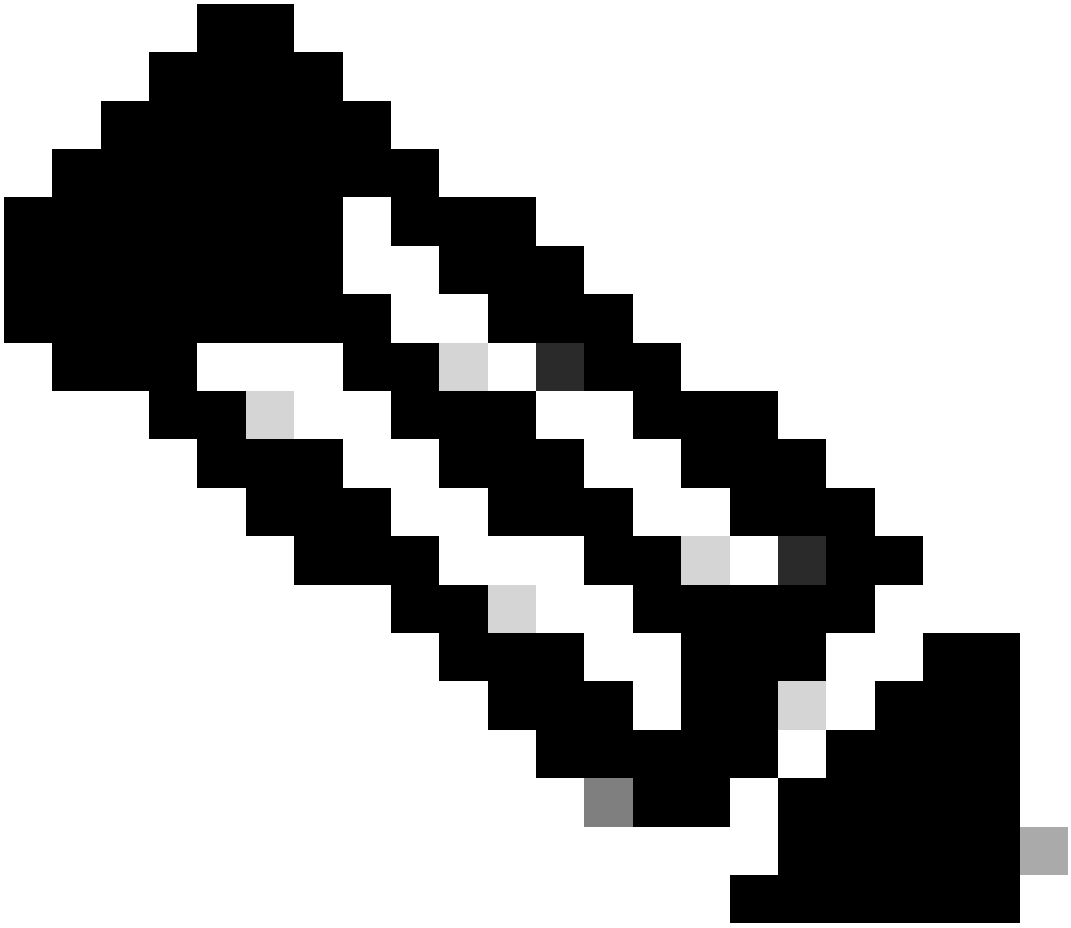
Vous pouvez vérifier quelle règle se développe en combien d'éléments de liste d'accès en utilisant la commande perl dans l'interface de ligne de commande FMC :

<#root>

perl /var/opt/CSCOpx/bin/access_rule_expansion_count.pl

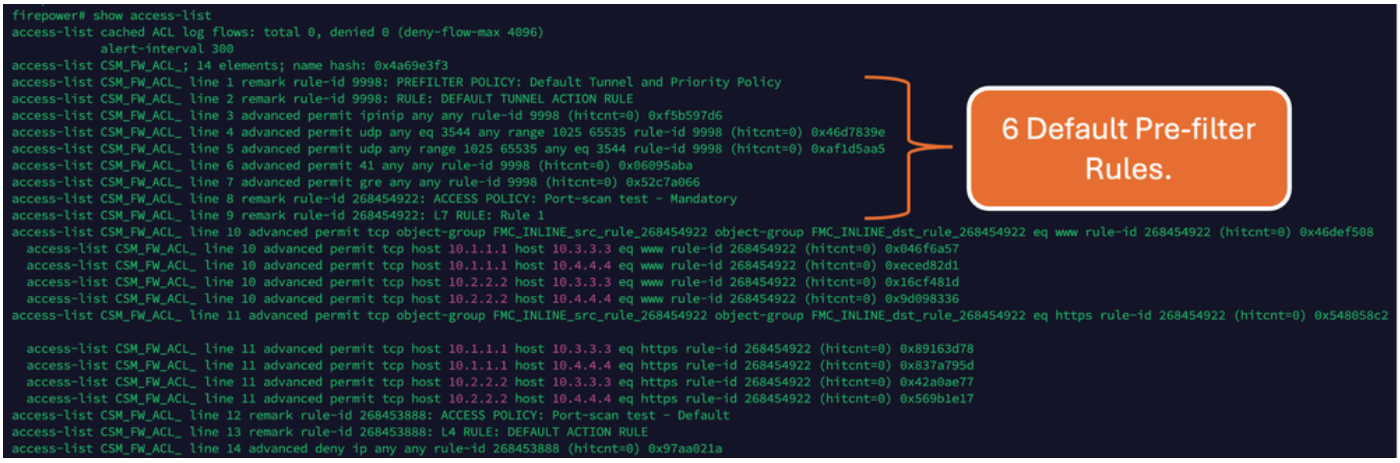
```
root@firepower:/Volume/home/admin# perl /var/opt/CSCOpx/bin/access_rule_expansion_count.pl

  Secure Firewall Management Center for VMware - v7.4.1 - (build 172)

  Access Control Rule Expansion Computer


  Enter FTD UUID or Name:

  > 10.70.73.44

------------------------------------------------------------------------------------------------------------

  Secure Firewall Management Center for VMware - v7.4.1 - (build 172)

  Access Control Rule Expansion Computer

  Device:

    UUID: 93cc359c-39be-11d4-9ae1-f2186cbddb11

    Name: 10.70.73.44

  Access Control Policy:

    UUID: 005056B9-F342-0ed3-0000-292057792375

    Name: Port-scan test

    Description:

  Intrusion Policies:
```

```
-----------------------------------------------------------------------------------------------

|  UUID                                    |  NAME                                              |

-----------------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------------

  Date: 2024-Jul-17 at 06:51:55 UTC

  NOTE: Computation is done on per rule basis. Count from shadow rules will not be applicable on device

  Run "Rule Conflict Detection" tool on AC Policy for specified device to detect and optimise such rules


-------------------------------------------------------------------------------------------------------
| UUID                                       | NAME                     |             COUNT
-------------------------------------------------------------------------------------------------------
| 005056B9-F342-0ed3-0000-000268454919       | Rule 1                   |               8
-------------------------------------------------------------------------------------------------------
|   TOTAL: 8
-------------------------------------------------------------------------------------------------------
| Access Rule Elements Count on FTD: 14
-------------------------------------------------------------------------------------------------------

>>> My JVM PID : 19417
```



Remarque : nombre d'éléments de règle d'accès sur FTD : 14. Cela inclut l'ensemble par défaut de règles FTD (préfiltre) et la règle de contrôle d'accès par défaut.

Les règles de pré-filtrage par défaut sont visibles dans l'interface de ligne de commande FTD :

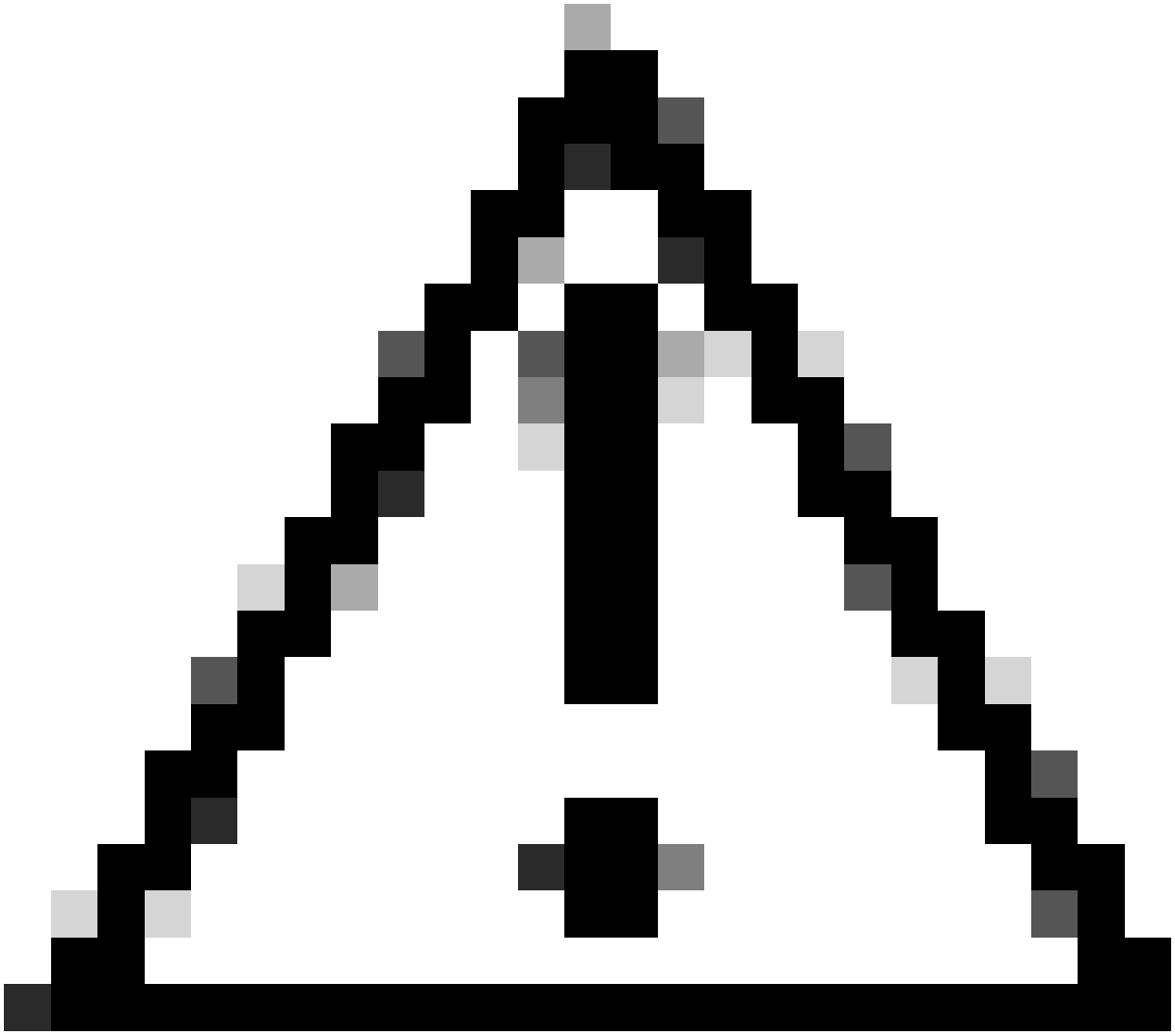


Impact d'un ACE élevé

- Un processeur élevé est visible.
- Une mémoire élevée est visible.
- La lenteur du périphérique peut être observée.
- Échec des déploiements/ Temps de déploiement plus long.

Choix du moment d'activation de la recherche de groupe d'objets (OGS)

- Le nombre d'ACE dépasse la limite d'ACE du périphérique.
- Le processeur du périphérique n'est pas déjà élevé, car l'activation d'OGS sollicite davantage le processeur du périphérique.
- Activez-le en dehors des heures de production.



Attention : activez asp rule-engine transactional-commit access-group à partir du mode d'interférence CLI FTD avant d'activer OGS. Ceci est configuré pour éviter les pertes de trafic pendant et juste après le processus de déploiement tout en activant OGS.

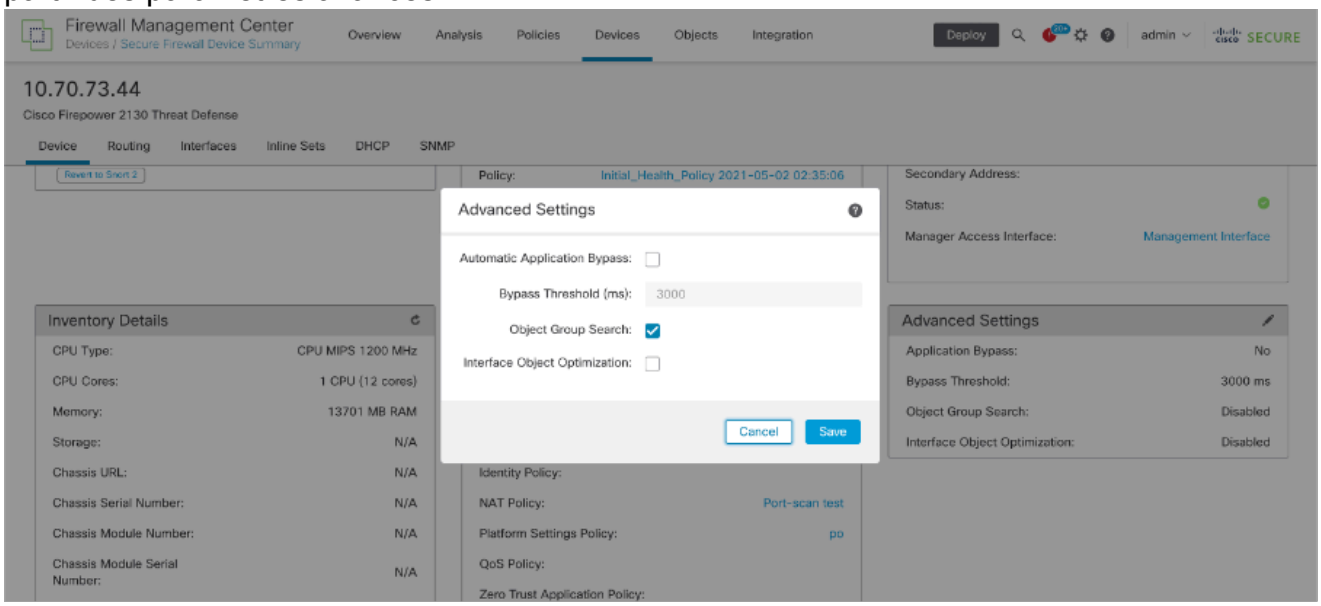
```
>
>
>
>
> asp rule-engine transactional-commit access-group
>
>
>
```

Activation de la recherche de groupes d'objets

Actuellement, OGS n'est pas activé :

```
firepower#
firepower#
firepower#
firepower# show run object-group-search
firepower#
firepower#
firepower#
```

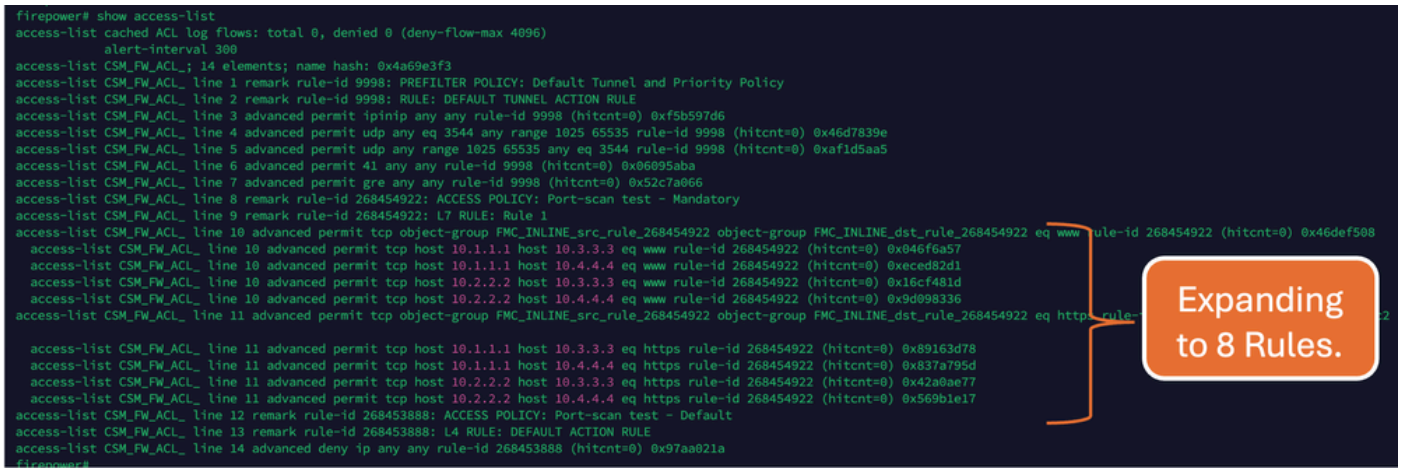
1. Connectez-vous à FMC CLI. Accédez à Périphériques > Gestion des périphériques > Sélectionnez le périphérique FTD > Périphérique. Activez la recherche de groupes d'objets à partir des paramètres avancés :



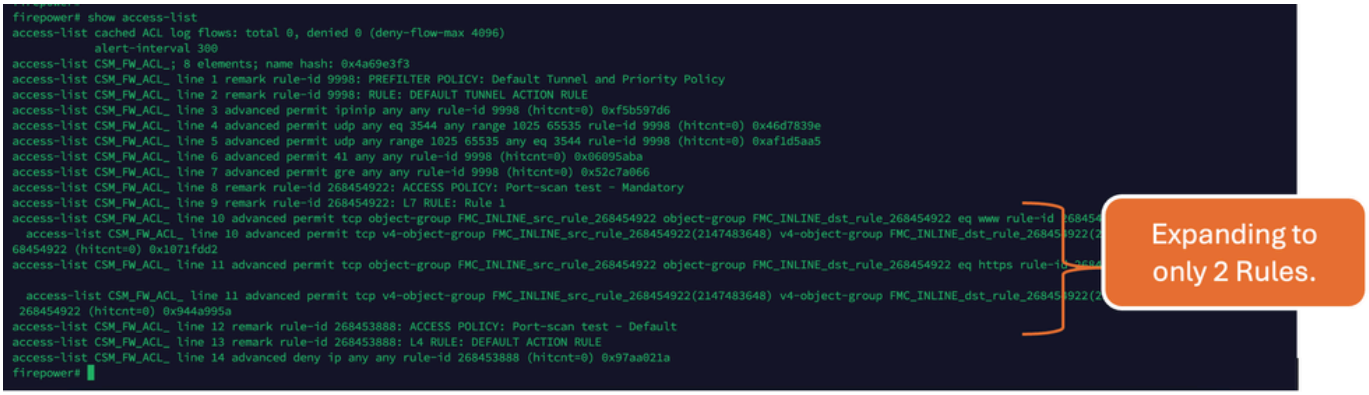
2. Cliquez sur Enregistrer et déployer.

Vérifier

Avant l'activation d'OGS :



Une fois OGS activé :



Informations connexes

Pour plus d'informations sur la façon dont les règles sont développées dans FTD, référez-vous au document Comprendre l'expansion des règles sur les périphériques FirePOWER.

Pour plus d'informations sur l'architecture FTD et le dépannage, référez-vous à Dissection de la défense contre les menaces Firepower (FTD).

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.