

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 :

The screenshot shows the FMC interface with the 'Policies' tab selected. The rule 'Port-scan test' is being edited. The configuration table is as follows:

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destina... Dynamic Attributes	Action	Icons
Mandatory - Port-scan test (1-1)															
1	Rule 1	Any	Any	10.1.1.1 10.2.2.2	10.3.3.3 10.4.4.4	Any	Any	Any	Any	TCP (6):80 TCP (6):443	Any	Any	Any	Allow	Icons
Default - Port-scan test (-)															

Below the table, it states: "There are no rules in this section. [Add Rule](#) or [Add Category](#)"

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.

```

Firepower# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
  alert-interval 300
access-list CSM_FW_ACL_ ; 14 elements; name hash: 0x4a59e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 5 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 6 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 7 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 8 remark rule-id 268454922: ACCESS POLICY: Port-scan test - Mandatory
access-list CSM_FW_ACL_ line 9 remark rule-id 268454922: L7 RULE: Rule 1
access-list CSM_FW_ACL_ line 10 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq www rule-id 268454922 (hitcnt=0) 0x46def508
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.1.1.1 host 10.3.3.3 eq www rule-id 268454922 (hitcnt=0) 0x046f6a57
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.1.1.1 host 10.4.4.4 eq www rule-id 268454922 (hitcnt=0) 0xeced82d1
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.2.2.2 host 10.3.3.3 eq www rule-id 268454922 (hitcnt=0) 0x16cf481d
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.2.2.2 host 10.4.4.4 eq www rule-id 268454922 (hitcnt=0) 0x9d998336
access-list CSM_FW_ACL_ line 11 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq http rule-id 268454922 (hitcnt=0) 0x89163d78
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.1.1.1 host 10.3.3.3 eq https rule-id 268454922 (hitcnt=0) 0x837a795d
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.2.2.2 host 10.3.3.3 eq https rule-id 268454922 (hitcnt=0) 0x42a0ae77
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.2.2.2 host 10.4.4.4 eq https rule-id 268454922 (hitcnt=0) 0x569b1e17
access-list CSM_FW_ACL_ line 12 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default
access-list CSM_FW_ACL_ line 13 remark rule-id 268453888: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcnt=0) 0x97aa021a
Firepower#

```

Expanding to 8 Rules.

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 rule

| 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 :

```
firepower# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
  alert-interval 300
access-list CSM_FW_ACL_ ; 14 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 5 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 6 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 7 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a866
access-list CSM_FW_ACL_ line 8 remark rule-id 268454922: ACCESS POLICY: Port-scan test - Mandatory
access-list CSM_FW_ACL_ line 9 remark rule-id 268454922: L7 RULE: Rule 1
access-list CSM_FW_ACL_ line 10 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq www rule-id 268454922 (hitcnt=0) 0x46def508
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.1.1.1 host 10.3.3.3 eq www rule-id 268454922 (hitcnt=0) 0x046f6a57
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.1.1.1 host 10.4.4.4 eq www rule-id 268454922 (hitcnt=0) 0xced82d1
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.2.2.2 host 10.3.3.3 eq www rule-id 268454922 (hitcnt=0) 0x16cf461d
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.2.2.2 host 10.4.4.4 eq www rule-id 268454922 (hitcnt=0) 0x9d098336
access-list CSM_FW_ACL_ line 11 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq https rule-id 268454922 (hitcnt=0) 0x548058c2
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.1.1.1 host 10.3.3.3 eq https rule-id 268454922 (hitcnt=0) 0x89163d78
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.1.1.1 host 10.4.4.4 eq https rule-id 268454922 (hitcnt=0) 0x837a795d
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.2.2.2 host 10.3.3.3 eq https rule-id 268454922 (hitcnt=0) 0x42a0ae77
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.2.2.2 host 10.4.4.4 eq https rule-id 268454922 (hitcnt=0) 0x569b1e17
access-list CSM_FW_ACL_ line 12 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default
access-list CSM_FW_ACL_ line 13 remark rule-id 268453888: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcnt=0) 0x97aa021a
```

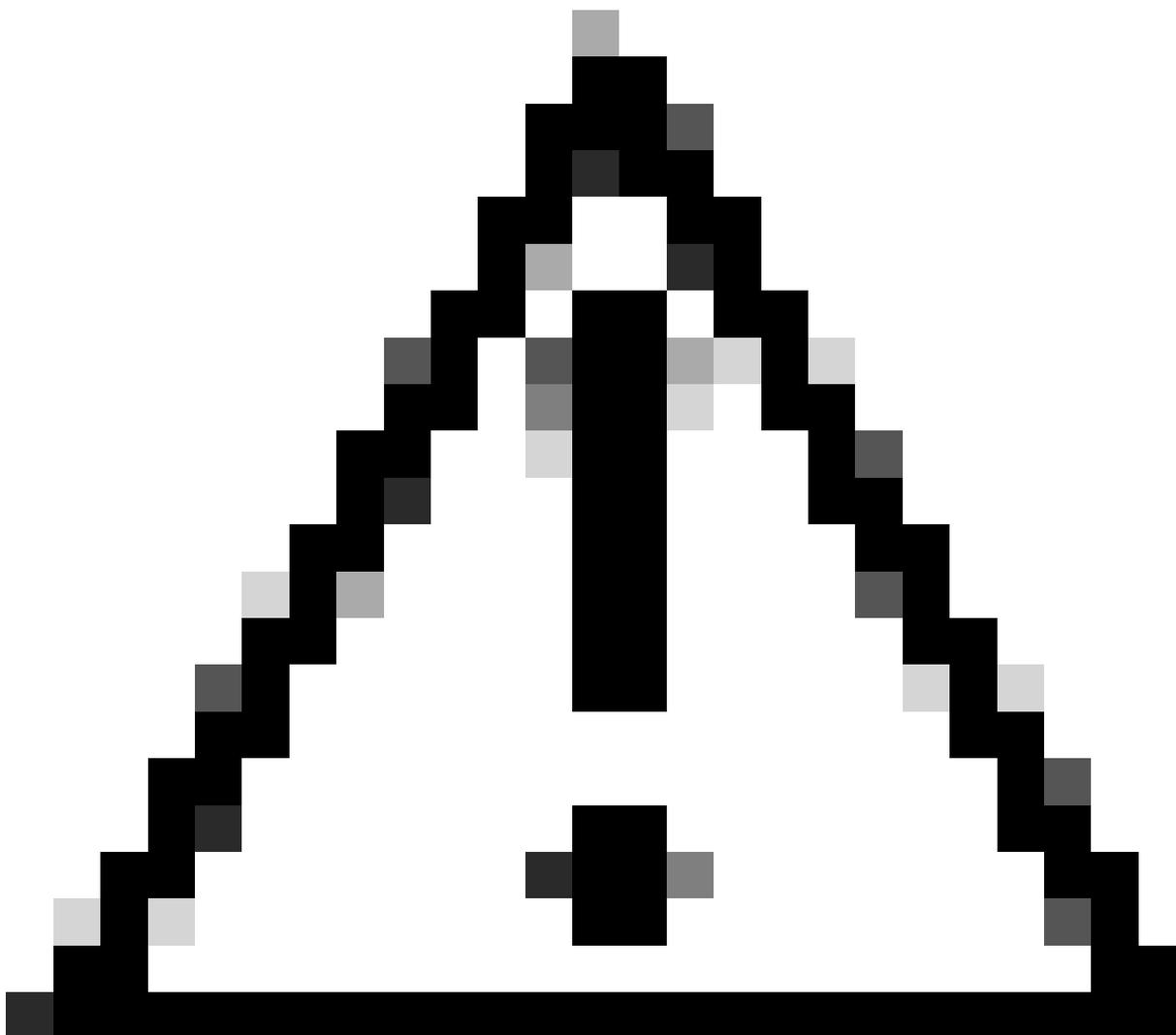
6 Default Pre-filter Rules.

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.

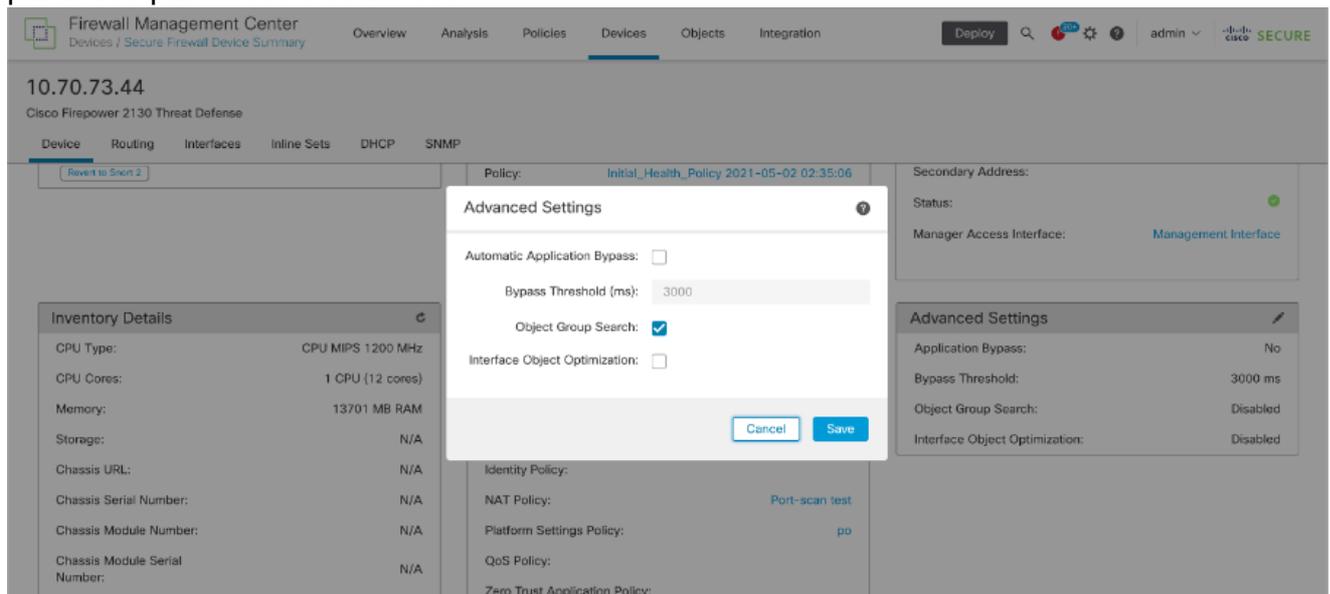
```
>  
>  
>  
>  
> asp rule-engine transactional-commit access-group  
>  
>  
>
```

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 :

```

Firepower# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
  alert-interval 300
access-list CSM_FW_ACL_ ; 14 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 5 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 6 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 7 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 8 remark rule-id 268454922: ACCESS POLICY: Port-scan test - Mandatory
access-list CSM_FW_ACL_ line 9 remark rule-id 268454922: L7 RULE: Rule 1
access-list CSM_FW_ACL_ line 10 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq www rule-id 268454922 (hitcnt=0) 0x46def508
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.1.1.1 host 10.3.3.3 eq www rule-id 268454922 (hitcnt=0) 0x046f6a57
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.1.1.1 host 10.4.4.4 eq www rule-id 268454922 (hitcnt=0) 0xeced82d1
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.2.2.2 host 10.3.3.3 eq www rule-id 268454922 (hitcnt=0) 0x16cf481d
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.2.2.2 host 10.4.4.4 eq www rule-id 268454922 (hitcnt=0) 0x9d998336
access-list CSM_FW_ACL_ line 11 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq http rule-id 268454922 (hitcnt=0) 0x46def508
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.1.1.1 host 10.3.3.3 eq https rule-id 268454922 (hitcnt=0) 0x89163d78
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.1.1.1 host 10.4.4.4 eq https rule-id 268454922 (hitcnt=0) 0x837a795d
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.2.2.2 host 10.3.3.3 eq https rule-id 268454922 (hitcnt=0) 0x42a0ae77
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.2.2.2 host 10.4.4.4 eq https rule-id 268454922 (hitcnt=0) 0x569b1e17
access-list CSM_FW_ACL_ line 12 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default
access-list CSM_FW_ACL_ line 13 remark rule-id 268453888: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcnt=0) 0x97aa021a
Firepower#

```

Expanding to 8 Rules.

Une fois OGS activé :

```

firepower# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
  alert-interval 300
access-list CSM_FW_ACL_ ; 8 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 5 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 6 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 7 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 8 remark rule-id 268454922: ACCESS POLICY: Port-scan test - Mandatory
access-list CSM_FW_ACL_ line 9 remark rule-id 268454922: L7 RULE: Rule 1
access-list CSM_FW_ACL_ line 10 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq www rule-id 268454922 (hitcnt=0) 0x46def508
access-list CSM_FW_ACL_ line 10 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922(2147483648) v4-object-group FMC_INLINE_dst_rule_268454922(2147483648) eq www rule-id 268454922 (hitcnt=0) 0x1071fdd2
access-list CSM_FW_ACL_ line 11 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq https rule-id 268454922 (hitcnt=0) 0x46def508
access-list CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922(2147483648) v4-object-group FMC_INLINE_dst_rule_268454922(2147483648) eq https rule-id 268454922 (hitcnt=0) 0x1071fdd2
access-list CSM_FW_ACL_ line 12 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default
access-list CSM_FW_ACL_ line 13 remark rule-id 268453888: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcnt=0) 0x97aa021a
firepower#

```

Expanding to only 2 Rules.

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.