

Calcola il numero di elementi ACE (Access List Element) tramite CLI di FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Come calcolare il conteggio degli elementi dell'elenco accessi \(ACE, Access List Element Count\) tramite CLI di FMC](#)

[Impatto dell'ACE elevato](#)

[Scelta dell'attivazione di OGS \(Object Group Search\)](#)

[Abilitazione della ricerca nel gruppo di oggetti](#)

[Verifica](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come individuare la regola nei criteri di controllo di accesso che si sta espandendo in base al numero di elementi dell'elenco di accesso.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza della tecnologia Firepower
- Conoscenze sulla configurazione dei criteri di controllo di accesso in FMC

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Una regola di controllo d'accesso viene creata utilizzando una o più combinazioni dei seguenti parametri:

- Indirizzo IP (origine e destinazione)
- Porte (origine e destinazione)
- URL (categorie fornite dal sistema e URL personalizzati)
- Rilevatori applicazioni
- VLAN
- Zone

In base alla combinazione di parametri utilizzata nella regola di accesso, l'espansione della regola nel sensore cambia. Il presente documento mette in evidenza varie combinazioni di norme relative al CCP e le rispettive espansioni associate sui sensori.

Come calcolare il numero di elementi dell'elenco accessi (ACE, Access List Element Count) utilizzando la CLI di FMC

Prendere in considerazione la configurazione di una regola di accesso da FMC, come illustrato nell'immagine:

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The main content area is titled 'Port-scan test' and shows the configuration of a rule. The rule is named 'Rule 1' and is configured with the following parameters:

#	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
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

The interface also shows a search bar for rules and a table of rule categories. The 'Mandatory - Port-scan test (1-1)' category contains the rule 'Rule 1'. The 'Default - Port-scan test (-)' category is empty.

Configurazione delle regole nei criteri di controllo di accesso

Se questa regola viene visualizzata nella CLI FTD, significa che è stata espansa in 8 regole.

```

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-
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.

È possibile verificare quale regola si sta espandendo in quanti elementi dell'elenco degli accessi utilizzando il comando perl nella CLI di 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

Nota: conteggio elementi regola di accesso su FTD: 14. Sono incluse anche l'insieme predefinito di regole FTD (Pre-filtro) e la regola di controllo di accesso predefinita.

Le regole predefinite di prefilter possono essere visualizzate nella CLI 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: 0x4a09e3f3
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) 0x06095baba
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) 0xecd82d1
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
```

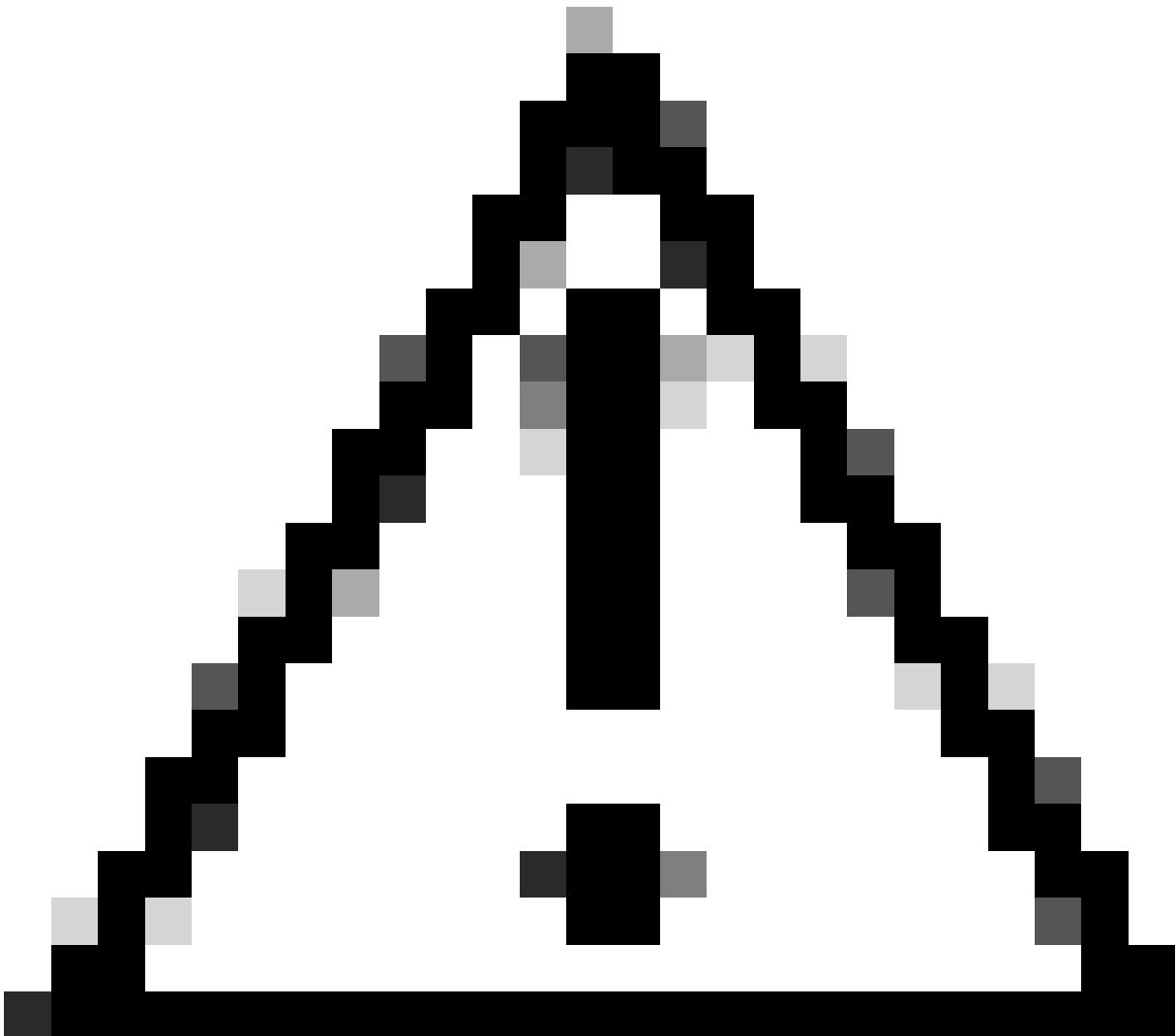
6 Default Pre-filter Rules.

Impatto dell'ACE elevato

- È possibile osservare un elevato livello di CPU.
- È possibile visualizzare la memoria elevata.
- È possibile osservare la lentezza del dispositivo.
- Distribuzioni non riuscite/tempi di distribuzione più lunghi.

Scelta dell'attivazione di OGS (Object Group Search)

- Il numero di ACE supera il limite ACE del dispositivo.
 - La CPU del dispositivo non è già elevata, in quanto l'abilitazione di OGS aumenta lo stress sulla CPU del dispositivo.
 - Abilitarlo durante le ore non di produzione.
-



Attenzione: abilitare il gruppo di accesso con commit transazionale del motore delle regole asp dalla modalità di chiusura CLI FTD prima di abilitare il gruppo di accesso globale. Questa opzione è configurata per evitare la perdita di traffico durante e subito dopo il processo di distribuzione durante l'abilitazione di OGS.

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

Abilitazione della ricerca nel gruppo di oggetti

Attualmente OGS non è abilitato:

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

1. Accedere alla CLI di FMC. Selezionare Dispositivi > Gestione dispositivi > Selezionare il dispositivo FTD > Dispositivo. Abilitare la ricerca del gruppo di oggetti da Impostazioni avanzate:

The screenshot displays the Cisco Firewall Management Center (FMC) interface. The main page shows the configuration for a device named '10.70.73.44', a Cisco Firepower 2130 Threat Defense. The 'Advanced Settings' dialog box is open, showing the following configuration:

- Automatic Application Bypass:
- Bypass Threshold (ms): 3000
- Object Group Search:
- Interface Object Optimization:


The dialog box also includes 'Cancel' and 'Save' buttons. The background shows the device configuration page with various tabs like 'Device', 'Routing', 'Interfaces', 'Inline Sets', 'DHCP', and 'SNMP'. The 'Advanced Settings' section on the right shows the current configuration for the device, including 'Application Bypass: No', 'Bypass Threshold: 3000 ms', 'Object Group Search: Disabled', and 'Interface Object Optimization: Disabled'.

2. Fare clic su Salva e distribuisce.

Verifica


Prima dell'abilitazione di 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_1; 14 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_1 line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_1 line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_1 line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_1 line 4 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_1 line 5 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_1 line 6 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_1 line 7 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_1 line 8 remark rule-id 268454922: ACCESS POLICY: Port-scan test - Mandatory
access-list CSM_FW_ACL_1 line 9 remark rule-id 268454922: L7 RULE: Rule 1
access-list CSM_FW_ACL_1 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_1 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_1 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_1 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_1 line 10 advanced permit tcp host 10.2.2.2 host 10.4.4.4 eq www rule-id 268454922 (hitcnt=0) 0x9d0998336
access-list CSM_FW_ACL_1 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_1 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_1 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_1 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_1 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_1 line 12 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default
access-list CSM_FW_ACL_1 line 13 remark rule-id 268453888: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_1 line 14 advanced deny ip any any rule-id 268453888 (hitcnt=0) 0x97aa021a
Firepower#
```



Dopo l'abilitazione di 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_1; 8 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_1 line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_1 line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_1 line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_1 line 4 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_1 line 5 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_1 line 6 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_1 line 7 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_1 line 8 remark rule-id 268454922: ACCESS POLICY: Port-scan test - Mandatory
access-list CSM_FW_ACL_1 line 9 remark rule-id 268454922: L7 RULE: Rule 1
access-list CSM_FW_ACL_1 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_1 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_1 line 11 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) 0x944a995a
access-list CSM_FW_ACL_1 line 12 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default
access-list CSM_FW_ACL_1 line 13 remark rule-id 268453888: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_1 line 14 advanced deny ip any any rule-id 268453888 (hitcnt=0) 0x97aa021a
Firepower#
```



Informazioni correlate

Per informazioni più dettagliate sull'espansione delle regole in FTD, consultare il documento [Informazioni sull'espansione delle regole nei dispositivi FirePOWER.](#)

Per ulteriori informazioni sull'architettura FTD e la risoluzione dei problemi, fare riferimento a [Dissezione \(FTD\) Firepower Threat Defense.](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).