

# 使用FMC CLI計算訪問清單元素(ACE)計數

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[如何使用FMC CLI計算訪問清單元素計數\(ACE\)](#)

[高ACE的影響](#)

[決定何時啟用物件群組搜尋\(OGS\)](#)

[啟用對象組搜尋](#)

[驗證](#)

[相關資訊](#)

---

## 簡介

本文檔介紹如何查詢訪問控制策略中的哪個規則正在擴展為多少個訪問清單元素。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Firepower技術知識
- 在FMC上配置訪問控制策略的知識

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全防火牆管理中心(FMC)
- Cisco Firepower威脅防禦(FTD)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

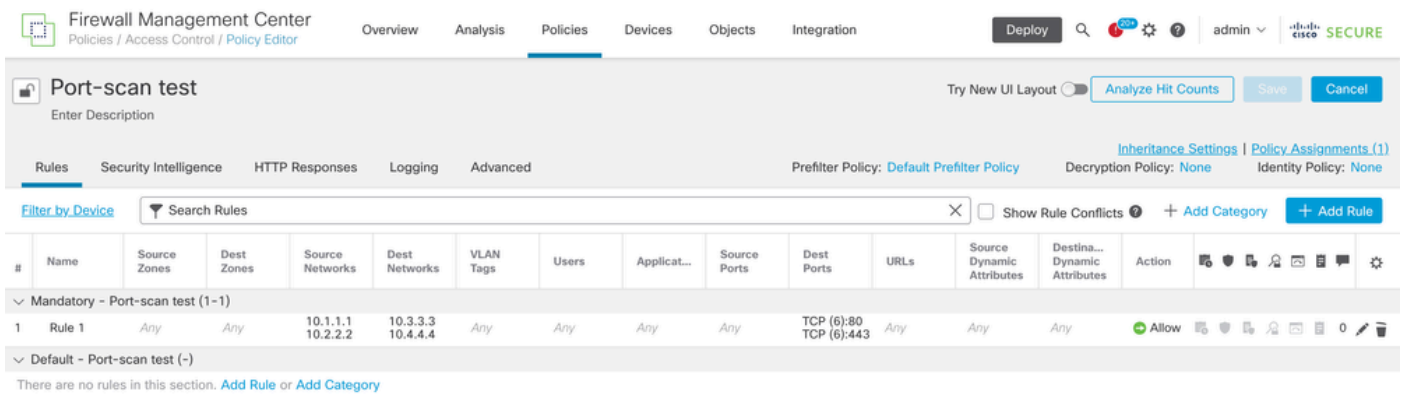
使用下列引數的一或多個組合來建立存取控制規則：

- IP位址（來源和目的地）
- 連線埠（來源和目的地）
- URL（系統提供的類別和自定義URL）
- 應用檢測器
- VLAN
- 區域

根據訪問規則中使用的參陣列合，感測器上的規則擴展會發生變化。本文檔重點介紹了FMC上的各種規則組合以及感測器上各自的關聯擴展。

## 如何使用FMC CLI計算訪問清單元素計數(ACE)

考慮從FMC配置訪問規則，如下圖所示：



The screenshot shows the Fire Management Center (FMC) interface. The main heading is "Port-scan test" with a sub-heading "Enter Description". Below this, there are tabs for "Rules", "Security Intelligence", "HTTP Responses", "Logging", and "Advanced". The "Rules" tab is selected. The interface includes a search bar for rules, a "Filter by Device" option, and a table of rules. The table has columns for #, 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, and icons for editing and deleting. The table shows one rule under the "Mandatory - Port-scan test (1-1)" category. The rule is "Rule 1" with source zones "Any" and destination zones "Any". The source networks are "10.1.1.1" and "10.2.2.2", and the destination networks are "10.3.3.3" and "10.4.4.4". The source ports are "TCP (6):80" and "TCP (6):443", and the destination ports are "Any". The action is "Allow".

#	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
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

訪問控制策略中的規則配置

如果您在FTD CLI中看到此規則，則會注意到此規則已擴充為8個規則。

```

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 ip ip ip 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.

可以使用FMC CLI中的perl 命令檢查正在將哪個規則擴展到多少個訪問清單元素：

```
<#root>
```

```
perl /var/opt/CSC0px/bin/access_rule_expansion_count.pl
```

```
root@firepower:/Volume/home/admin# perl /var/opt/CSC0px/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

備註：FTD上的存取規則要素計數：14。這包括FTD規則的預設集（預先篩選）和「預設存取控制」規則。

預設預先篩選規則可在FTD CLI中看到：

```
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) 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) 0x8ced82d1
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) 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
```

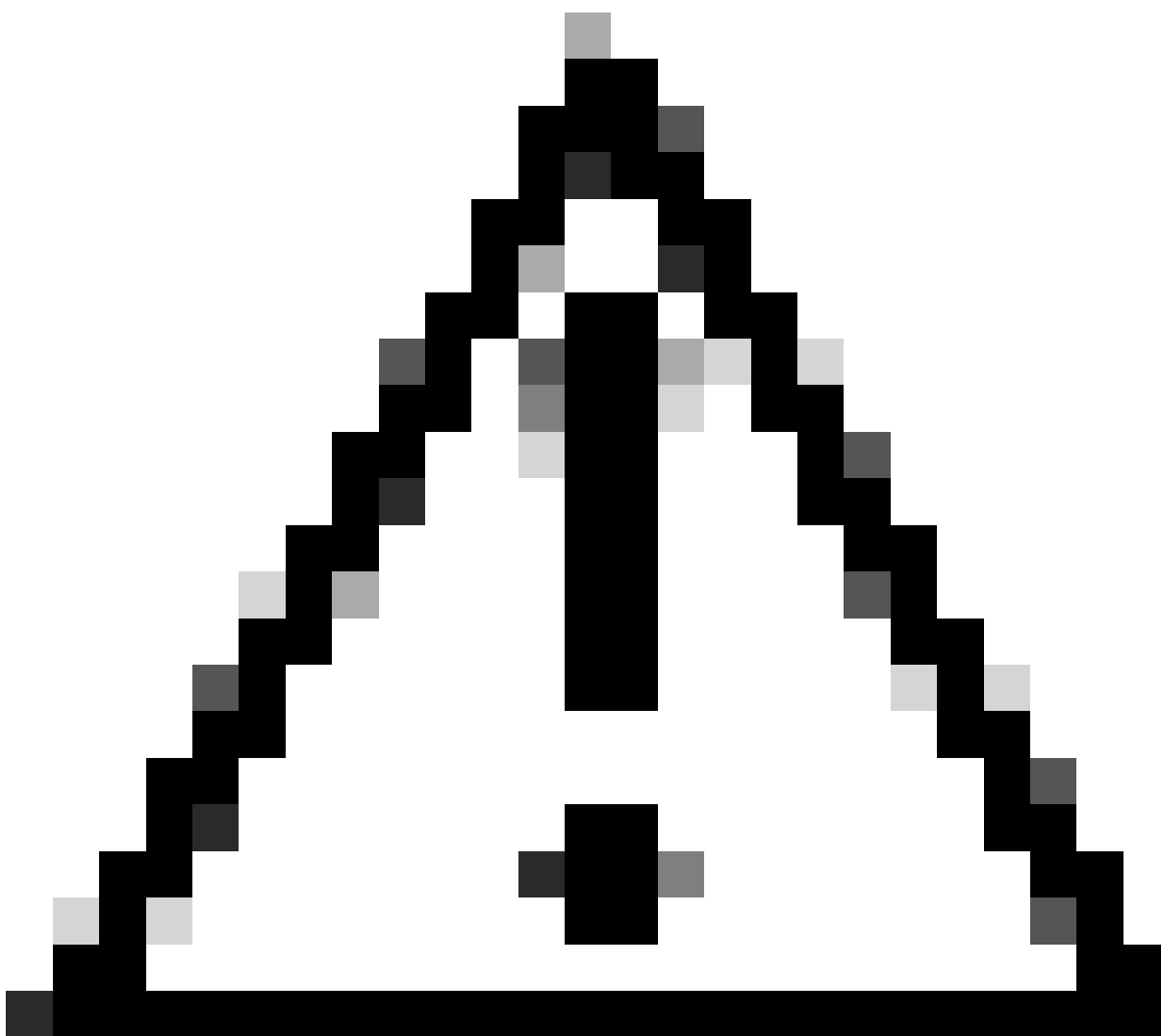
6 Default Pre-filter Rules.

## 高ACE的影響

- CPU使用率過高。
- 記憶體過高。
- 可以觀察到裝置速度緩慢。
- 部署失敗/部署時間更長。

## 決定何時啟用物件群組搜尋(OGS)

- ACE計數超過裝置ACE限制。
- 裝置的CPU不是很高，因為啟用OGS會給裝置CPU帶來更多壓力。
- 在非生產時間啟用它。



注意：請在啟用OGS之前，先從FTD CLI關閉模式啟用asp rule-engine transactional-

commit access-group。這配置為在啟用OGS時，避免在部署過程中和部署後丟棄流量。

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

## 啟用對象組搜尋

目前未啟用OGS：

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

1. 登入到FMC CLI。導覽至Devices > Device Management > Select the FTD device > Device。從「進階設定」啟用物件群組搜尋：

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

Setting	Value
Automatic Application Bypass	<input type="checkbox"/>
Bypass Threshold (ms)	3000
Object Group Search	<input checked="" type="checkbox"/>
Interface Object Optimization	<input type="checkbox"/>

The background page shows the 'Inventory Details' section with the following information:

Property	Value
CPU Type	CPU MIPS 1200 MHz
CPU Cores	1 CPU (12 cores)
Memory	13701 MB RAM
Storage	N/A
Chassis URL	N/A
Chassis Serial Number	N/A
Chassis Module Number	N/A
Chassis Module Serial Number	N/A

## 2. 按一下儲存和部署。

## 驗證

啟用OGS之前：

```
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) 0x846f6a57
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) 0xecd82d1
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) 0x89163d78
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#
```

Expanding to 8 Rules.

啟用OGS之後：

```
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 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 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 object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq https rule-id 268454922 (hitcnt=0) 0x89163d78
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) 0x89163d78
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#
```

Expanding to only 2 Rules.

## 相關資訊

有關如何在FTD中擴展規則的詳細資訊，請參閱文檔[瞭解FirePOWER裝置上的規則擴展](#)。

有關FTD架構和故障排除的詳細資訊，請參閱[剖析\(FTD\) Firepower威脅防禦](#)。



## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。