

Calculate Access List Element (ACE) Count Using FMC CLI

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[How To Calculate Access List Element Count \(ACE\) Using FMC CLI](#)

[Impact of High ACE](#)

[Deciding When To Enable Object Group Search \(OGS\)](#)

[Enabling Object Group Search](#)

[Verify](#)

[Related Information](#)

Introduction

This document describes how you can find which rule in your access control policy is expanding to how many access list elements.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Firepower technology
- Knowledge on configuring Access control policies on FMC

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Firepower Threat Defence (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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

An Access control rule is created with the use of one or multiple combinations of these parameters:

- IP Address (Source and Destination)
- Ports (Source and Destination)
- URL (System provided Categories and Custom URLs)
- Application Detectors
- VLANs
- Zones

Based on the combination of parameters used in the access rule, the rule expansion changes on the sensor. This document highlights various combinations of rules on the FMC and their respective associated expansions on the sensors.

How To Calculate Access List Element Count (ACE) Using FMC CLI

Consider the configuration of an access rule from the FMC, as shown in the image:

The screenshot shows the FMC interface with the 'Policies' tab selected. The rule 'Port-scan test' 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

Rule Configuration in Access Control Policy

If you see this rule in FTD CLI, you notice that this rule got expanded into 8 Rules.

```
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 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) 0x846f6a57
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) 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.

You can check which rule is expanding into how many access list elements using the **perl** command in FMC CLI:

```
<#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                                     |
```

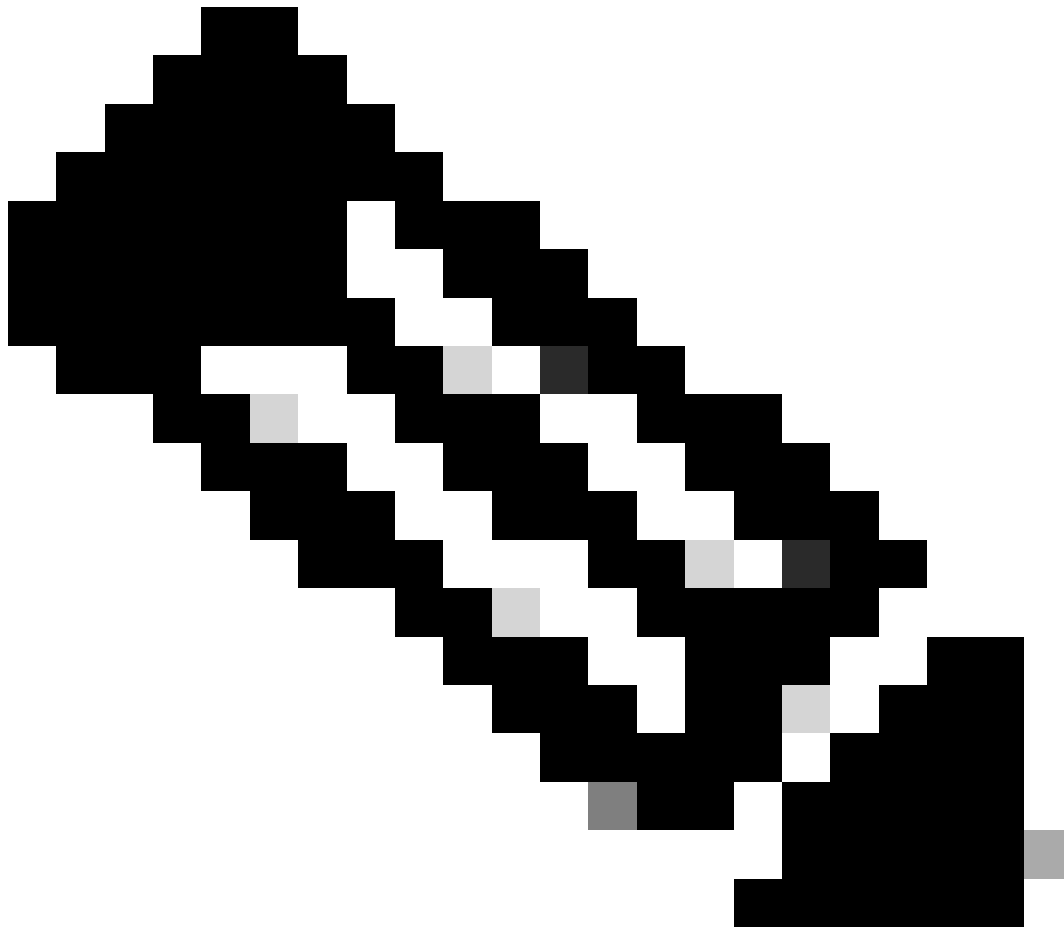
```
Date: 2024-Jul-17 at 06:51:55 UTC
```

```
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



Note: Access Rule Elements Count on FTD: 14. This includes the default set of FTD rules (Pre-filter) and Default Access control rule as well.

The default Pre-filter rules can be seen in FTD CLI:

```
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) 0x06995aba
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) 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
```

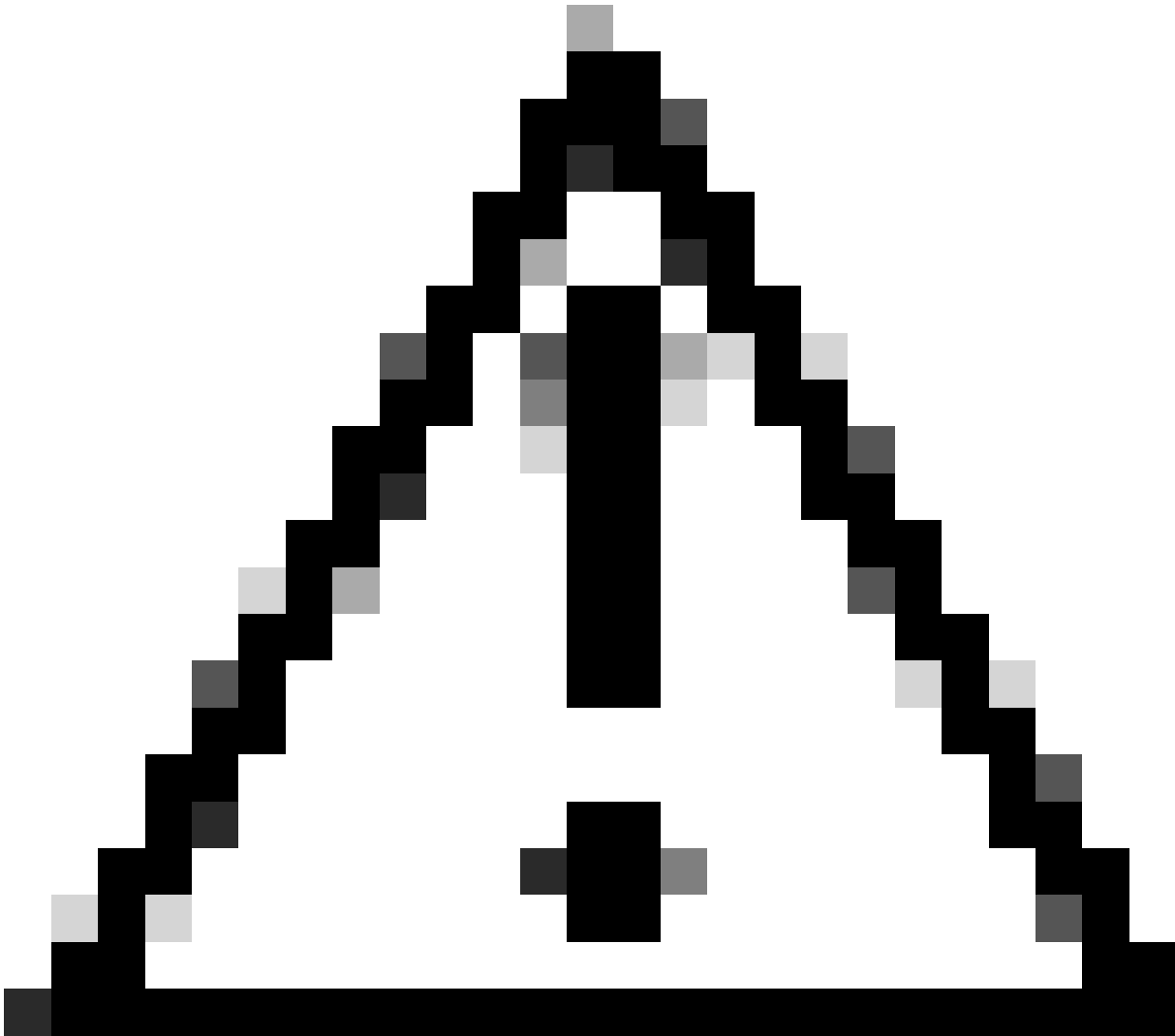
6 Default Pre-filter Rules.

Impact of High ACE

- High CPU can be seen.
- High Memory can be seen.
- Device slowness can be observed.
- Deployments failure/ Longer deployment time.

Deciding When To Enable Object Group Search (OGS)

- Count of ACE is exceeding the device ACE limit.
- The CPU of the device is not already high as enabling OGS puts more stress on the device CPU.
- Enable it during non Production hours.



Caution: Please enable **asp rule-engine transactional-commit access-group** from FTD CLI clish mode before enabling the OGS. This is configured to avoid traffic drops during and just after the deployment process while enabling OGS.

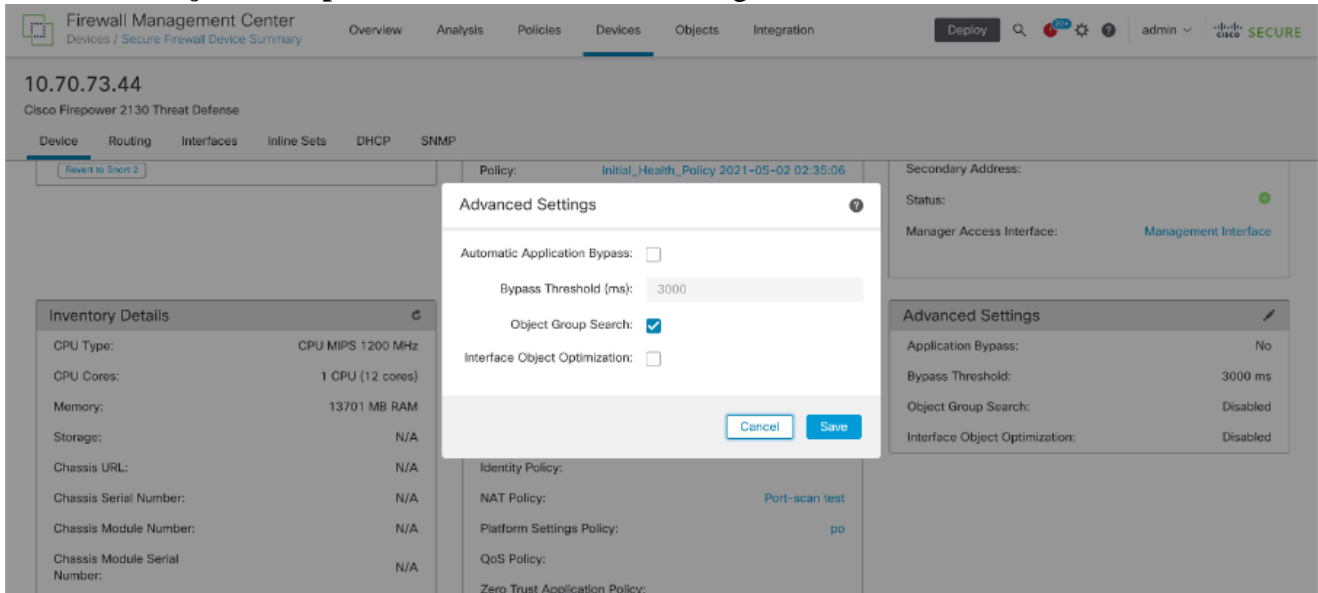
```
>  
>  
>  
>  
> asp rule-engine transactional-commit access-group  
>  
>  
>
```

Enabling Object Group Search

Currently OGS is not enabled:

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

1. Log in to FMC CLI. Navigate to **Devices > Device Management > Select the FTD device > Device**. Enable the **Object Group Search** from Advanced Settings:



2. Click **Save** and **deploy**.

Verify

Before OGS is enabled:

```
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) 0x46def588
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) 0x846f6a57
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.

After OGS is enabled:

```
firepower# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4996)
  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) 0x1071fdd2
access-list CSM_FW_ACL_ line 11 advanced permit tcp object-group FMC_INLINE_src_rule_268454922(2147483648) v4-object-group FMC_INLINE_dst_rule_268454922(2147483648) eq https rule-id 268454922 (hitcnt=0) 0x944a995a
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.

Related Information

For more detailed information on how rules are expanded in FTD, refer to the document [Understand the Rule Expansion on FirePOWER Devices](#).

For more information on the FTD Architecture and Troubleshooting, refer to [Dissecting \(FTD\) Firepower Threat Defense](#).