

Berechnen der Anzahl von Access List-Elementen (ACE) mithilfe der FMC-CLI

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Berechnung der Anzahl von Access List-Elementen \(ACE\) mithilfe der FMC-CLI](#)

[Auswirkungen eines hohen ACE-Werts](#)

[Festlegen, wann die Objektgruppensuche \(OGS\) aktiviert werden soll](#)

[Aktivieren der Objektgruppensuche](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie feststellen können, welche Regel in Ihrer Zugriffskontrollrichtlinie auf die Anzahl der Zugriffslistenelemente erweitert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse der FirePOWER-Technologie
- Kenntnisse bei der Konfiguration von Zugriffskontrollrichtlinien auf FMC

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Eine Zugriffskontrollregel wird mit einer oder mehreren Kombinationen dieser Parameter erstellt:

- IP-Adresse (Quelle und Ziel)
- Ports (Quelle und Ziel)
- URL (Vom System bereitgestellte Kategorien und benutzerdefinierte URLs)
- Anwendungserkennung
- VLANs
- Zonen

Basierend auf der Kombination der in der Zugriffsregel verwendeten Parameter ändert sich die Regelerweiterung auf dem Sensor. In diesem Dokument werden verschiedene Kombinationen von Regeln für das FMC und die entsprechenden Erweiterungen für die Sensoren vorgestellt.

Berechnung der Access List Element Count (ACE) mithilfe der FMC-CLI

Berücksichtigen Sie die Konfiguration einer Zugriffsregel vom FMC aus, wie in der Abbildung dargestellt:

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

Regelkonfiguration in einer Zugriffskontrollrichtlinie

Wenn Sie diese Regel in der FTD CLI sehen, stellen Sie fest, dass diese Regel in 8 Regeln erweitert wurde.

```

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.

Mit dem Befehl perl in der FMC-CLI können Sie überprüfen, welche Regel auf wie viele Zugriffslistenelemente erweitert wird:

```
<#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



Hinweis: Access Rule Elements Count on FTD: 14 (Zugriffsregel-Elemente zählen auf FTD) Dies umfasst auch die Standardeinstellungen für FTD-Regeln (Vorfilter) und die Standardzugriffskontrollregeln.

Die Standard-Vorfilterregeln sind in der FTD-CLI zu sehen:

```
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) 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) 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) 0x89163d70
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) 0x42a8ae77
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
```

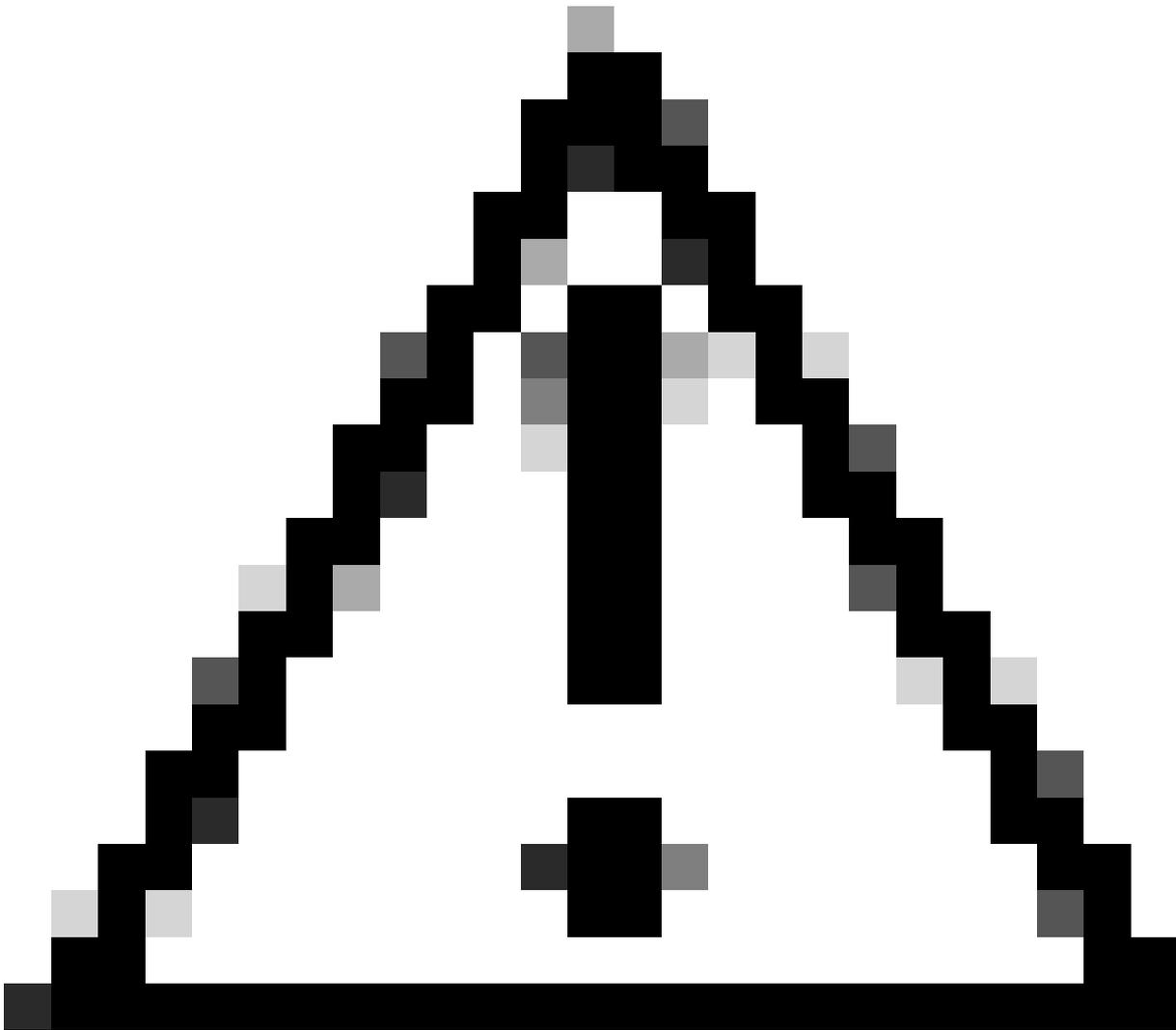
6 Default Pre-filter Rules.

Auswirkungen eines hohen ACE-Werts

- Eine hohe CPU ist sichtbar.
- Der hohe Speicher ist sichtbar.
- Es kann eine langsame Geräteentwicklung beobachtet werden.
- Bereitstellungsfehler/Längere Bereitstellungszeit.

Festlegen, wann die Objektgruppensuche (OGS) aktiviert werden soll

- Die Anzahl der ACEs überschreitet den ACE-Grenzwert für das Gerät.
- Die CPU des Geräts ist nicht bereits hoch, da die Aktivierung von OGS die CPU des Geräts stärker belastet.
- Aktivieren Sie es außerhalb der Produktionszeiten.



Vorsicht: Aktivieren Sie `asp rule-engine transactional-commit access-group` aus dem FTD CLI clish mode, bevor Sie das OGS aktivieren. Diese Funktion ist so konfiguriert, dass Datenverkehrsverluste während und unmittelbar nach der Bereitstellung bei der Aktivierung von OGS vermieden werden.

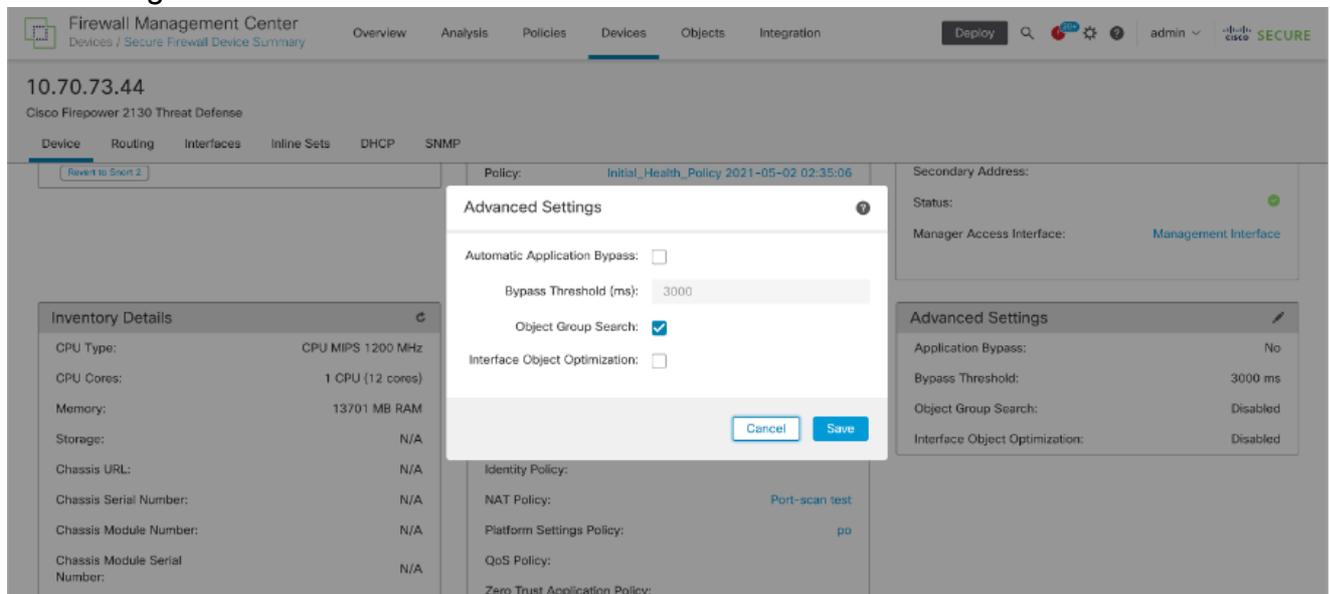
```
>  
>  
>  
>  
> asp rule-engine transactional-commit access-group  
>  
>  
>
```

Aktivieren der Objektgruppensuche

Derzeit ist OGS nicht aktiviert:

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

1. Melden Sie sich bei FMC CLI an. Navigieren Sie zu Geräte > Geräteverwaltung > Wählen Sie das FTD-Gerät > Gerät aus. Aktivieren Sie die Objektgruppensuche in den erweiterten Einstellungen:



2. Klicken Sie auf Speichern und bereitstellen.

Überprüfung

Bevor OGS aktiviert wird:

```

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.

Nach Aktivierung von 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_ ; 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) 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.

Zugehörige Informationen

Weitere Informationen zur Erweiterung von Regeln in FTD finden Sie im Dokument [Understanding the Rule Expansion on FirePOWER Devices \(Erläuterung der Regelerweiterung auf FirePOWER-Geräten\)](#).

Weitere Informationen zur FTD-Architektur und Fehlerbehebung finden Sie unter [Dissecting \(FTD\) Firepower Threat Defense](#).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.