

# Calcular el recuento de elementos de lista de acceso (ACE) mediante CLI de FMC

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Cómo calcular el recuento de elementos de la lista de acceso \(ACE\)Utilizando la CLI de FMC](#)

[Impacto de la alta ACE](#)

[Decidir cuándo habilitar la búsqueda de grupos de objetos \(OGS\)](#)

[Habilitación de Búsqueda de Grupos de Objetos](#)

[Verificación](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe cómo puede encontrar qué regla de su política de control de acceso se expande a cuántos elementos de la lista de acceso.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de la tecnología Firepower
- Conocimientos sobre la configuración de las políticas de control de acceso en FMC

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Una regla de control de acceso se crea con el uso de una o varias combinaciones de estos parámetros:

- Dirección IP (origen y destino)
- Puertos (origen y destino)
- URL (categorías proporcionadas por el sistema y URL personalizadas)
- Detectores de aplicaciones
- VLAN
- Zonas

En función de la combinación de parámetros utilizada en la regla de acceso, la expansión de la regla cambia en el sensor. Este documento destaca varias combinaciones de reglas sobre el CSP y sus respectivas expansiones asociadas en los sensores.

## Cómo calcular el recuento de elementos de la lista de acceso (ACE) mediante la CLI de FMC

Considere la configuración de una regla de acceso desde el FMC, como se muestra en la imagen:

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 includes a search bar, 'Analyze Hit Counts', 'Save', and 'Cancel' buttons. Below the title, there are tabs for 'Rules', 'Security Intelligence', 'HTTP Responses', 'Logging', and 'Advanced'. The 'Rules' tab is active, showing 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, and Action. A single rule is listed under the 'Mandatory - Port-scan test (1-1)' section.

#	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

Configuración de reglas en la política de control de acceso

Si ve esta regla en la CLI de FTD, observará que esta regla se expandió en 8 reglas.

```

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-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.

Puede verificar qué regla se expande en cuántos elementos de la lista de acceso mediante el comando perl en la CLI de 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: Los elementos de reglas de acceso cuentan con FTD: 14. Esto también incluye el conjunto predeterminado de reglas de FTD (filtro previo) y la regla de control de acceso predeterminada.

Las reglas de prefiltrado predeterminadas se pueden ver en la CLI de 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 4l 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) 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) 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) 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
```

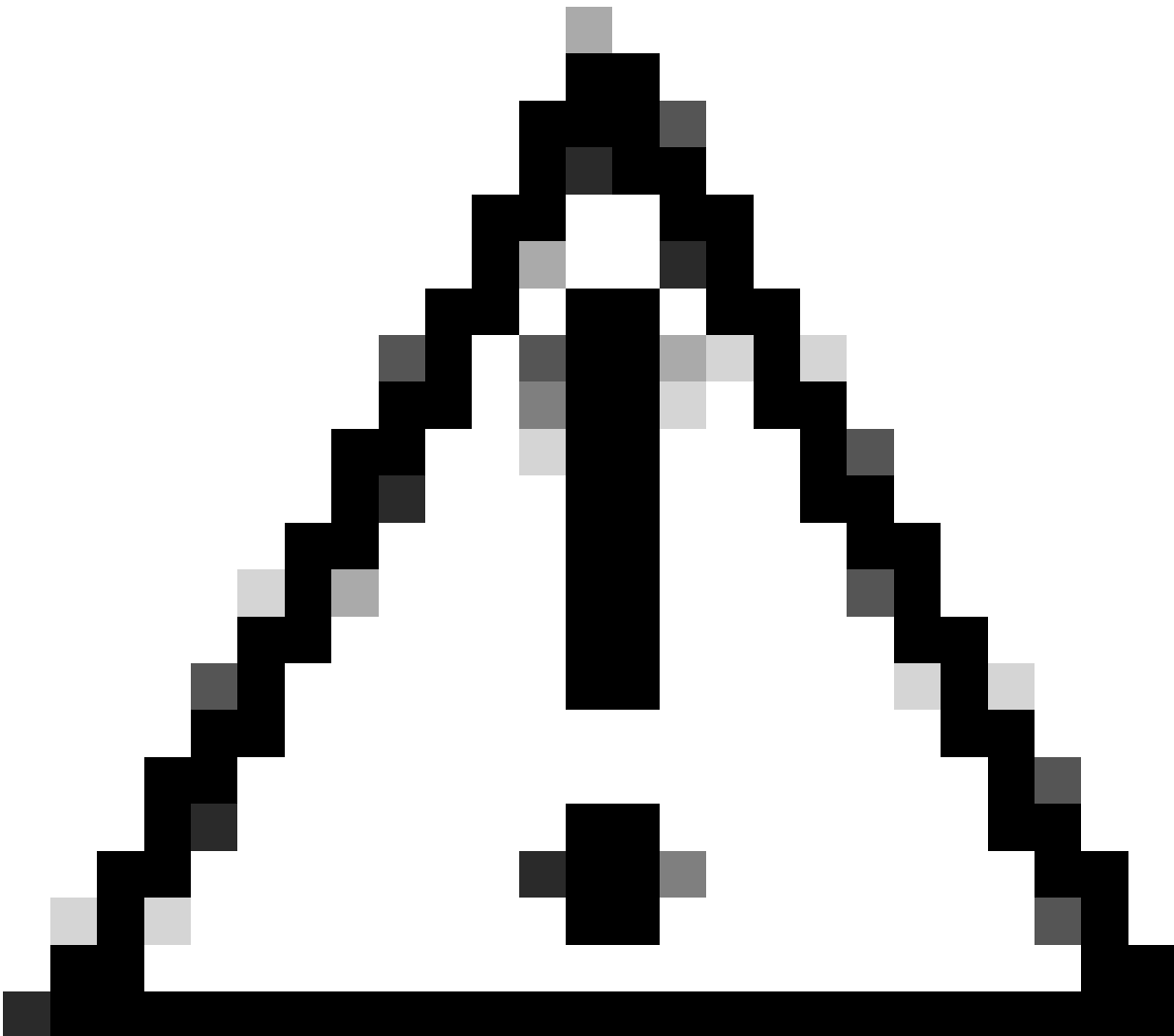
6 Default Pre-filter Rules.

## Impacto de la alta ACE

- Se puede ver una CPU alta.
- Se puede ver memoria alta.
- Se puede observar lentitud en los dispositivos.
- Fallo en las implementaciones/Mayor tiempo de implementación.

## Decidir cuándo habilitar la búsqueda de grupos de objetos (OGS)

- El recuento de ACE supera el límite de ACE del dispositivo.
  - La CPU del dispositivo aún no es alta, ya que la activación de OGS ejerce más presión sobre la CPU del dispositivo.
  - Actívela durante las horas no de producción.
- 



Precaución: habilite asp rule-engine transactional-commit access-group desde el modo de cierre CLI de FTD antes de habilitar el OGS. Esto se configura para evitar caídas de tráfico durante y justo después del proceso de implementación mientras se habilita el OGS.

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

## Habilitación de Búsqueda de Grupos de Objetos

Actualmente, OGS no está habilitado:

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

1. Inicie sesión en FMC CLI. Vaya a Devices > Device Management > Select the FTD device > Device. Habilite la Búsqueda de Grupo de Objetos desde Configuración Avanzada:

The screenshot displays the Cisco Firepower Management Center (FMC) interface. The main window shows the configuration for a Cisco Firepower 2130 Threat Defense device. A modal dialog titled "Advanced Settings" is open, showing the following configuration:

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

The dialog has "Cancel" and "Save" buttons. In the background, the "Inventory Details" section is visible, showing hardware specifications such as CPU Type (CPU MIPS 1200 MHz), CPU Cores (1 CPU (12 cores)), and Memory (13701 MB RAM).

2. Haga clic en Guardar e implementar.

## Verificación

Antes de activar 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) 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) 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.

Después de habilitar 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 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) 0x1871fd02
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) 0x944a995a
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.

## Información Relacionada

Para obtener información más detallada sobre cómo se amplían las reglas en FTD, consulte el documento [Comprensión de la expansión de reglas en los dispositivos FirePOWER](#).

Para obtener más información sobre la arquitectura de FTD y la resolución de problemas, consulte [Diseción \(FTD\) de Firepower Threat Defence](#).



## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).