# Comprender la expansión de reglas en dispositivos FirePOWER

## Contenido



## Introducción

Este documento describe la traducción de las reglas de control de acceso al sensor cuando se implementa desde Firepower Management Center (FMC).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de la tecnología Firepower
- Conocimientos sobre la configuración de 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.

- Firepower Management Center versión 6.0.0 y posterior
- Imagen de ASA Firepower Defense (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) que ejecuta la versión de software 6.0.1 y posterior

- Imagen de ASA Firepower SFR (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) que ejecuta la versión de software 6.0.0 y posterior

- Sensor de la serie Firepower 7000/8000 versión 6.0.0 y posterior

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, make sure that you understand the potential impact of any command.

# Antecedentes

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

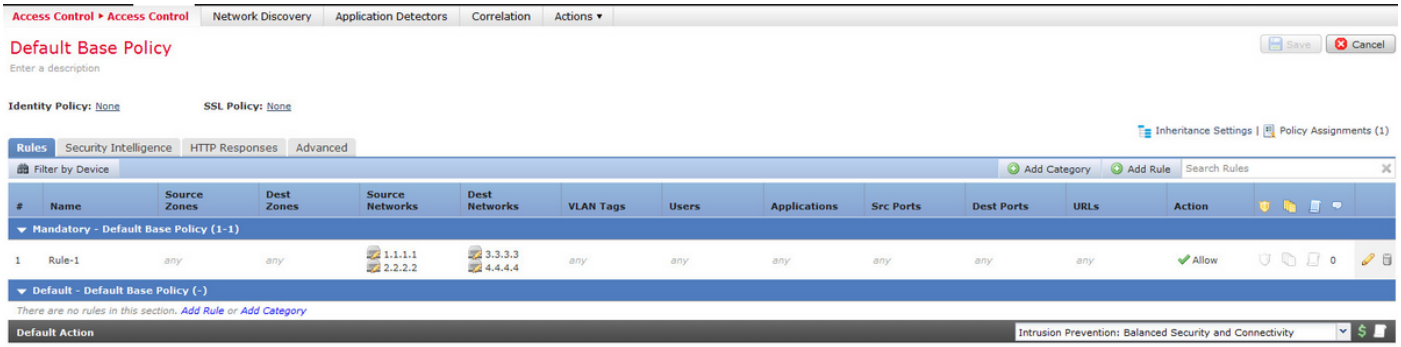
- Dirección IP (origen y destino)
- Puertos (origen y destino)
- URL (categorías proporcionadas por el sistema y URL personalizadas)
- Detectores de aplicaciones
- VLAN
- Zonas

Basándose en la combinación de parámetros utilizados en la regla de acceso, la expansión de reglas cambia en el sensor. Este documento destaca diversas combinaciones de reglas en el FMC y sus respectivas expansiones asociadas en los sensores.

# Introducción a la expansión de reglas

## Expansión de una Regla Basada en IP

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




Se trata de una única regla en el Management Center. Sin embargo, después de implementarlo en el sensor, se expande en **cuatro** reglas como se muestra en la imagen:

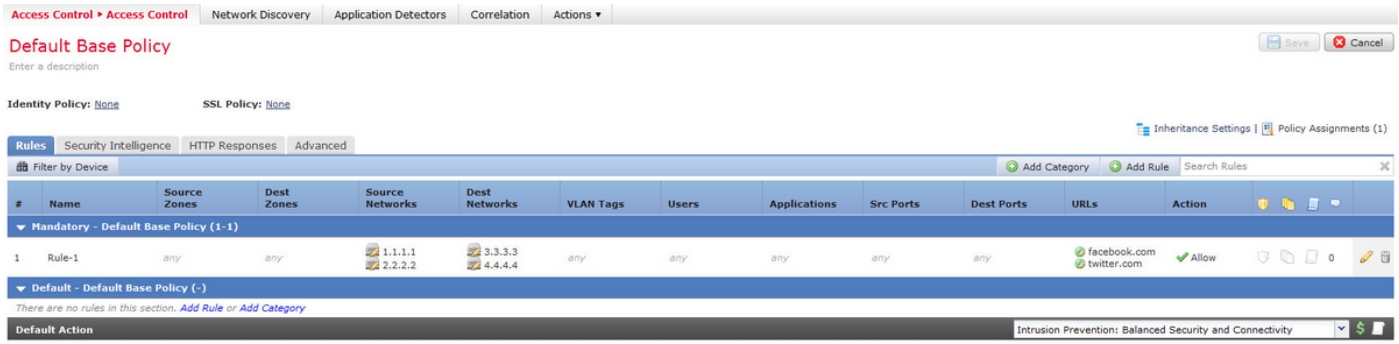
```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

Cuando se implementa una regla con dos subredes configuradas como Origen y dos hosts configurados como direcciones de destino, esta regla se expande a cuatro reglas en el sensor.

> **Nota:** Si el requisito es bloquear el acceso basado en las redes de destino, una mejor manera de hacerlo es utilizar la función de listas negras bajo Inteligencia de seguridad.

## Expansión de una regla basada en IP mediante URL personalizada

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



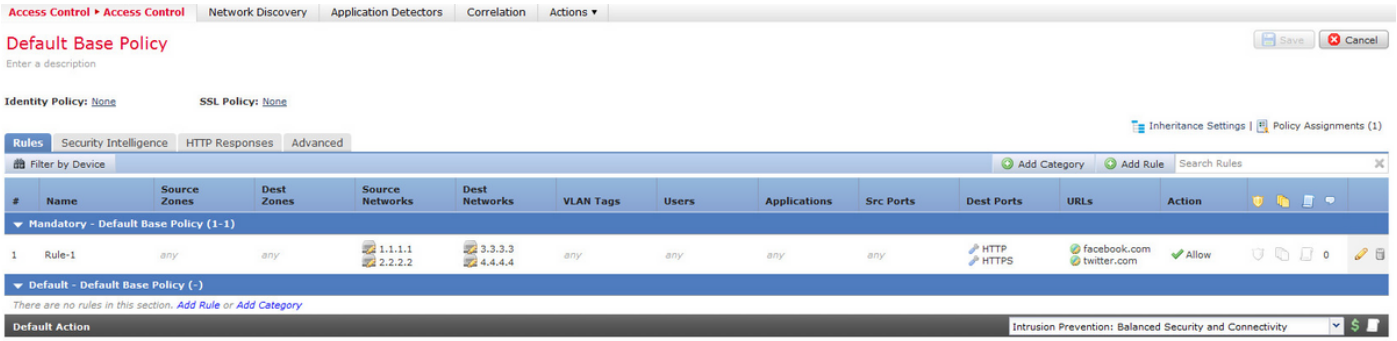

Se trata de una única regla en el Management Center. Sin embargo, después de implementarlo en el sensor, se expande a ocho reglas como se muestra en la imagen:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

Cuando se implementa una regla con dos subredes configuradas como Origen, dos hosts configurados como direcciones de destino y dos objetos URL personalizados en una sola regla en el Centro de administración , esta regla se expande a ocho reglas en el sensor. Esto significa que para cada categoría de URL personalizada hay una combinación de intervalos de IP/puertos de origen y de destino, que se configuran y crean.

## Expansión de una regla basada en IP mediante puertos

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



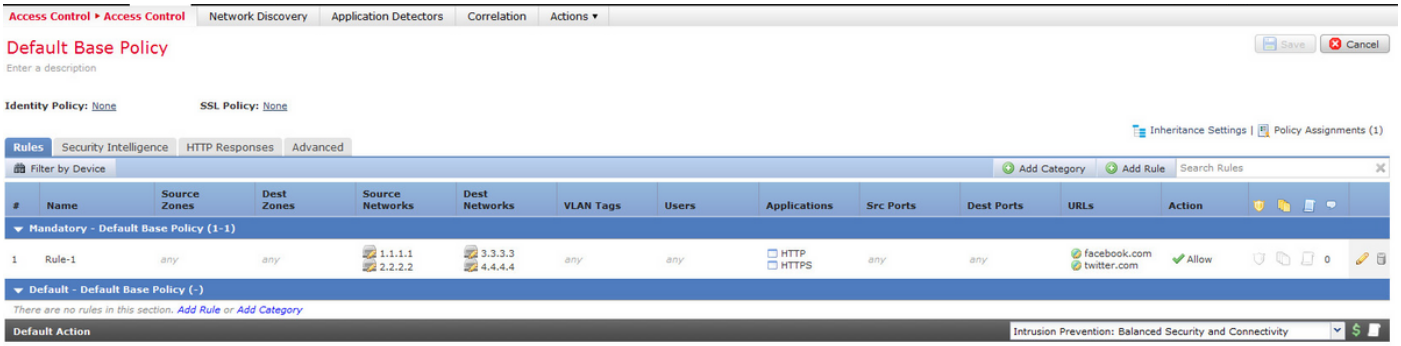

Se trata de una única regla en el Management Center. Sin embargo, después de implementarlo en el sensor, se expande en dieciséis reglas, como se muestra en la imagen:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268435456 allow any any any any any any any any (ipspolicy 2)
```

Cuando se implementa una regla con dos subredes configuradas como Origen, dos hosts configurados como direcciones de destino y dos objetos URL personalizados destinados a dos puertos, esta regla se expande a dieciséis reglas en el sensor.

> **Nota**: Si hay un requisito para utilizar los puertos en la regla de acceso, utilice **detectores de aplicaciones** presentes para las aplicaciones estándar. Esto ayuda a que la expansión de las reglas se lleve a cabo de forma eficaz.

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

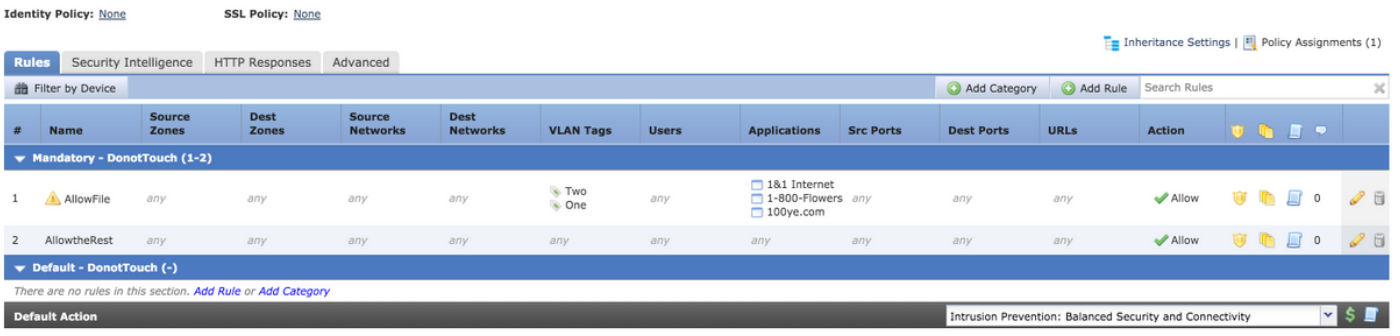



Cuando utiliza detectores de aplicaciones en lugar de puertos, el número de reglas expandidas se reduce de dieciséis a ocho, como se muestra en la imagen:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
```

## Expansión de una Regla Basada en IP Usando VLAN

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




La regla **AllowFile** tiene una sola línea que coincide con dos ID de VLAN con algunos detectores de aplicación, políticas de intrusión y políticas de archivo. La regla AllowFile se expandirá a dos reglas.

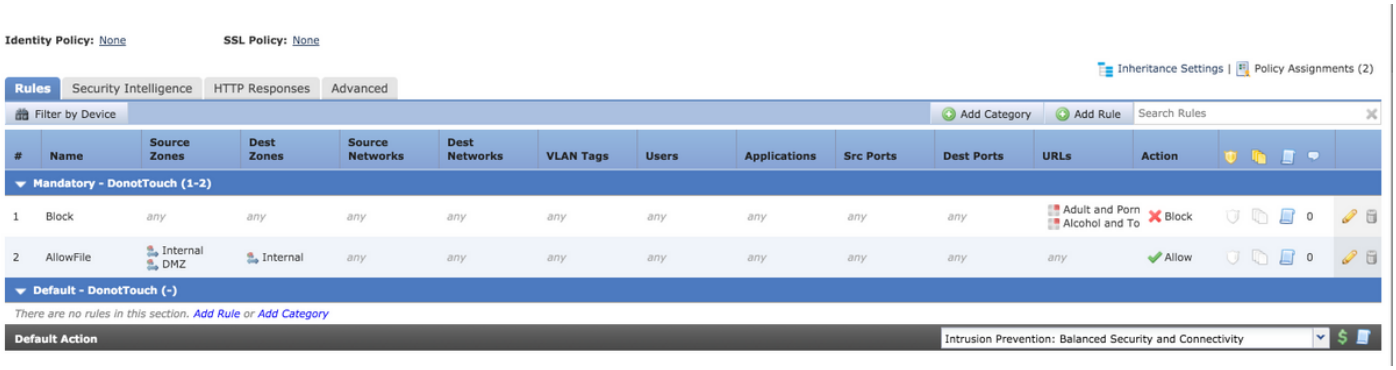
```
268436480 allow any any any any any any 1 any (log dcforward flowstart) (ipspolicy 5)
(filepolicy 1 enable) (appid 535:4, 1553:4, 3791:4)
268436480 allow any any any any any any 2 any (log dcforward flowstart) (ipspolicy 5)
(filepolicy 1 enable) (appid 535:4, 1553:4, 3791:4)
```

Las políticas IPS y las políticas de archivos son únicas para cada regla de control de acceso, pero se hace referencia a varios detectores de aplicaciones en la misma regla y, por lo tanto, no

participan en la expansión. Cuando considera una regla con dos ID de VLAN y tres detectores de aplicaciones, sólo hay dos reglas, una para cada VLAN.

## Expansión de una regla basada en IP con categorías de URL

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




La Regla de Bloqueo bloquea las categorías de URL para **Adultos y pornografía Cualquier reputación** y **reputación de alcohol y tabaco 1-3.** Se trata de una única regla en el Management Center, pero cuando la implementa en el sensor se expande en dos reglas, como se muestra en la siguiente:

```
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 11)
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 76) (urlrep
le 60)
```

Cuando implementa una única regla con dos subredes configuradas como Origen y dos hosts configurados como direcciones de destino, junto con dos objetos URL personalizados destinados a dos puertos con dos categorías de URL, esta regla se expande a treinta y dos reglas en el sensor.

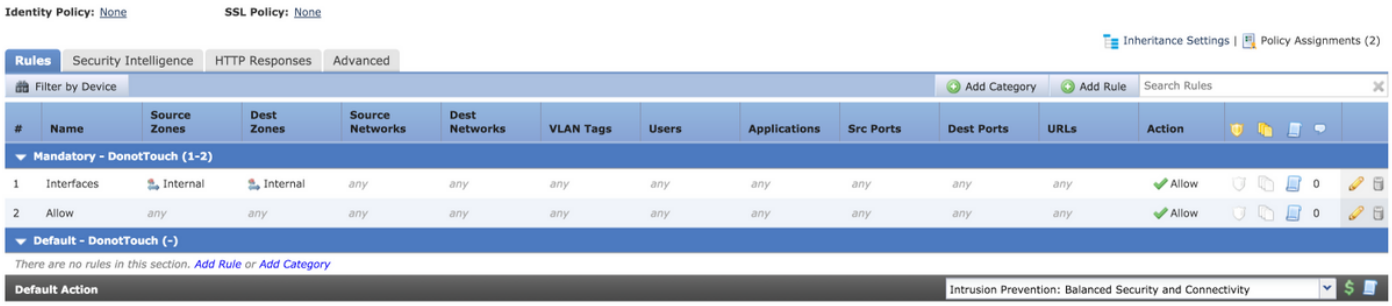
## Expansión de una regla basada en IP con zonas

Las zonas son números asignados a los que se hace referencia en las políticas.

Si se hace referencia a una zona en una política pero esa zona no se asigna a ninguna interfaz en el dispositivo al que se envía la política, la zona se considera como **any** y **any** no conduce a ninguna expansión de reglas.

Si la zona de origen y la zona de destino son iguales en la regla, el factor de zona se considera **cualquiera** y sólo se agrega una regla, ya que ANY no produce ninguna expansión de reglas.

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



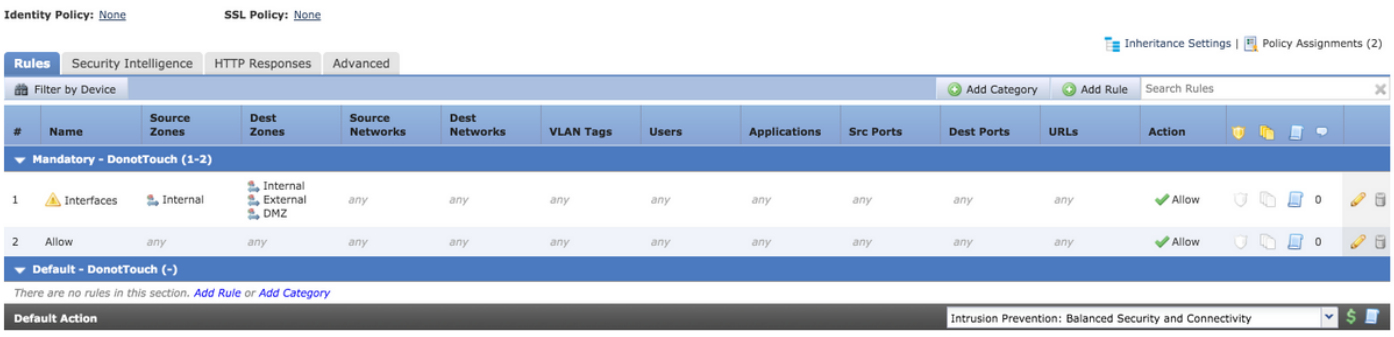

Hay dos reglas. Una regla tiene Zones configuradas pero la zona de origen y destino es la misma. La otra regla no tiene una configuración específica. En este ejemplo, la regla de acceso **Interfaces** no se traduce en una regla.

```
268438531 allow any any any any any any any any (log dcforward flowstart)<-----Allow Access Rule
268434432 allow any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<-------
---Default Intrusion Prevention Rule
```

En el sensor ambas reglas aparecen como las mismas porque el control basado en zonas que involucra las mismas interfaces no conduce a una expansión.

La expansión de reglas para el acceso a la regla de control de acceso basado en zona se produce cuando la zona a la que se hace referencia en la regla se asigna a una interfaz en el dispositivo.

Considere la configuración de una regla de acceso desde el FMC como se muestra a continuación:




La regla Interfaces implica reglas basadas en zonas con zona de origen como zonas internas y de destino como Internas, Externas y DMZ. En esta regla, las zonas de interfaz interna y DMZ se configuran en las interfaces y External no existe en el dispositivo.Ésta es la expansión de lo mismo:

```
268436480 allow 0 any any 2 any any any any (log dcforward flowstart) <------Rule for Internal
to DMZ)
268438531 allow any any any any any any any any (log dcforward flowstart)<--------Allow Access
rule
268434432 allow any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<-------
-Default Intrusion Prevention: Balanced Security over Connectivity
```

Se crea una regla para un par de interfaces específico que es **Internal > DMZ** con especificación de zona clara y una **Internal > Internal** no se crea la regla.

El número de reglas expandidas es proporcional al número de pares de origen y destino de zona que se pueden crear para las zonas **válidas** asociadas y esto incluye las mismas reglas de zona de origen y destino.

> **Nota:** Las reglas desactivadas del FMC no se propagan y no se expanden al sensor durante la implementación de la política.

## Fórmula general para la expansión de reglas

**Número de reglas en el sensor = (Número de subredes de origen o hosts) * (Número de destino S) * (Número de puertos de origen) * (Número de puertos de destino) * (Número de URL personalizadas)* (Número de etiquetas de VLAN)* (Número de categorías de URL)** (Número de pares de zonas de origen y destino válidos)**

> **Nota:** Para los cálculos, **cualquier** valor del campo se sustituye por 1.El valor **any** en la combinación de reglas se considera como 1 y no aumenta ni expande la regla.

## Resolución de problemas de falla de implementación debido a expansión de reglas

Cuando se produzca un error de implementación después de agregar la regla de acceso, siga los pasos mencionados a continuación para los casos en los que se haya alcanzado el límite de expansión de la regla

Verifique **/var/log/action.queue.log** para ver mensajes con las siguientes palabras clave :

**Error: demasiadas reglas: escribir regla 28, reglas máx. 9094**

El mensaje anterior indica que hay un problema con el número de reglas que se están expandiendo. Verifique la configuración en el FMC para optimizar las reglas en función de la situación descrita anteriormente.

## Información Relacionada

- Guía de Configuración de Firepower Management Center, Versión 6.0
- Soporte Técnico y Documentación - Cisco Systems