Entender a expansão de regra em dispositivos FirePOWER

Contents

Introdução

Este documento descreve a conversão das regras de controle de acesso para o sensor quando implantado do Firepower Management Center (FMC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento da tecnologia Firepower
- Conhecimento sobre a configuração das políticas de controle de acesso no FMC

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Firepower Management Center versão 6.0.0 e posterior
- Imagem do ASA Firepower Defense (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X,

ASA 5585-X) executando a versão de software 6.0.1 e posterior

- ASA Firepower SFR Image (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) executando a versão de software 6.0.0 e posterior
- Sensor Firepower 7000/8000 series versão 6.0.0 e superior

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Uma regra de controle de acesso é criada com o uso de uma ou várias combinações destes parâmetros:

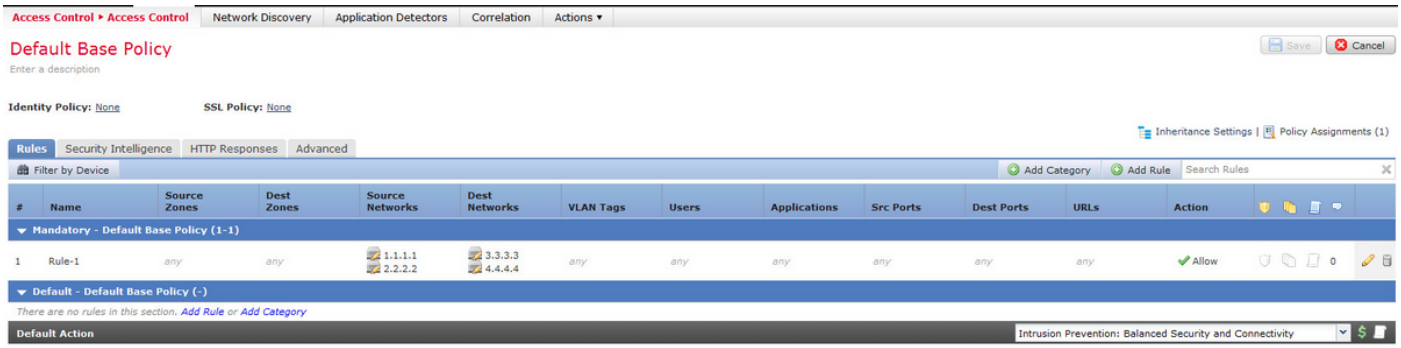
- Endereço IP (origem e destino)
- Portas (origem e destino)
- URL (Categorias fornecidas pelo sistema e URLs personalizadas)
- Detectores de aplicativos
- VLANs
- Zonas

Com base na combinação de parâmetros usados na regra de acesso, a expansão da regra muda no sensor. Este documento destaca várias combinações de regras no FMC e suas respectivas expansões associadas nos sensores.

Compreendendo a expansão de regra

Expansão de uma regra baseada em IP

Considere a configuração de uma regra de acesso do FMC, como mostrado na imagem:



Essa é uma regra única no Management Center. No entanto, depois de implantá-lo no sensor, ele se expande em quatro regras, como mostrado na imagem:

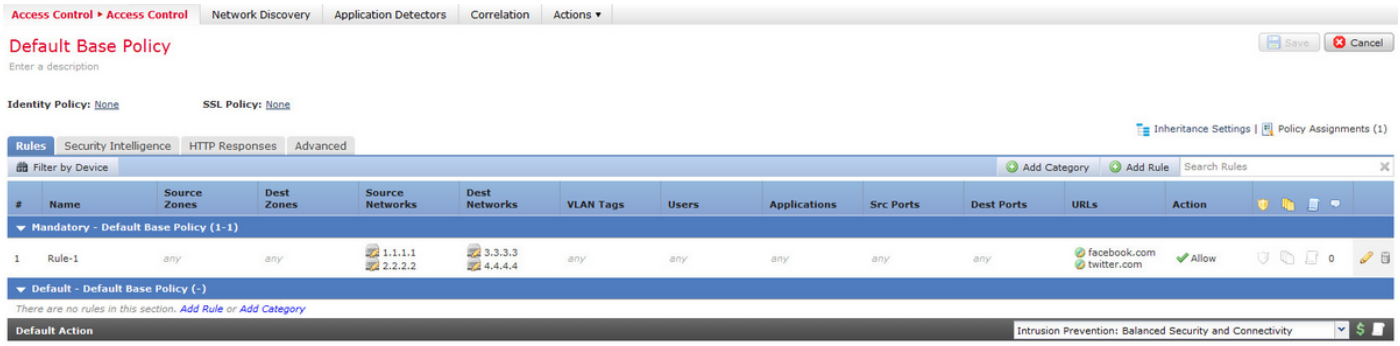
```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32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

Quando você implanta uma regra com duas sub-redes configuradas como Origem e dois hosts configurados como endereços de destino, essa regra é expandida para quatro regras no sensor.

> Observação: se o requisito for bloquear o acesso com base nas redes de destino, uma maneira melhor de fazer isso é usar o recurso Listas negras em Inteligência de segurança.

Expansão de uma Regra Baseada em IP Usando URL Personalizada

Considere a configuração de uma regra de acesso do FMC como mostrado na imagem:



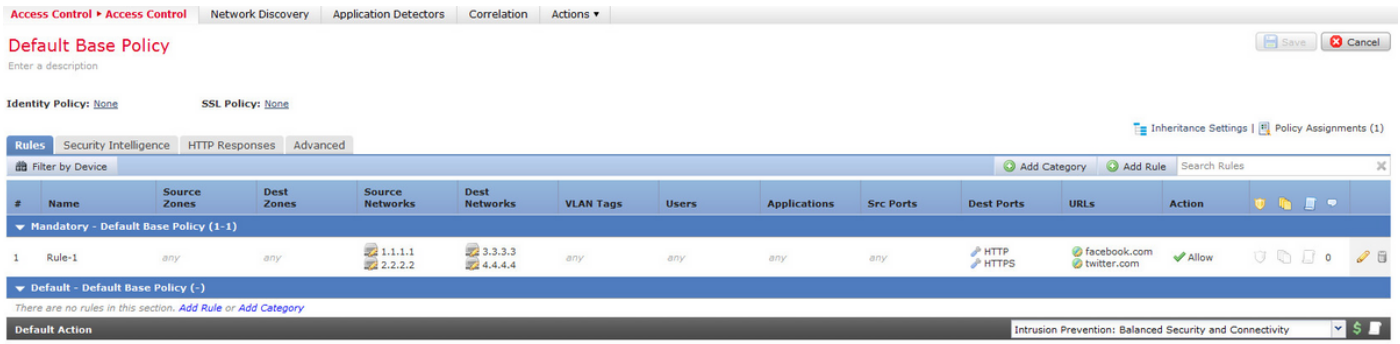
Essa é uma regra única no Management Center. No entanto, depois de implantá-lo no sensor, ele é expandido em oito regras, como mostrado na imagem:

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

Quando você implanta uma regra com duas sub-redes configuradas como Origem, dois hosts configurados como endereços de destino e dois objetos de URL personalizados em uma única regra no Management Center , essa regra é expandida para oito regras no sensor. Isso significa que para cada categoria de URL personalizada há uma combinação de intervalos de IP/porta origem e destino, que são configurados e criados.

Expansão de uma regra baseada em IP usando portas

Considere a configuração de uma regra de acesso do FMC como mostrado na imagem:



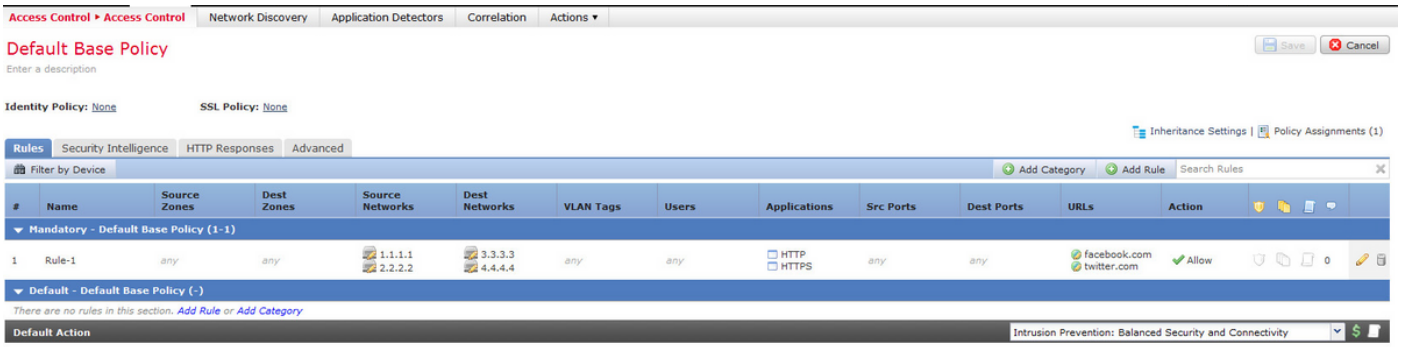
Essa é uma regra única no Management Center. No entanto, depois de implantá-lo no sensor, ele é expandido em dezesseis regras, como mostrado na imagem:

```
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.co
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.co
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.co
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.co
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)
```

Quando você implanta uma regra com duas sub-redes configuradas como Origem, dois hosts configurados como endereços de destino e dois objetos de URL personalizados destinados a duas portas, essa regra se expande para dezesseis regras no sensor.

> Observação: se houver um requisito para usar as portas na regra de acesso, use detectores de aplicativo que estão presentes para aplicativos padrão. Isso ajuda a expandir as regras de forma eficiente.

Considere a configuração de uma regra de acesso do FMC como mostrado na imagem:

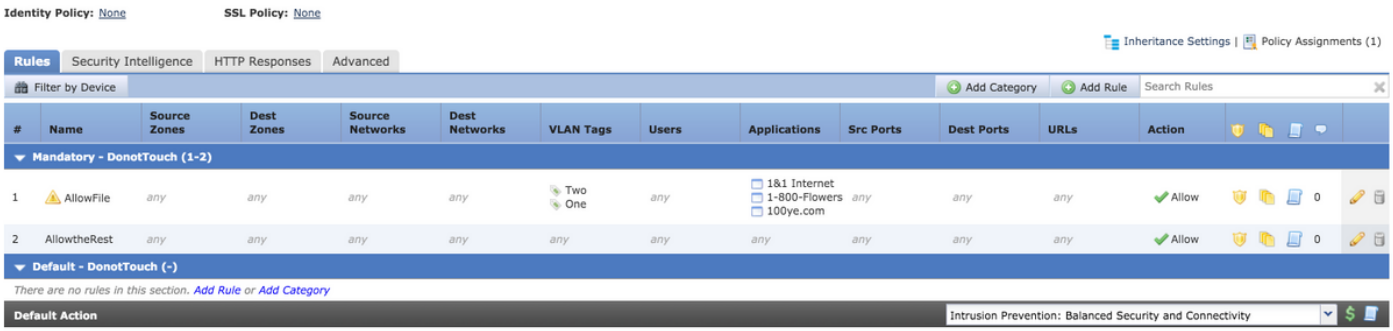


Quando você usa detectores de aplicativo em vez de portas, o número de regras expandidas é reduzido de dezesseis para oito, como mostrado na imagem:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1
```

Expansão de uma regra baseada em IP usando VLANs

Considere a configuração de uma regra de acesso do FMC como mostrado na imagem:



A regra AllowFile tem uma única linha que corresponde a duas IDs de VLAN com alguns detectores de aplicativos, políticas de intrusão e políticas de arquivo. A regra AllowFile será expandida para duas regras.

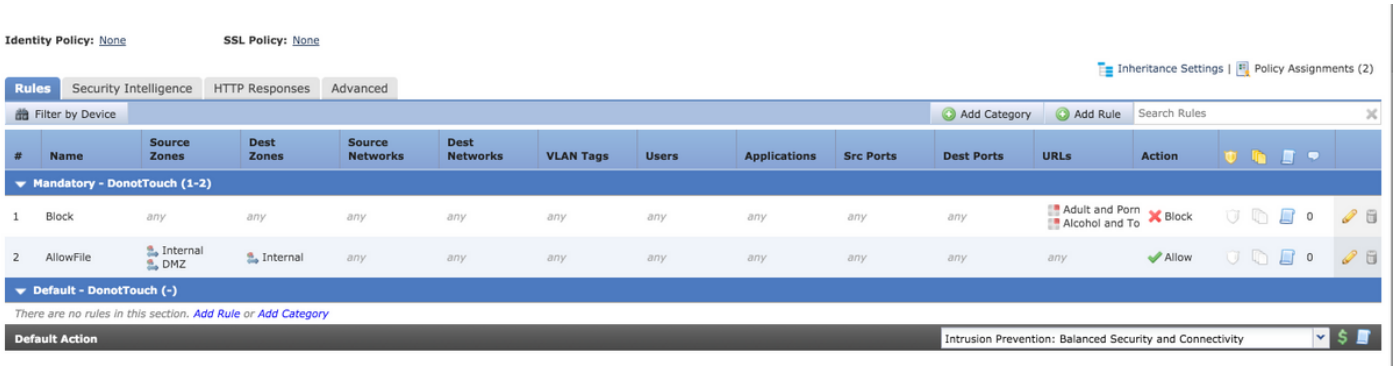
```
268436480 allow any any any any any any 1 any (log dcforward flowstart) (ipspolicy 5) (filepolicy 1 ena
268436480 allow any any any any any any 2 any (log dcforward flowstart) (ipspolicy 5) (filepolicy 1 ena
```

As políticas de IPS e de arquivo são exclusivas para cada Regra de controle de acesso, mas

vários detectores de aplicativo são mencionados na mesma regra e, portanto, não participam da expansão. Quando você considera uma regra com duas IDs de VLAN e três detectores de aplicativos, há apenas duas regras, uma para cada VLAN.

Expansão de uma regra baseada em IP com categorias de URL

Considere a configuração de uma regra de acesso do FMC como mostrado na imagem:



A Regra de Bloqueio bloqueia categorias de URL para adultos e pornografia Qualquer Reputação e Reputações de Álcool e Cigarro 1-3. Essa é uma regra única no Management Center, mas quando você a implanta no sensor, ela é expandida em duas regras, conforme mostrado a seguir:

```
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)
```

Quando você implanta uma única regra com duas sub-redes configuradas como Origem e dois hosts configurados como endereços de destino, juntamente com dois objetos de URL personalizados destinados a duas portas com duas categorias de URL, essa regra se expande para trinta e duas regras no sensor.

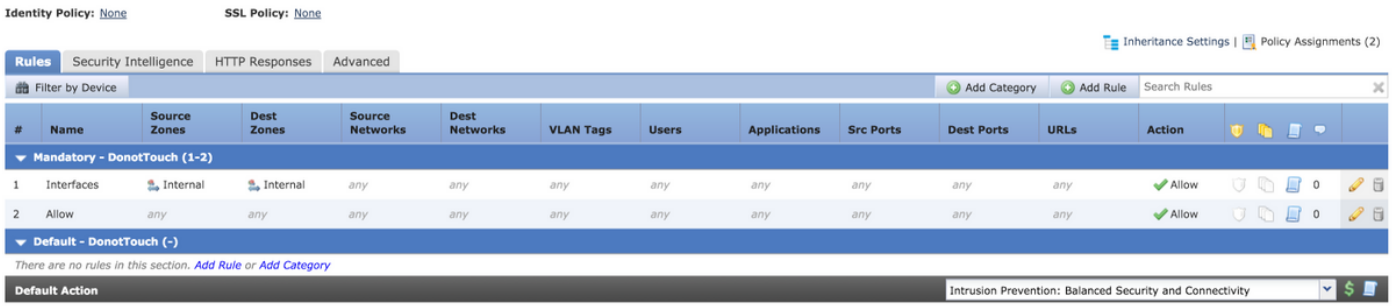
Expansão de uma regra baseada em IP com regiões

As zonas recebem números que são referenciados em políticas.

Se uma região for referenciada em uma política, mas essa região não for atribuída a nenhuma interface no dispositivo para o qual a política está sendo enviada, a região será considerada como any e any não levará a nenhuma expansão das regras.

Se a zona de origem e a zona de destino forem as mesmas na regra, o fator de zona será considerado como qualquer e apenas uma regra será adicionada, pois QUALQUER não leva a nenhuma expansão das regras.

Considere a configuração de uma regra de acesso do FMC como mostrado na imagem:



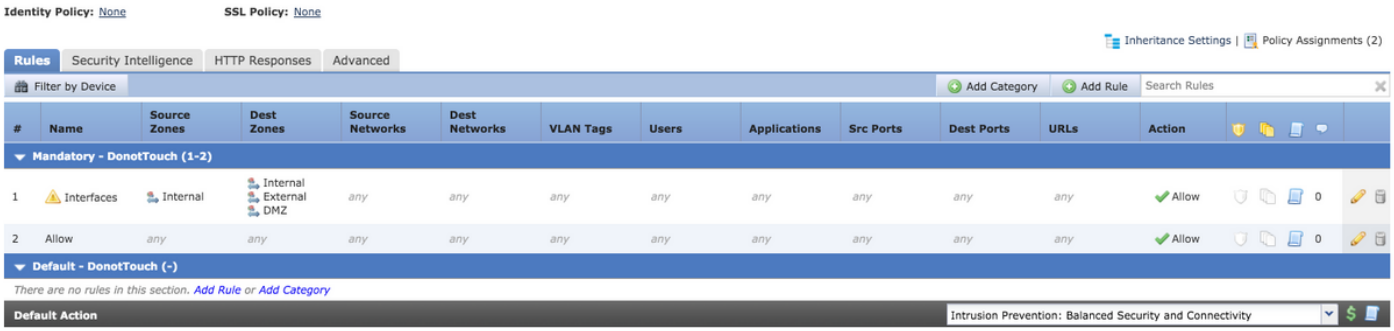
Há duas regras. Uma regra tem Zonas configuradas, mas as zonas de origem e destino são as mesmas. A outra regra não tem configuração específica. Neste exemplo, a regra de acesso Interfaces não se traduz em uma regra.

```
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)<----------Defa
```

No sensor, ambas as regras aparecem como as mesmas porque o controle baseado em zona envolvendo as mesmas interfaces não leva a uma expansão.

A expansão de regras para o acesso à Regra de controle de acesso baseada em zona ocorre quando a zona mencionada na regra é atribuída a uma interface no dispositivo.

Considere a configuração de uma regra de acesso do FMC como mostrado abaixo:



As Interfaces de regra envolvem regras baseadas em zona com a zona de origem como Interna e as zonas de destino como Interna, Externa e DMZ. Nesta regra, as zonas de interface interna e DMZ são configuradas nas interfaces e Externa não existe no dispositivo.Esta é a expansão do mesmo:

```
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)<--------Defaul
```

Uma regra é criada para um par de interfaces específico que é Internal > DMZ com especificação de zona clara e uma regra Internal > Internal não é criada.

O número de regras expandidas é proporcional ao número de pares de origem e destino de zona que podem ser criados para zonas válidas associadas e isso inclui as mesmas regras de zona de origem e destino.

> Observação: as regras desativadas do FMC não são propagadas nem expandidas para o sensor durante a implantação da política.

Fórmula Geral para Expansão de Regra

Número de regras no sensor = (Número de sub-redes de origem ou hosts) * (Número de destino S) * (Número de portas de origem) * (Número de portas de destino) * (Número de URLs personalizadas) * (Número de marcas de VLAN)* (Número de categorias de URL)* (Número de pares válidos de zonas de origem e de destino)

> Nota: Para os cálculos, qualquer valor no campo é substituído por 1. O valor any na combinação de regras é considerado como 1 e não aumenta nem expande a regra.

Troubleshooting de Falha de Implantação devido à Expansão da Regra

Quando houver uma falha de implantação após a adição à regra de acesso, siga as etapas mencionadas abaixo para os casos em que o limite de expansão da regra foi atingido

Verifique se há mensagens no /var/log/action.queue.log com as seguintes palavras-chave:

Erro - muitas regras - regra de gravação 28, máximo de regras 9094

A mensagem acima indica que há um problema com o número de regras que estão sendo expandidas. Verifique a configuração no FMC para otimizar as regras com base nos cenários discutidos acima.

Informações Relacionadas

- Guia de configuração do Firepower Management Center, versão 6.0
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.