Calcule a contagem de elementos da lista de acesso (ACE) usando a CLI do FMC

Contents

Introdução

Este documento descreve como você pode localizar qual regra em sua política de controle de acesso está se expandindo para quantos elementos da lista de acesso.

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:

- Cisco Secure Firewall Management Center (FMC)
- Defesa contra ameaças (FTD) do Cisco Firepower

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 rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Informações de Apoio

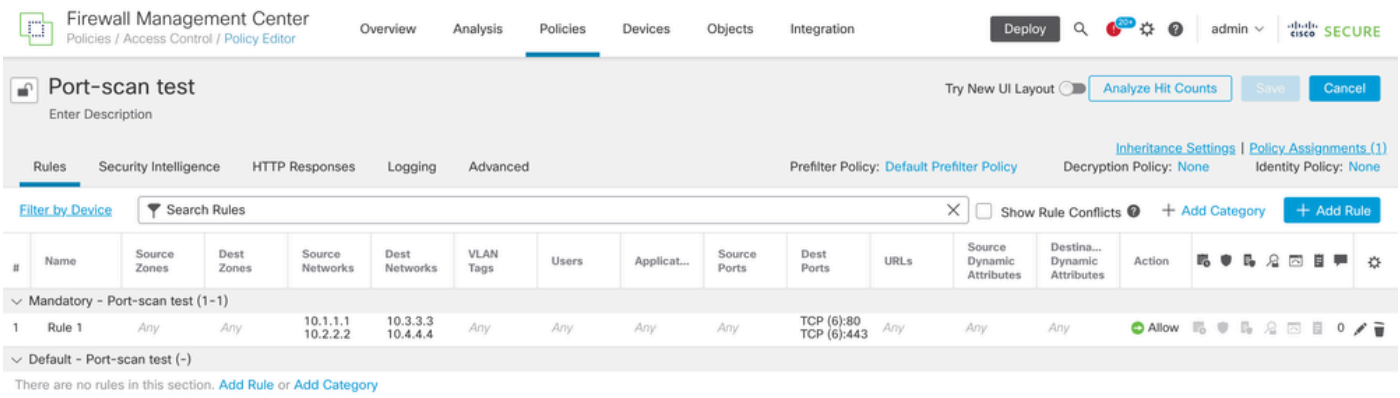
Uma regra de controle de acesso é criada com o uso de uma ou várias combinações destes parâmetros:

- 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.

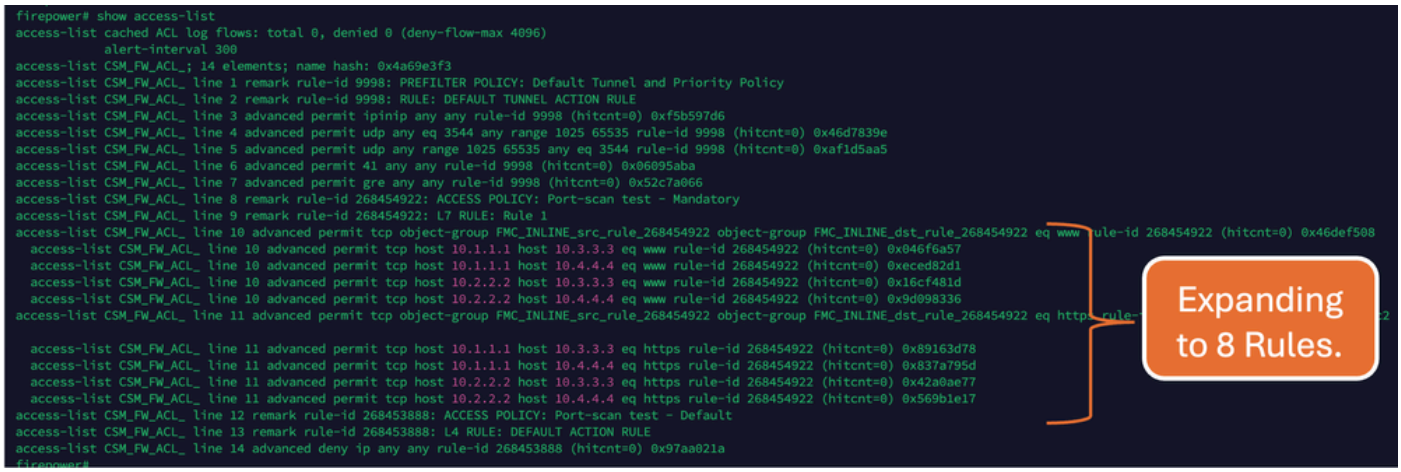
Como calcular a ACE (Access List Element Count, contagem de elementos da lista de acesso) usando a CLI do FMC

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



Configuração de Regra na Política de Controle de Acesso

Se você vir essa regra na CLI de FTD, perceberá que essa regra foi expandida em 8 Regras.



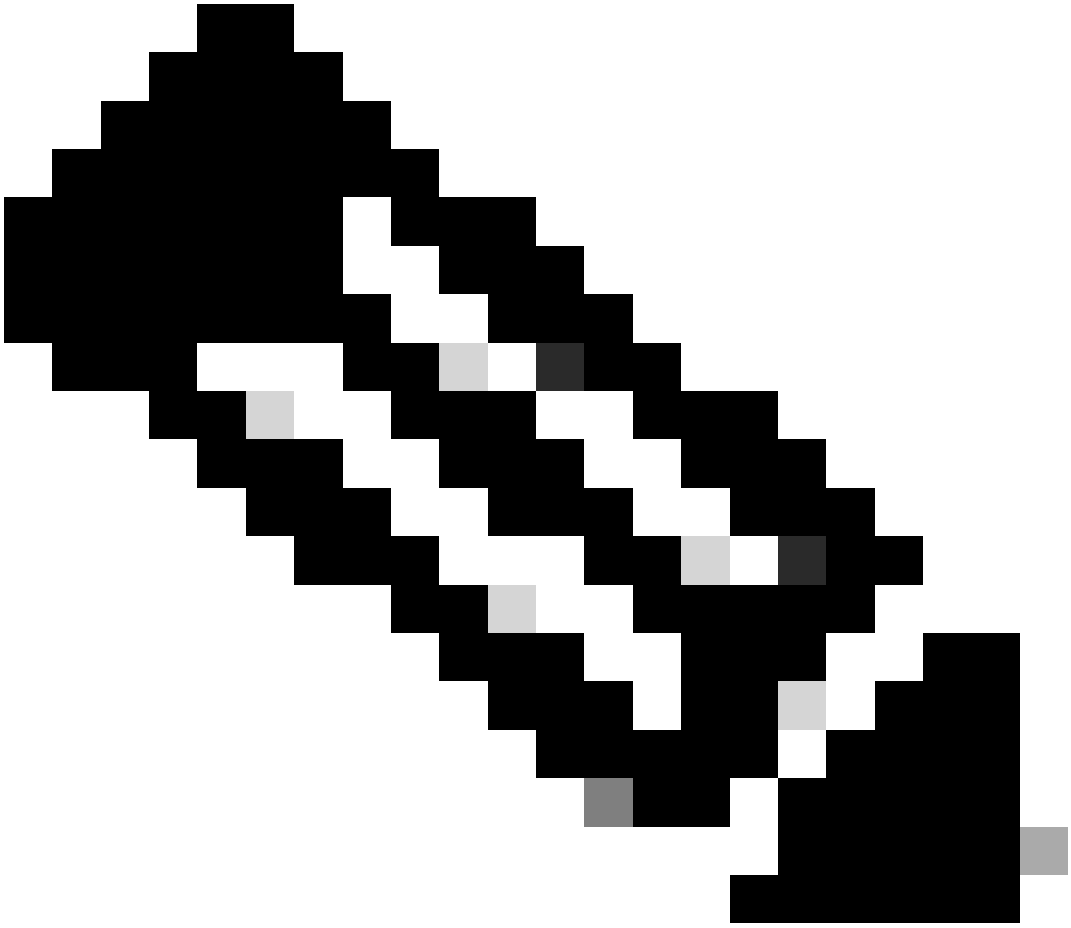
Você pode verificar qual regra está se expandindo para quantos elementos da lista de acesso usando o comando perl na CLI do FMC:

<#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 rules


-------------------------------------------------------------------------------------------------------
| 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: Elementos da Regra de Acesso Contam no FTD: 14. Isso também inclui o conjunto padrão de regras de FTD (pré-filtro) e a regra de controle de acesso padrão.

As regras de pré-filtro padrão podem ser vistas na CLI do 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 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) 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
```

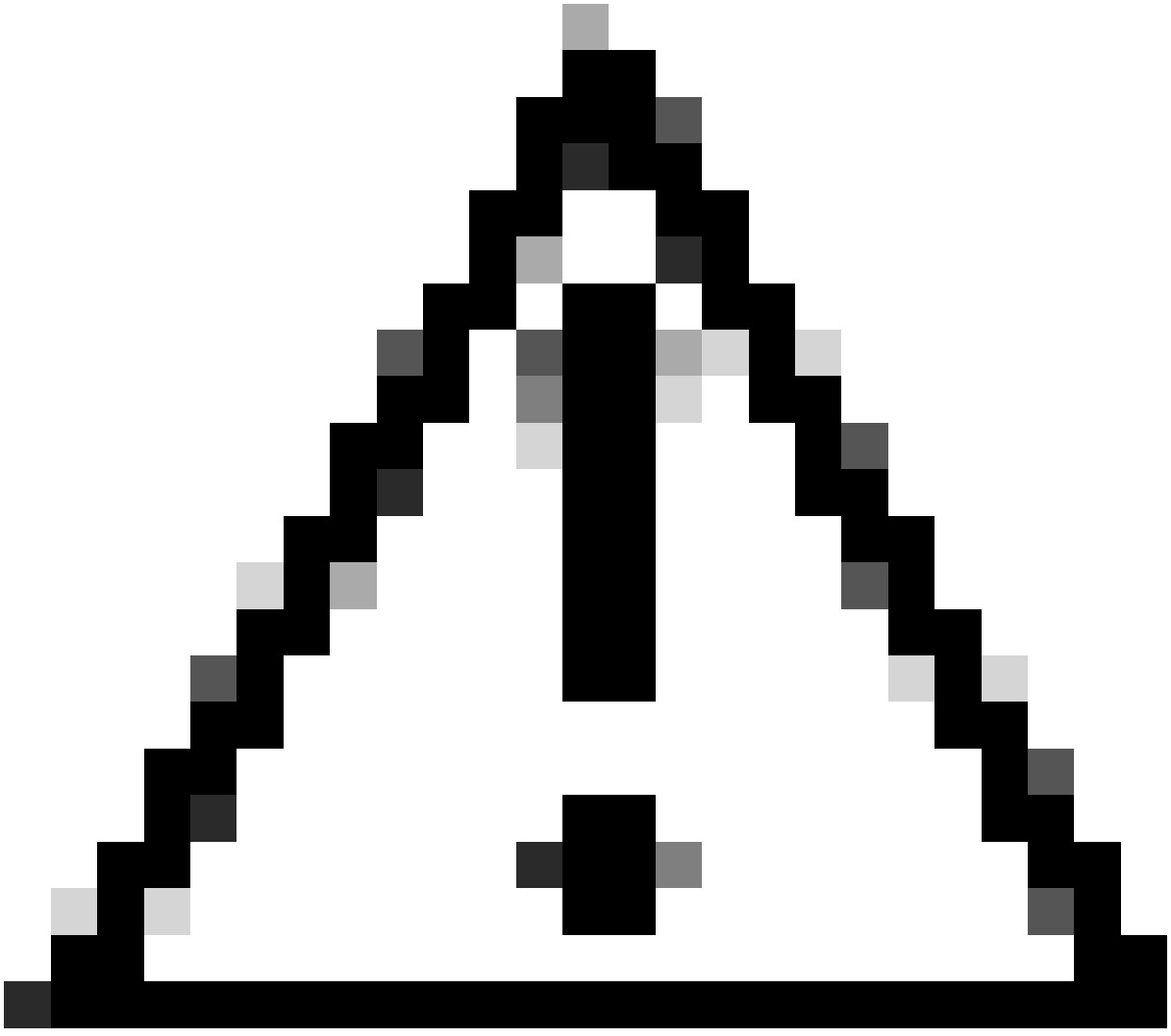
6 Default Pre-filter Rules.

Impacto da alta ACE

- Pode-se ver uma CPU alta.
- A memória alta pode ser vista.
- A lentidão do dispositivo pode ser observada.
- Falha nas implantações/Tempo de implantação mais longo.

Decidir Quando Ativar a Pesquisa de Grupos de Objetos (OGS)

- A contagem de ACEs está excedendo o limite de ACEs do dispositivo.
- A CPU do dispositivo ainda não está alta, pois a ativação de OGS aumenta a pressão sobre a CPU do dispositivo.
- Habilite-o durante horas que não sejam de Produção.



Cuidado: habilite o asp rule-engine transactional-commit access-group do modo de clish FTD CLI antes de habilitar o OGS. Isso é configurado para evitar quedas de tráfego durante e logo após o processo de implantação ao habilitar o OGS.

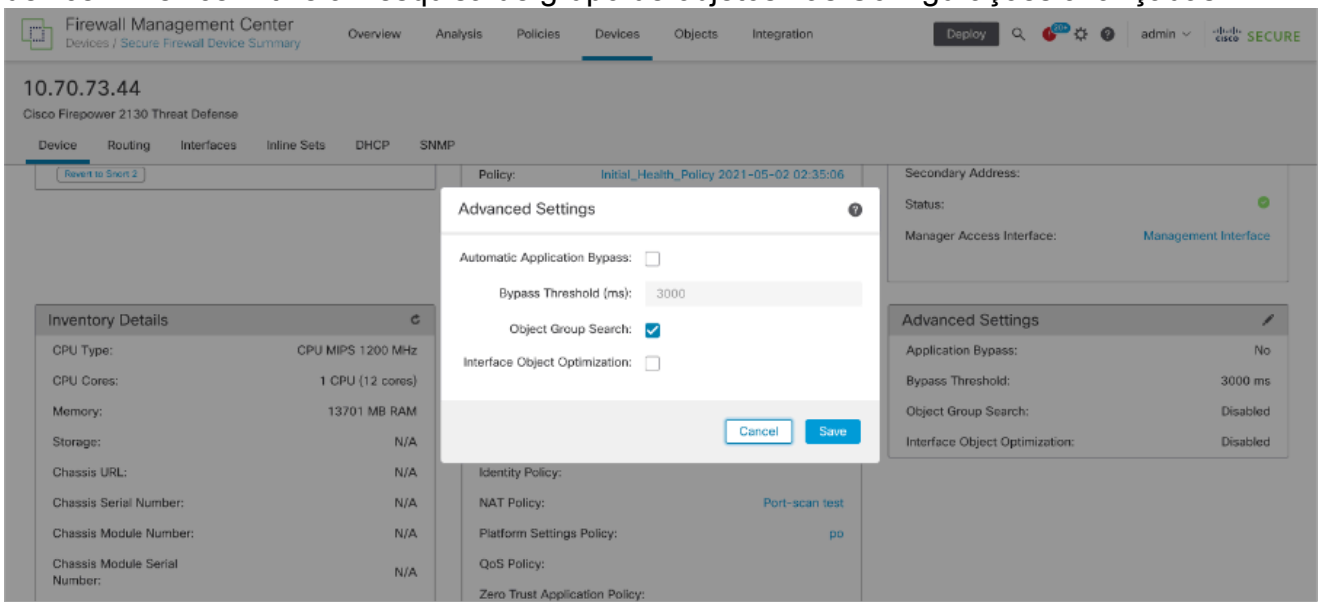
```
>
>
>
>
> asp rule-engine transactional-commit access-group
>
>
>
```

Ativando a Pesquisa de Grupos de Objetos

No momento, o OGS não está habilitado:

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

1. Faça login na CLI do FMC. Navegue até Devices > Device Management > Select the FTD device > Device. Ative a Pesquisa de grupo de objetos nas Configurações avançadas:

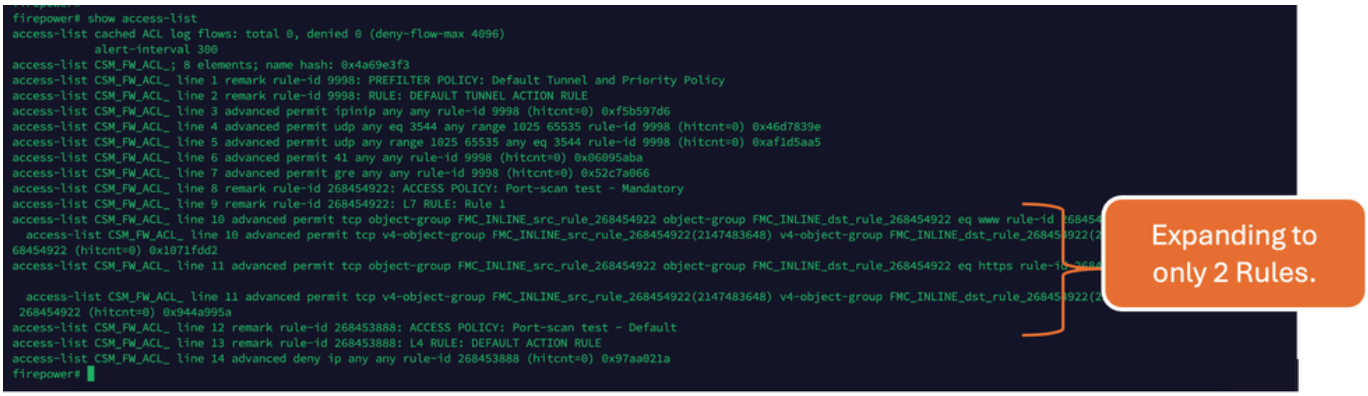


2. Clique em Salvar e implantar.

Verificar

Antes de o OGS ser habilitado:

Depois que o OGS for habilitado:



Informações Relacionadas

Para obter informações mais detalhadas sobre como as regras são expandidas no FTD, consulte o documento Compreender a expansão de regras em dispositivos FirePOWER.

Para obter mais informações sobre a arquitetura e a solução de problemas do FTD, consulte Dissecting (FTD) Firepower Threat Defense.

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.