Configurar objeto FQDN na ACL estendida para PBR no FMC

Contents

Introdução

Este documento descreve o procedimento para configurar um objeto FQDN em uma lista de acesso estendida (ACL) para uso no Roteamento Baseado em Políticas (PBR - Policy Based Routing).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento sobre estes produtos:

- Centro de gerenciamento seguro de firewall (FMC)
- Defesa contra ameaças de firewall (FTD) segura
- PBR

Componentes Utilizados

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

- Firepower Threat Defense para VMware versão 7.6.0
- Secure Firewall Management Center for VMware versão 7.6.0

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

Atualmente, o FTD não permite a filtragem de tráfego não HTTP usando objetos Fully Qualified Domain Name (FQDN), conforme mencionado no bug da Cisco ID CSCuz98322.

Essa funcionalidade é suportada em plataformas ASA, no entanto, somente redes e aplicativos podem ser filtrados no FTD.

Você pode adicionar um objeto FQDN a uma lista de acesso estendida para configurar o PBR usando esse método.

Configurar

Etapa 1. Crie objetos FQDN conforme necessário.

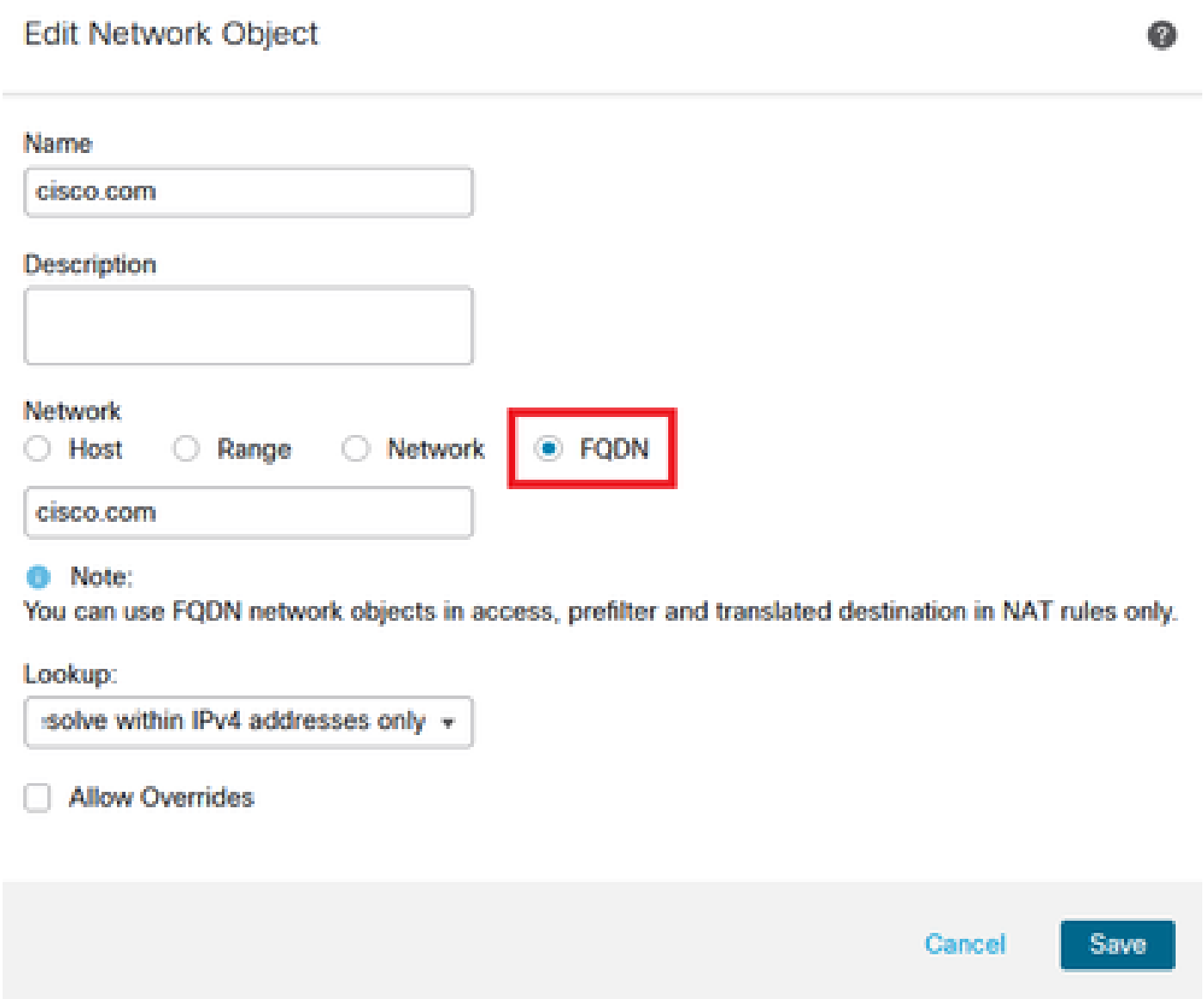

Imagem 1. Menu do objeto de rede

Etapa 2. Crie uma lista de acesso estendida em Objetos > Gerenciamento de objetos > Lista de

acesso > Estendida.

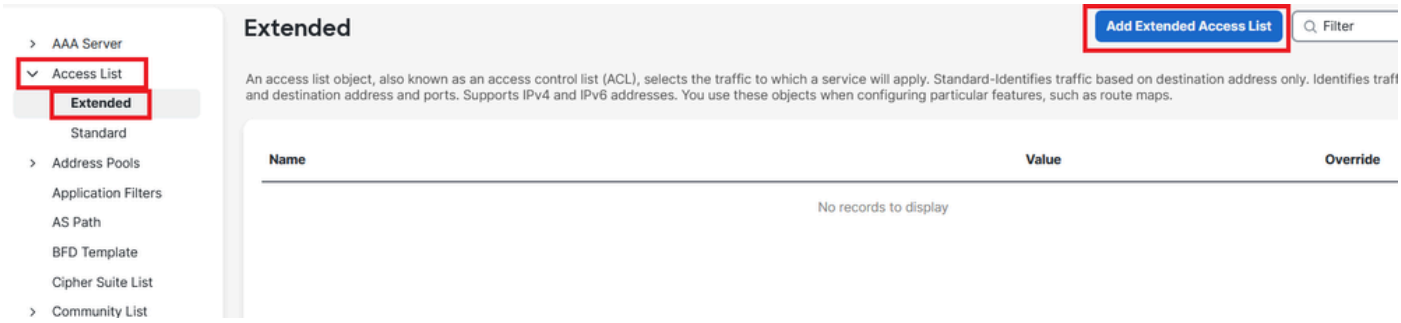

Imagem 2. Menu da Lista de Acesso Estendida

Ao adicionar uma nova regra, observe que você não pode ver o objeto FQDN configurado ao fazer uma pesquisa nos Objetos de Rede para selecionar a origem e o destino.

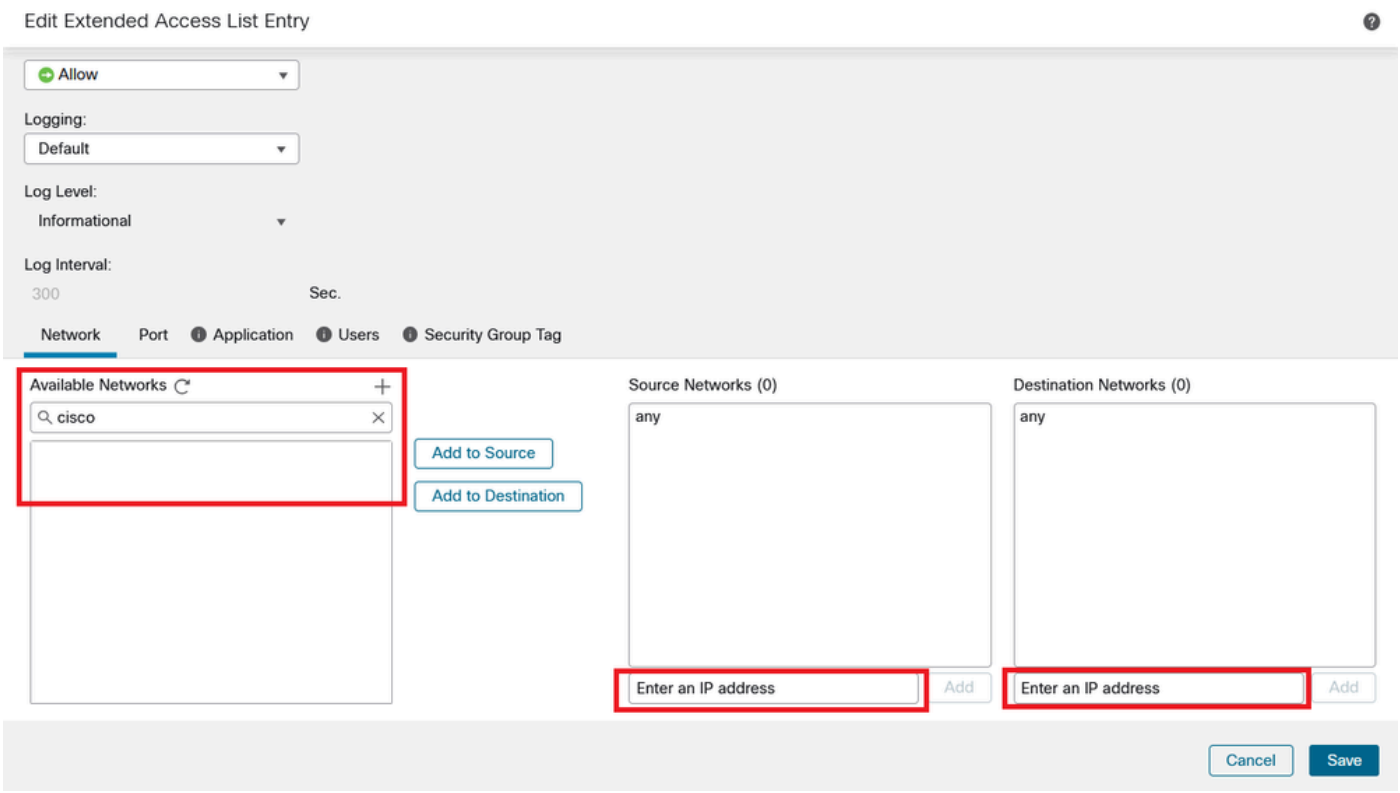

Imagem 3. Novo Menu de Regra da Lista de Acesso Estendida

Etapa 3. Crie uma regra que não possa ser atingida para que a ACL estendida seja criada e disponibilizada para a configuração do PBR.

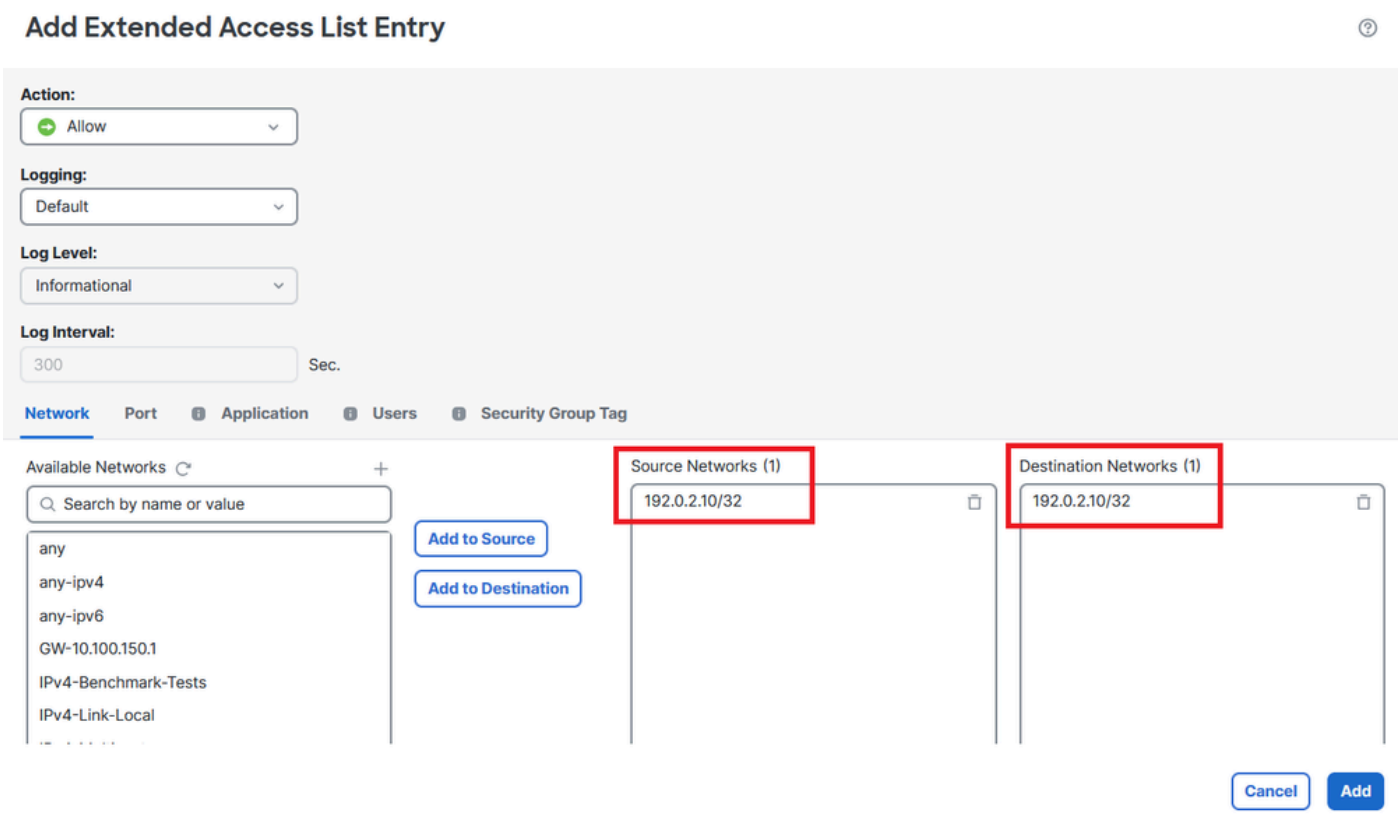

Imagem 4. Configuração de regra de lista de acesso que não pode ser atingida

Etapa 4. Você precisa criar uma regra na ACP (Access-Control Policy, Política de controle de acesso) direcionando seu FTD com o objeto FQDN. O FMC implanta o objeto FQDN no FTD para que você possa referenciá-lo por meio de um objeto FlexConfig.

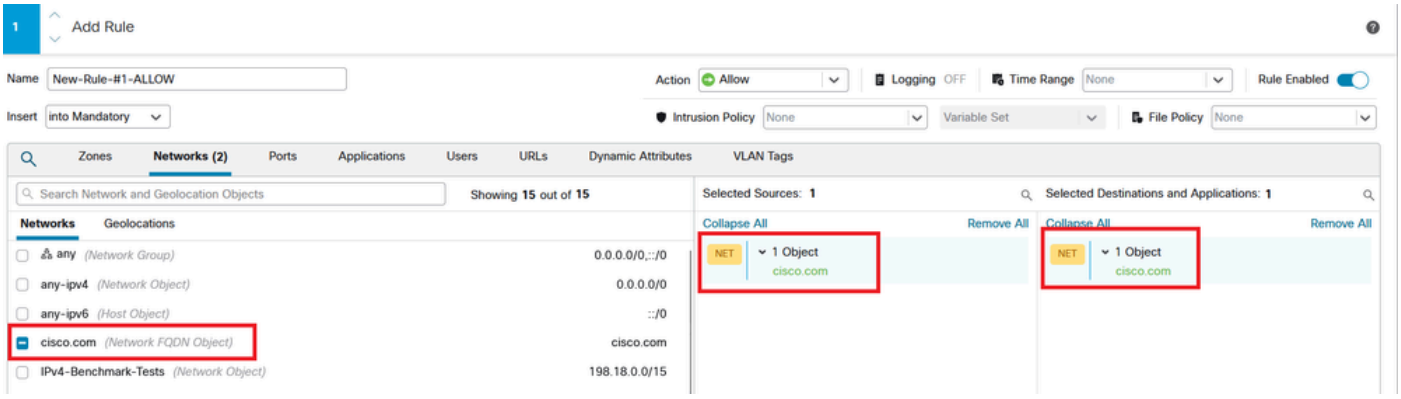

Imagem 5. Regra ACP com Objeto FQDN

Etapa 5. Navegue até o FTD em Devices > Device Management e selecione a guia Routing e navegue até a seção Policy Based Routing .

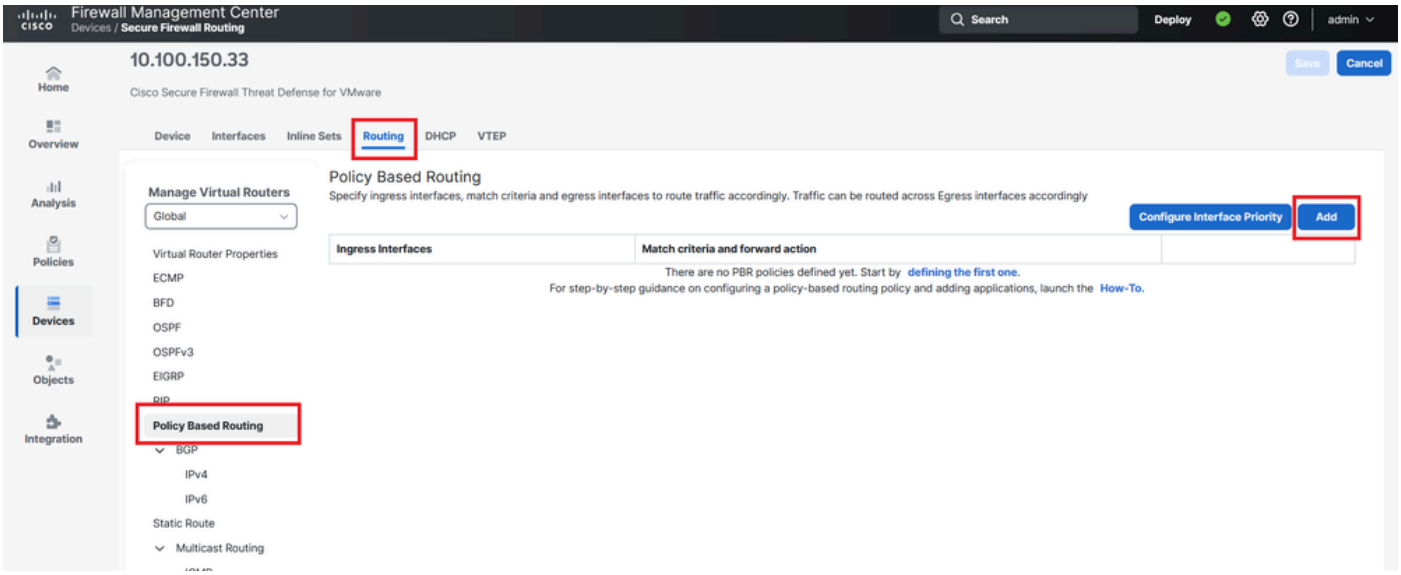

Imagem 6. Menu PBR

Etapa 6. Configure o PBR em uma interface usando a ACL configurada anteriormente e implante.

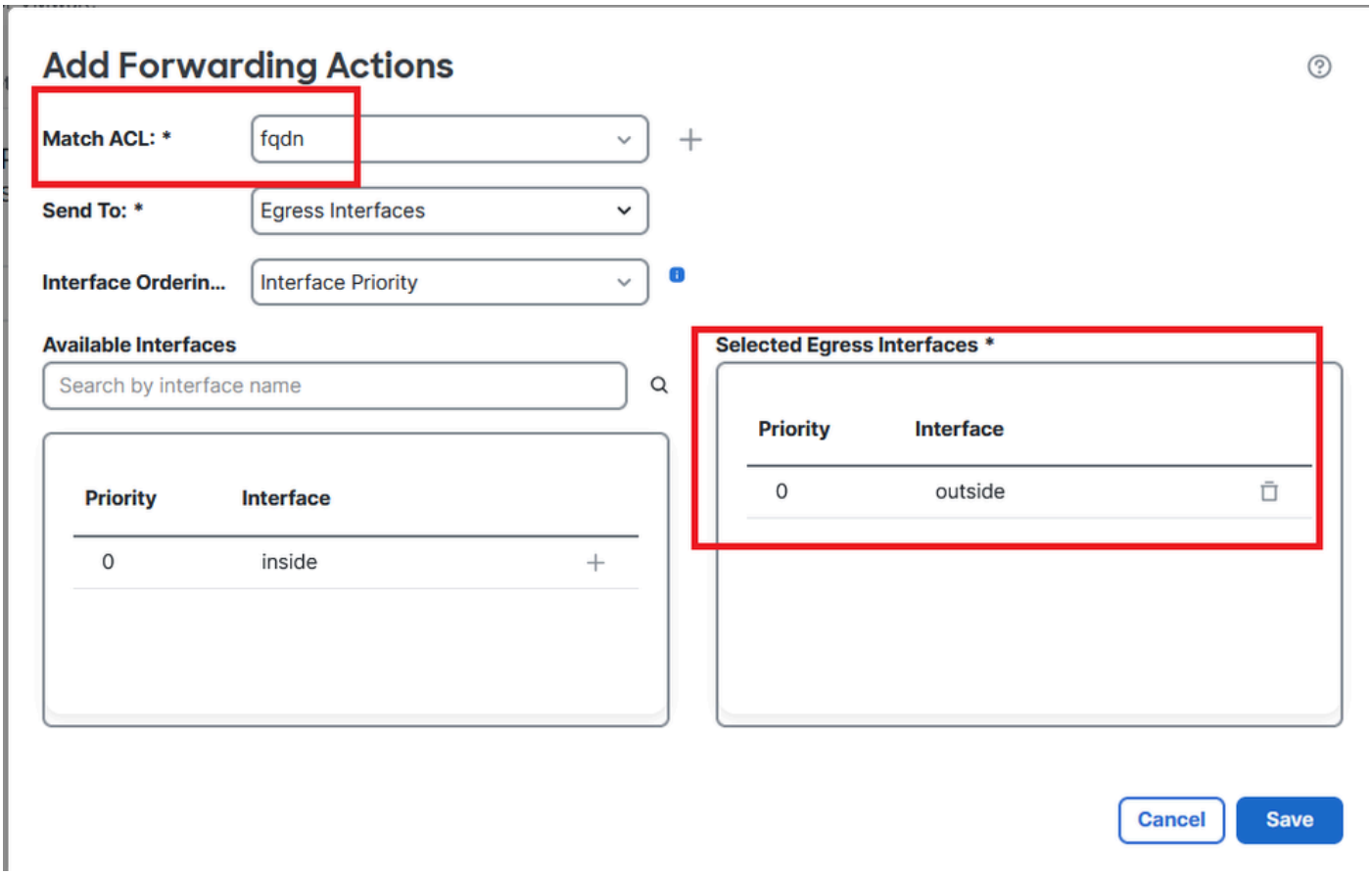

Imagem 7. Interface PBR e menu de seleção de ACL

Passo 7. Navegue até Objetos > Gerenciamento de objetos > FlexConfig > Objeto e crie um novo objeto.

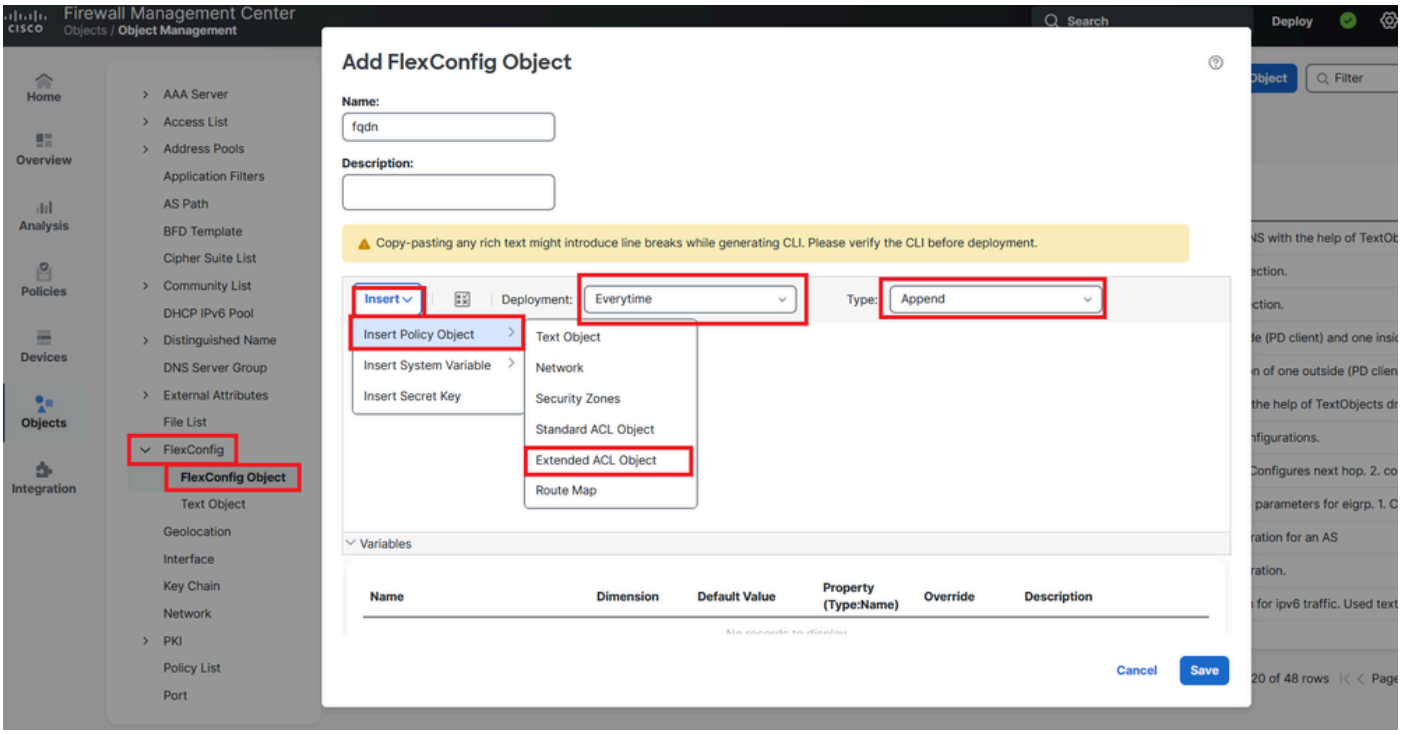

Imagem 8. Menu de configuração do objeto FlexConfig

Etapa 8. Selecione Insert > Extended ACL Object, nomeie sua variável e selecione sua ACL estendida criada anteriormente. A variável é adicionada com o nome que você usou.

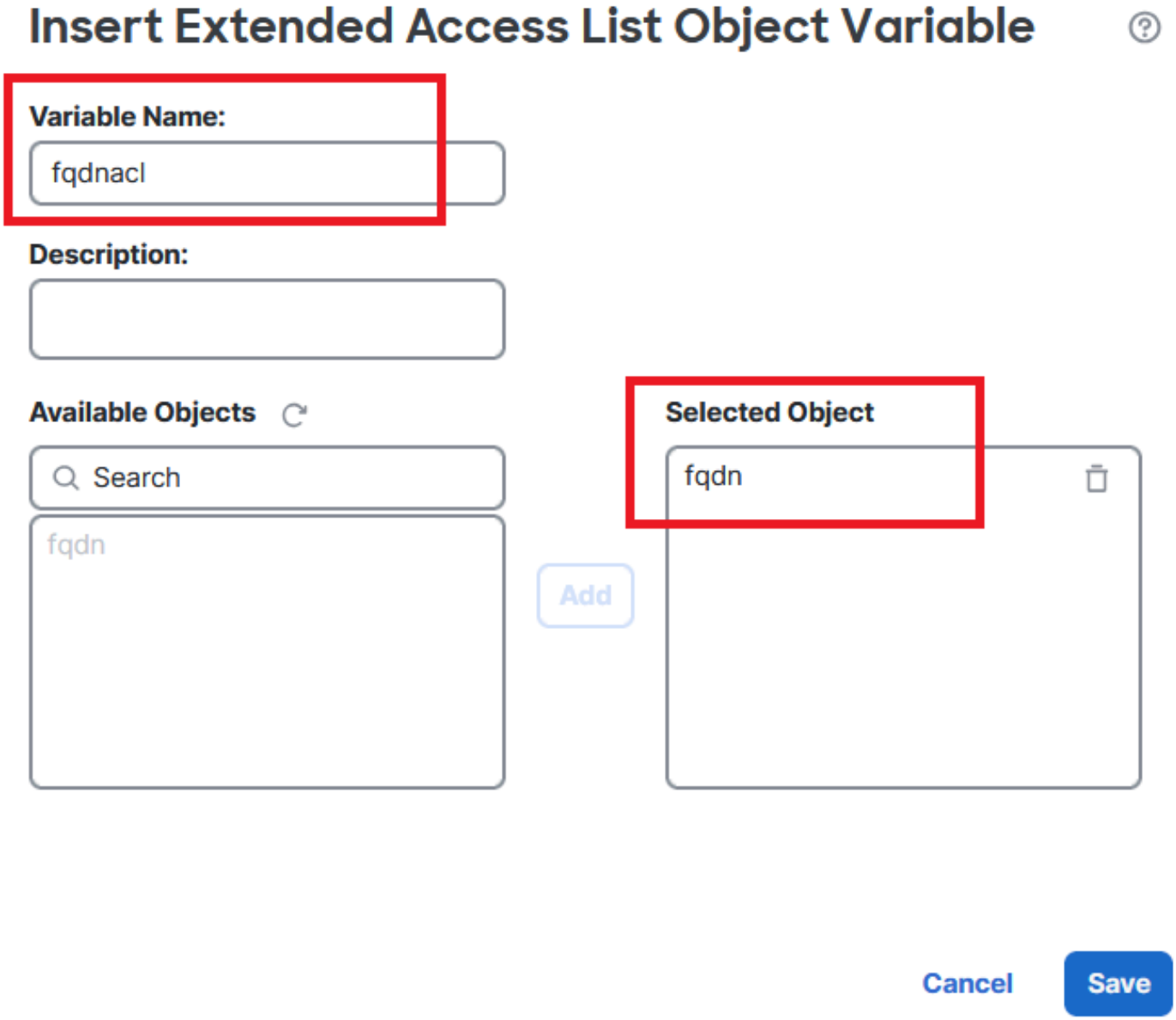

Imagem 9. Criação de variável para objeto FlexConfig

Etapa 9. Insira esta linha para cada objeto FQDN que deseja acessar sua ACL.

<#root>

```
access-li $
```

```
extended permit ip any object
```

Etapa 10. Salve o Objeto FlexConfig como Todos os dias > Anexar.

Etapa 11.Navegue até o menu FlexConfig Policy em Devices > FlexConfig.

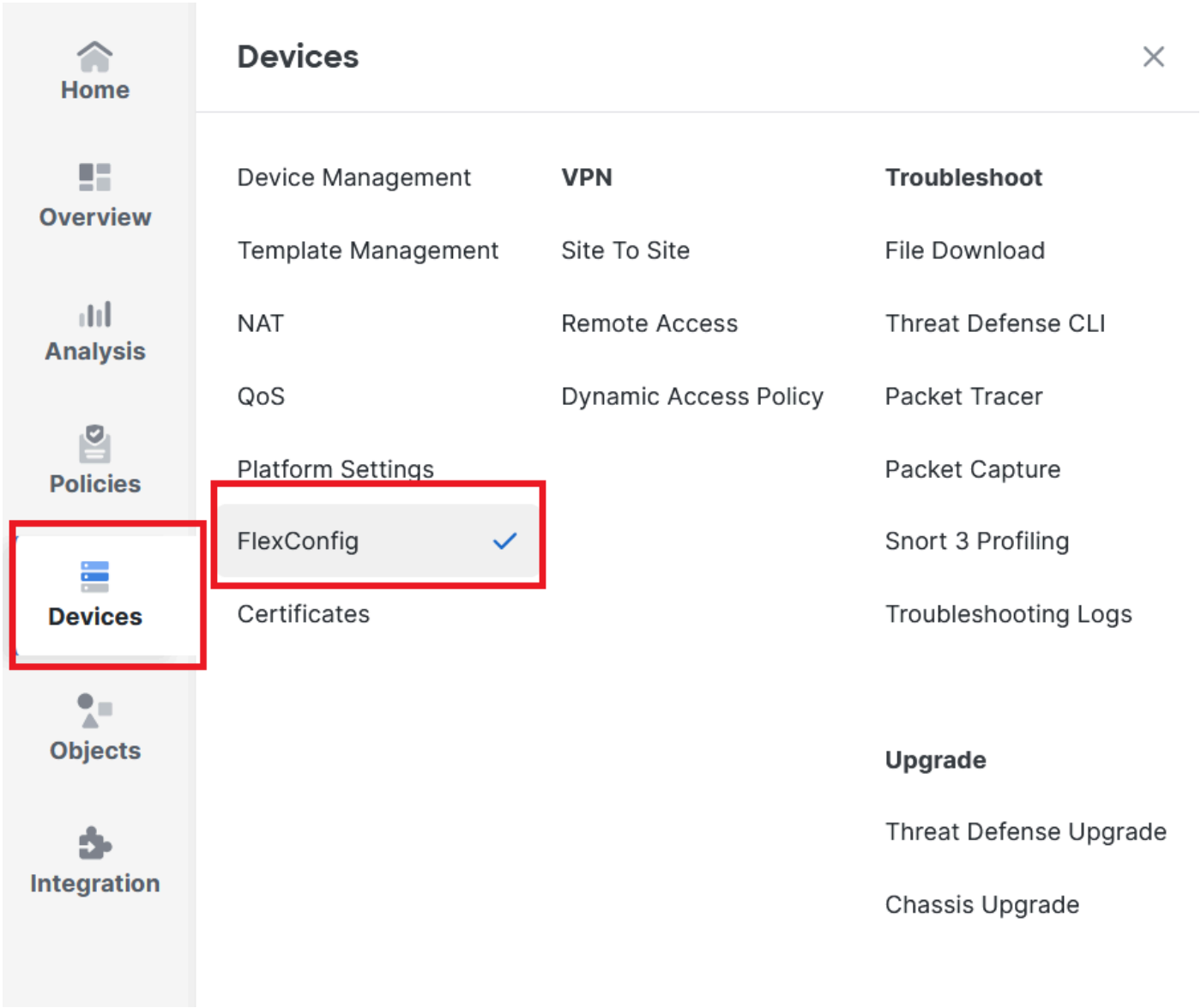

Imagem 10. Caminho para o menu de política FlexConfig

Etapa 12. Crie uma nova Política FlexConfig ou selecione uma Política já atribuída ao seu FTD.

Imagem 11. Editar ou criar uma nova política do FlexConfig

Etapa 13. Adicione o objeto FlexConfig à política, salve e implante.

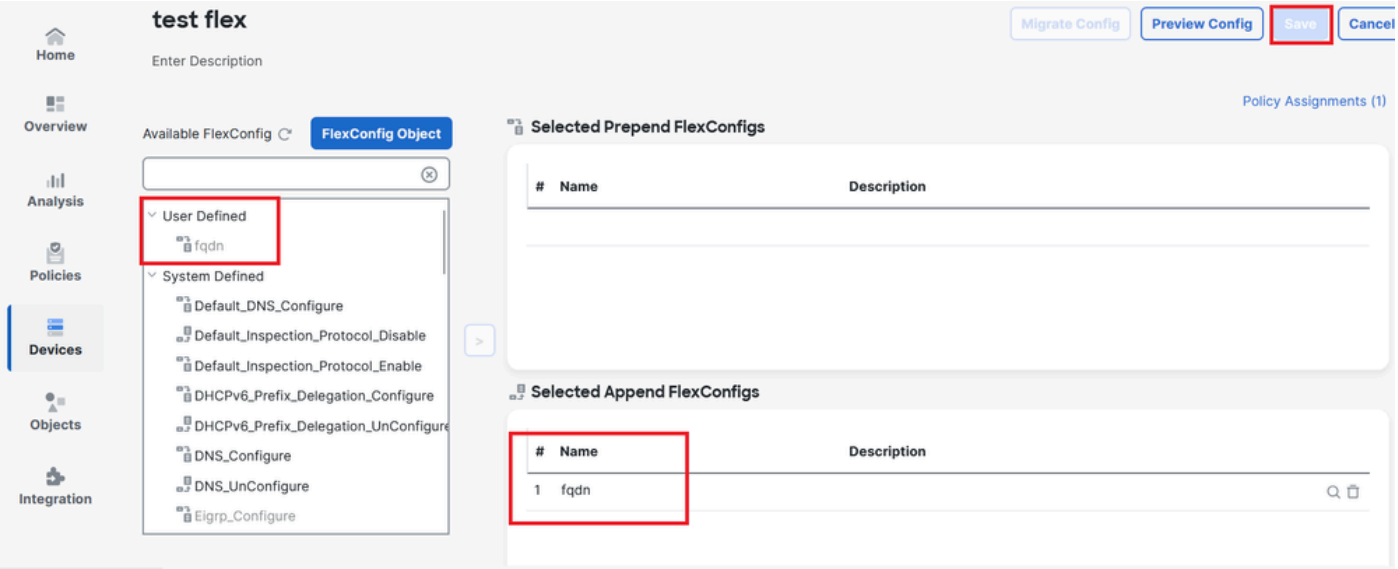

Imagem 12. Objeto FlexConfig adicionado à política FlexConfig

Verificar

Sua interface de entrada tem a rota de política com o mapa de rota gerado automaticamente.

<#root>

```
firepower#
```

show run interface gi0/0

```
!
interface GigabitEthernet0/0
 nameif inside
 security-level 0
 ip address 10.100.151.2 255.255.255.0
```

policy-route route-map FMC_GENERATED_PBR_1727116778384

O mapa de rota contém a ACL selecionada com a interface de destino usada.

<#root>

```
firepower#
```

show run route-map FMC_GENERATED_PBR_1727116778384

```
!
route-map FMC_GENERATED_PBR_1727116778384 permit 5
```

match ip address fqdn

set adaptive-interface cost outside

Sua lista de acesso contém o host usado para referência e a regra adicional adicionada por meio do FlexConfig.

```
<#root>

firepower#

show run access-list fqdn


access-list fqdn extended permit ip host 192.0.2.10 host 192.0.2.10

access-list fqdn extended permit ip any object cisco.com
```

Você pode fazer um packet tracer a partir da interface de entrada como uma origem para verificar se atingiu a fase PBR.

```
<#root>

firepower#

packet-tracer input inside tcp 10.100.150.1 12345 fqdn cisco.com 443


Mapping FQDN cisco.com to IP address 72.163.4.161


[...]
Phase: 3

Type: PBR-LOOKUP


Subtype: policy-route
Result: ALLOW
Elapsed time: 1137 ns

Config:


route-map FMC_GENERATED_PBR_1727116778384 permit 5


 match ip address fqdn


 set adaptive-interface cost outside


Additional Information:


 Matched route-map FMC_GENERATED_PBR_1727116778384, sequence 5, permit
```

```
 Found next-hop 10.100.150.1 using egress ifc outside

[...]
Result:
input-interface: inside(vrfid:0)

input-status: up
input-line-status: up
output-interface: outside(vrfid:0)

output-status: up
output-line-status: up
Action: allow
Time Taken: 140047752 ns
```

Problemas comuns

O PBR pára de funcionar após uma segunda implantação

Verifique se a lista de acesso ainda contém a regra de objeto FQDN.

Nesse caso, você pode ver que a regra não está mais aqui.

```
firepower# show run access-list fqdn
access-list fqdn extended permit ip host 192.0.2.10 host 192.0.2.10
firepower#
```

Verifique se o objeto FlexConfig está configurado como Deployment: Everytime e Type: Append. A regra é aplicada sempre em implantações futuras.

FQDN não Resolve

Ao tentar fazer ping no FQDN, você recebe uma mensagem sobre o nome de host inválido.

```
<#root>
firepower#
ping cisco.com

               ^
ERROR: % Invalid Hostname
```

Verifique a configuração do DNS. Você deve ter servidores DNS acessíveis em seu grupo de servidores, e as interfaces de pesquisa de domínio devem ser capazes de acessá-los.

```
<#root>

firepower#

show run dns


dns domain-lookup outside


DNS server-group DefaultDNS
DNS server-group dns

name-server 208.67.222.222


name-server 208.67.220.220


dns-group dns

firepower#

ping 208.67.222.222


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 208.67.222.222, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 170/202/280 ms
firepower#

ping cisco.com


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 72.163.4.161, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/140/190 ms.
```

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.