Configurar o PBR baseado em aplicativo FTD para Umbrella SIG

Contents

Introdução

Este documento descreve como configurar o Firewall Threat Defense (FTD), o roteamento baseado em políticas (PBR - Policy Based Routing) para o Umbrella SIG.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso ao painel do Umbrella
- Acesso administrativo ao FMC que executa o 7.1.0+ para implantar a configuração no FTD versão 7.1.0+. O PBR baseado em aplicativos é suportado apenas na versão 7.1.0 e superior
- (Preferido) Conhecimentos sobre a configuração do CVP/DTF e do Umbrella SIG
- (Opcional, mas altamente recomendado): Certificado raiz de guarda-chuva instalado, usado pelo SIG quando o tráfego é encaminhado por proxy ou bloqueado. Para obter mais detalhes sobre a instalação do certificado raiz, leia mais na documentação do Umbrella.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella Secure Internet Gateway (SIG).

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.

Overview

As informações neste documento destinam-se a cobrir as etapas de configuração sobre como implantar o PBR baseado em aplicativo no FTD ao estabelecer um Túnel VTI IPsec SIG para o Umbrella, para que você possa excluir ou incluir o tráfego em uma VPN baseada em aplicativos que usam o PBR.

O exemplo de configuração descrito neste artigo enfoca como excluir certos aplicativos da VPN IPsec enquanto envia tudo o resto pela VPN.

Informações completas sobre o PBR no FMC podem ser encontradas na documentação da Cisco.

Limitações

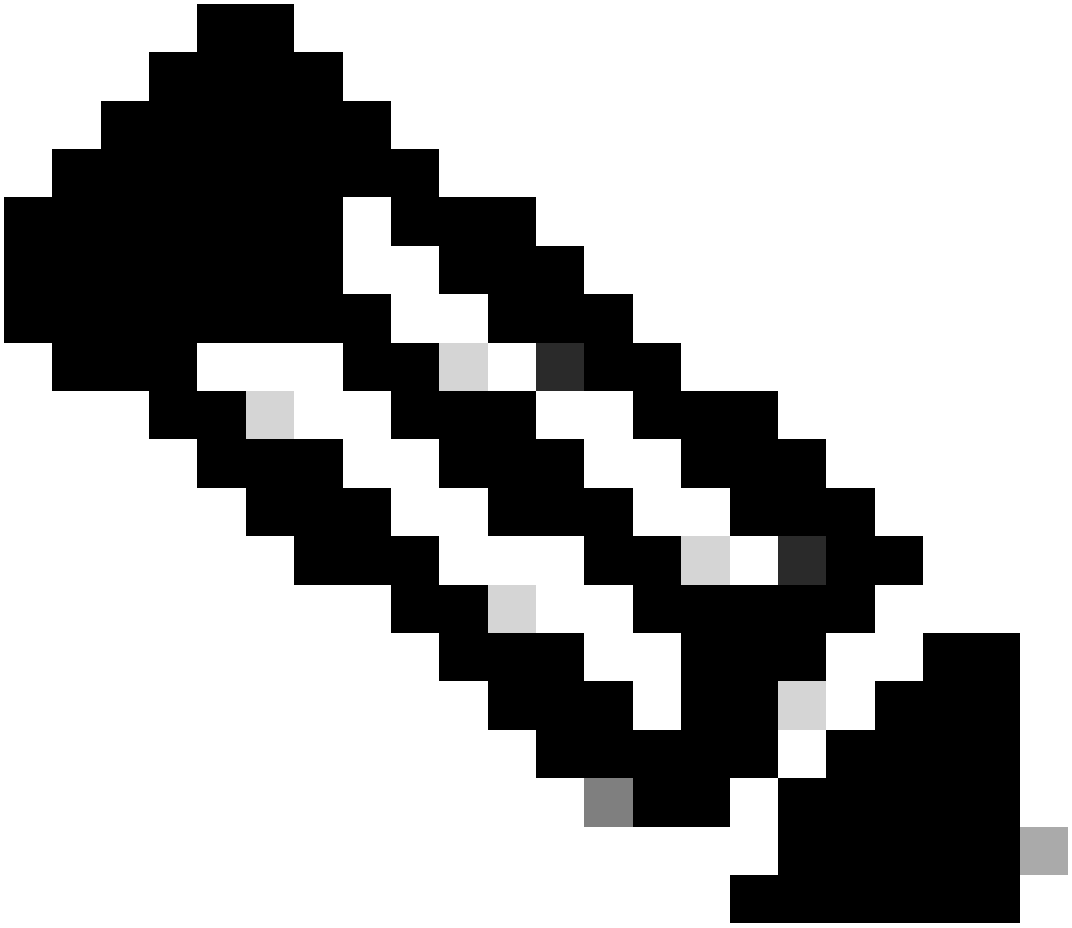
- Você não pode ter endereços de aplicativo e destino definidos em um ACE.
- Ao definir a ACL para os critérios de correspondência da política, você pode selecionar vários aplicativos de uma lista de aplicativos predefinidos para formar uma entrada de controle de acesso (ACE).
  No momento, não é possível adicionar ou modificar a lista de aplicativos predefinidos.
- Para as aplicações não enumeradas na lista de aplicações predefinidas no CVP ou qualquer comportamento inesperado com uma aplicação, podem ser utilizados IP em vez de aplicações no PBR.
- Para obter uma lista de limitações completas, consulte a documentação do PBR.

PBR baseado em aplicativo

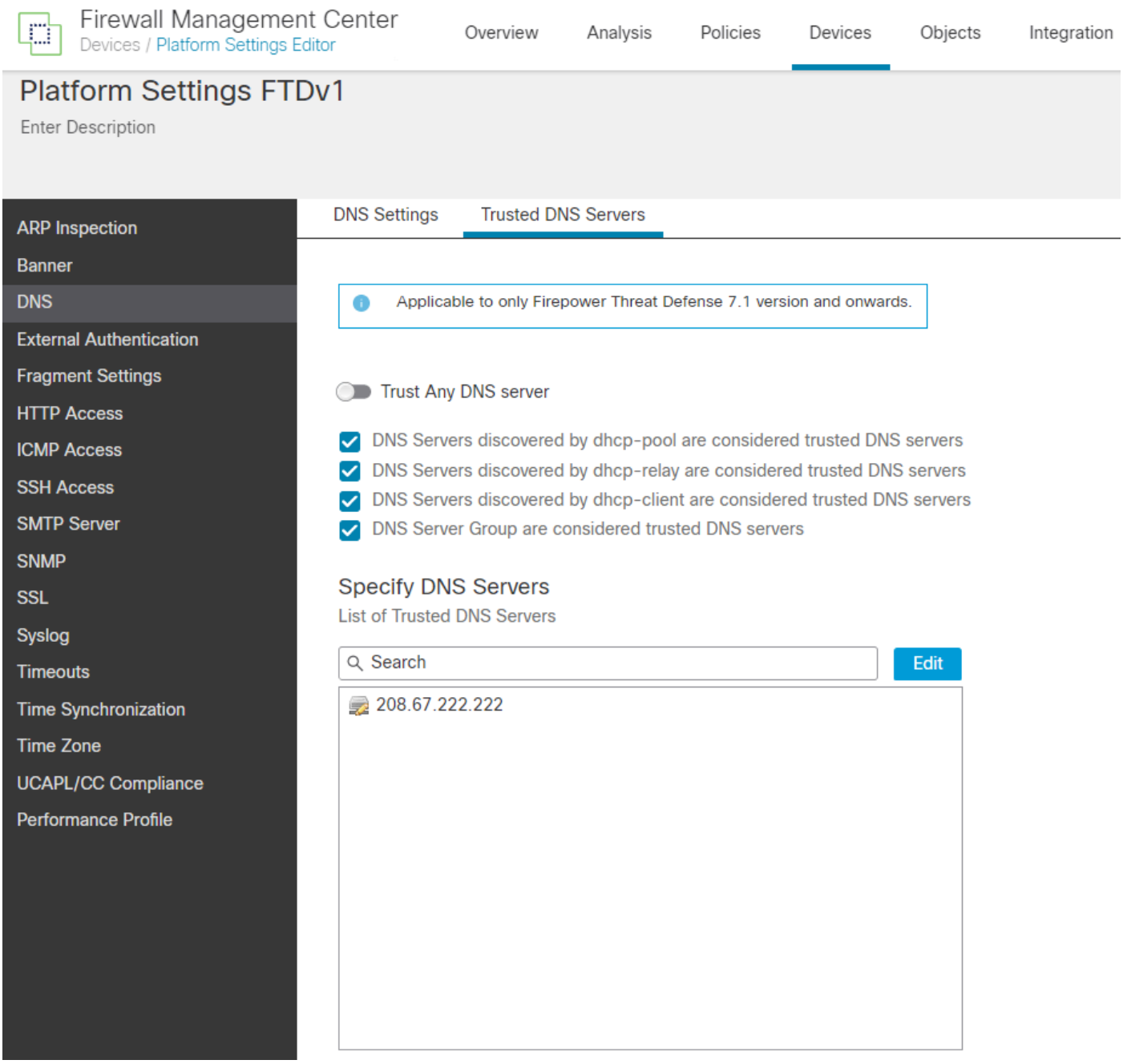
1. Comece configurando o túnel IPsec no FMC e no Umbrella Dashboard. As instruções de como executar essa configuração podem ser encontradas na documentação do Umbrella.

2. Verifique se o servidor DNS que o dispositivo do usuário final por trás do FTD está usando está listado como um servidor DNS confiável em Devices > Platform Settings > DNS > Trusted DNS Servers.

Se os dispositivos estiverem usando um servidor DNS que não esteja listado, o rastreamento de DNS poderá falhar e, portanto, o PBR baseado em aplicativos não funcionará. Opcionalmente (mas não recomendado por motivos de segurança), você pode ativar Confiar em qualquer servidor DNS para que seja necessário adicionar o(s) servidor(es) DNS.



Note: Se os VAs forem usados como resolvedores de DNS interno, eles deverão ser adicionados como Servidores DNS Confiáveis.



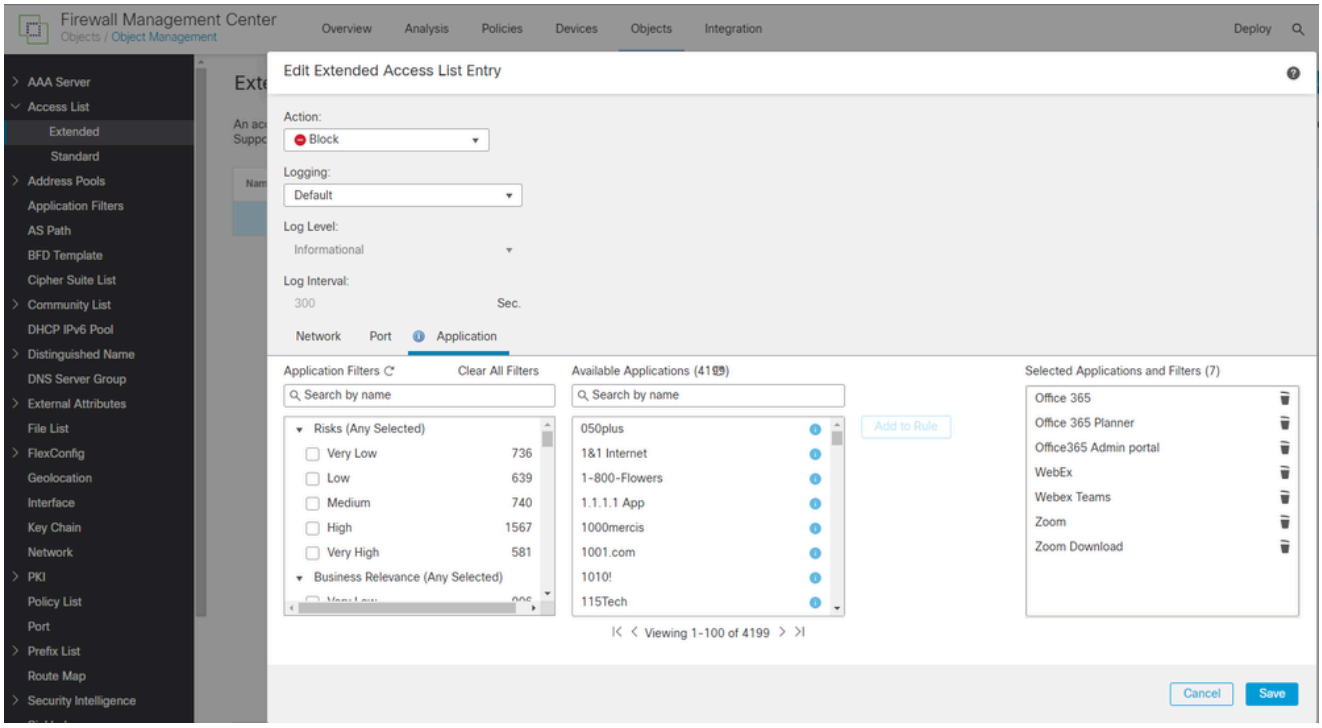
15669097907860

3. Crie uma ACL estendida que possa ser usada pelo FTD para o processo PBR para decidir se o tráfego é enviado para o Umbrella para SIG ou se é excluído do IPsec e não é enviado para o Umbrella.

- Uma ACE deny na ACL significa que o tráfego é excluído do SIG.
- Uma entrada permit na ACL significa que o tráfego é enviado pelo IPsec e pode aplicar uma política SIG (CDFW, SWG, etc).

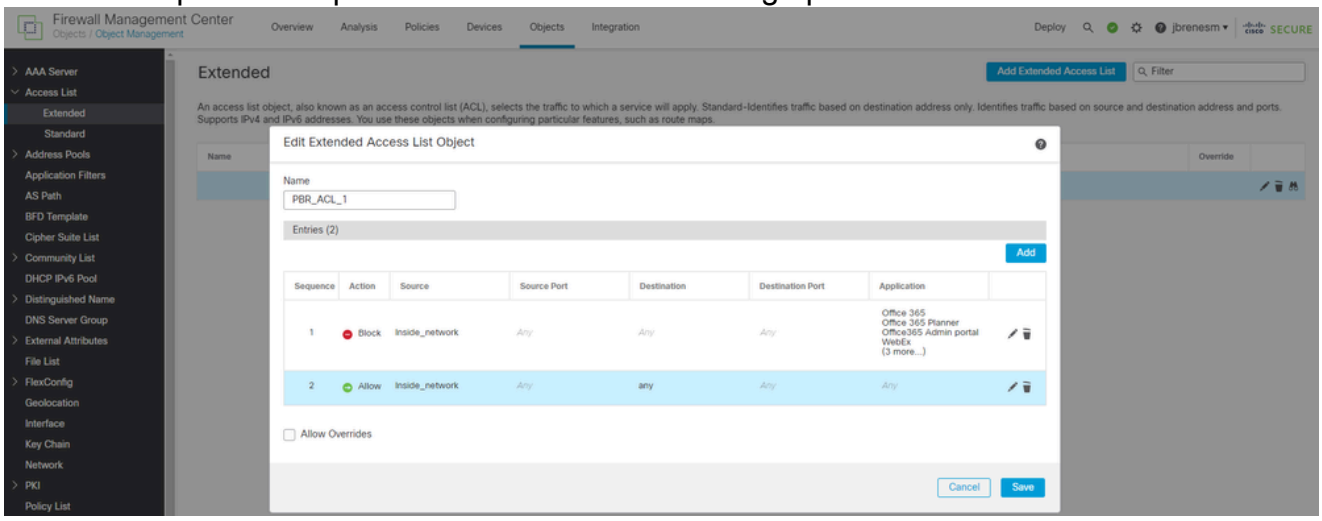
Este exemplo exclui os aplicativos "Office365", "Zoom" e "Cisco Webex" com uma ACE deny. O restante do tráfego está sendo enviado para a Umbrella para inspeção adicional.

1. Vá para Objeto > Gerenciamento de objetos > Lista de acesso > Estendido.
2. Defina a rede e as portas de origem como faria normalmente e adicione os aplicativos para participar no PBR.



15669947000852

A primeira ACE pode "negar" para os aplicativos mencionados anteriormente, e a segunda ACE é uma permissão para enviar o restante do tráfego pelo IPsec.

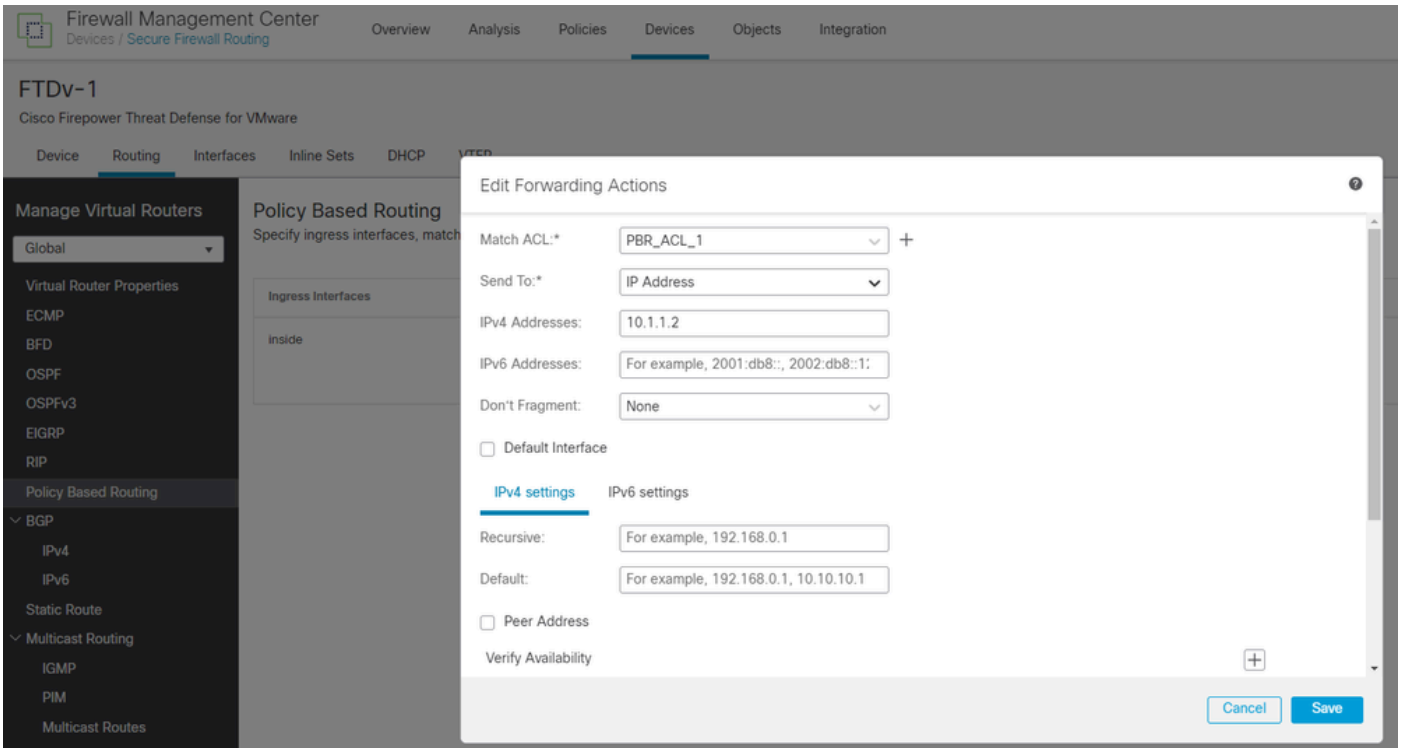


15670006987156

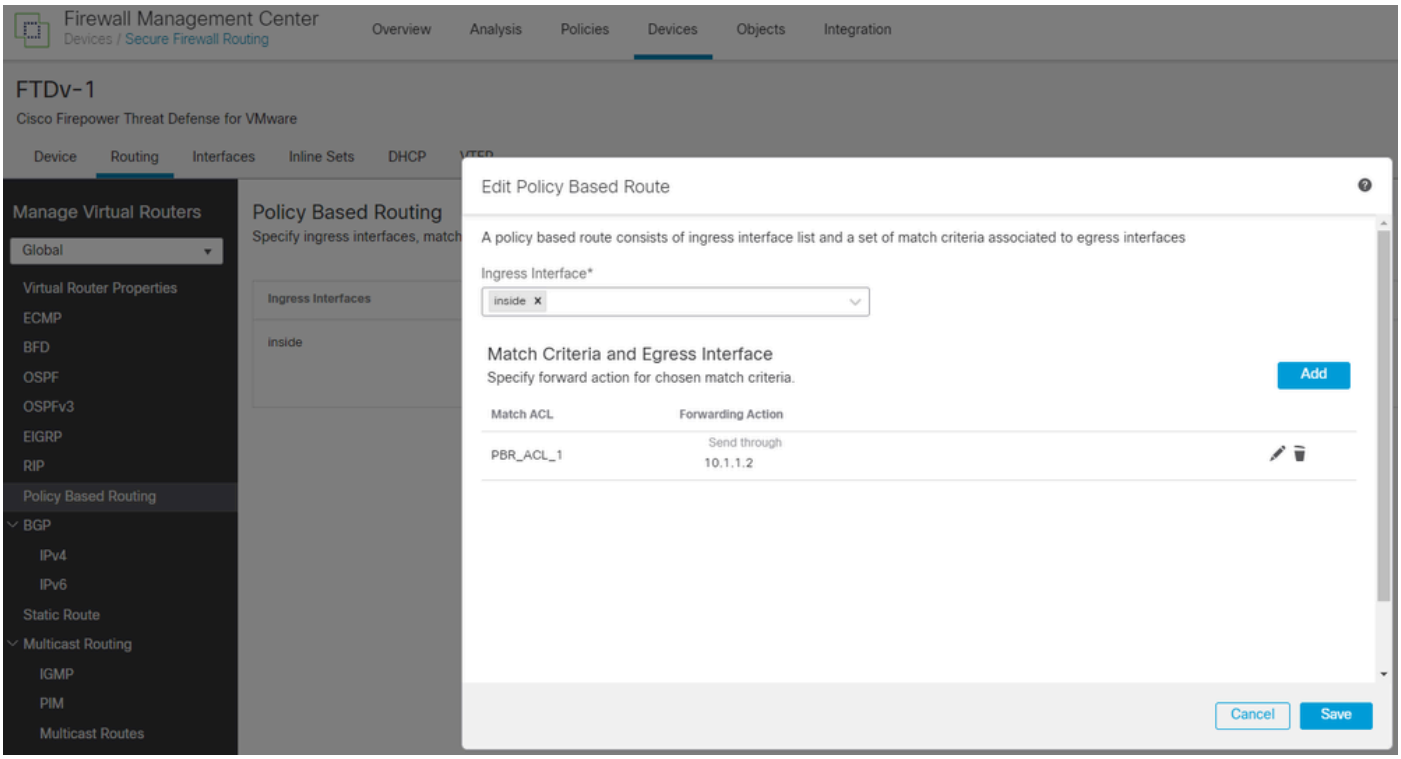
4. Crie o PBR em Devices > Device Management > [selecione o dispositivo FTD] > Routing > Policy Based Routing.

- Interface de entrada: A interface de onde vem o tráfego local.
- ACL correspondente: ACL estendida criada na etapa anterior, ACL "PBR_ACL_1".
- Enviar para: IP Address
- Endereços IPv4: Próximo salto quando o PBR encontrar uma instrução permit, de modo que o tráfego seja roteado para o IP que você adicionar aqui. Neste exemplo, este é o IPsec da Umbrella. Se o IP de sua VPN VTI for 10.1.1.1, o IPsec do Umbrella seria qualquer coisa

dentro dessa mesma rede (10.1.1.2, por exemplo).



15670209158036



15670247521556

5. Implantar as alterações no CVP.

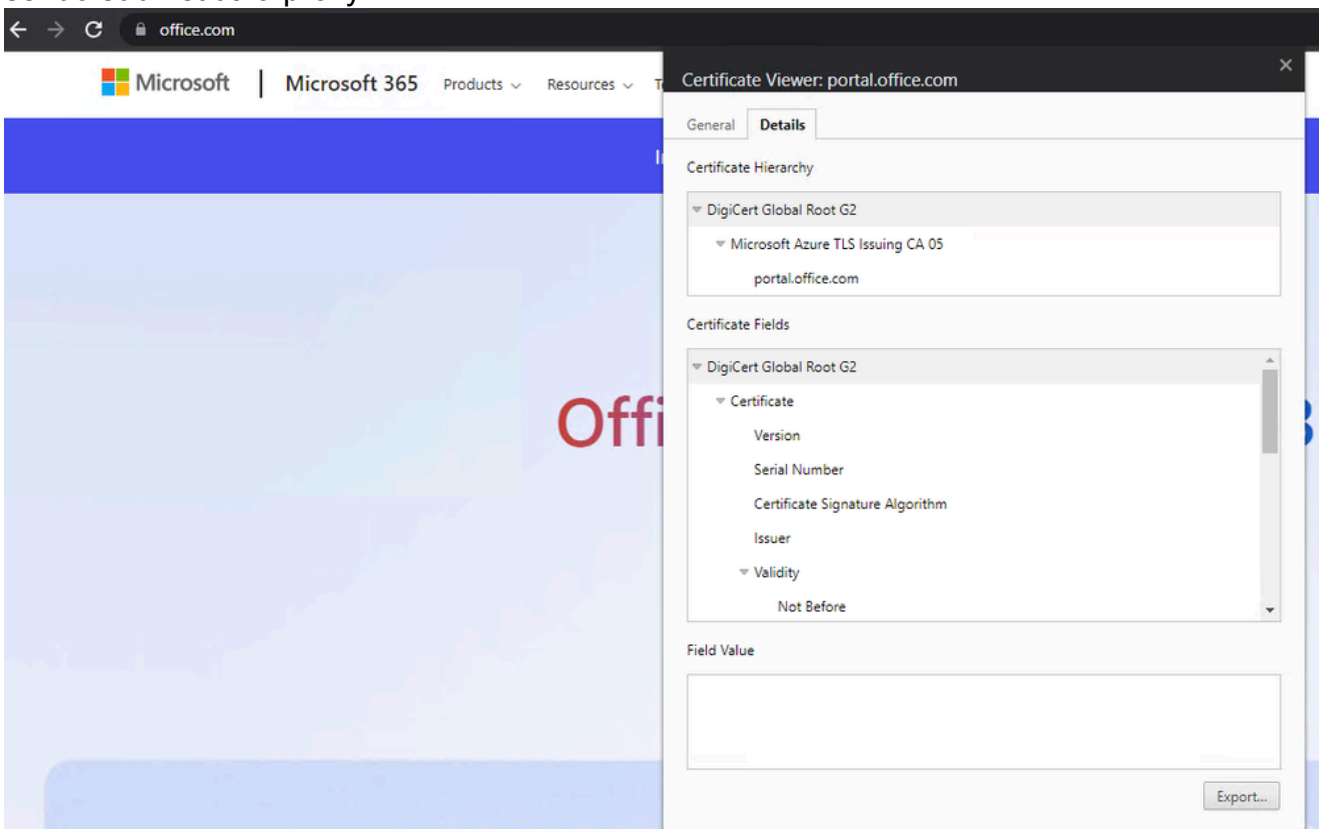
Verificação

No PC de teste localizado atrás do FTD, verifique:

- Na verdade, o tráfego do PC está sendo enviado pelo IPsec para o Umbrella.
  Ir para: https://policy-debug.checkumbrella.com/

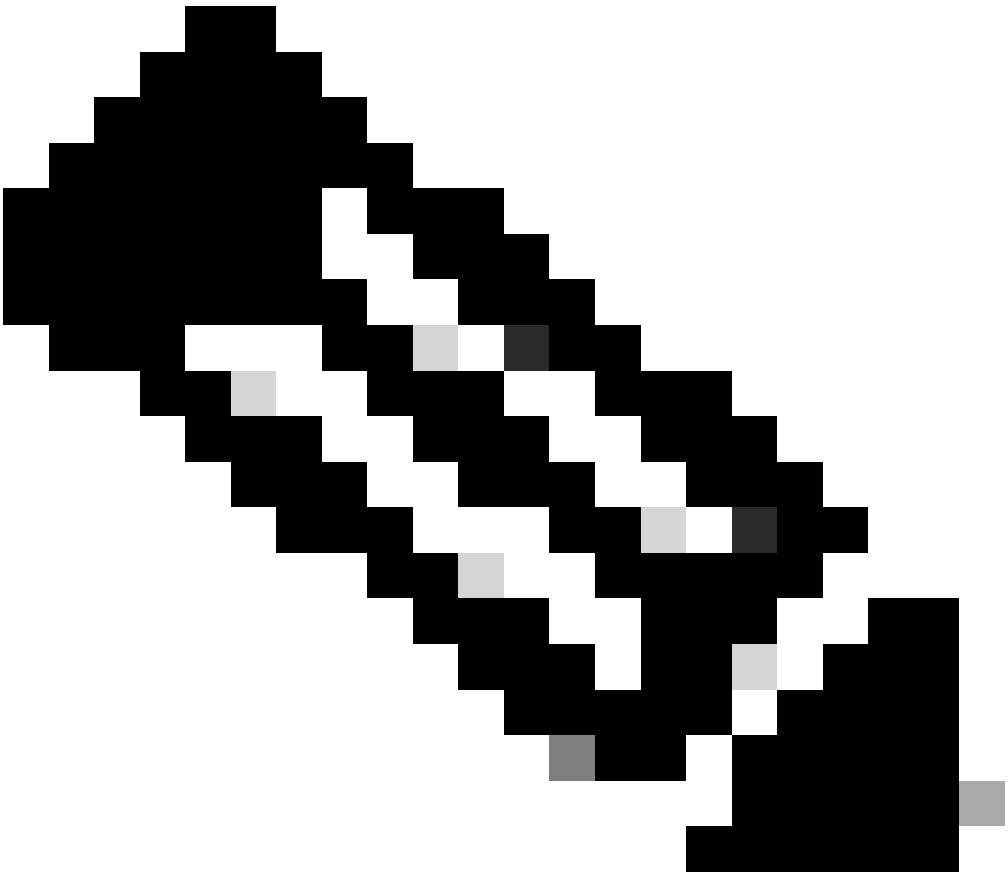
15670737148948

- Tente ir para qualquer um dos sites excluídos na configuração de PBR/ACL e verifique se a CA raiz do guarda-chuva não está apresentada, o que significa que a conexão não está sendo submetida a proxy:

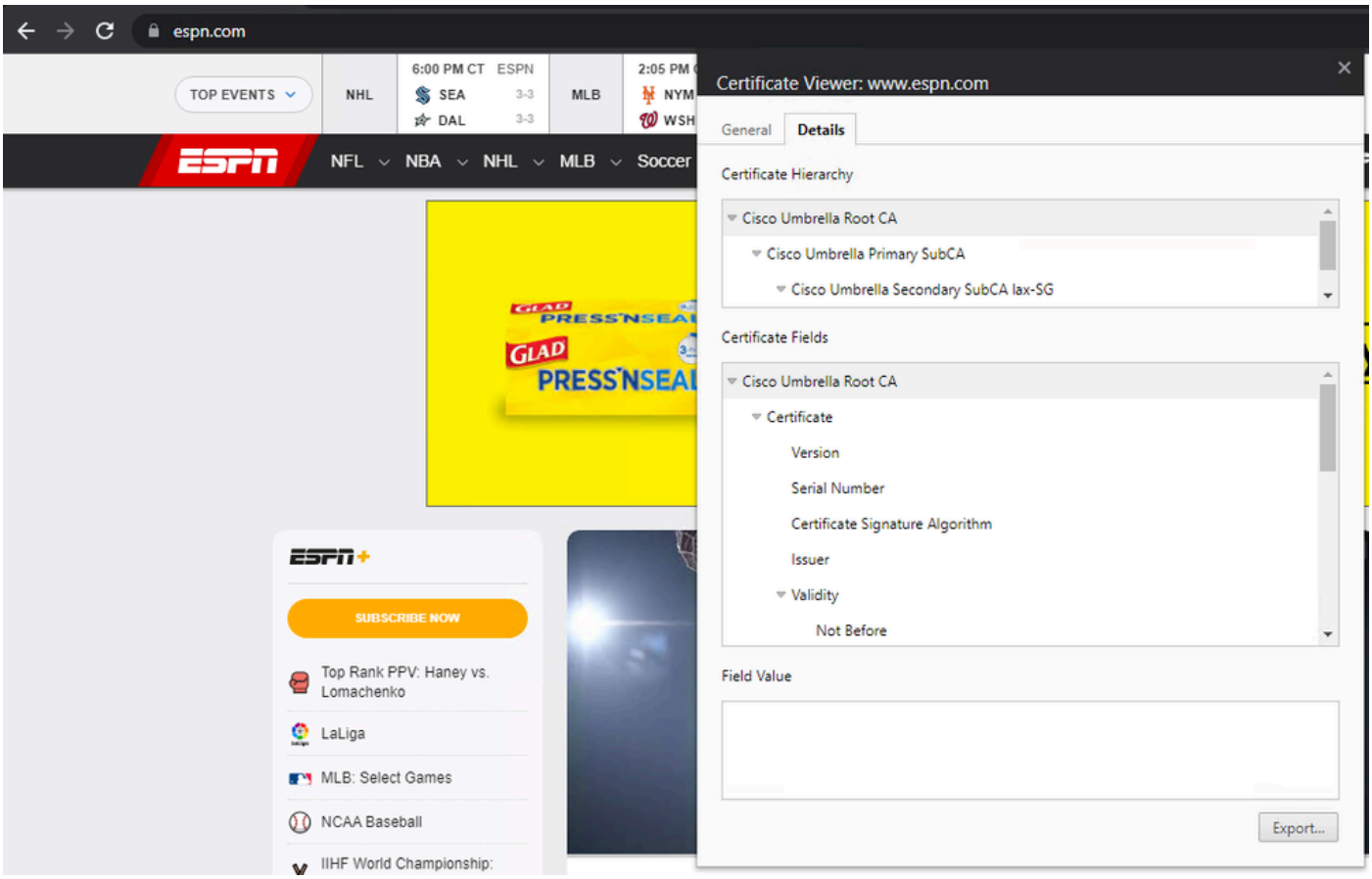


15670820980756

- Tente ir para qualquer outro site que não seja baseado nos aplicativos excluídos do PBR e certifique-se de que o Umbrella esteja realmente fazendo o proxy da conexão:



Note: Para evitar problemas com uma página de aviso não confiável, verifique se o Certificado de CA Raiz do Umbrella está instalado.



- Na CLI do FTD, você pode executar alguns comandos para confirmar se a configuração foi enviada corretamente e está funcionando:
  - `show run route-map` (verifica a configuração do PBR):

```
ftd# sh run route-map
!
route-map FMC_GENERATED_PBR_1682004086289 permit 5
 match ip address PBR_ACL_1
 set ip next-hop 10.1.1.2

!
ftd#
```

15670322054036

  - `show run interface gigabitEthernet 0/1` (verifica se o PBR está aplicado à interface apropriada)

```
ftd# sh run interface gigabitEthernet 0/1
!
interface GigabitEthernet0/1
 nameif inside
 security-level 0
 ip address 172.16.72.1 255.255.255.0
 policy-route route-map FMC_GENERATED_PBR_1682004086289
ftd#
```

15678344219540

- `show run access-list PBR_ACL_1, show object-group id FMC_NSG_17179869596` (confirma os domínios adicionados à ACL para exclusão)

```
ftd# sh run access-list PBR_ACL_1
access-list PBR_ACL_1 extended deny ip object Inside_network object-group-network-service FMC_NSG_17179869596
access-list PBR_ACL_1 extended permit ip object Inside_network any
ftd# sh object-group id FMC_NSG_17179869596
object-group network-service FMC_NSG_17179869596 (id=f1000001)
 network-service-member "Office 365" dynamic
  description Traffic generated by MS Office 365 applications and web services.
  app-id 2812
  domain nexus.officeapps.live.com (bid=-1815422039) ip (hitcnt=0)
  domain officehome.msocdn.com (bid=-1815266895) ip (hitcnt=0)
  domain scuofficehome.msocdn.com (bid=-1815215737) ip (hitcnt=0)
  domain eusofficehome.msocdn.com (bid=-1814954697) ip (hitcnt=0)
  domain seaofficehome.msocdn.com (bid=-1814948459) ip (hitcnt=0)
  domain msauth.net (bid=-1814770899) ip (hitcnt=0)
  domain msauthimages.net (bid=-1814643885) ip (hitcnt=0)
  domain msftauth.net (bid=-1814478573) ip (hitcnt=0)
  domain msftauthimages.net (bid=-1814363583) ip (hitcnt=0)
  domain officecdn.microsoft.com.edgesuite.net (bid=-1814169495) ip (hitcnt=0)
  domain staffhub.ms (bid=-1814084129) ip (hitcnt=0)
  domain mem.gfx.ms (bid=-1813977425) ip (hitcnt=0)
  domain assets.onestore.ms (bid=-1813901907) ip (hitcnt=0)
  domain o365weve.com (bid=-1813725851) ip (hitcnt=0)
  domain msappproxy.net (bid=-1813517013) ip (hitcnt=0)
  domain officeppe.com (bid=-1813427701) ip (hitcnt=0)
  domain Portal.Office.com (bid=-1813355559) ip (hitcnt=0)
  domain Home.Office.com (bid=-1813195231) ip (hitcnt=0)
  domain office365.com (bid=-1813005001) ip (hitcnt=0)
  domain office.com (bid=-1812953305) ip (hitcnt=0)
  domain office.net (bid=-1812729659) ip (hitcnt=0)
  domain microsoftonline.com (bid=-1812611427) ip (hitcnt=0)
  domain onmicrosoft.com (bid=-1812561405) ip (hitcnt=0)
  domain glbdns.microsoft.com (bid=-1812432381) ip (hitcnt=0)
  domain login.windows.net (bid=-1812242319) ip (hitcnt=0)
  domain login.microsoftonline.com (bid=-1812155687) ip (hitcnt=0)
  domain office365servicehealthcommunications.cloudapp.net (bid=-1812019313) ip (hitcnt=0)
  domain prod.msocdn.com (bid=-1811890529) ip (hitcnt=0)
  domain office.microsoft.com (bid=-1811800355) ip (hitcnt=0)
```

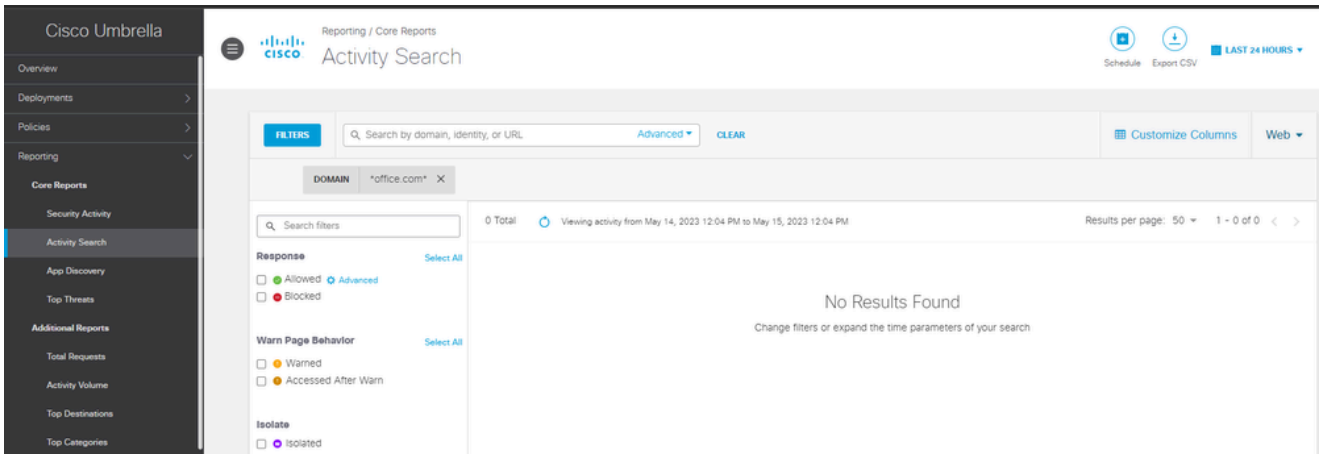
15670420887316

```
ftd# sh object-group id FMC_NSG_17179869596 | i office.com
  domain office.com (bid=-1812953305) ip (hitcnt=8)
  domain tasks.office.com (bid=-1674300035) ip (hitcnt=0)
  domain controls.office.com (bid=-1674092701) ip (hitcnt=0)
  domain clientlog.portal.office.com (bid=-1673794351) ip (hitcnt=0)
  domain portal.office.com (bid=88903411) ip (hitcnt=0)
ftd#
```

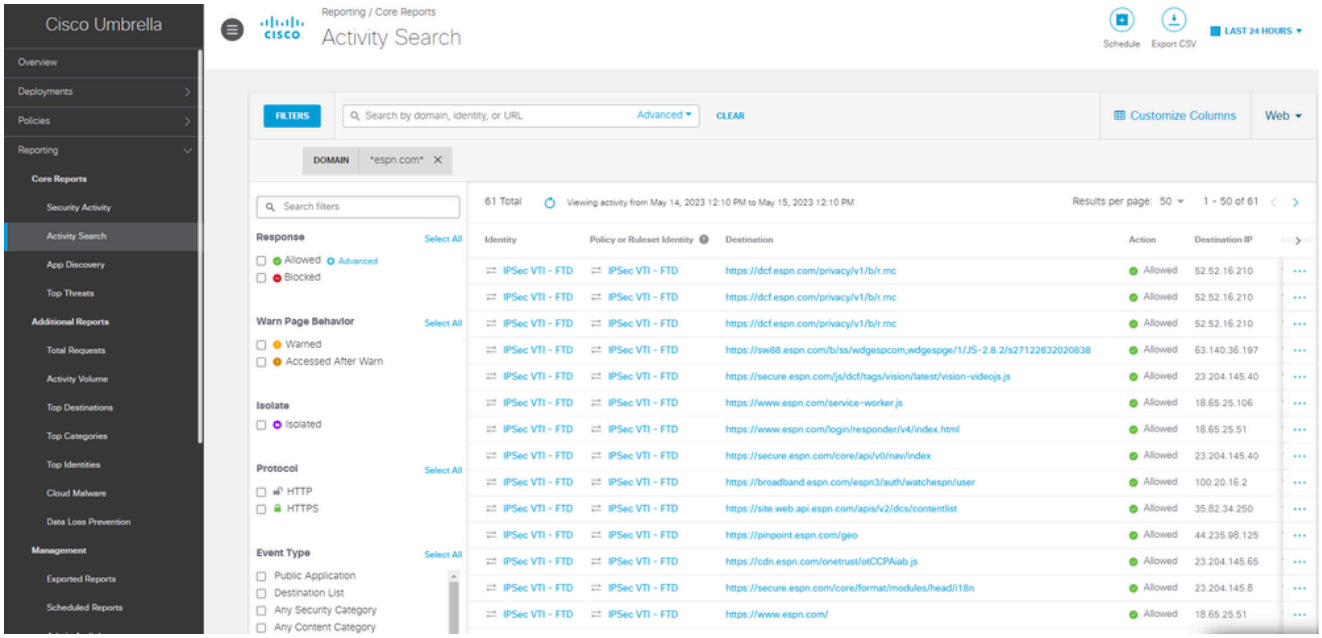
15670635784852

- `packet-tracer input inside tcp 172.16.72.10 1234 fqdn office.com 443 detailed` (verifica se a interface externa é usada como saída e não como VTI)

- No Painel do Umbrella, em pesquisa de atividade, você pode ver que o tráfego da Web que vai para office.com nunca foi enviado para o Umbrella, enquanto o tráfego que vai para espn.com foi enviado.



15671098042516



15671302832788

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.