Alterar o túnel de firewall fornecido pela nuvem do RSA para a autenticação PSK

Contents

Introdução

Este documento descreve as etapas para reconfigurar o mecanismo de autenticação do túnel de firewall fornecido pela nuvem da RSA para a PSK no Cisco ASA.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella.

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.

Passo 1: Verificar um túnel existente usando a autenticação RSA

Verifique se você tem um túnel existente usando a autenticação RSA e se o status do túnel no ASA está mostrando conectado com esse tipo de autenticação.

1. No painel Umbrella, localize o túnel de rede com o ASA mostrando uma impressão digital de autenticação de dispositivo.

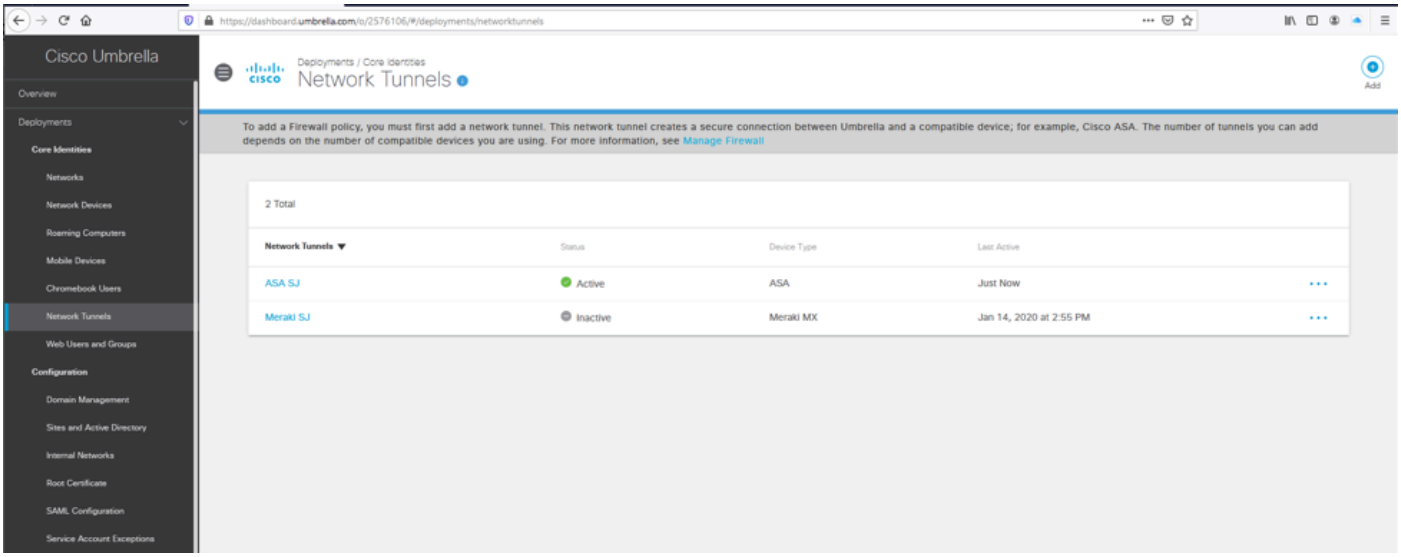

Imagem1.png

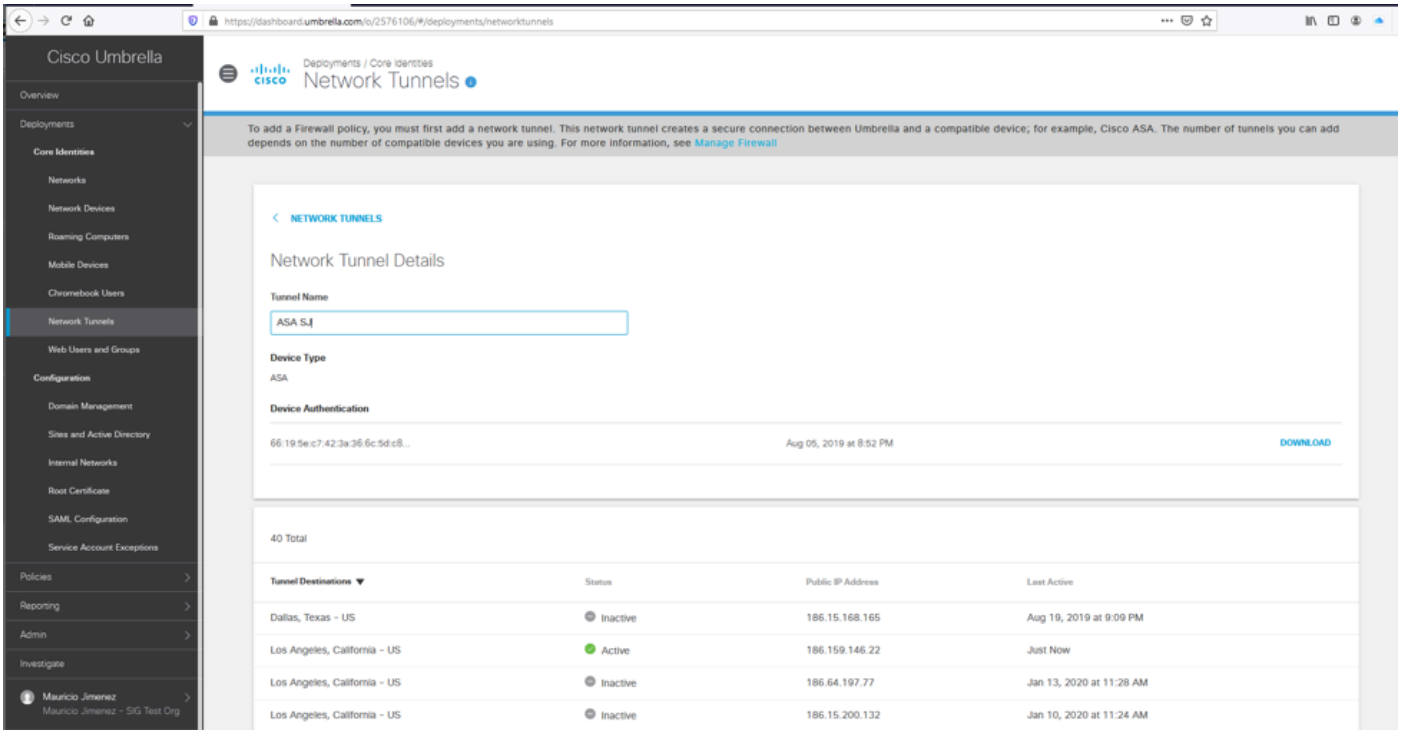

Imagem2.png

2. No Cisco ASA, você pode executar esses comandos para verificar o tipo de autenticação e o IP do ponto inicial que está sendo usado para o túnel.

show crypto ikev2 sa

e

show crypto ipsec sa

```
ASA-SJ# sh crypto ikev2 sa

IKEv2 SAs:

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                         Remote
                                    Status          Role
 26325699 186.159.146.22/4500                           146.112.67.2/4500
                                     READY    INITIATOR
      Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:19, Auth sign: RSA, Auth
verify: RSA
      Life/Active Time: 86400/4542 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xeccfd18d/0xccb02302
ASA-SJ#
```

Imagem3.png

```
ASA-SJ# sh crypto ipsec sa
interface: vti
    Crypto map tag: __vti-crypto-map-5-0-1, seq num: 65280, local addr: 186.159.
146.22

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 146.112.67.2


      #pkts encaps: 1734481, #pkts encrypt: 1734481, #pkts digest: 1734481
      #pkts decaps: 3553655, #pkts decrypt: 3553655, #pkts verify: 3553655
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 1734482, #pkts comp failed: 0, #pkts decomp failed:
0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 186.159.146.22/4500, remote crypto endpt.: 146.112.67
.2/4500
      path mtu 1500, ipsec overhead 82(52), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: CCB02302
      current inbound spi : ECCFD18D

<--- More --->
```

Imagem4.png

Passo 2: Registrar o IP público do ASA

1. Certifique-se de que seu IP público usado pela interface externa do ASA esteja registrado como uma rede no painel Umbrella.

2. Se a Rede não existir, continue a adicioná-la e confirme o IP público usado pela interface ASA. O objeto Network usado para esse túnel deve ser definido com uma máscara de sub-rede /32.

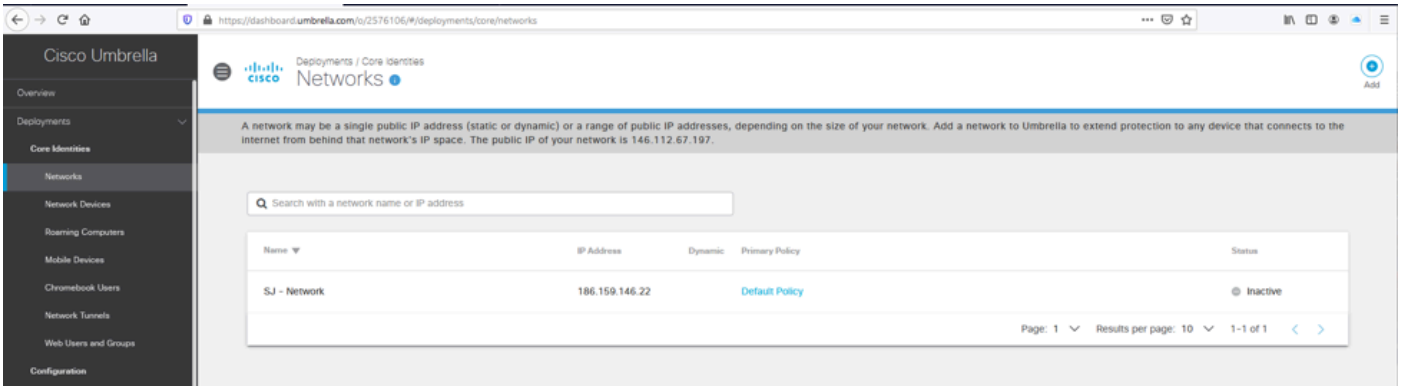

Imagem5.png

Passo 3: Criar novo túnel ASA

1. No painel Umbrella em Deployments/Network Tunnels, crie um novo túnel selecionando a opção Add.

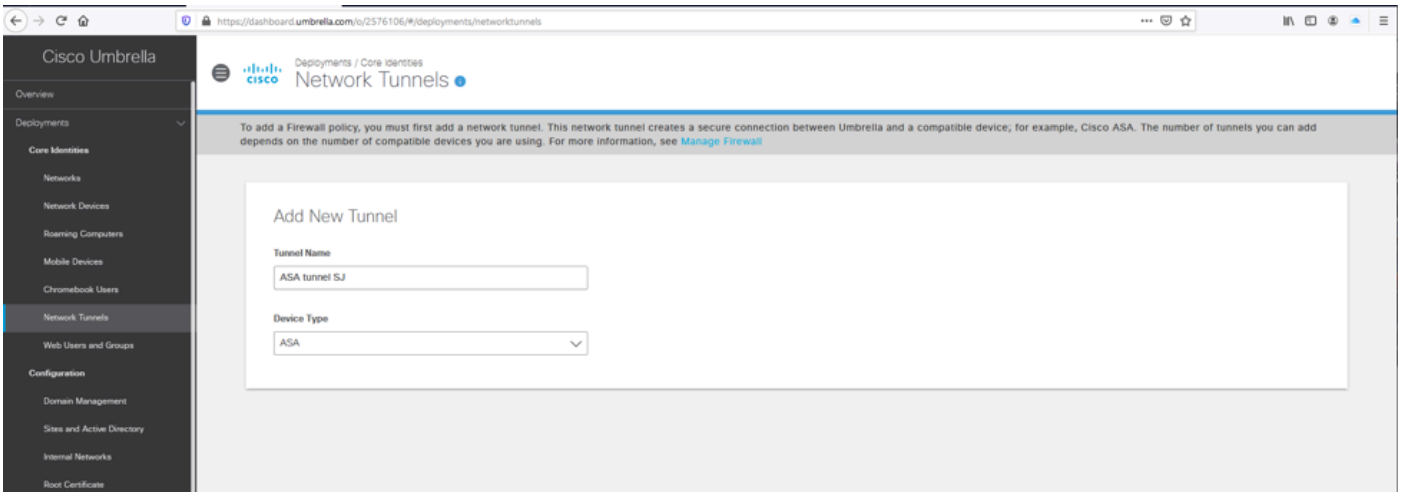

Imagem6.png

2. Selecione a ID do túnel com base na rede que corresponde ao IP público da interface externa do ASA e configure uma senha para a autenticação PSK.

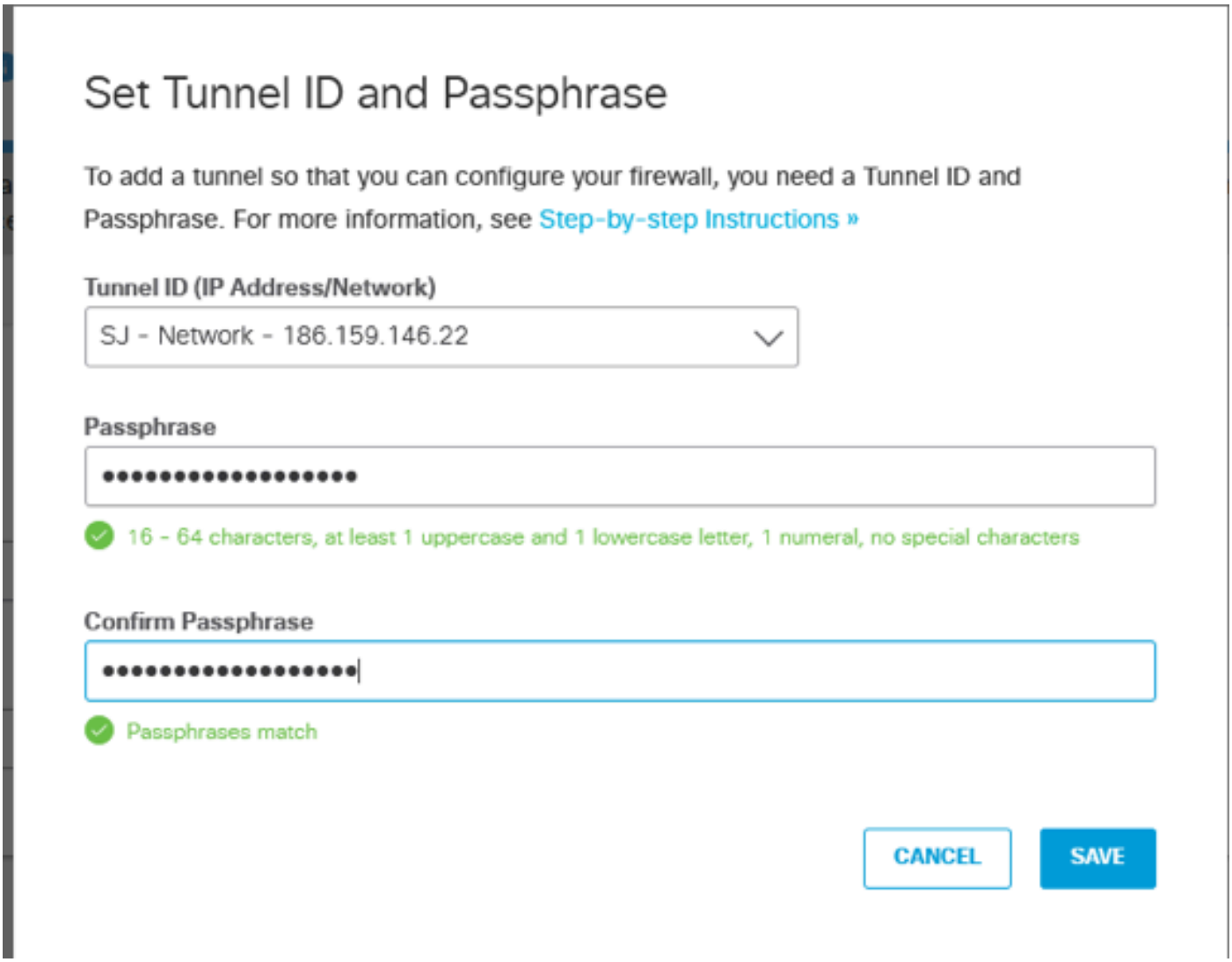

Imagem7.png

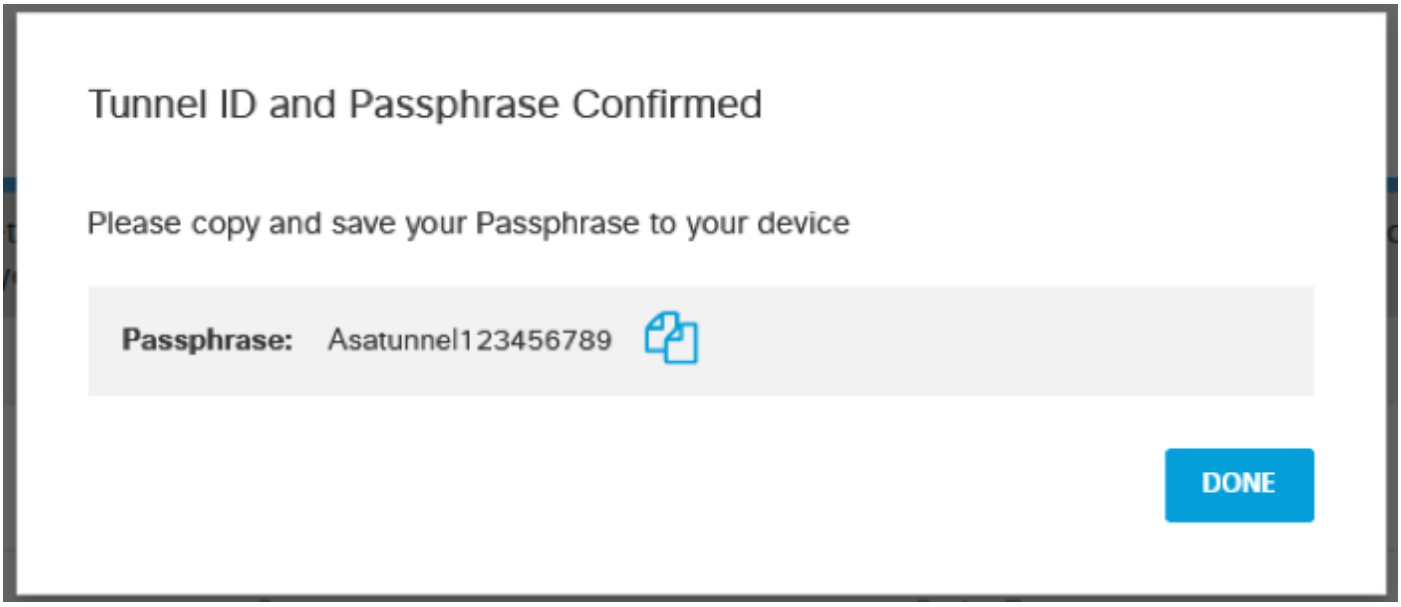

Imagem8.png

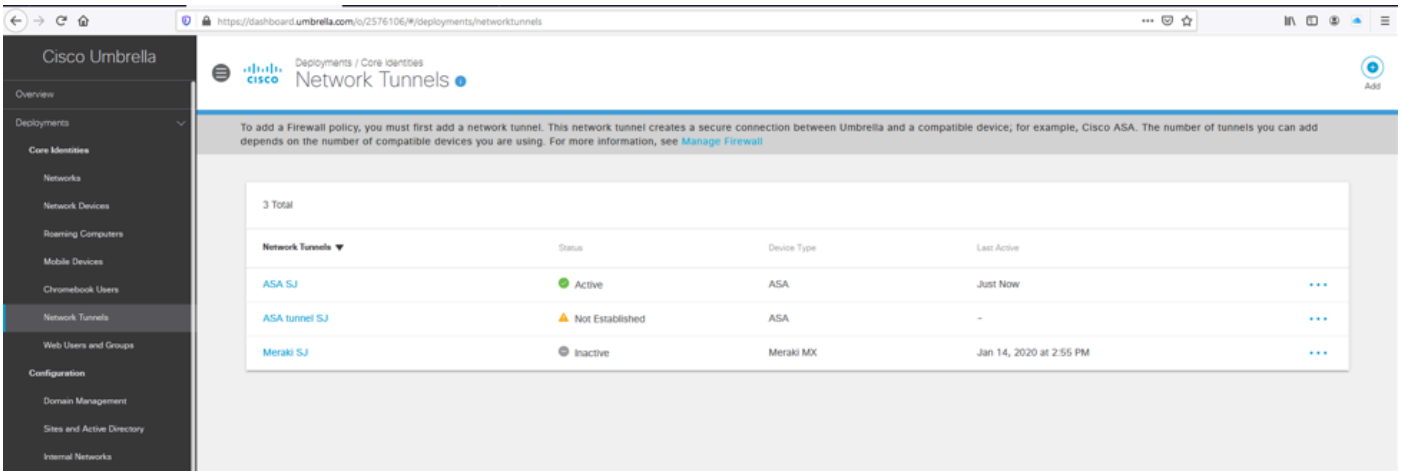

Imagem9.png

Passo 4: Criar novo grupo de túneis

1. No ASA, crie um novo grupo de túneis usando o novo IP de headend para Umbrella e especifique a senha definida no painel Umbrella para a autenticação PSK.

2. A lista atualizada de data centers e IPs Umbrella para os headends pode ser encontrada na documentação Umbrella.

```
tunnel-group <UMB DC IP address .8> type ipsec-l2l
tunnel-group <UMB DC IP address .8> general-attributes
 default-group-policy umbrella-policy
tunnel-group <UMB DC IP address .8> ipsec-attributes
 peer-id-validate nocheck
ikev2 local-authentication pre-shared-key 0 <passphrase>
ikev2 remote-authentication pre-shared-key 0 <passphrase>
```

```
ASA-SJ(config-tunnel-ipsec)# sh run tunnel-group 146.112.67.8
tunnel-group 146.112.67.8 type ipsec-l2l
tunnel-group 146.112.67.8 general-attributes
 default-group-policy umbrella-policy
tunnel-group 146.112.67.8 ipsec-attributes
 peer-id-validate nocheck
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

Imagem10.png

Passo 5: Localize o perfil IPSec usado para a interface de túnel

1. Procure o "crypto ipsec profile" que está sendo usado na interface do túnel para a configuração baseada em rota para o headend do Umbrella (o # é substituído pelo ID usado para a interface do túnel para o Umbrella):

```
show run interface tunnel#
```

```
ASA-SJ(config-tunnel-ipsec)# sh run interface tunnel1
!
interface Tunnel1
 nameif vti
 ip address 11.11.11.11 255.255.255.0
 tunnel source interface outside
 tunnel destination 146.112.67.2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile umbrella-profile
ASA-SJ(config-tunnel-ipsec)#
```

Imagem11.png

2. Se você não tiver certeza sobre o ID do túnel, poderá usar este comando para verificar as interfaces de túnel existentes e determinar qual é o usado para a configuração baseada no túnel Umbrella:

```
show run interface tunnel
```

Passo 6: Remover Ponto de Confiança Antigo do Perfil IPSec

1. Remova o ponto confiável de seu perfil IPSec que faz referência à autenticação RSA para o túnel. Você pode verificar a configuração usando este comando:

```
show crypto ipsec
```

```
ASA-SJ(config-ipsec-profile)# sh run crypto ipsec
crypto ipsec ikev2 ipsec-proposal umbrella-ipsec
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal l2l-proposal
 protocol esp encryption aes-256
 protocol esp integrity md5
crypto ipsec profile umbrella-profile
 set ikev2 ipsec-proposal umbrella-ipsec
 set trustpoint umbrella-trustpoint
crypto ipsec security-association pmtu-aging infinite
```

Imagem12.png

2. Continue a remover o ponto confiável com estes comandos:

```
crypto ipsec profile <profile name>
no set trustpoint umbrella-trustpoint
```

```
ASA-SJ(config-ipsec-profile)# crypto ipsec profile umbrella-profile
ASA-SJ(config-ipsec-profile)# no set trustpoint umbrella-trustpoint
```

Imagem13.png

3. Confirme se o ponto confiável foi removido do perfil crypto ipsec:

```
ASA-SJ(config-if)# sh run crypto ipsec
crypto ipsec ikev2 ipsec-proposal umbrella-ipsec
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal l2l-proposal
 protocol esp encryption aes-256
 protocol esp integrity md5
crypto ipsec profile umbrella-profile
 set ikev2 ipsec-proposal umbrella-ipsec
crypto ipsec security-association pmtu-aging infinite
```

Imagem14.png

Passo 7: Atualizar interface de túnel com o novo Umbrella Headend IP

1. Substitua o destino da interface de túnel para o novo endereço IP do ponto inicial do Umbrella que termina em .8.

- Você pode usar esse comando para verificar o destino atual para que ele seja substituído pelo IP dos novos intervalos de endereço IP do data center, que podem ser encontrados na [documentação do Umbrella:]

```
show run interface tunnel
```

```
ASA-SJ(config-tunnel-ipsec)# sh run interface tunnel1
!
interface Tunnel1
 nameif vti
 ip address 11.11.11.11 255.255.255.0
 tunnel source interface outside
 tunnel destination 146.112.67.2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile umbrella-profile
ASA-SJ(config-tunnel-ipsec)#
```

Imagem15.png

```
Interface tunnel#
No tunnel destination <UMBRELLA DC IP address.2>
Tunnel destination <UMBRELLA DC IP address .8>
```

```
ASA-SJ(config-if)# interface Tunnel1
ASA-SJ(config-if)# no  tunnel destination 146.112.67.2
ASA-SJ(config-if)#  tunnel destination 146.112.67.8
```

Imagem16.png

2. Confirme a alteração com o comando:

```
show run interface tunnel#
```

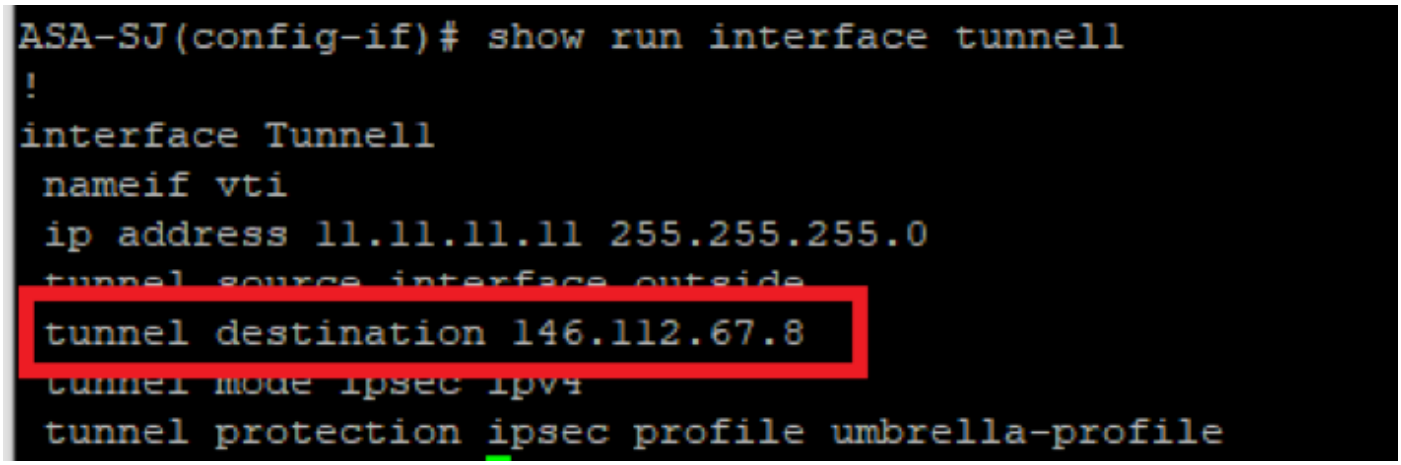

Imagem17.png

Passo 8: A Configuração De Confirmação Do Novo Túnel Estabelece Com Sucesso

1. Confirme se a conexão do túnel com o Umbrella foi restabelecida corretamente com o IP do ponto inicial atualizado e usando a autenticação PSK com este comando:

```
show crypto ikev2 sa
```

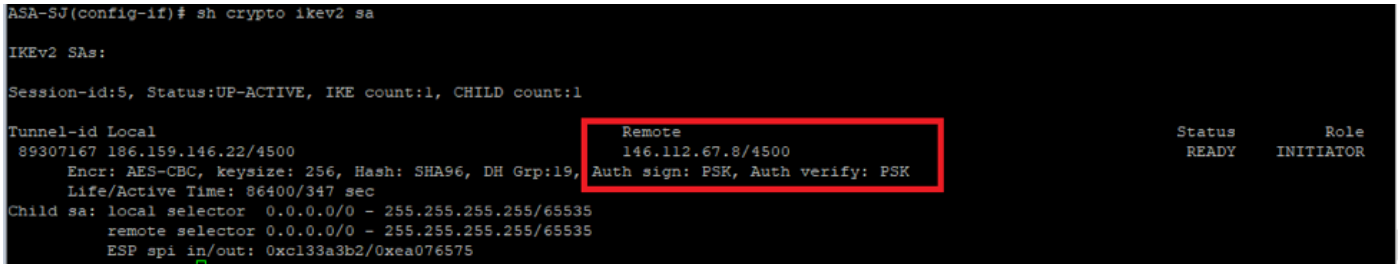

Imagem18.png

```
show crypto ipsec sa
```

```
ASA-SJ(config-if)# show crypto ipsec sa
interface: vti
    Crypto map tag: __vti-crypto-map-5-0-1, seq num: 65280, local addr: 186.159.146.22

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 146.112.67.8


      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 186.159.146.22/4500, remote crypto endpt.: 146.112.67.8/4500
      path mtu 1500, ipsec overhead 82(52), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: EA076575
      current inbound spi : C133A3B2
```

Imagem19.png

Etapa 9 (opcional): Remova o grupo de túnel antigo

1. Remova o grupo de túneis antigo que apontava para o intervalo IP do headend anterior do Umbrella .2.

Você pode usar este comando para identificar o túnel correto antes de remover a configuração:

```
show run tunnel-group
```

```
ASA-SJ(config)# sh run tunnel-group
tunnel-group DefaultL2LGroup general-attributes
 default-group-policy l2lpolicy
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
tunnel-group 146.112.67.2 type ipsec-l2l
tunnel-group 146.112.67.2 general-attributes
 default-group-policy umbrella-policy
tunnel-group 146.112.67.2 ipsec-attributes
 peer-id-validate nocheck
 ikev2 remote-authentication certificate
 ikev2 local-authentication certificate umbrella-trustpoint
tunnel-group 146.112.67.8 type ipsec-l2l
tunnel-group 146.112.67.8 general-attributes
 default-group-policy umbrella-policy
tunnel-group 146.112.67.8 ipsec-attributes
 peer-id-validate nocheck
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

Imagem20.png

2. Remova qualquer referência do antigo grupo de túneis usando este comando:

```
clear config tunnel-group <UMB DC IP address .2>
```

```
ASA-SJ(config)# clear config tunnel-group 146.112.67.2
```

Imagem21.png

Etapa 10 (opcional): Remover Ponto de Confiança Antigo

1. Remova qualquer referência do ponto confiável usado anteriormente com a configuração baseada em túnel Umbrella com este comando:

```
sh run crypto ipsec
```

O nome amigável usado para o ponto de confiança pode ser encontrado quando você revisa o "perfil ipsec de criptografia":

```
ASA-SJ(config-ipsec-profile)# sh run crypto ipsec
crypto ipsec ikev2 ipsec-proposal umbrella-ipsec
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal l2l-proposal
 protocol esp encryption aes-256
 protocol esp integrity md5
crypto ipsec profile umbrella-profile
 set ikev2 ipsec-proposal umbrella-ipsec
 set trustpoint umbrella-trustpoint
crypto ipsec security-association pmtu-aging infinite
```

Imagem22.png

2. Você pode executar este comando para confirmar a configuração do ponto confiável. Verifique se o nome amigável corresponde à configuração usada no comando crypto ipsec profile:

```
sh run crypto ca trustpoint
```

```
ASA-SJ(config-if)# sh run crypto ca trustpoint
crypto ca trustpoint umbrella-trustpoint
 keypair umbrella-trustpoint
 crl configure
crypto ca trustpoint asaconnector-trust
 enrollment terminal
 crl configure
```

Imagem23.png

3. Para obter mais detalhes sobre o certificado, use o comando:

```
show crypto ca certificate <trustpoint-name>
```

```
ASA-SJ(config-if)# show crypto ca certificates umbrella-trustpoint
Certificate
  Status: Available
  Certificate Serial Number: 365510264a580b66b1f5a2b6b8a618ec
  Certificate Usage: Signature
  Public Key Type: RSA (3072 bits)
  Signature Algorithm: SHA384 with RSA Encryption
  Issuer Name:
    cn=Cisco Umbrella CA
    o=Cisco Umbrella
    c=US
  Subject Name:
    cn=cdfw-2576106-293960662-umbrella.com
  Validity Date:
    start date: 20:52:11 CST Aug 5 2019
    end   date: 20:52:11 CST Aug 5 2021
  Storage: config
  Associated Trustpoints: umbrella-trustpoint

CA Certificate
  Status: Available
  Certificate Serial Number: 60fa7229af4c481e
  Certificate Usage: General Purpose
  Public Key Type: RSA (4096 bits)
  Signature Algorithm: SHA1 with RSA Encryption
  Issuer Name:
```

Imagem24.png

4. Remova o ponto confiável com o comando:

```
no crypto ca trustpoint <trustpoint-name>
```

```
ASA-SJ(config)# no crypto ca trustpoint umbrella-trustpoint
WARNING: Removing an enrolled trustpoint will destroy all
certificates received from the related Certificate Authority.

Are you sure you want to do this? [yes/no]: yes
INFO: Be sure to ask the CA administrator to revoke your certificates.
ASA-SJ(config)#
```

Imagem25.png

Etapa 11 (opcional): Excluir túnel de rede antigo

1. Exclua o túnel de rede antigo do painel do Umbrella navegando até Network Tunnel Details e selecionando Delete.

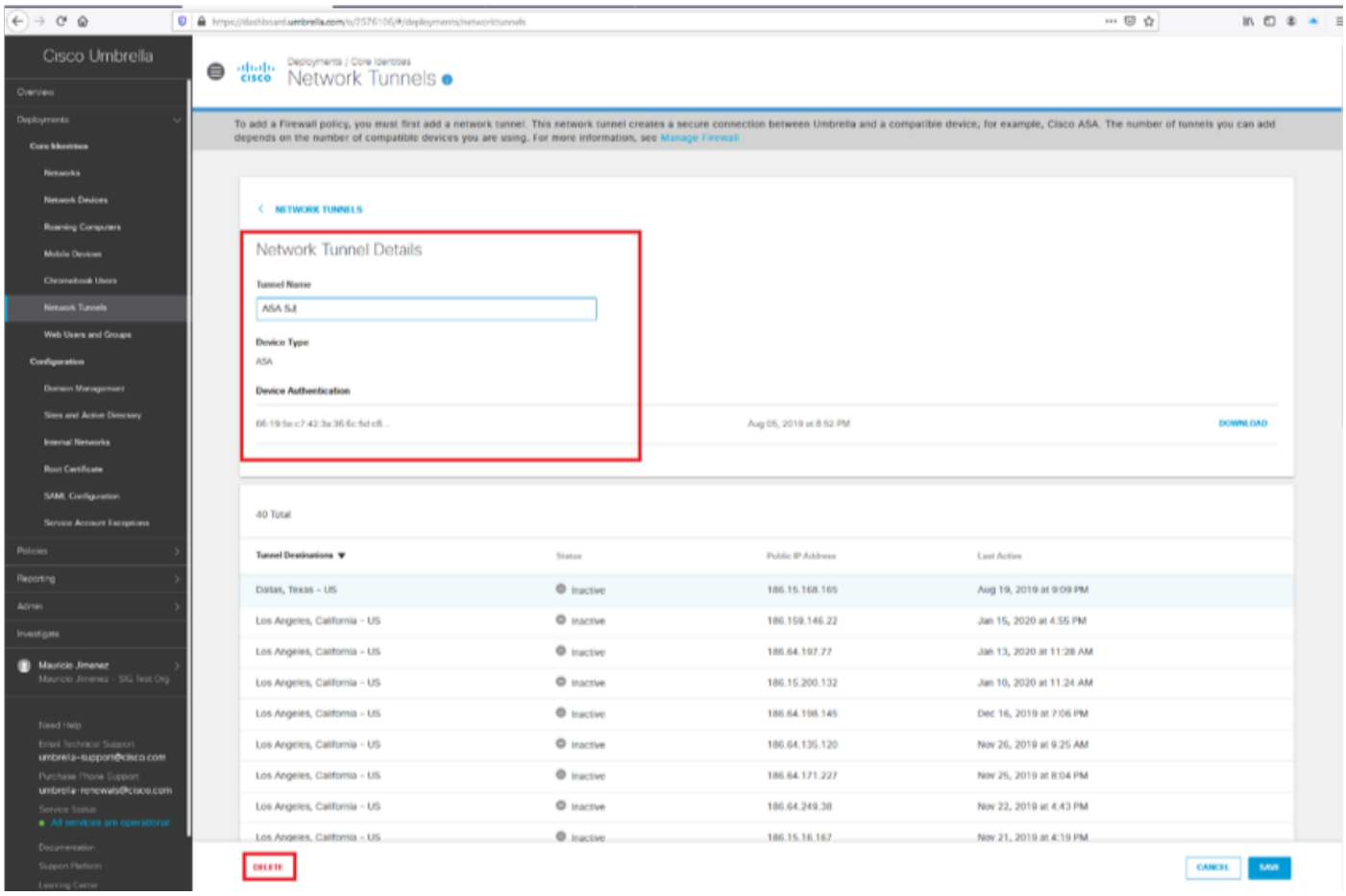

Imagem26.png

2. Confirme a deleção selecionando a opção Eu entendo e quero deletar este túnel no pop-up e, em seguida, selecione Deletar.

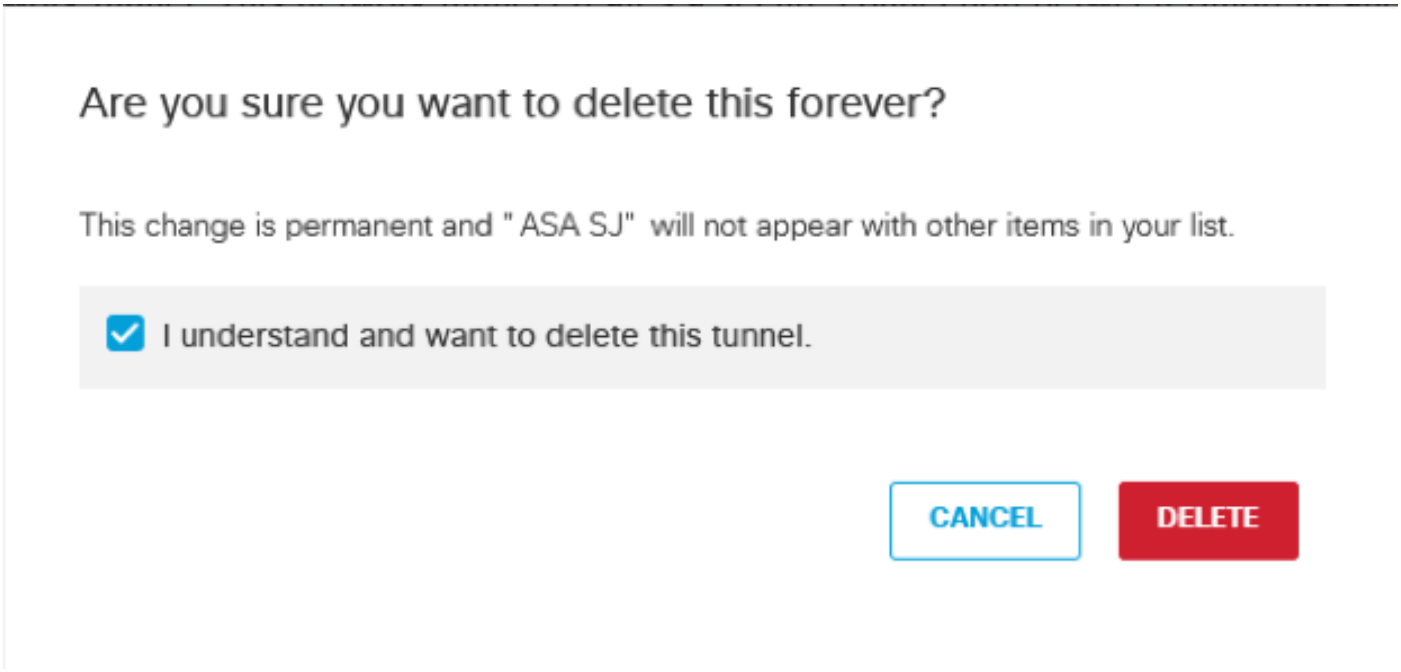

Imagem27.png

Etapa 12: Atualizar políticas da Web com a nova identidade de

túnel

Confirme se suas políticas da Web têm a identidade atualizada com o novo túnel de rede:

1. No painel Umbrella, navegue para Policies > Management > Web Policies.

2. Revise a seção Túneis e confirme se suas políticas da Web têm a identidade atualizada com o novo túnel de rede.

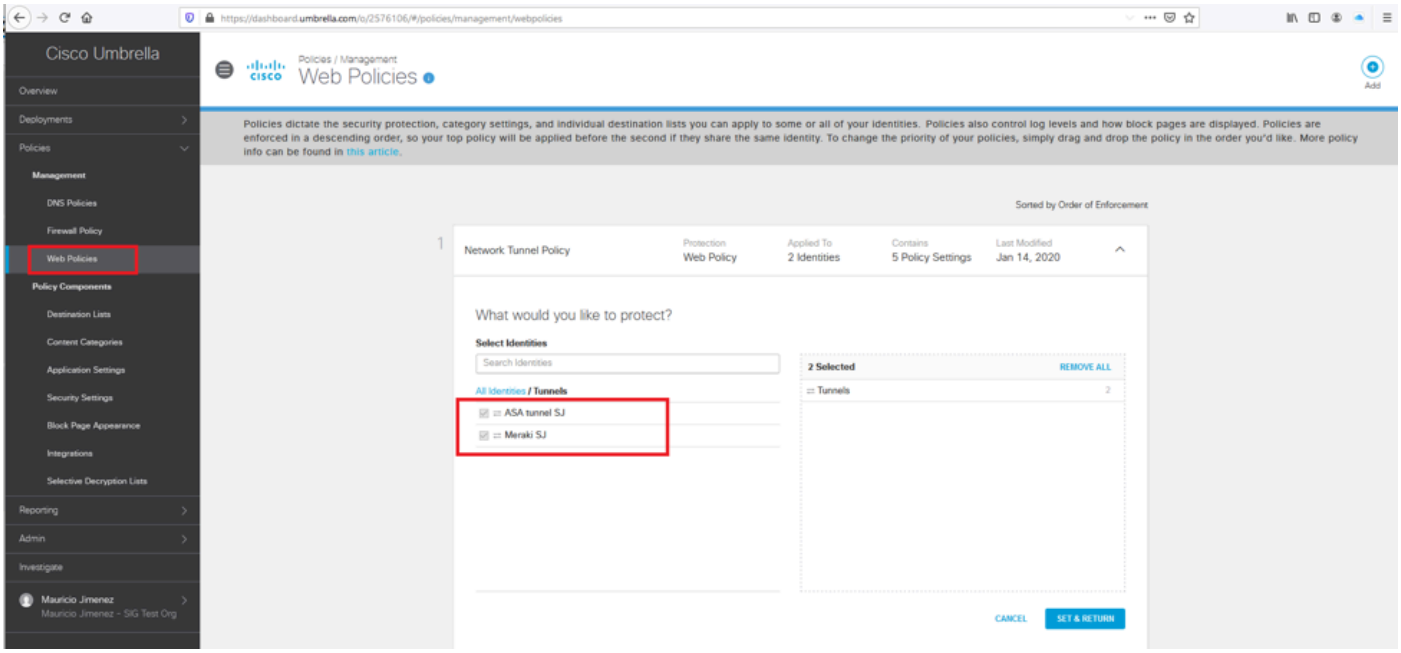

Imagem28.png

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.