Solucionar Problemas de Falha de Autenticação Baseada em Certificado de Ponto de Acesso por FTD

Problema

Esses sintomas são relatados após a migração do Cisco Adaptive Security Appliance 5508 para o Cisco Secure Firewall (CSF) Threat Defense (FTD) 1230 na filial principal (HQ):

1. Os pontos de acesso (AP) localizados nas filiais não conseguem se autenticar no servidor RADIUS na matriz usando a autenticação de certificado.

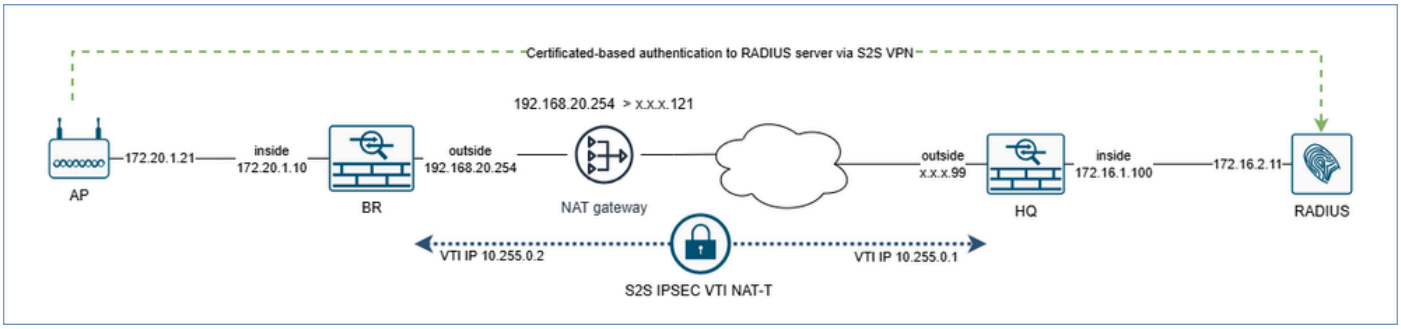
2. Autenticação com nome de usuário e senha bem-sucedida.

Os sintomas são observados para pontos de acesso em todas as filiais.

Ambiente

CSF 1230 gerenciado pelo FMC em configuração de alta disponibilidade executando a versão 7.7.10.1 no HQ e vários Firepower 1010 autônomos executando a versão 7.4.2.4 em filiais, outras versões de software também podem ser afetadas. Os sintomas, nesse caso, são independentes de hardware.

Topologia



inline_image_0.png

Pontos principais sobre a topologia:

- Na camada de rede, o ponto de acesso está na sub-rede da interface interna do firewall BR (filial).
- O roteador como um gateway NAT converte o endereço IP da interface externa do firewall BR em um endereço público x.x.x.121. Isso significa que o firewall BR está a pelo menos 1 salto de distância do firewall HQ.
- Os firewalls HQ e BR são conectados usando Redes Virtuais Privadas (VPN S2S) site a site usando Segurança de Protocolo Internet (IPsec) com Encapsulating Security Payload (ESP) e a Interface de Túnel Virtual (VTI) sobre NAT.
- No nível da rede, o servidor RADIUS está na sub-rede da interface interna do firewall HQ.

Resolução

Para análise técnica, as capturas de pacotes foram coletadas dos firewalls HQ e BR.

Em capturas de entrada/saída de plano de dados de firewall HQ e BR em interfaces físicas, capturas em interfaces VTI, capturas de queda ASP para tráfego interno e externo com base no endereço IP do peer:

Firewall BR:

```
cap br_inside interface inside packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16
cap br_vti interface vti-hq packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16.2.
cap br_asp match ip host x.x.x.99 any
cap br_asp match ip host 172.20.1.21 host 172.16.2.11
cap br_outside interface outside packet-length 9000 buffer 33554400 match ip host x.x.x.99 any
```

Observe que x.x.x.99 é substituído por um endereço IP real.

Firewall HQ:

```
cap hq_inside interface inside packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16
cap hq_vti interface vti-br packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16.2.
```

```
cap hq_asp match ip host x.x.x.121 any
cap hq_asp match ip host 172.20.1.21 host 172.16.2.11
cap hq_outside interface outside packet-length 9000 buffer 33554400 match ip host x.x.x.121 any
```

Observe que x.x.x.121 é substituído por um endereço IP real.

Além disso, no firewall HQ, colete capturas de switch internas bidirecionais nas interfaces do chassi com base no nome externo e em todas as interfaces de uplink:

```
cap hqfxos switch interface outside direction both packet-length 2048 match ip x.x.177.121
cap hqfxos switch interface in_data_uplink1 direction both packet-length 2048 match ip x.x.x.121
cap hqfxos switch interface in_data_uplink2 direction both packet-length 2048 match ip x.x.x.121
cap hqfxos switch interface in_data_uplink3 direction both packet-length 2048 match ip x.x.x.121
no cap hqfxos switch stop.
```

Análise técnica

Firewall HQ

1. As capturas de queda do Caminho de segurança acelerado (ASP) no firewall HQ indicam que os fragmentos são descartados com o motivo fragment-reassembly-failed:

<#root>

>

show capture hq_asp

```
Target:     OTHER
Hardware:   CSF-1230
Cisco Adaptive Security Appliance Software Version 99.23(37)127
ASLR enabled, text region aaaae5d50000-aaaae902d504
172.20.1.21.38676 > 172.16.2.11.1812:  udp 1913 Drop-reason: (fragment-reassembly-failed) Fragment reas
Drop-reason: (
```

fragment-reassembly-failed

```
) Fragment reassembly failed, Drop-location: frame snp_fh_destroy:1055 flow (NA)/NA
172.20.1.21.38676 > 172.16.2.11.1812:  udp 1913 Drop-reason: (fragment-reassembly-failed) Fragment reas
Drop-reason: (
```

fragment-reassembly-failed

```
) Fragment reassembly failed, Drop-location: frame snp_fh_destroy:1055 flow (NA)/NA
172.20.1.21.56952 > 172.16.2.11.1812:  udp 1913 Drop-reason: (fragment-reassembly-failed) Fragment reas
Drop-reason: (
```

```
fragment-reassembly-failed

) Fragment reassembly failed, Drop-location: frame snp_fh_destroy:1055 flow (NA)/NA
```

2. O contador Timeout para a interface VTI na saída do comando show fragment no firewall HQ aumenta:

```
<#root>

>

show fragment

Interface: vti-br
    Configuration: Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Run-time stats: Queue: 0, Full assembly: 0
    Drops: Size overflow: 0,

Timeout: 1217

,
            Chain overflow: 0, Fragment queue threshold exceeded: 0,
            Small fragments: 0, Invalid IP len: 0,
            Reassembly overlap: 0, Fraghead alloc failed: 0,
            SGT mismatch: 0, Block alloc failed: 0,
            Invalid IPV6 header: 0, Passenger flow assembly failed: 0
            Cluster reinsert collision: 0
```

De acordo com a referência de comando (https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/S/asa-command-ref-S/show-f-to-show-ipu-commands.html#wp4144096608), o Timeout é "O número máximo de segundos a aguardar até que um pacote inteiro fragmentado chegue". O valor padrão é de 5 segundos. Isso significa que se toda a cadeia de fragmentos não chegar ao firewall dentro de 5 segundos, os fragmentos recebidos serão descartados e a remontagem do fragmento falhará.

3. Com base no ponto anterior, o firewall HQ não recebe a cadeia completa de fragmentos que resulta em falha de remontagem de fragmentos.

Firewall BR

1. Com base nas capturas, o AP envia a solicitação de autenticação RADIUS baseada em certificado em 2 fragmentos separados para o firewall BR. A captura br_inside mostra 2 fragmentos de entrada de 1514 bytes e 475 bytes, respectivamente. Os mesmos pacotes são vistos nas capturas de interface BR VTI que mostram o pacote antes da criptografia:

172.20.1.21	172.16.2.11	IPv4			1514	0xf20b (61963)	64		Fragmented IP protocol (proto=UDP 17, off=0, ID=f20b) [Reassembled in #9]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20b (61963)	64		Access-Request id=255
172.20.1.21	172.16.2.11	IPv4			1514	0xf20c (61964)	64		Fragmented IP protocol (proto=UDP 17, off=0, ID=f20c) [Reassembled in #11]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20c (61964)	64		Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf20d (61965)	64		Fragmented IP protocol (proto=UDP 17, off=0, ID=f20d) [Reassembled in #13]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20d (61965)	64		Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf20e (61966)	64		Fragmented IP protocol (proto=UDP 17, off=0, ID=f20e) [Reassembled in #15]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20e (61966)	64		Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf20f (61967)	64		Fragmented IP protocol (proto=UDP 17, off=0, ID=f20f) [Reassembled in #17]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20f (61967)	64		Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf210 (61968)	64		Fragmented IP protocol (proto=UDP 17, off=0, ID=f210) [Reassembled in #19]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf210 (61968)	64		Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf211 (61969)	64		Fragmented IP protocol (proto=UDP 17, off=0, ID=f211) [Reassembled in #21]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf211 (61969)	64		Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf212 (61970)	64		Fragmented IP protocol (proto=UDP 17, off=0, ID=f212) [Reassembled in #23]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf212 (61970)	64		Access-Request id=255, Duplicate Request

inline_image_0.png

A Unidade Máxima de Transmissão (MTU) da interface externa do BR é de 1500 bytes. Por esse motivo, o fragmento de 1.514 bytes deve ser fragmentado em 2 pacotes antes da criptografia.

2. As capturas de queda de ASP br_asp para o tráfego RADIUS interno no firewall BR não mostram pacotes descartados. Enquanto isso, para o tráfego externo, há quedas de pacotes de 226 bytes com o motivo pacote inesperado:

<#root>

```
firepower#

show capture br_asp

Target:     OTHER
Hardware:   FPR-1010
Cisco Adaptive Security Appliance Software Version 9.20(2)121
ASLR enabled, text region 560817d6b000-56081d1ae26d
103 packets captured
   1: 10:13:22.160239       192.168.20.254.4500 > x.x.x.99.4500:  udp 184 Drop-reason: (unexpected-pack
   2: 10:13:23.160727       192.168.20.254.4500 > x.x.x.99.4500:  udp 184 Drop-reason: (unexpected-pack
   3: 10:13:24.161200       192.168.20.254.4500 > x.x.x.99.4500:  udp 184 Drop-reason: (unexpected-pack
```

192.168.20.254	.99	ESP	4500	4500	226	0x7254 (29268)	64	6275	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	226	0x7e97 (32407)	64	6278 ✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	226	0x0fc6 (4038)	64	6281 ✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	226	0x3511 (13585)	64	6284 ✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	226	0x5868 (22632)	64	6287 ✓	ESP (SPI=0x1592a843)

inline_image_1.png

Observe que a saída do comando show capture br_asp mostra 184 bytes de comprimento de payload, enquanto o comprimento total de cada pacote é 226 bytes.

3. Para verificar se os pacotes ESP descartados de 226 bytes são relevantes para o tráfego afetado entre o AP e o servidor RADIUS, a captura br_inside foi repetida no laboratório interno usando as mesmas configurações de política de segurança dos firewalls HQ e BR. A captura br_vti do dispositivo do laboratório mostra fragmentos de 1514 bytes e 475 bytes, isto é, antes da criptografia:

Source	Destination	Protocol	Sport	Dport	Length	IP ID	IP TTL	Info
172.20.1.21	172.16.2.11	IPv4			1514	0xe69d (59037)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e69d) [Reassembled in #9
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe69d (59037)	63	Access-Request id=218
172.20.1.21	172.16.2.11	IPv4			1514	0xe69e (59038)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e69e) [Reassembled in #1
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe69e (59038)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe69f (59039)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e69f) [Reassembled in #1
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe69f (59039)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a0 (59040)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a0) [Reassembled in #1
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a0 (59040)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a1 (59041)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a1) [Reassembled in #1
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a1 (59041)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a2 (59042)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a2) [Reassembled in #1
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a2 (59042)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a3 (59043)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a3) [Reassembled in #2
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a3 (59043)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a4 (59044)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a4) [Reassembled in #2
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a4 (59044)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a5 (59045)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a5) [Reassembled in #2
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a5 (59045)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a6 (59046)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a6) [Reassembled in #2
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a6 (59046)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a7 (59047)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a7) [Reassembled in #2
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a7 (59047)	63	Access-Request id=218, Duplicate Request

inline_image_2.png

4. As capturas de br_outside mostram a falta de pacotes de 226 bytes e a lacuna nos números de sequência ESP entre os pacotes de 562 bytes e de 1506 bytes:

Source	Destination	Protocol	Sport	Dport	Length	IP ID	IP TTL	ESP Sequence	Wrong Sequence Number	Info
192.168.20.254	.99	ESP	4500	4500	1506	0x2d7e (11646)	64	6448		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x0b2c (2860)	64	6450	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x6ca9 (27817)	64	6451		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x51cf (20943)	64	6453	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x7d60 (32096)	64	6454		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x42de (17118)	64	6456	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x4553 (17747)	64	6457		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x7389 (29577)	64	6459	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x50f9 (20729)	64	6460		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x169f (5791)	64	6462	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	178	0x32d8 (13016)	64	6463		ESP (SPI=0x1592a843)

inline_image_3.png

Pontos principais:

- A captura br_outside não contém 226 bytes, pois foi descartada no ASP do firewall BR com o motivo de queda do ASP expected-packet.
- O descarte de pacote explica a lacuna nos números de sequência ESP.
- Além disso, o número de sequência ausente no intervalo significa que o pacote ESP de 226 bytes foi gerado pelo firewall BR, mas não foi transmitido para fora da interface externa.
- Como o pacote de 226 bytes não foi enviado para a interface externa do firewall BR, o firewall HQ nunca o recebeu.
- A falta do pacote de 226 bytes no firewall HQ resultou na falha de remontagem do fragmento, como mostrado na "seção do firewall HQ".

Explicação

As descobertas da seção de análise técnica correspondem aos sintomas da ID de bug Cisco CSCwp10123.

Visão geral de alto nível das ações de firewall para gerar pacotes ESP e transmiti-los pela interface de saída:

1. O firewall recebe pacotes fragmentados que devem ser enviados pelo túnel VTI.
2. Se o comprimento do pacote interno for maior que o tamanho do MTU da interface menos a sobrecarga de IPSEC, o pacote será fragmentado.
3. Com base na pesquisa da tabela de roteamento, o próximo salto é encontrado. No caso do VTI, o próximo salto é o endereço IP do VTI do peer.
4. Com base no endereço destino do túnel, a interface de saída e o próximo salto são identificados (por exemplo, a interface externa).
5. Os pacotes originais são encapsulados dentro de pacotes ESP.
6. A consulta de adjacência para o próximo salto da etapa 3 é executada e os pacotes são enviados pela interface de saída.

Devido ao bug da Cisco ID CSCwp10123, para pacotes subsequentes de fragmentos encapsulados ESP (não iniciais) na etapa 4 é realizada uma nova consulta de rota. Se o firewall tiver rotas mais específicas para o endereço IP do peer (ou sub-rede), a nova rota será usada em vez da rota para o pacote inicial. Neste exemplo, o endereço IP da interface do firewall HQ é x.x.x.99. O firewall HQ anuncia sua sub-rede externa ao firewall BR através do BGP (Border Gateway Protocol) sendo executado sobre o VTI:

<#root>

>

show route bgp

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRFGateway of last resort is 192.168.20.1 to network 0.0.0.0
```

B   x.x.x.96 255.255.255.224 [20/0] via 10.255.0.1, 13:57:43

```
<--BR firewall learns /27 route via BGP over VTI
```

<#root>

>

show bgp summary

```
BGP router identifier 192.168.179.10, local AS number 65001
BGP table version is 25, main routing table version 25
23 network entries using 4600 bytes of memory
24 path entries using 1920 bytes of memory
2/2 BGP path/bestpath attribute entries using 416 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 6960 total bytes of memory
BGP activity 23/0 prefixes, 24/0 paths, scan interval 60 secs
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
```

10.255.0.1 4 65000 762 761 25 0 0 13:59:01 18

```
>
```

show ip

```
…
Tunnel1                vti-hq                 10.255.0.2      255.255.255.252 CONFIG <--
```

10.255.0.1

```
 is the peer VTI IP
…
```

<#root>

```
>
```

show ip

```
…
Tunnel1                vti-hq                 10.255.0.2      255.255.255.252 CONFIG <--
```

10.255.0.1

```
 is the peer VTI IP in the same subnet
…
```

O pacote ESP de 1.514 bytes é enviado para a interface externa. Mas para os 226 bytes, o firewall na etapa 3 executa uma consulta de rota e encontra uma rota específica para o endereço IP do peer através do VTI. Em outras palavras, em vez de enviar os pacotes para fora da interface de terminação VPN, o firewall usa a interface VTI e tenta resolver a adjacência na interface VTI. Como as interfaces VTI não têm um conceito de adjacência, os pacotes são eventualmente descartados com a razão de descarte de pacote inesperado.

Como solução alternativa, no CSF1230, o usuário incluiu a lista de acesso (ACL) no mapa de rota. Após a implantação da política, a ACL negou a sub-rede externa HQ, removendo efetivamente a propagação da sub-rede externa HQ do roteamento BGP. Devido a essa alteração, os firewalls BR não recebem o prefixo de sub-rede externo HQ na interface de túnel.

Por que os pacotes de 266 bytes são descartados após a migração do ASA para o Secure Firewall?

A configuração do firewall ASA bloqueou explicitamente a propagação da sub-rede da interface externa de HQ para as filiais:

ASA5508

```
router bgp 65000
...
  redistribute connected route-map BGP_RM
route-map BGP_RM permit 10
 match ip address bgp-connected-routes
access-list bgp-connected-routes standard deny x.x.x.96 255.255.255.224 <-- deny = do not redistribute
```

CSF1230

```
router bgp 65000
...
  redistribute connected route-map BGP_RM
route-map BGP_RM permit 40 <-- No match, means redistribute all connected routes
```

Causa

O problema foi disparado por uma diferença de configuração na redistribuição de rota BGP entre o ASA 5508 original e o novo FTD 1230. O ASA 5508 tinha uma lista de controle de acesso que negava a redistribuição da sub-rede x.x.x.96/27, enquanto o FTD 1230 foi configurado para redistribuir todas as rotas conectadas. Essa diferença de configuração acionou o bug da Cisco ID CSCwp10123.

Conteúdo relacionado

- ID de bug da Cisco CSCwp10123

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.