

Roteador do IOS VPN: Adicionar ou remova uma rede em um exemplo da configuração de túnel L2L VPN

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Remova uma rede de um túnel de IPsec](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento fornece uma configuração de exemplo para que como adicione ou remova uma rede em um túnel existente do LAN para LAN (L2L) VPN.

[Pré-requisitos](#)

[Requisitos](#)

Assegure-se de que você configure corretamente seu túnel atual do IPSec VPN L2L antes que você tente esta configuração.

[Componentes Utilizados](#)

A informação neste documento é baseada em dois Roteadores do [®] do Cisco IOS que executa a versão de software 12.4(15)T1.

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Informações de Apoio

Há atualmente um túnel L2L VPN entre as matrizes (QG) escritório e o escritório filial (BO). O escritório QG apenas adicionou uma rede nova a ser usada pelo equipe de vendas. Esta equipe exige o acesso aos recursos que residem no escritório BO. A tarefa à mão é adicionar uma rede nova ao túnel já existente L2L VPN.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configurações

Este documento usa as configurações descritas nesta seção. Estas configurações incluem um L2L VPN que seja executado entre a rede de 172.16.10.0 do escritório QG e a rede de 10.10.10.0 do escritório BO. A saída indicada no texto em **negrito** mostra a configuração requerida para integrar a rede nova 192.168.10.0 do escritório QG no mesmo túnel VPN com 10.10.10.0 que a rede de destino.

QG-roteador

```
HQ-Router#show running-config Building configuration...
Current configuration : 1439 bytes ! version 12.4
service timestamps debug uptime service timestamps log
uptime no service password-encryption ! hostname HQ-
Router ! !--- Output suppressed. ! crypto isakmp policy
1 hash md5 authentication pre-share crypto isakmp key
cisco123 address 209.165.200.225 ! ! crypto ipsec
transform-set rtpset esp-des esp-md5-hmac ! crypto map
rtp 1 ipsec-isakmp set peer 209.165.200.225 set
transform-set rtpset match address 115 ! interface
Ethernet0 ip address 172.16.10.1 255.255.255.0 ip nat
inside ! interface Ethernet1 ip address 209.165.201.2
255.255.255.224 ip nat outside crypto map rtp !
interface Ethernet2 ip address 192.168.10.1
255.255.255.0 ip nat inside ! interface Serial0 no ip
address shutdown no fair-queue ! interface Serial1 no ip
address shutdown ! ip nat inside source route-map nonat
interface Ethernet1 overload ip classless ip route
0.0.0.0 0.0.0.0 209.165.201.1 ! !--- Output suppressed.
access-list 110 deny ip 172.16.10.0 0.0.0.255 10.10.10.0
```

```

0.0.0.255 access-list 110 permit ip 172.16.10.0
0.0.0.255 any ! !--- Add this ACL entry to include
192.168.10.0 !--- network with the nat-exemption rule.
access-list 110 deny ip 192.168.10.0 0.0.0.255
10.10.10.0 0.0.0.255 access-list 110 permit ip
192.168.10.0 0.0.0.255 any access-list 115 permit ip
172.16.10.0 0.0.0.255 10.10.10.0 0.0.0.255 ! !--- Add
this ACL entry to include 192.168.10.0 !--- network into
the crypto map. access-list 115 permit ip 192.168.10.0
0.0.0.255 10.10.10.0 0.0.0.255 route-map nonat permit 10
match ip address 110 ! !--- Output suppressed. end

```

BO-roteador

```

BO-Router#show running-config Building configuration...
Current configuration : 2836 bytes ! version 12.4
service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname BO-Router ! !--- Output
suppressed. ! crypto isakmp policy 1 hash md5
authentication pre-share crypto isakmp key cisco123
address 209.165.201.2 ! ! crypto ipsec transform-set
rtpset esp-des esp-md5-hmac ! crypto map rtp 1 ipsec-
isakmp set peer 209.165.201.2 set transform-set rtpset
match address 115 ! !--- Output suppressed. interface
FastEthernet0/0 ip address 209.165.200.225
255.255.255.224 ip nat outside ip virtual-reassembly
duplex auto speed auto crypto map rtp ! interface
FastEthernet0/1 ip address 10.10.10.1 255.255.255.0 ip
nat inside ip virtual-reassembly duplex auto speed auto
! ip route 0.0.0.0 0.0.0.0 FastEthernet0/1 ! !--- Output
suppressed. ! ip http server no ip http secure-server ip
nat inside source route-map nonat interface
FastEthernet0/0 overload ! !--- Add this ACL entry to
include 192.168.10.0 !--- network with the nat-exemption
rule. access-list 110 deny ip 10.10.10.0 0.0.0.255
192.168.10.0 0.0.0.255 access-list 110 deny ip
10.10.10.0 0.0.0.255 172.16.10.0 0.0.0.255 access-list
110 permit ip 10.10.10.0 0.0.0.255 any access-list 115
permit ip 10.10.10.0 0.0.0.255 172.16.10.0 0.0.0.255 !
!--- Add this ACL entry to include 192.168.10.0 !---
network into the crypto map. access-list 115 permit ip
10.10.10.0 0.0.0.255 192.168.10.0 0.0.0.255 ! route-map
nonat permit 10 match ip address 110 ! !--- Output
suppressed. ! end

```

Remova uma rede de um túnel de IPsec

Termine as etapas descritas nesta seção a fim remover a rede da configuração do túnel de IPsec. Note que a rede 192.168.10.0/24 esteve removida da configuração de roteador QG.

1. Use este comando a fim rasgar para baixo a conexão IPsec:HQ-Router#**clear crypto sa**
2. Use este comando a fim cancelar as associações de ISAKMP Security (SA):HQ-Router#**clear crypto isakmp**
3. Use este comando a fim remover o tráfego interessante ACL para o túnel de IPsec:HQ-Router(config)#**no access-list 115 permit ip 192.168.10.0 0.0.0.255 10.10.10.0 0.0.0.255**
4. Use este comando a fim remover a indicação NAT-isenta ACL para a rede de 192.168.10.0:HQ-Router(config)#**no access-list 110 deny ip 192.168.10.0 0.0.0.255 10.10.10.0 0.0.0.255**
5. Use este comando a fim cancelar a tradução NAT:HQ-Router#**clear ip nat translation ***
6. Use estes comandos a fim remover e reuplicar o crypto map na relação para assegurar-se

de que a configuração de criptografia atual tome o efeito:

```
HQ-Router(config)#int ethernet 1
HQ-Router(config-if)#no crypto map rtp *May 25 10:35:12.153: %CRYPTO-6-ISAKMP_ON_OFF:
ISAKMP is OFF HQ-Router(config-if)#crypto map rtp *May 25 10:36:09.305: %CRYPTO-6-
ISAKMP_ON_OFF: ISAKMP is ON
```

Nota: Remover o crypto map da relação rasga todas as conexões de VPN existentes associadas com esse crypto map. Antes de fazer isto, certifique-se por favor de que você tomou o tempo ocioso da máquina exigido e seguiu a política de controle de alterações de sua organização em conformidade.

7. Use o comando **write memory** a fim salvar a configuração ativa ao flash.
8. Termine estas etapas na outra extremidade do túnel VPN (BO-roteador) a fim remover as configurações.
9. Inicie o túnel de IPsec e verifique a conexão.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Use esta sequência do sibiló a fim assegurar-se de que a rede nova possa passar dados através do túnel VPN:

```
HQ-Router#clear crypto sa HQ-Router# HQ-Router#ping 10.10.10.1 source 172.16.10.1 Type escape
sequence to abort. Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds: Packet
sent with a source address of 172.16.10.1 !!!!! Success rate is 80 percent (4/5), round-trip
min/avg/max = 20/20/20 ms HQ-Router#ping 10.10.10.1 source 192.168.10.1 Type escape sequence to
abort. Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds: Packet sent with a
source address of 192.168.10.1 !!!!! Success rate is 80 percent (4/5), round-trip min/avg/max =
20/20/20 ms HQ-Router#ping 10.10.10.1 source 192.168.10.1 Type escape sequence to abort. Sending
5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds: Packet sent with a source address of
192.168.10.1 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

show crypto ipsec sa

```
HQ-Router#show crypto ipsec sa interface: Ethernet1
Crypto map tag: rtp, local addr. 209.165.201.2 local
ident (addr/mask/prot/port):
(192.168.10.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
current_peer: 209.165.200.225 PERMIT,
flags={origin_is_acl,} #pkts encaps: 9, #pkts encrypt:
9, #pkts digest 9 #pkts decaps: 9, #pkts decrypt: 9,
#pkts verify 9 #pkts compressed: 0, #pkts decompressed:
0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts
decompress failed: 0 #send errors 1, #recv errors 0
local crypto endpt.: 209.165.201.2, remote crypto
endpt.: 209.165.200.225 path mtu 1500, ip mtu 1500, ip
mtu interface Ethernet1 current outbound spi: FB52B5AB
inbound esp sas: spi: 0x612332E(101856046) transform:
esp-des esp-md5-hmac , in use settings = {Tunnel, } slot:
0, conn id: 2002, flow_id: 3, crypto map: rtp sa timing:
remaining key lifetime (k/sec): (4607998/3209) IV size:
8 bytes replay detection support: Y inbound ah sas:
inbound pcp sas: outbound esp sas: spi:
0xFB52B5AB(4216501675) transform: esp-des esp-md5-hmac ,
in use settings = {Tunnel, } slot: 0, conn id: 2003,
flow_id: 4, crypto map: rtp sa timing: remaining key
lifetime (k/sec): (4607998/3200) IV size: 8 bytes replay
detection support: Y outbound ah sas: outbound pcp sas:
local ident (addr/mask/prot/port):
(172.16.10.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
```

```
current_peer: 209.165.200.225 PERMIT,
flags={origin_is_acl,} #pkts encaps: 4, #pkts encrypt:
4, #pkts digest 4 #pkts decaps: 4, #pkts decrypt: 4,
#pkts verify 4 #pkts compressed: 0, #pkts decompressed:
0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts
decompress failed: 0 #send errors 1, #recv errors 0
local crypto endpt.: 209.165.201.2, remote crypto
endpt.: 209.165.200.225 path mtu 1500, ip mtu 1500, ip
mtu interface Ethernet1 current outbound spi: C9E9F490
inbound esp sas: spi: 0x1291F1D3(311554515) transform:
esp-des esp-md5-hmac , in use settings ={Tunnel, } slot:
0, conn id: 2000, flow_id: 1, crypto map: rtp sa timing:
remaining key lifetime (k/sec): (4607999/3182) IV size:
8 bytes replay detection support: Y inbound ah sas:
inbound pcp sas: outbound esp sas: spi:
0xC9E9F490(3387552912) transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, } slot: 0, conn id: 2001,
flow_id: 2, crypto map: rtp sa timing: remaining key
lifetime (k/sec): (4607999/3182) IV size: 8 bytes replay
detection support: Y outbound ah sas: outbound pcp sas:
```

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

[Troubleshooting](#)

Use esta seção para fazer o troubleshooting da sua configuração.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

- **IPsec do debug crypto** — Indica as negociações de IPSEC de fase 2.
- **isakmp do debug crypto** — Indica as negociações de ISAKMP de fase 1.
- **motor do debug crypto** — Indica as sessões de criptografia.

[Informações Relacionadas](#)

- [Uma introdução à criptografia do protocolo de segurança IP \(IPSEC\)](#)
- [Página de Suporte de Negociação IPsec/Protocolos IKE](#)
- [Configurando um par dinâmico e clientes VPN do LAN para LAN do roteador de IPsec](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)