Router del IOS VPN: Agregue o quite una red en un ejemplo de la configuración del túnel L2L VPN

Contenido

Introducción

Este documento proporciona una configuración de muestra para que cómo agregue o quite una red en un túnel existente del LAN a LAN (L2L) VPN.

prerrequisitos

Requisitos

Asegúrese de que usted configure correctamente su túnel actual del IPSec VPN L2L antes de que usted intente esta configuración.

Componentes Utilizados

La información en este documento se basa en dos Routers del ® del Cisco IOS que funcione con la versión de software 12.4(15)T1.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Hay actualmente un túnel L2L VPN entre las jefaturas (HQ) oficina y la sucursal (BO). La oficina HQ acaba de agregar una nueva red que se utilizará por el equipo de ventas. Este equipo requiere el acceso a los recursos que residen en la oficina BO. La tarea a mano es agregar una nueva red al túnel ya existente L2L VPN.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Configuraciones

Este documento utiliza las configuraciones descritas en esta sección. Estas configuraciones incluyen un L2L VPN que se ejecute entre la red de 172.16.10.0 de la oficina HQ y la red de 10.10.10.0 de la oficina BO. La salida visualizada en el texto en negrita muestra la configuración necesaria para integrar la nueva red 192.168.10.0 de la oficina HQ en el mismo túnel VPN con 10.10.10.0 que la red de destino.

HQ-router

```
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-router

```
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
```

Quite una red de un túnel IPsec

Complete los pasos descritos en esta sección para quitar la red de la configuración del túnel IPsec. Observe que la red 192.168.10.0/24 se ha quitado de la configuración del router HQ.

1. Utilice este comando para derribar conexión IPSec:`HQ-Router#clear crypto sa`
2. Utilice este comando para borrar las asociaciones de ISAKMPSecurity (SA):`HQ-Router#clear crypto isakmp`
3. Utilice este comando para quitar el tráfico interesante ACL para el túnel 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. Utilice este comando para quitar la declaración NAT-exenta ACL para la red 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. Utilice este comando para borrar la traducción de NAT:`HQ-Router#clear ip nat translation *`
6. Utilice estos comandos para quitar y reaplicar la correspondencia de criptografía en la

interfaz para asegurarse de que la configuración de criptografía actual toma el efecto:`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:** La eliminación de la correspondencia de criptografía de la interfaz rasga todas las conexiones VPN existentes asociadas a esa correspondencia de criptografía. Antes de hacer esto, aseegurese por favor que usted ha tardado el tiempo muerto requerido y ha seguido la directiva de control de cambios de su organización por consiguiente.

7. Utilice el **comando write memory** para salvar la configuración activa al flash.
8. Complete estos pasos en el otro extremo del túnel VPN (BO-router) para quitar las configuraciones.
9. Inicie el túnel IPsec y verifique la conexión.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Utilice esta secuencia del ping para asegurarse de que la nueva red puede pasar los datos a través del 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:
```

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Troubleshooting

Use esta sección para resolver problemas su configuración.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **IPSec del debug crypto** — Visualiza los IPSec Negotiations de la fase 2.
- **isakmp del debug crypto** — Visualiza negociaciones ISAKMP de la fase 1.
- **motor del debug crypto** — Visualiza a las sesiones encriptadas.

Información Relacionada

- Una Introducción al Cifrado de Seguridad IP (IPSec)
- Página de Soporte de IPSec Negotiation/IKE Protocols
- Configurar un par dinámico y a los clientes VPN del LAN a LAN del router IPSec
- Soporte Técnico y Documentación - Cisco Systems