IOS VPN-router: Een netwerk aan een L2L VPN-tunnelconfiguratievoorbeeld toevoegen of verwijderen

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor het toevoegen of verwijderen van een netwerk in een bestaande LAN-to-LAN (L2L) VPN-tunnel.

Voorwaarden

Vereisten

Zorg ervoor dat u uw huidige L2L IPsec VPN-tunnel correct configureren voordat u deze configuratie probeert.

Gebruikte componenten

De informatie in dit document is gebaseerd op twee Cisco IOS® routers die softwareversie 12.4(15)T1 uitvoeren.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Er is momenteel een L2L VPN-tunnel tussen het hoofdkantoor (HQ) kantoor en bijkantoor (BO). Het kantoor van het hoofdkwartier heeft net een nieuw netwerk toegevoegd dat door het verkoopteam moet worden gebruikt. Dit team heeft toegang nodig tot middelen die in het BO-kantoor wonen. De taak is om een nieuw netwerk toe te voegen aan de reeds bestaande L2L VPN-tunnel.

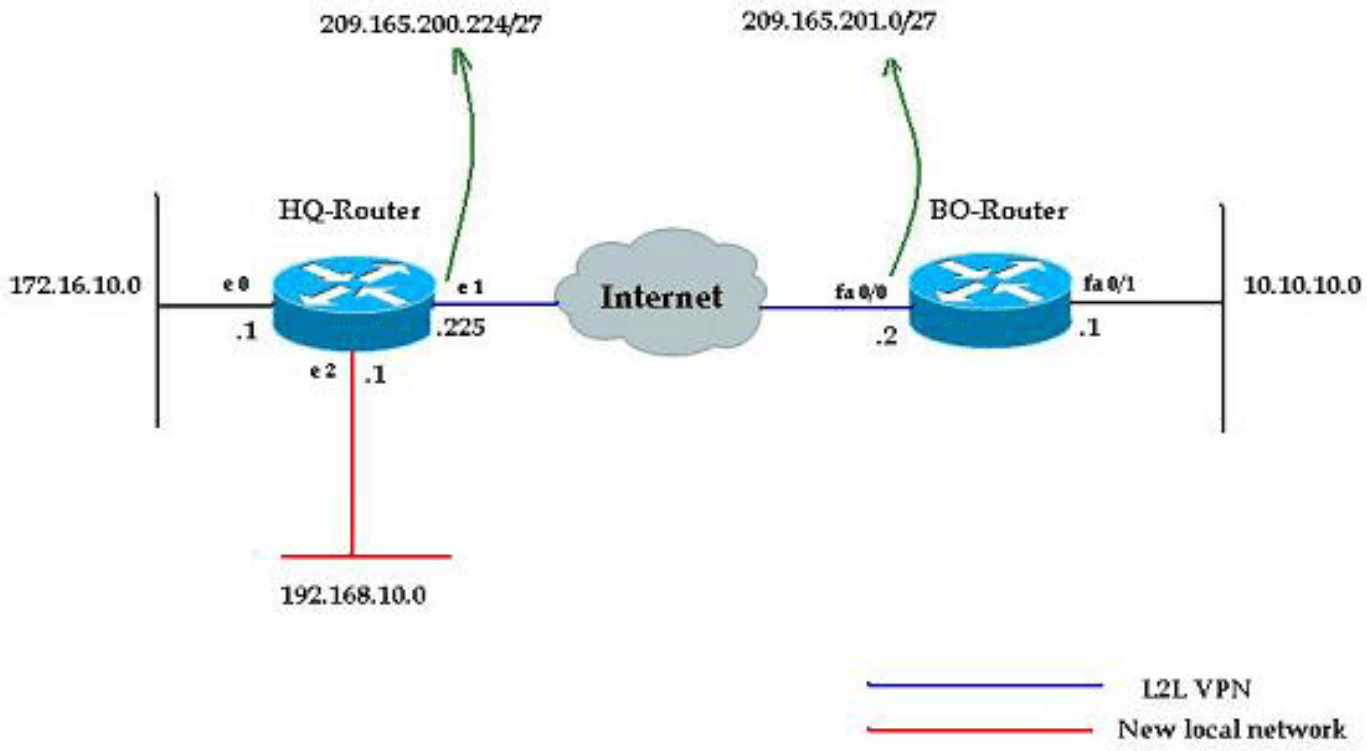
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt de configuraties die in dit hoofdstuk worden beschreven. Deze configuraties omvatten een L2L VPN dat loopt tussen het 172.16.10.0 netwerk van het kantoor van het Hoofdkantoor en het 10.10.10.0 netwerk van het bureau van de BO. De in vet weergegeven

uitvoer toont de gewenste configuratie om het nieuwe netwerk 192.168.10.0 van het hoofdkwartier te integreren in dezelfde VPN-tunnel met 10.10.10.0 als het doelnetwerk.

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
```

Verwijder een netwerk uit een IPsec-tunnel

Voltooi de in dit gedeelte beschreven stappen om het netwerk uit de IPsec-tunnelconfiguratie te verwijderen. Merk op dat het netwerk 192.168.10.0/24 is verwijderd uit de HQ routerconfiguratie.

1. Gebruik deze opdracht om de verbinding van IPsec af te breken:
   ```
   HQ-Router#clear crypto sa
   ```

2. Gebruik deze opdracht om de ISAKMPS Security Associations (SA's) te wissen:
   ```
   HQ-Router#clear crypto isakmp
   ```

3. Gebruik deze opdracht om het interessante verkeer ACL voor de IPsec-tunnel te verwijderen:
   ```
   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. Gebruik deze opdracht om de niet-vrijgestelde ACL-verklaring voor het 192.168.10.0-netwerk te verwijderen:
   ```
   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. Gebruik deze opdracht om de NAT-vertaling te verwijderen:
   ```
   HQ-Router#clear ip nat translation *
   ```

6. Gebruik deze opdrachten om de crypto-map op de interface te verwijderen en opnieuw toe te passen, om er zeker van te zijn dat de huidige configuratie van crypto-encryptie van kracht wordt:

```
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
```

Opmerking: Het verwijderen van de crypto kaart van de interface tranen alle bestaande VPN verbindingen die met die crypto kaart verbonden zijn. Zorg ervoor dat u, voordat u dit doet, de vereiste tijd hebt genomen en het veranderingscontrolebeleid van uw organisatie heeft gevolgd.

7. Gebruik de opdracht **schrijfgeheugen** om de actieve configuratie in de flitser op te slaan.
8. Voltooi deze stappen aan het andere eind van de VPN-tunnel (BO-router) om de configuraties te verwijderen.
9. Start de IPsec-tunnel en controleer de verbinding.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Gebruik deze ping-volgorde om er zeker van te zijn dat het nieuwe netwerk gegevens door de VPN-tunnel kan passeren:

```
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:
```

Het Uitvoer Tolk (geregistreerde klanten slechts) (OIT) steunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Problemen oplossen

Deze sectie bevat troubleshooting-informatie voor uw configuratie.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **debug crypto ipsec**-displays de IPsec onderhandelingen van fase 2.
- **debug crypto isakmp** — Hiermee geeft u de ISAKMP-onderhandelingen van fase 1 weer.
- **debug van crypto motor**-displays de versleutelde sessies.

Gerelateerde informatie

- Een Inleiding aan IP Security (IPSec) encryptie
- Ondersteuning van IPSec-onderhandeling/IKE-protocollen
- Een IPsec router Dynamic LAN-to-LAN peer en VPN-clients configureren
- Technische ondersteuning en documentatie – Cisco Systems