IOS-VPN-Router: Hinzufügen oder Entfernen eines Netzwerks auf einem L2L-VPN-Tunnel - Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration zum Hinzufügen oder Entfernen eines Netzwerks in einem vorhandenen LAN-to-LAN (L2L)-VPN-Tunnel.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie den aktuellen L2L IPsec VPN-Tunnel korrekt konfigurieren, bevor Sie diese Konfiguration durchführen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf zwei Cisco IOS® Routern, auf denen die Softwareversion 12.4(15)T1 ausgeführt wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Zwischen der Hauptniederlassung (HQ) und der Außenstelle (BO) besteht derzeit ein L2L-VPN-Tunnel. Die Zentrale hat soeben ein neues Netzwerk für das Vertriebsteam hinzugefügt. Dieses Team benötigt Zugriff auf Ressourcen, die sich im Büro der BO befinden. Es geht darum, dem bereits vorhandenen L2L VPN-Tunnel ein neues Netzwerk hinzuzufügen.

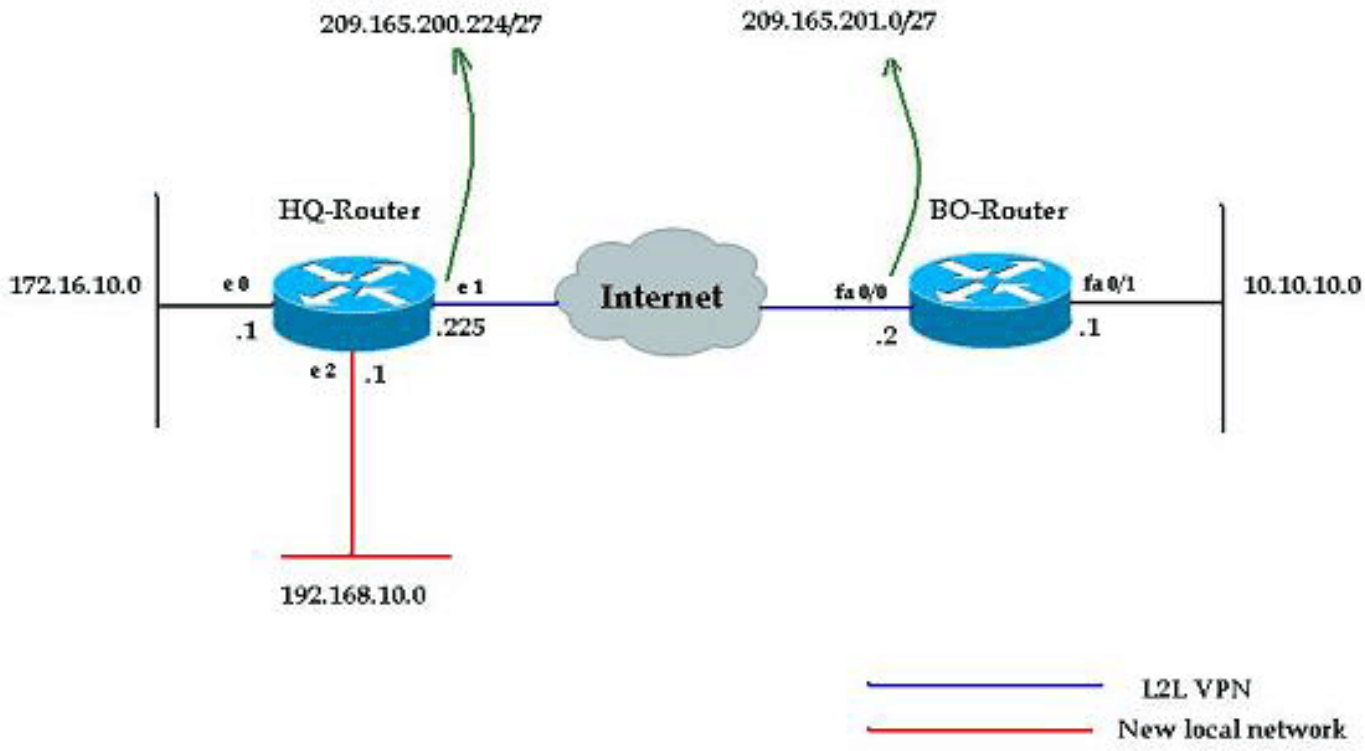
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden die in diesem Abschnitt beschriebenen Konfigurationen verwendet. Zu diesen Konfigurationen gehört ein L2L-VPN, das zwischen dem Netzwerk 172.16.10.0 des Hauptsitzes und dem Netzwerk 10.10.10.0 des Büros der BO läuft. Die fett formatierte Ausgabe

zeigt die erforderliche Konfiguration für die Integration des neuen Netzwerks 192.168.10.0 des Hauptsitzes in denselben VPN-Tunnel mit 10.10.10.0 als Zielnetzwerk.

Hauptsitz-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
```

Entfernen eines Netzwerks aus einem IPsec-Tunnel

Gehen Sie wie in diesem Abschnitt beschrieben vor, um das Netzwerk aus der IPsec-Tunnelkonfiguration zu entfernen. Beachten Sie, dass das Netzwerk 192.168.10.0/24 aus der Konfiguration des Routers im Hauptsitz entfernt wurde.

1. Verwenden Sie diesen Befehl, um die IPsec-Verbindung zu beenden:
   ```
   HQ-Router#clear crypto sa
   ```

2. Verwenden Sie diesen Befehl, um die ISAKMPSecurity Associations (SAs) zu löschen:
   ```
   HQ-Router#clear crypto isakmp
   ```

3. Verwenden Sie diesen Befehl, um die ACL für den interessanten Datenverkehr für den IPsec-Tunnel zu entfernen:
   ```
   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. Verwenden Sie diesen Befehl, um die nicht-exklusive ACL-Anweisung für das Netzwerk 192.168.10.0 zu entfernen:
   ```
   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. Verwenden Sie diesen Befehl, um die NAT-Übersetzung zu löschen:
   ```
   HQ-Router#clear ip nat translation *
   ```

6. Verwenden Sie diese Befehle, um die Crypto Map auf der Schnittstelle zu entfernen und

erneut anzuwenden, um sicherzustellen, dass die aktuelle Crypto-Konfiguration wirksam wird:

```
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
```

Hinweis: Wenn Sie die Crypto Map von der Schnittstelle entfernen, werden alle vorhandenen VPN-Verbindungen für diese Crypto Map gelöscht. Bevor Sie dies tun, vergewissern Sie sich, dass Sie die erforderliche Ausfallzeit genommen haben und die Änderungskontrollrichtlinie Ihres Unternehmens entsprechend befolgt haben.

7. Verwenden Sie den Befehl **write memory**, um die aktive Konfiguration im Flash zu speichern.
8. Führen Sie diese Schritte am anderen Ende des VPN-Tunnels (BO-Router) aus, um die Konfigurationen zu entfernen.
9. Initiieren Sie den IPsec-Tunnel, und überprüfen Sie die Verbindung.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Verwenden Sie diese Ping-Sequenz, um sicherzustellen, dass das neue Netzwerk Daten durch den VPN-Tunnel übertragen kann:

```
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:
```

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Fehlerbehebung

In diesem Abschnitt finden Sie Fehlerbehebungen für Ihre Konfiguration.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug crypto ipsec**: Zeigt die IPsec-Aushandlungen für Phase 2 an.
- **debug crypto isakmp**: Zeigt die ISAKMP-Verhandlungen für Phase 1 an.
- **debug crypto engine**: Zeigt die verschlüsselten Sitzungen an.

Zugehörige Informationen

- Eine Einführung in die IP Security (IPSec)-Verschlüsselung
- Support-Seite für IPSec-Aushandlung/IKE-Protokolle
- Konfigurieren eines IPsec-Routers Dynamische LAN-to-LAN-Peer- und VPN-Clients

- Technischer Support und Dokumentation - Cisco Systems