IOS VPN Router: Esempio di configurazione di aggiunta o rimozione di una rete in un tunnel VPN L2L

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per aggiungere o rimuovere una rete in un tunnel VPN da LAN a LAN (L2L) esistente.

Prerequisiti

Requisiti

Prima di provare a configurare questa configurazione, verificare di aver configurato correttamente il tunnel VPN IPsec L2L corrente.

Componenti usati

Per questo documento, sono stati usati due router Cisco IOS® con software versione 12.4(15)T1.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

Attualmente è disponibile un tunnel VPN L2L tra la sede centrale (HQ) e la succursale (BO). L'ufficio centrale ha appena aggiunto una nuova rete che sarà utilizzata dal sales team. Questo team richiede l'accesso alle risorse che risiedono nell'ufficio del responsabile del servizio directory. L'attività consiste nell'aggiungere una nuova rete al tunnel VPN L2L esistente.

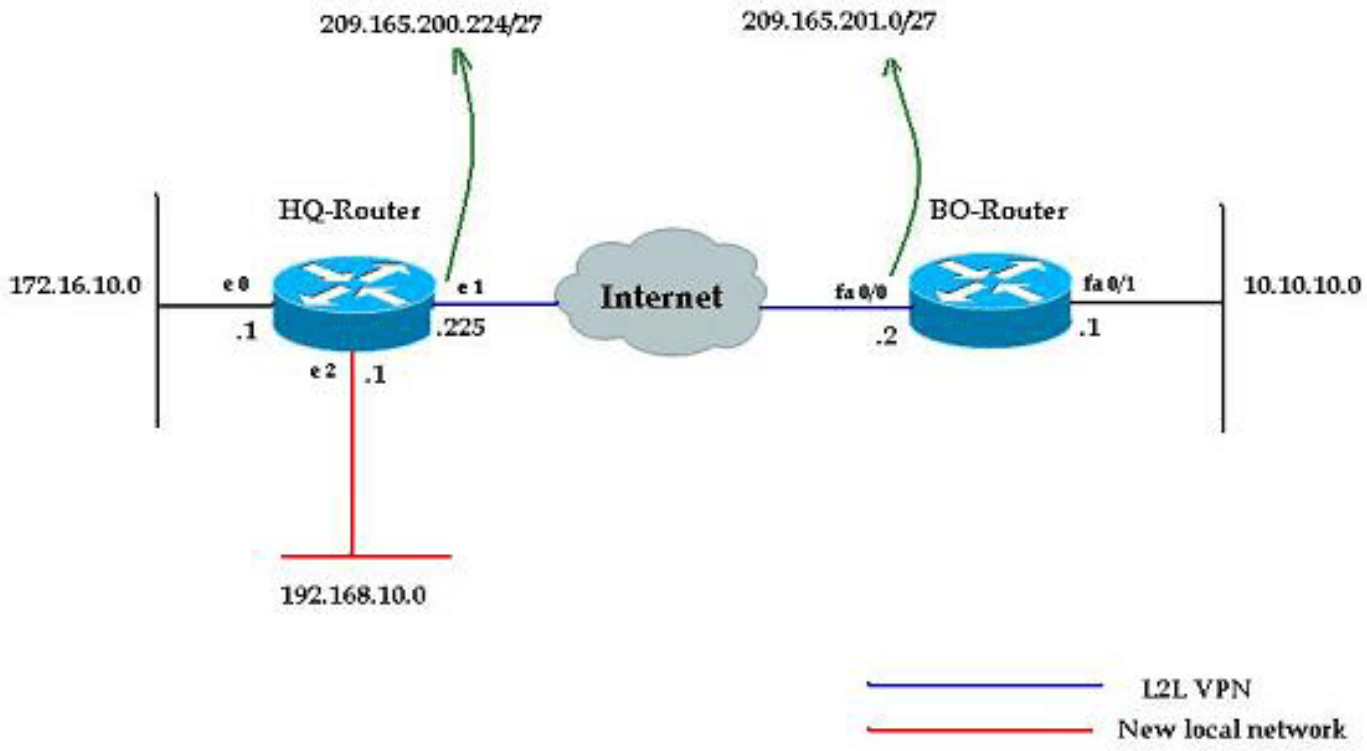
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate le configurazioni descritte in questa sezione. Queste configurazioni includono una VPN L2L eseguibile tra la rete 172.16.10.0 dell'ufficio principale e la rete 10.10.10.0 dell'ufficio principale. L'output mostrato in grassetto mostra la configurazione richiesta per

integrare la nuova rete 192.168.10.0 dell'ufficio centrale nella stessa rete VPN con 10.10.10.0 come rete di destinazione.

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
```

Rimuovere una rete da un tunnel IPsec

Per rimuovere la rete dalla configurazione del tunnel IPsec, completare la procedura descritta in questa sezione. Notare che la rete 192.168.10.0/24 è stata rimossa dalla configurazione del router HQ.

1. Utilizzare questo comando per interrompere la connessione IPSec:
   ```
   HQ-Router#clear crypto sa
   ```

2. Utilizzare questo comando per cancellare le associazioni di sicurezza ISAKMPS:
   ```
   HQ-Router#clear crypto isakmp
   ```

3. Utilizzare questo comando per rimuovere l'ACL del traffico interessante per il tunnel 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. Utilizzare questo comando per rimuovere l'istruzione ACL con esenzione nat per la rete 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. Utilizzare questo comando per cancellare la traduzione NAT:
   ```
   HQ-Router#clear ip nat translation *
   ```

6. Utilizzare questi comandi per rimuovere e applicare nuovamente la mappa crittografica sull'interfaccia in modo da assicurare che la configurazione crittografica corrente abbia

effetto:

```
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 rimozione della mappa crittografica dall'interfaccia comporta il danneggiamento di tutte le connessioni VPN esistenti associate a tale mappa crittografica. Prima di procedere, verificare di aver rispettato i tempi di inattività richiesti e di aver rispettato i criteri di controllo delle modifiche dell'organizzazione.

7. Per salvare la configurazione attiva sulla memoria flash, usare il comando **write memory**.
8. Completare questa procedura sull'altra estremità del tunnel VPN (BO-Router) per rimuovere le configurazioni.
9. Avviare il tunnel IPsec e verificare la connessione.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Utilizzare questa sequenza di ping per verificare che la nuova rete possa passare i dati attraverso il tunnel 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:
```

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Risoluzione dei problemi

Consultare questa sezione per risolvere i problemi di configurazione.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug crypto ipsec**: visualizza le negoziazioni IPsec della fase 2.
- **debug crypto isakmp**: visualizza le negoziazioni ISAKMP della fase 1.
- **debug crypto engine**: visualizza le sessioni crittografate.

Informazioni correlate

- Introduzione alla crittografia IP Security (IPSec)
- Pagina di supporto per la negoziazione IPSec/i protocolli IKE
- Configurazione di un router IPsec come peer LAN-to-LAN dinamico e client VPN
- Documentazione e supporto tecnico – Cisco Systems