IOS VPN ルータ： L2L VPN トンネルのネットワークの追加または削除の設定例

目次

概要

このドキュメントでは、既存の LAN-to-LAN (L2L) VPN トンネル上でネットワークを追加または削除する方法の設定例を説明します。

前提条件

要件

この設定を試みる前に、現在の L2L IPSec VPN トンネルを正しく設定していることを確認してください。

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 12.4(15)T1 が稼働している 2 台の Cisco IOS® ルータに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

現在、本社（HQ）オフィスとブランチ オフィス（BO）の間に、L2L VPN トンネルが存在しています。 HQ オフィスは、営業チームが使用する新しいネットワークを増設したばかりです。 このチームは BO オフィスにあるリソースにアクセスする必要があります。 次に取り組む作業は、既存の L2L VPN トンネルに新しいネットワークを追加することです。

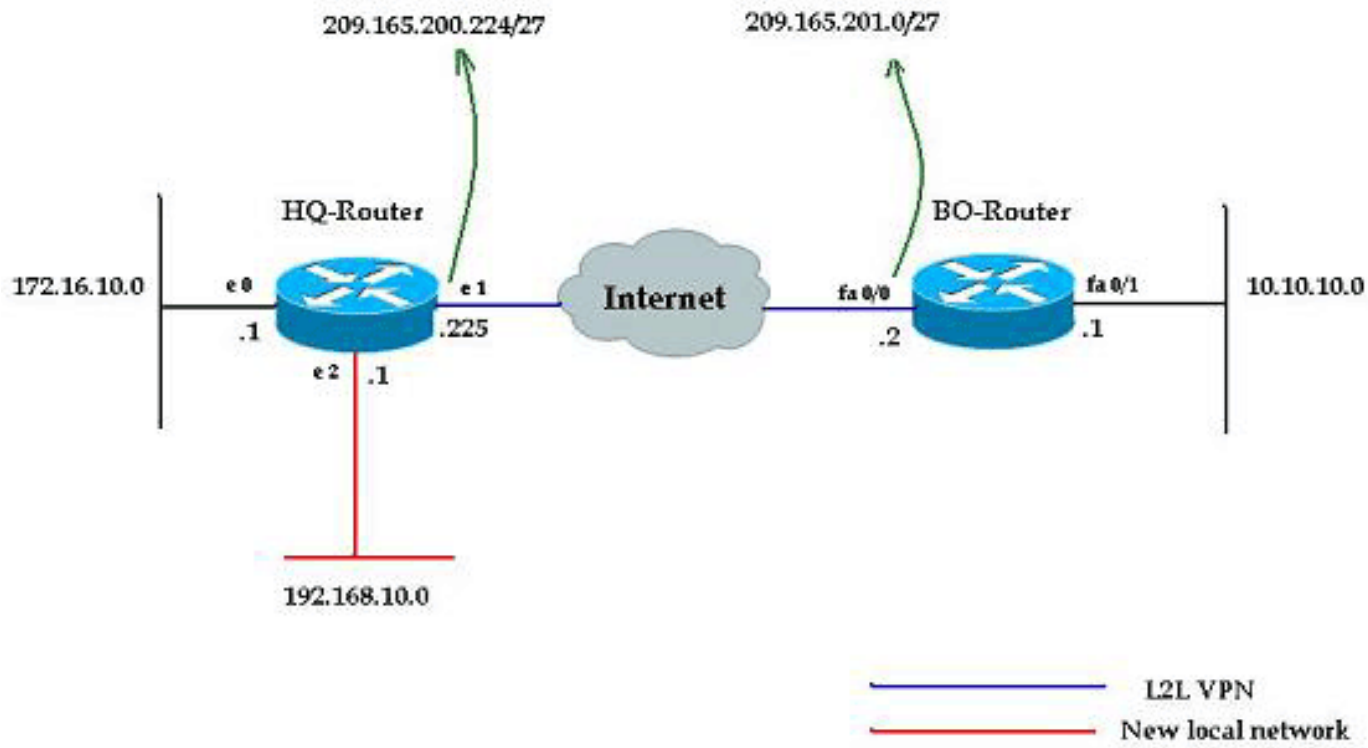
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



設定

このドキュメントでは、このセクションで示す設定を使用しています。 これらの設定には、HQ オフィスの 172.16.10.0 ネットワークと、BO オフィスの 10.10.10.0 ネットワーク間で動作している L2L VPN が含まれます。 太字のテキストで示された出力は、HQ オフィスの新しいネットワーク 192.168.10.0 を、10.10.10.0 を宛先ネットワークとする同じ VPN トンネルに統合するために必要な設定を示しています。

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
```

IPSec トンネルからのネットワークの削除

このセクションで説明する手順を実行して、IPSec トンネル設定からネットワークを削除します。 ネットワーク 192.168.10.0/24 が、HQ ルータ設定から削除されていることに注意してください。

1. 次のコマンドを使用して、IPSec 接続を切断します。HQ-Router#**clear crypto sa**
2. 次のコマンドを使用して、ISAKMP セキュリティ アソシエーション（SA）をクリアします。HQ-Router#**clear crypto isakmp**
3. 次のコマンドを使用して、IPSec トンネルの対象トラフィックの ACL を削除します。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. 次のコマンドを使用して、192.168.10.0 ネットワークに対する NAT 免除の ACL ステートメントを削除します。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. 次のコマンドを使用して、NAT トランスレーションをクリアします。HQ-Router#**clear ip nat translation ***
6. 次のコマンドを使用して、インターフェイスのcrypto マップを削除して再度適用し、現在のクリプト設定が確実に反映されるようにします。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 **注:** インターフェイスからcrypto マップを削除すると、そのcrypto マップに関連付けられている既存のすべての VPN 接続が切断されます。 この作業を行う前に、必要なダウンタイムを確保し、組織の変更管理ポリシーに従って適切に対処していることを確認してください。
7. **write memory** コマンドを使用して、アクティブな設定をフラッシュに保存します。
8. これらの手順を VPN トンネルの他端（BO-Router）で実行し、設定を削除します。
9. IPSec トンネルを起動して接続を確認します。

確認

このセクションでは、設定が正常に機能していることを確認します。

次の ping シーケンスを使用して、新しいネットワークが VPN トンネル経由でデータを渡せることを確認します。

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:
```

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

トラブルシューティング

このセクションでは、設定のトラブルシューティングについて説明します。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **debug crypto ipsec**：フェーズ 2 の IPSec ネゴシエーションを表示します。
- **debug crypto isakmp**：フェーズ 1 の ISAKMP ネゴシエーションを表示します。
- **debug crypto engine**：—暗号化されたセッションを表示します。

関連情報

- IP セキュリティ（IPSec）暗号化の概要

- IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ
- IPSec ルータでのダイナミック LAN-to-LAN ピアと VPN Client の設定
- テクニカルサポートとドキュメント - Cisco Systems