

IOS VPN Router: Add or Remove a Network on an L2L VPN Tunnel Configuration Example

Document ID: 112004

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Configure

- Network Diagram
- Configurations
- Remove a Network from an IPsec Tunnel

Verify

Troubleshoot

Related Information

Introduction

This document provides a sample configuration for how to add or remove a network on an existing LAN-to-LAN (L2L) VPN tunnel.

Prerequisites

Requirements

Ensure that you correctly configure your current L2L IPsec VPN tunnel before you attempt this configuration.

Components Used

The information in this document is based on two Cisco IOS[®] routers that run software version 12.4(15)T1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

There is currently an L2L VPN tunnel between the headquarters (HQ) office and branch office (BO). The HQ office just added a new network to be used by the sales team. This team requires access to resources that reside in the BO office. The task at hand is to add a new network to the already existing L2L VPN tunnel.

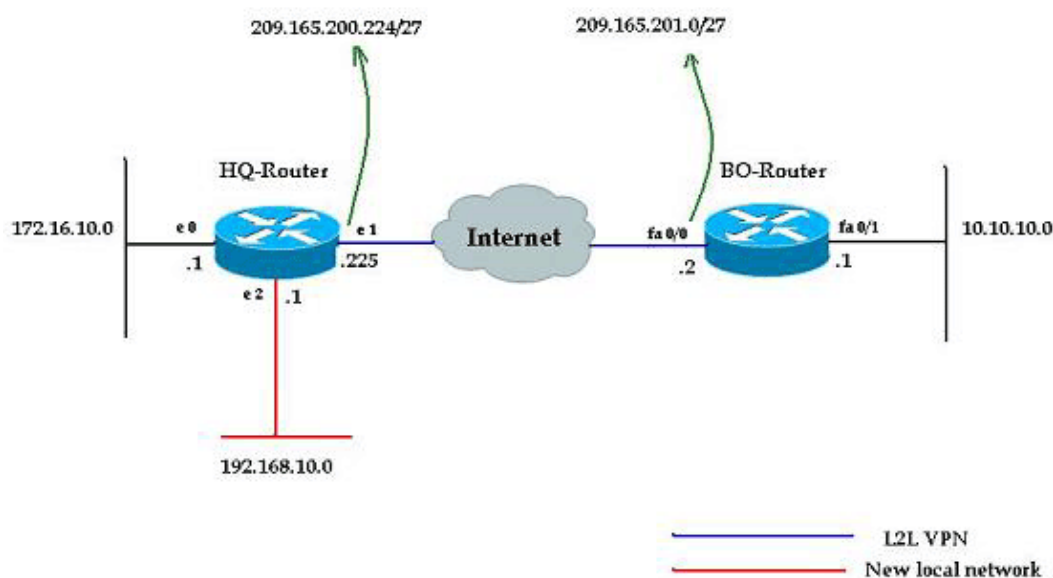
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Configurations

This document uses the configurations described in this section. These configurations include an L2L VPN that runs between the 172.16.10.0 network of the HQ office and the 10.10.10.0 network of the BO office. The output displayed in bold text shows the required configuration to integrate the new network 192.168.10.0 of the HQ office into the same VPN tunnel with 10.10.10.0 as the destination network.

HQ-Router
<pre>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</pre>

```

!
!
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

```

Remove a Network from an IPsec Tunnel

Complete the steps described in this section in order to remove the network from the IPsec tunnel configuration. Note that the network 192.168.10.0/24 has been removed from the HQ router configuration.

1. Use this command in order to tear down the IPsec connection:

```
HQ-Router#clear crypto sa
```

2. Use this command in order to clear the ISAKMP Security Associations (SAs):

```
HQ-Router#clear crypto isakmp
```

3. Use this command in order to remove the interesting traffic ACL for the IPsec tunnel:

```
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. Use this command in order to remove the nat-exempt ACL statement for the 192.168.10.0 network:

```
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. Use this command in order to clear the NAT translation:

```
HQ-Router#clear ip nat translation *
```

6. Use these commands in order to remove and re-apply the crypto map on the interface to ensure that the current crypto configuration takes effect:

```
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
```

Note: Removing the crypto map from the interface tears all the existing VPN connections associated with that crypto map. Before doing this, please make sure that you have taken the required down time and followed the change control policy of your organization accordingly.

7. Use the **write memory** command in order to save the active configuration to the flash .
8. Complete these steps on the other end of the VPN tunnel (BO-Router) in order to remove the configurations.
9. Initiate the IPsec tunnel and verify the connection.

Verify

Use this section in order to confirm that your configuration works properly.

Use this ping sequence in order to ensure that the new network can pass data through the VPN tunnel:

```
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:

```

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Troubleshoot

Use this section in order to troubleshoot your configuration.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug crypto ipsec** Displays the IPsec negotiations of phase 2.
- **debug crypto isakmp** Displays the ISAKMP negotiations of phase 1.
- **debug crypto engine** Displays the encrypted sessions.

Related Information

- **An Introduction to IP Security (IPSec) Encryption**
 - **IPSec Negotiation/IKE Protocols Support Page**
 - **Configuring an IPsec Router Dynamic LAN-to-LAN Peer and VPN Clients**
 - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 27, 2010

Document ID: 112004
