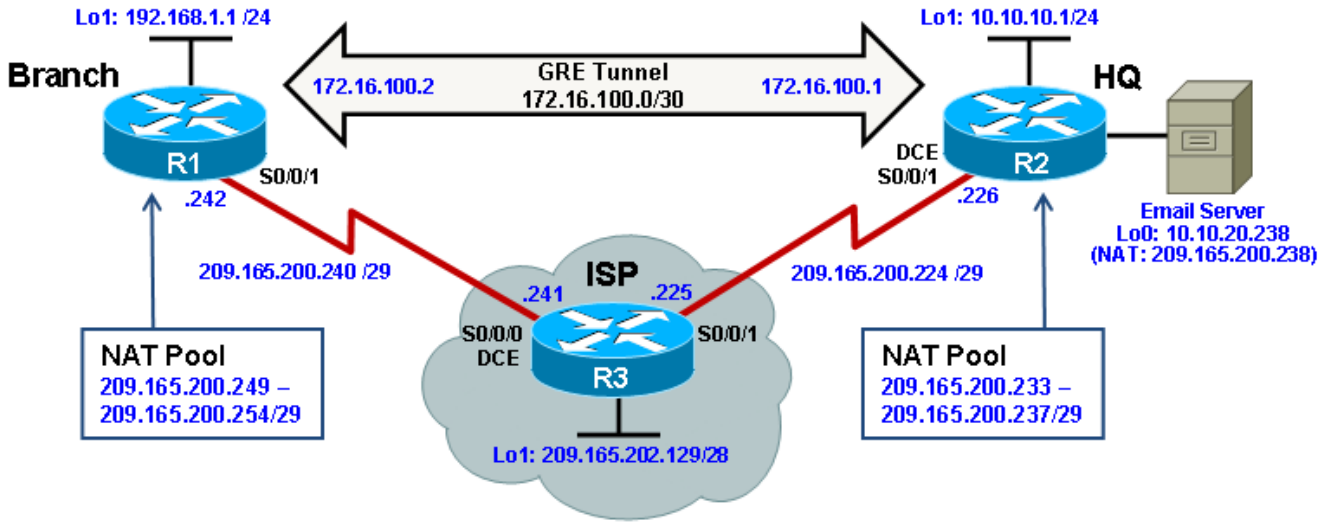
Chapter 7 Lab 7-1, Configure Routing Facilities to the Branch Office

Topology



Objectives

- Configure NAT.
- Configure an IPsec VPN.
- Configure a GRE tunnel over IPsec.
- Enable dynamic routing over a GRE tunnel.
- Verify the configuration and operation using **show** and **debug** commands.

Background

Your organization is expanding its operation and wants to connect a branch site. To avoid expensive WAN costs, the decision was made to use the Internet as the WAN link. You suggest using a test network to implement an IPsec VPN to support all traffic going between corporate sites. In addition, you want to configure dynamic routing between sites, by implementing Generic Routing Encapsulation (GRE).

Note: The intent of this lab is to illustrate the impact on routing services and addressing schemes when deploying IPsec VPNs at branch office routers. Although sample configurations are provided, detailed explanations of Network Address Translation (NAT), IPsec VPNs, and GRE are beyond the scope of this course. For more details on these technologies, see the Cisco Networking Academy CCNA Security course or www.cisco.com.

Note: This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T1 and the Advanced IP Services image c1841-advipservicesk9-mz.124-24.T1.bin. You can use other routers (such as a 2801 or 2811) and

Cisco IOS Software versions if they have comparable capabilities and features. Depending on the router and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Services or comparable)
- Serial and console cables

Step 1: Prepare the routers and configure the router hostname and interface addresses.

a. Cable the network as shown in the topology diagram. Erase the startup configuration and reload each router to clear previous configurations. Using the addressing scheme in the diagram, apply the IP addresses to the interfaces on Branch, HQ, and ISP.

You can copy and paste the following configurations into your routers to begin.

Note: Depending on the router model, interfaces might be numbered differently than those listed. You might need to alter the designations accordingly.

Branch (R1)

```
hostname Branch
!
interface Loopback1
 description Branch LAN
 ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0/1
 description Connection to ISP
 ip address 209.165.200.242 255.255.255.248
 bandwidth 64
 no shut
!
end
```

HQ (R2)

```
hostname HQ
!
interface Loopback1
 description Headquarters LAN
 ip address 10.10.10.1 255.255.255.0
!
interface Serial0/0/1
 description Connection to ISP
 ip address 209.165.200.226 255.255.255.248
 clock rate 64000
 bandwidth 64
 no shut
!
end
```

ISP (R3)

```
hostname ISP
!
interface Loopback1
 description Simulating the Internet
 ip address 209.165.202.129 255.255.255.240
```

```
!
interface Serial0/0/0
 description Connection to Branch
 ip address 209.165.200.241 255.255.255.248
 clock rate 64000
 bandwidth 64
 no shut
!
interface Serial0/0/1
 description Connection to HQ
 ip address 209.165.200.225 255.255.255.248
 bandwidth 64
 no shut

ip route 209.165.200.232 255.255.255.248 Serial0/0/1
ip route 209.165.200.248 255.255.255.248 Serial0/0/0
!
end
```

b. Verify your configuration by using the **show ip interface brief** command. The output from the Branch router is shown here as an example.

```
Branch# show ip interface brief
Interface          IP-Address      OK? Method Status                Protocol
FastEthernet0/0    unassigned      YES unset  administratively down  down
FastEthernet0/1    unassigned      YES unset  administratively down  down
Serial0/0/0        unassigned      YES unset  administratively down  down
Serial0/0/1        209.165.200.242 YES manual up                    up
Loopback1          192.168.1.1     YES manual up                    up
```

c. From the Branch LAN interface, use an extended ping to verify connectivity to the directly connected interface of the ISP, the ISPs loopback interface, and the HQ Internet interface. Run the following Tcl script on the Branch router to verify connectivity.

```
Branch# tclsh

foreach address {
209.165.200.241
209.165.202.129
209.165.200.226
} { ping $address}

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.241, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.202.129, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Branch(tcl)#
```

Why do the pings to the ISPs loopback and HQ router address fail?

El piing falló porque los routers Branch y HQ necesitan estar ruteados en el ISP

d. Configure a default static route to ISP on the Branch and HQ routers.

You can copy and paste the following configurations into your routers.

```
Branch(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.241

HQ(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

e. From the Branch router, run the following Tcl script on the Branch router to verify connectivity.

```
Branch# tclsh

foreach address {
209.165.200.241
209.165.202.129
209.165.200.226
+>} { ping $address}

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.241, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.202.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
Branch(tcl)#
```

Are the pings now successful?

Si, ahora todos los pings funcionaron porque ya se ruteó todo.

f. Connectivity from the Branch router to external addresses has been established. But could a Branch LAN user successfully reach those external addresses? To verify, initiate pings sourced from the Branch LAN interface to the ISP interface, the ISPs loopback interface, and the HQ Internet interface. Run the following Tcl script on the Branch router to verify connectivity.

```
Branch# tclsh

foreach address {
209.165.200.241
209.165.202.129
209.165.200.226
} { ping $address source 192.168.1.1}

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.241, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
.....
```

```
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.202.129, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
.....
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
.....
Success rate is 0 percent (0/5)
Branch(tcl)#
```

Note: You can also specify the router interface designator (for example, S0/0/0, Fa0/0, or Lo1) as the source for the extended ping, as follows:

```
Branch# ping 209.165.200.226 source Lo1
```

Why are the pings unsuccessful?

Los pings fallaron porque la dirección IP origen 192.168.1.1 es una dirección privada interna y el ISP n la conoce, por eso nunca llega el ping.

The ISP cannot route back to the internal private address of the Branch LAN.

Step 2: Configure NAT on the Branch and HQ routers.

The internal LAN private IP addresses will be translated to global public IP addresses using NAT. The ISP has provided the HQ and Branch sites with the following pools of public addresses:

- HQ: 209.165.200.233 – 209.165.200.238 (209.165.200.232/29)
- Branch: 209.165.200.249 – 209.165.200.254 (209.165.200.248/29)

The HQ site also has an email server that must be accessible to mobile users and Branch office users. Therefore, static NAT must also be configured to use a public address to reach the email server.

a. The NAT pool identifies public IP addresses, while the NAT ACL identifies which inside hosts can use these public IP addresses. For the Branch router, this means that the NAT ACL must identify the 192.168.1.0 LAN, and the NAT pool must identify addresses 209.165.200.248 /29. The LAN interface must be identified as an inside NAT interface, and the Internet interface must be identified as an outside NAT interface.

Note: The NAT ACL must not translate the Branch LAN addresses if they are destined to the corporate HQ LAN. Therefore, the NAT ACL denies the Branch LAN public addresses from being translated when attempting to connect to the HQ LANs. This will be required when the IPsec VPN is configured.

You can copy and paste the following configuration into the Branch router.

Branch Router

```
ip access-list extended BRANCH-NAT-ACL
 remark Do not translate Local LAN to HQ LAN addresses
 deny ip 192.168.1.0 0.0.0.255 10.10.0.0 0.0.255.255
 remark Translate Local LAN to all other Internet destinations
 permit ip 192.168.1.0 0.0.0.255 any
 exit
!
ip nat pool BRANCH-NAT-POOL 209.165.200.249 209.165.200.254 prefix-length 29
!
```

```
ip nat inside source list BRANCH-NAT-ACL pool BRANCH-NAT-POOL
!
interface Loopback 1
 ip nat inside
exit
!
interface Serial0/0/1
 ip nat outside
end
```

b. On the HQ router, the NAT ACL must identify the 10.10.10.0 and the 10.10.20.0 LANs. The NAT pool must identify addresses 209.165.200.232 /29. The LAN interface must be identified as an inside NAT interface, and the Internet interface must be identified as an outside NAT interface.

The email server with private IP address 10.10.20.238 will be statically assigned the last public IP address from the NAT pool, 209.165.200.238. Interface loopback 0 on HQ simulates this server.

Note: Again the NAT ACL denies the HQ LAN public addresses from being translated when attempting to connect to the Branch LAN which will be required when the IPsec VPN is configured.

You can copy and paste the following configuration into the HQ router.

HQ Router

```
interface Loopback 0
 description HQ email server address
 ip add 10.10.20.238 255.255.255.0
!
ip nat pool HQ-NAT-POOL 209.165.200.233 209.165.200.237 prefix-length 29
ip nat inside source list HQ-NAT-ACL pool HQ-NAT-POOL
ip nat inside source static 10.10.20.238 209.165.200.238
!
ip access-list extended HQ-NAT-ACL
 remark Do not translate HQ LAN to Branch LAN addresses
 deny ip 10.10.0.0 0.0.255.255 192.168.1.0 0.0.0.255
 remark Translate Local LAN to all other Internet destinations
 permit ip 10.10.0.0 0.0.255.255 any
 exit
!
interface Loopback 0
 ip nat inside
!
interface Loopback 1
 ip nat inside
!
interface Serial0/0/1
 ip nat outside
end
```

c. Verify the NAT configuration by using the **show ip nat statistics** and **show ip nat translations** commands.

```
Branch# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 0, occurred 00:018:28 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Loopback1
Hits: 0  Misses: 0
```

```
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list BRANCH-NAT-ACL pool BRANCH-NAT-POOL refcount 0
 pool BRANCH-NAT-POOL: netmask 255.255.255.248
        start 209.165.200.249 end 209.165.200.254
        type generic, total addresses 6, allocated 0 (0%), misses 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

As shown above, the pool has been configured and the interfaces assigned. The output of the **show ip nat translations** command confirms that there are currently no active NAT translations:

```
Branch# show ip nat translations

Branch#
```

d. Initiate NAT traffic by pinging from the Branch LAN to the ISP interface, ISP's loopback, the HQ Internet interface, and this time also include the HQ public email server address. Run the following Tcl script on the Branch router to verify connectivity.

```
Branch# tclsh

foreach address {
209.165.200.241
209.165.202.129
209.165.200.226
209.165.200.238
} { ping $address source 192.168.1.1}

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.241, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.202.129, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.238, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms
Branch(tcl)#
```

All pings should be successful.

e. Verify that NAT is occurring by using the **show ip nat statistics** and **show ip nat translations** commands.

```
Branch# show ip nat statistics
Total active translations: 5 (0 static, 5 dynamic; 4 extended)
Peak translations: 5, occurred 00:00:12 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Loopback1
Hits: 40  Misses: 0
CEF Translated packets: 20, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list BRANCH-NAT-ACL pool BRANCH-NAT-POOL refcount 5
 pool BRANCH-NAT-POOL: netmask 255.255.255.248
        start 209.165.200.249 end 209.165.200.254
        type generic, total addresses 6, allocated 1 (16%), misses 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
Branch#
Branch# show ip nat translations
Pro Inside global      Inside local     Outside local      Outside global
icmp 209.165.200.249:9 192.168.1.1:9    209.165.200.241:9  209.165.200.241:9
icmp 209.165.200.249:10 192.168.1.1:10  209.165.202.129:10 209.165.202.129:10
icmp 209.165.200.249:11 192.168.1.1:11  209.165.200.226:11 209.165.200.226:11
icmp 209.165.200.249:12 192.168.1.1:12  209.165.200.238:12 209.165.200.238:12
--- 209.165.200.249    192.168.1.1      ---                ---
Branch#
```

Notice that translations are occurring. The output lists the details of the NAT translations sourced by the 192.168.1.1 Branch LAN IP address, which was translated to public IP address 209.165.200.249.

f. Now clear the NAT translations, verify connectivity from the Branch LAN to the HQ LAN interface and then display the NAT translations.

```
Branch# clear ip nat translation *
Branch#
Branch# ping 10.10.10.1 source 192.168.1.1

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 192.168.1.1
.....
Success rate is 0 percent (0/5)
Branch#
Branch# show ip nat translations

Branch#
```

As expected, Branch LAN traffic going to the HQ LAN is not translated by NAT. The ISP cannot route the pings to the private address on HQ and, therefore, the pings fail.

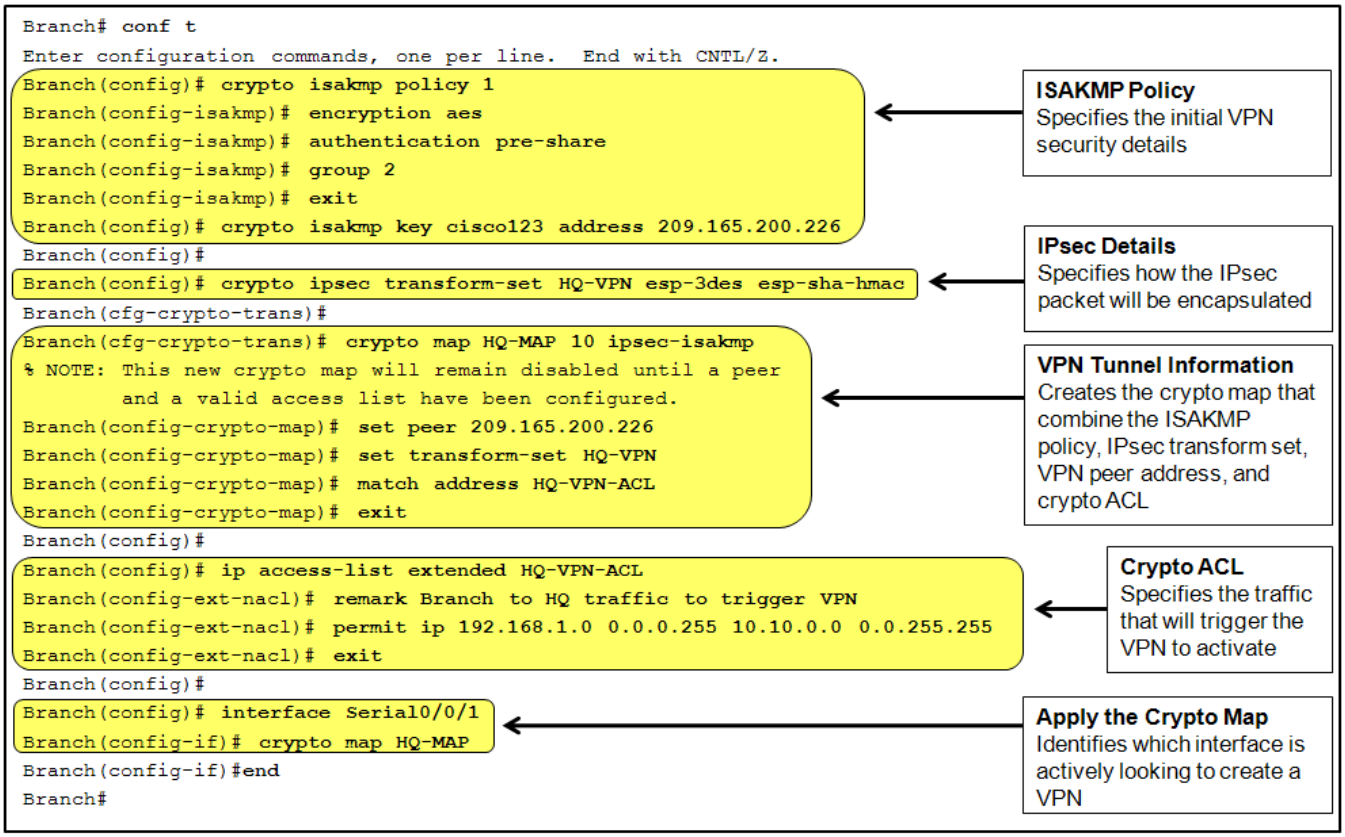
NAT works as expected. Traffic source from the Branch LAN going to Internet destinations is translated while traffic sourced from the Branch LAN to the HQ LAN is not translated. However, this traffic should be protected when traversing the public Internet. To solve this problem, an IPsec VPN will be configured next.

Step 3: Implement an IPsec VPN between the Branch and HQ sites.

An IPsec VPN can secure and protect all unicast IP traffic within it. IPsec cannot forward multicast or broadcast traffic, which means it cannot support interior gateway protocols such as EIGRP and OSPF.

For this lab, assume that the network security team has provided a basic IPsec VPN configuration with which to test your network design. As shown in the following figure, it consists of several configuration components:

- The ISAKMP policy identifies the specifics for the initial key and secure parameters exchange.
- The IPsec details define how the IP packet is encapsulated.
- The VPN tunnel information is identified in a named crypto map which combines the ISAKMP policies, IPsec packet detail, the peer address, and the crypto ACL.
- The crypto ACL identifies traffic that will trigger the tunnel to activate. This component must sometimes be tuned when implemented along with other services such as NAT and GRE.
- The crypto map is then applied to the tunnel interface.



Note: How to configure an IPsec VPN is beyond the scope of this lab. For more information on cryptography, IPsec VPNs, and GRE, see the Cisco Networking Academy CCNA Security courses or www.cisco.com.

a. Copy and paste the following configurations on the routers.

Branch Router

```
crypto isakmp policy 1
 encryption aes
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 209.165.200.226
!
crypto ipsec transform-set HQ-VPN esp-3des esp-sha-hmac
```

```
!
crypto map HQ-MAP 10 ipsec-isakmp
 set peer 209.165.200.226
 set transform-set HQ-VPN
 match address HQ-VPN-ACL
!
ip access-list extended HQ-VPN-ACL
 remark Branch to HQ traffic to trigger VPN
 permit ip 192.168.1.0 0.0.0.255 10.10.0.0 0.0.255.255
!
interface Serial0/0/1
 crypto map HQ-MAP
end
```

HQ Router

```
crypto isakmp policy 1
 encryption aes
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 209.165.200.242
!
crypto ipsec transform-set Branch-VPN esp-3des esp-sha-hmac
!
crypto map Branch-MAP 10 ipsec-isakmp
 set peer 209.165.200.242
 set transform-set Branch-VPN
 match address Branch-VPN-ACL
!
ip access-list extended Branch-VPN-ACL
 remark HQ to Branch traffic to trigger VPN
 permit ip 10.10.0.0 0.0.255.255 192.168.1.0 0.0.0.255
!
interface Serial0/0/1
 crypto map Branch-MAP
 end
```

Notice that the crypto ACLs are referring to the public IP addresses and not the private IP addresses. This is because the crypto map applies to the traffic after the NAT has already taken place. Another alternative approach would be to exempt site-to-site traffic from the NAT translation pool and have the crypto ACLs trigger based on private addresses instead of the public address pool.

b. Use the **show crypto session detail** command on the Branch router to verify the overall configuration of the IPsec VPN.

```
Branch# show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Serial0/0/1
Session status: DOWN
Peer: 209.165.200.226 port 500 fvrf: (none) ivrf: (none)
      Desc: (none)
```

```
      Phase1_id: (none)
  IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 10.10.0.0/255.255.0.0
        Active SAs: 0, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0

Branch#
```

The VPN tunnel is currently down because the traffic identified in the IPSEC FLOW has not yet been processed.

c. To test the VPN link, use an extended ping from the Branch LAN interface to the HQ LAN interface.

```
Branch# ping 10.10.10.1 source 192.168.1.1

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 192.168.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 84/86/88 ms
Branch#
```

This time 80% of the pings were successful. This is typical because the VPN tunnel requires a few seconds to negotiate the security parameters specified in the crypto map.

d. Now display the VPN tunnel details again.

```
Branch# show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Serial0/0/1
Uptime: 00:00:10
Session status: UP-ACTIVE
Peer: 209.165.200.226 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 209.165.200.226
      Desc: (none)
  IKE SA: local 209.165.200.242/500 remote 209.165.200.226/500 Active
          Capabilities:(none) connid:1001 lifetime:23:59:49
  IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 10.10.0.0/255.255.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4430126/3589
        Outbound: #pkts enc'ed 4 drop 1 life (KB/Sec) 4430126/3589

Branch#
```

The VPN tunnel did become active as indicated by the UP-ACTIVE session status. Also notice that it was the **permit** statement is referring to the private addresses defined in the crypto ACL and that it encrypted and decrypted four packets, with only one packet dropped due to the IPsec negotiation.

e. Before proceeding, manually disable the IPsec VPN tunnel using the **clear crypto isakmp** and **clear crypto sa** commands on the Branch router.

```
Branch# clear crypto isakmp
Branch# clear crypto sa
Branch#
```

You now have encrypted connectivity from the Branch LAN to HQ LAN. the problem with an IPsec VPN is that it does not allow dynamic routing protocols to operate over it. However, GRE can help solve this problem.

Step 4: Implement GRE over IPsec.

A GRE tunnel over IPsec can be implemented between the Branch and HQ sites. The tunnel will protect all corporate LAN traffic. As a bonus, GRE can forward multicast and broadcast traffic, so dynamic routing can also be enabled.

a. Configure the tunnel interfaces on the Branch router and HQ routers with GRE encapsulation. Copy and paste the following configurations on the routers.

Branch Router

```
interface Tunnel0
 ip address 172.16.100.2 255.255.255.252
 tunnel source 209.165.200.242
 tunnel destination 209.165.200.226
```

HQ Router

```
interface Tunnel0
 ip address 172.16.100.1 255.255.255.252
 tunnel source 209.165.200.226
 tunnel destination 209.165.200.242
```

You should notice the state of the tunnel interfaces to change to up on both routers.

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
```

b. Verify that the tunnel interface is up and running using the **show interface tunnel 0** command.

```
Branch# show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.100.2/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.200.242, destination 209.165.200.226
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
```

```
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
Branch#
```

The tunnel interface is up. Also notice that the encapsulation and tunnel transport protocol is GRE/IP.

c. Verify connectivity across the tunnel by pinging the tunnel destination on the HQ router. The pings should be successful.

```
Branch# ping 172.16.100.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/70/72 ms
```

d. The pings successfully reach the other side of the tunnel. But is the traffic being encrypted? Display the IPsec VPN specifics.

```
Branch# show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Serial0/0/1
Session status: DOWN-NEGOTIATING
Peer: 209.165.200.226 port 500 fvrf: (none) ivrf: (none)
      Desc: (none)
      Phase1_id: (none)
  IKE SA: local 209.165.200.242/500 remote 209.165.200.226/500 Inactive
          Capabilities:(none) connid:1001 lifetime:0
  IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 10.10.0.0/255.255.0.0
        Active SAs: 0, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0

Branch#
```

The IPsec VPN is down because the tunnel traffic has not been identified in the crypto ACL.

e. To solve this problem, replace the crypto ACL to make GRE traffic interesting on the Branch and HQ routers. Copy and paste the following configurations on the routers.

Branch Router

```
no ip access-list extended HQ-VPN-ACL
ip access-list extended HQ-VPN-ACL
 remark HQ to Branch GRE traffic to trigger VPN
 permit gre host 209.165.200.242 host 209.165.200.226
```

HQ Router

```
no ip access-list extended Branch-VPN-ACL
ip access-list extended Branch-VPN-ACL
 remark Branch to HQ GRE traffic to trigger VPN
 permit gre host 209.165.200.226 host 209.165.200.242
```

f. Test the link again. Notice the pings are 80% successful again.

```
Branch# ping 172.16.100.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.100.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 96/98/100 ms
```

g. Display the IPsec session details.

```
Branch# show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Serial0/0/1
Uptime: 00:00:05
Session status: UP-ACTIVE
Peer: 209.165.200.226 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 209.165.200.226
      Desc: (none)
  IKE SA: local 209.165.200.242/500 remote 209.165.200.226/500 Active
          Capabilities:(none) connid:1003 lifetime:23:59:54
  IPSEC FLOW: permit 47 host 209.165.200.242 host 209.165.200.226
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4422647/3594
        Outbound: #pkts enc'ed 4 drop 1 life (KB/Sec) 4422647/3594
```

The IPsec tunnel is now up and active. The “permit 47” identifies GRE traffic as interesting. The value 47 refers to the GRE protocol number.

h. Ping from LAN to LAN.

```
Branch# ping 10.10.10.1 source 192.168.1.1

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 192.168.1.1
.....
Success rate is 0 percent (0/5)
Branch#
```

The pings are unsuccessful. Does the Branch router have an entry to the 10.10.10.0 network?

i. Verify the routing table.

```
Branch# show ip route

<output omitted>
```

```
Gateway of last resort is 209.165.200.241 to network 0.0.0.0

     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.100.0 is directly connected, Tunnel0
     209.165.200.0/29 is subnetted, 1 subnets
C       209.165.200.240 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Loopback1
S*   0.0.0.0/0 [1/0] via 209.165.200.241
Branch#
```

The pings are unsuccessful because there is no specific route to the other LAN. The traffic is finally routed using the default route, which bypasses the GRE tunnel. The Branch router and the HQ router must be configured to share each other's LAN information.

This could be accomplished using static routes pointing to the GRE tunnel destination IP address. Although this is valid option, GRE tunnels also support multicast and broadcast traffic. Therefore, a dynamic routing protocol should be configured.

j. Configure EIGRP, and advertise the LANs and the tunnel segment on the Branch and HQ routers. Copy and paste the following configurations on the routers.

Branch Router

```
router eigrp 1
network 192.168.1.0 0.0.0.255
network 172.16.100.0 0.0.0.3
```

HQ Router

```
router eigrp 1
network 10.10.0.0 0.0.255.255
network 172.16.100.0 0.0.0.3
```

An EIGRP neighbor adjacency message should appear almost immediately.

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 172.16.100.2 (Tunnel0) is up: new
adjacency
```

k. Verify the routing table.

```
Branch# show ip route

<output omitted>

Gateway of last resort is 209.165.200.241 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:00:22, Null0
C       172.16.100.0/30 is directly connected, Tunnel0
     209.165.200.0/29 is subnetted, 1 subnets
C       209.165.200.240 is directly connected, Serial0/0/1
D    10.0.0.0/8 [90/27008000] via 172.16.100.1, 00:00:10, Tunnel0
C    192.168.1.0/24 is directly connected, Loopback1
S*   0.0.0.0/0 [1/0] via 209.165.200.241
Branch#
```

l. Display the IPsec session detail.

```
Branch# show crypto session detail
Crypto session current status
```

```
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Serial0/0/1
Uptime: 00:02:36
Session status: UP-ACTIVE
Peer: 209.165.200.226 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 209.165.200.226
      Desc: (none)
  IKE SA: local 209.165.200.242/500 remote 209.165.200.226/500 Active
          Capabilities:(none) connid:1002 lifetime:23:57:23
  IPSEC FLOW: permit 47 host 209.165.200.242 host 209.165.200.226
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 18 drop 0 life (KB/Sec) 4436519/3443
        Outbound: #pkts enc'ed 21 drop 1 life (KB/Sec) 4436519/3443

Branch#
```

m. Test the LAN-to-LAN connectivity, and display the IPsec session detail.

```
Branch# ping 10.10.10.1 source 192.168.1.1

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 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/100/100 ms

Branch# show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Serial0/0/1
Uptime: 00:03:15
Session status: UP-ACTIVE
Peer: 209.165.200.226 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 209.165.200.226
      Desc: (none)
  IKE SA: local 209.165.200.242/500 remote 209.165.200.226/500 Active
          Capabilities:(none) connid:1002 lifetime:23:56:44
  IPSEC FLOW: permit 47 host 209.165.200.242 host 209.165.200.226
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 31 drop 0 life (KB/Sec) 4436517/3404
        Outbound: #pkts enc'ed 34 drop 1 life (KB/Sec) 4436517/3404

Branch#
```

The pings are successful, but notice that the packet counters have increased by more than five ping packets. The reason is because EIGRP is also exchanging hello packets and therefore increasing the counters.

n. Trace the path that the packets take from the Branch LAN to the email server using the inside private address.

```
Branch# trace 10.10.20.238 source 192.168.1.1

Type escape sequence to abort.
Tracing the route to 10.10.20.238

  1 172.16.100.1 68 msec 68 msec *
```

Notice that the packet hops only to the end of the tunnel. It is completely unaware that it actually traversed the public Internet.

o. To prove that you still have Internet access without going through the GRE tunnel, trace the path from the Branch LAN to the email server using the outside static NAT address.

```
Branch# trace 209.165.200.238 source 192.168.1.1

Type escape sequence to abort.
Tracing the route to 209.165.200.238

  1 209.165.200.241 12 msec 12 msec 16 msec
  2 209.165.200.238 28 msec 28 msec *
```

The packet now hops across the ISP router and then to the HQ router. In essence, this proves that Internet-bound traffic will not be encrypted.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. Rather than list all combinations of configurations for each router class, this table includes identifiers for the possible combinations of Ethernet and serial interfaces in the device. The table does not include any other type of interface, even though a specific router might contain one. For example, for an ISDN BRI interface, the string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				