



## Lab 4.4.8a Configure a Cisco GRE over IPsec Tunnel using SDM

### Objective

In this lab, the students will complete the following tasks:

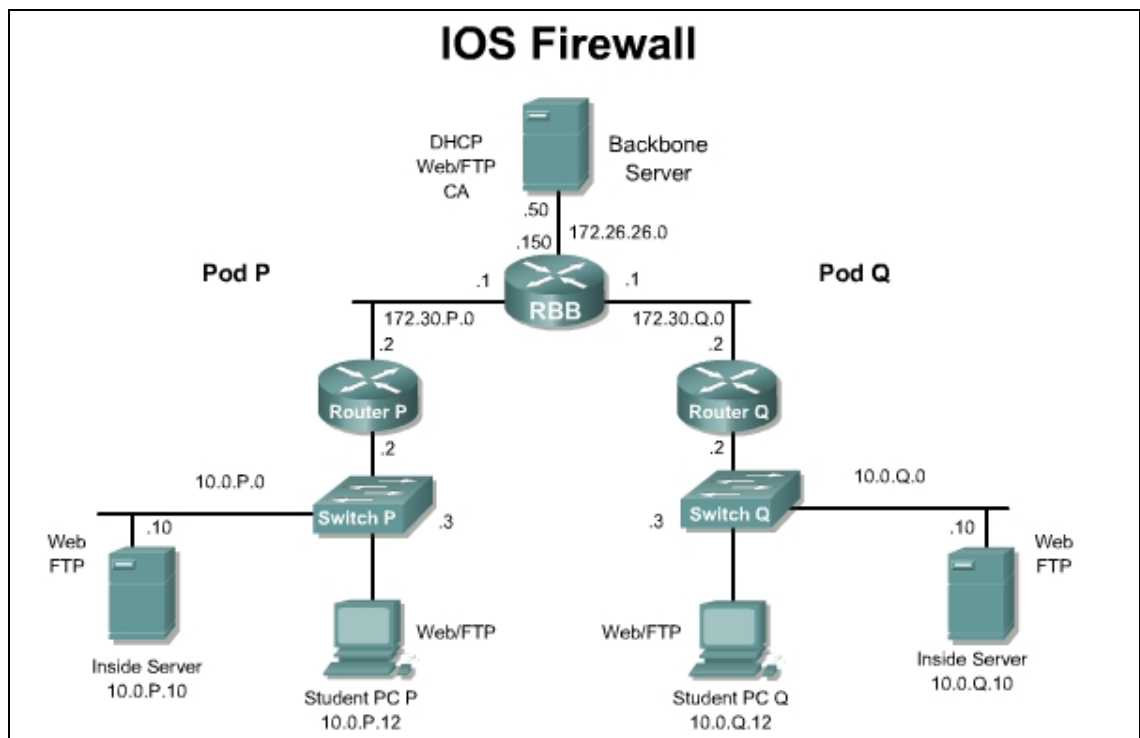
- Prepare to configure Virtual Private Network (VPN) Support
- Configure GRE over IPsec tunnel using SDM VPN Wizard
- Modify GRE over IPsec configuration
- Verify and test GRE over IPsec configuration

### Scenario

The XYZ Company has Cisco routers at two branch offices, with SDM installed, and wants to create a secure VPN over the Internet between the two sites. The company needs to support IP, IPX, and Appletalk traffic across the WAN. Therefore a GRE over IPsec tunnel must be configured.

### Topology

This figure illustrates the lab network environment.



## Preparation

Begin with the standard lab topology and verify the startup router configuration on the pod routers. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal emulator on the Windows 2000 server. If desired, save the router configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

## Tools and resources or equipment

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal

## Additional materials

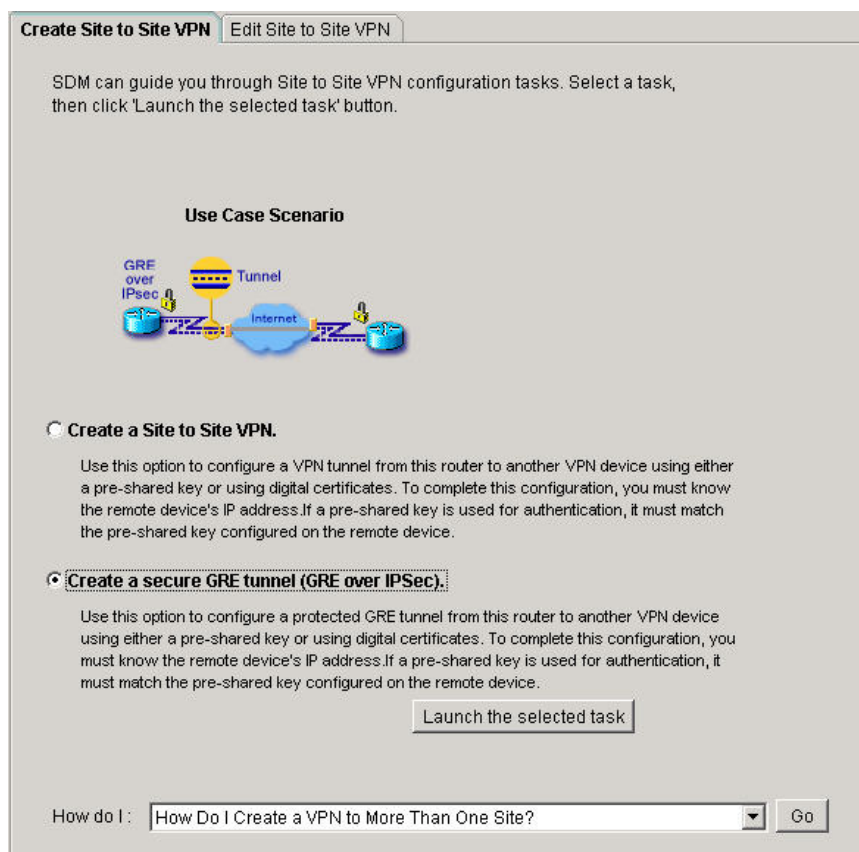
Further information about the objectives covered in this lab can be found at the following websites:

[http://www.cisco.com/en/US/products/sw/secursw/ps5318/products\\_user\\_guide\\_chapter09186a008040443e.html](http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_user_guide_chapter09186a008040443e.html)

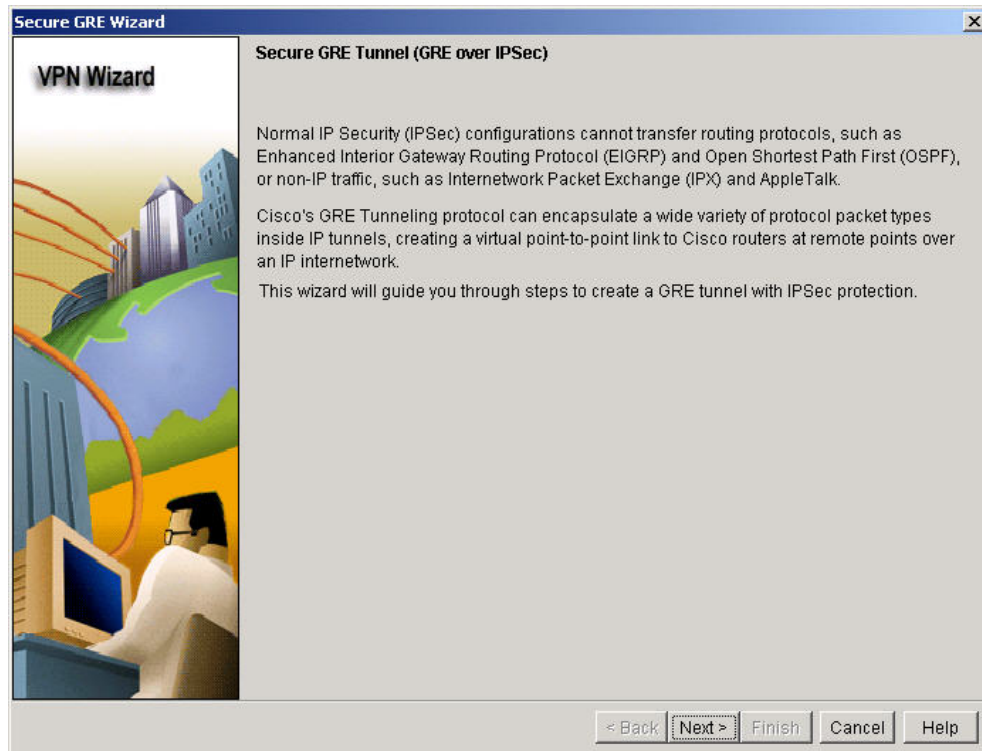
## Step 1 Configure GRE over IPSec VPN Parameters

Work with the members of the pod group to complete the VPN configuration.

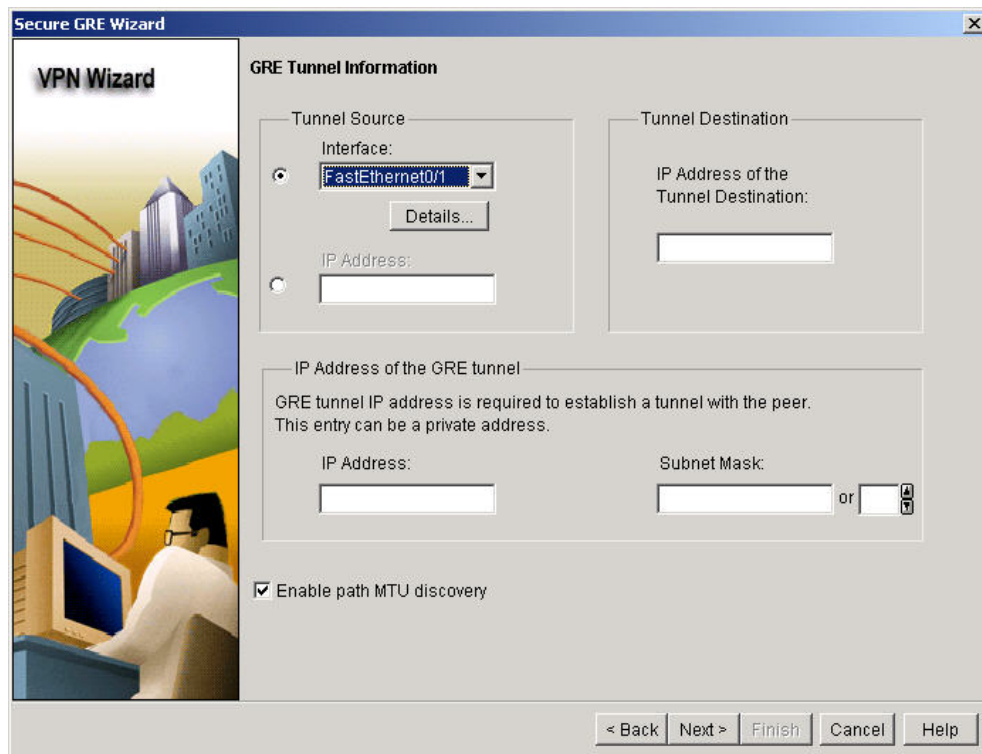
- Establish an SDM session with the pod router. When prompted for a username and password, use **sdm/sdm**.
- In SDM, select **VPN** from the Tasks panel of the **Configuration** page.
- Select the **Create a secure GRE tunnel (GRE over IPSec)**. Option from the **Site to Site VPN** tab.



- d. Click **Launch the selected task** button.



- e. Click the **Next** button.
- f. Select the outside interface (Fa0/1) for the Tunnel Source Interface.



- g. Click on the Details button to verify the proper external address.  
**172.30.P.2 / 255.255.255.0**

**Details of the Interface: FastEthernet0/1** [X]

| Item Name               | Item Value               |
|-------------------------|--------------------------|
| IP Address/Subnet Mask  | 172.30.1.2/255.255.255.0 |
| NAT                     | <None>                   |
| Access Rule - inbound   | <None>                   |
| Access Rule - outbound  | <None>                   |
| IPSec Policy            | <None>                   |
| Inspect Rule - inbound  | <None>                   |
| Inspect Rule - outbound | <None>                   |
| Easy VPN Remote         | <None>                   |
| QoS Policy - outbound   | <None>                   |

Close

- h. Set the Tunnel Destination as **172.30.Q.2** (where Q = peer pod number).
- i. Enter the IP address and subnet mask of the GRE Tunnel.  
**172.16.1.P**  
**255.255.255.0 or 24**
- j. Click the **Next** button.
- k. Skip the Backup GRE Tunnel Window and click the **Next** button. A backup will not be configured.
- l. In the VPN Authentication window, enter and re-enter to confirm a pre-shared key to be used for authentication. (make sure the CAPS lock is not on)

**cisco1234**

**VPN Authentication Information**

**Authentication**  
 Authentication ensures that each end of the VPN connection uses the same secret key.


☒ Pre-Shared Keys    Pre-Shared Key:     ☐ Digital Certificates  
                                  Re-enter Key:

- m. Click the **Next** button.
- n. In the **IKE Proposal** window, notice the default policy.

### IKE Proposals

The IKE proposals specifies the encryption algorithm, authentication algorithm, and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Click the Add... button to add more policies and the Edit... button to edit an existing policy.

|   | Priority | Encryption | Hash  | D-H Group | Authentication | Type        |
|---|----------|------------|-------|-----------|----------------|-------------|
|  | 1        | 3DES       | SHA_1 | group2    | PRE_SHARE      | SDM Default |

Add...

Edit...

- o. Click the **Next** button
- p. An information window will appear about IKE.
- q. The **Transform Set** window will appear.

### Transform Set


The Transform Set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel. Since the two devices must use the same algorithms to communicate, the remote device must be configured with the same transform set as the one selected below.

Click the Add... button to add a new Transform Set and the Edit... button to edit the selected Transform Set.

Select Transform Set:

SDM Default Transform Set ▼

Details of the selected transform set

|   | Name         | ESP Encryption | ESP Integrity | AH Integrity |
|---|--------------|----------------|---------------|--------------|
|  | ESP-3DES-SHA | ESP_3DES       | ESP_SHA_HMAC  |              |

Add...

Edit...

- r. Click the **Next** button
- s. The **Select Routing Protocol** window will appear.
- t. Select **EIGRP** and click the **Next** button

### Select Routing Protocol

You can use dynamic routing or static routing to specify the traffic that should pass through this GRE tunnel.

Select a dynamic routing protocol when the GRE over IPsec VPN includes a large number of private networks. The dynamic routing protocol will advertise these networks to other VPN routers. Select static routing when the GRE over IPsec VPN includes only a few private networks.

- ☒ EIGRP
- ☐ OSPF
- ☐ RIP
- ☐ Static Routing

- u. The **Routing Information** window will appear for EIGRP.

### Routing Information

- ☒ Select an existing EIGRP AS number:
- ☐ Create a new EIGRP AS number:

Add the private networks that you want to advertise to the other routers in this GRE over IPsec VPN. Other routers in this GRE over IPsec VPN must be in the same autonomous system.

Private networks advertised using EIGRP

| Network    | Wild card mask |
|------------|----------------|
| 10.0.0.0   |                |
| 172.30.0.0 |                |

Add...

Edit...

Delete

- v. Click the **Next** button.
- w. The **Configuration Summary** window will appear.

Summary of the configuration

Please click Finish to deliver to the router.

GRE Tunnel Information

Tunnel Source: FastEthernet0/1  
Tunnel Destination: 172.30.2.2  
TunnelIP Address:172.16.1.1/255.255.255.0  
Path MTU discovery is enabled

Authentication Type : Preshared Key  
Pre-Shared Key:\*\*\*\*\*

IKE policies:

| Hash  | DH Group | Authentication | Encryption |
|-------|----------|----------------|------------|
| SHA_1 | group2   | PRE_SHARE      | 3DES       |

Transform Set:

Name:ESP-3DES-SHA  
ESP Encryption:ESP\_3DES

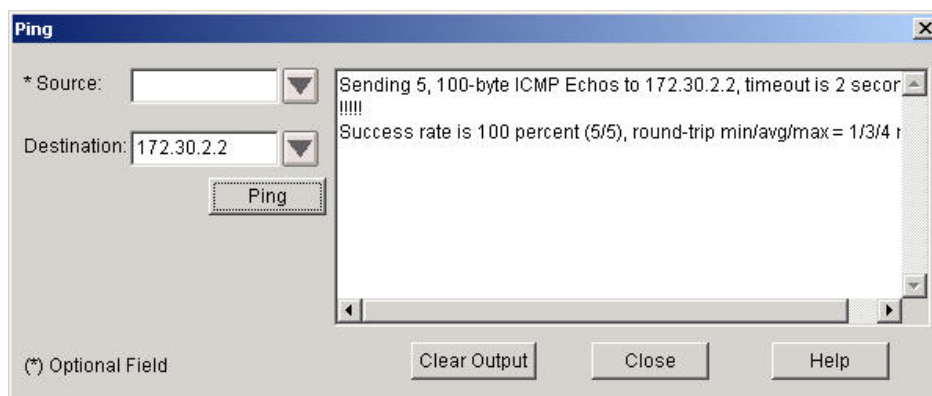
- x. Verify the configuration.
- y. Click the **Finish** button
- z. Click the **OK** button on the **Command Deliver Status** window to complete the configuration delivery.



## Step 2 Verify and Monitor the VPN Tunnel

Work with the members of the pod group to verify the VPN Tunnel.

- Navigate to the **Tools>Ping**.
- Ping the peer's router outside address at 172.30.Q.2.



- The ping should be successful. Most likely, the tunnel is already established due to the EIGRP routing update traffic.
- Click on the **Close** button.
- Now click on the **Monitor** button on the top navigation bar.

**Resource Status**

**CPU Usage:** 0%

**Memory Usage:** 13%  
Available: 74 MB

**Flash Usage:** Available/Total flash: (MB) 12/31

**Interface Status**

**Total Interface(s) Up:** 3      **Total Interface(s) Down:** 0

| Interface       | IP         | Status | Bandwidth Usage | Description |
|-----------------|------------|--------|-----------------|-------------|
| FastEthernet0/0 | 10.0.1.2   | Up     | 0%              | inside      |
| FastEthernet0/1 | 172.30.1.2 | Up     | 0%              | outside     |
| Tunnel0         | 172.16.1.1 | Up     | 0%              |             |

**Firewall Status**

**No. of Attempts Denied:** 0  
**Firewall Log:** Not Configured

**QoS**

**No. of QoS-enabled Interfaces:** 0

**VPN Status**

**No. of Open IPSec Tunnels:** 1      **No. of DMVPN Clients:** 0  
**No. of Open IKE SAs:** 1      **No. of Active VPN Clients:** 0

- Notice the VPN Status box where one open IKE SA and one open IPSec tunnel are now shown.
- Click on **VPN Status** in the **Tasks** panel to view detailed information about the established VPN tunnel. The VPN tunnel status should display as Up by the green icon.

**VPN Status**

**IPSec Tunnels**    DMVPN Tunnels    EasyVPN Server    IKE SAs

Each row represents one IPSec Tunnel      **Test Tunnel...**      **Update**

| Local IP   | Remote IP  | Peer           | Tunnel Status | Encapsulation P | Decapsulation P | Send Error Pack | Received Error P |
|------------|------------|----------------|---------------|-----------------|-----------------|-----------------|------------------|
| 172.30.1.2 | 172.30.2.2 | 172.30.2.2:500 | Up            | 198             | 0               | 121             | 0                |



- h. Select the **IKE SAs** tab to view the active IKE SAs.

| Source IP  | Destination IP | State   |
|------------|----------------|---------|
| 172.30.1.2 | 172.30.2.2     | QM_IDLE |

- i. Select **VPN** from the Tasks panel of the **Configuration** page.

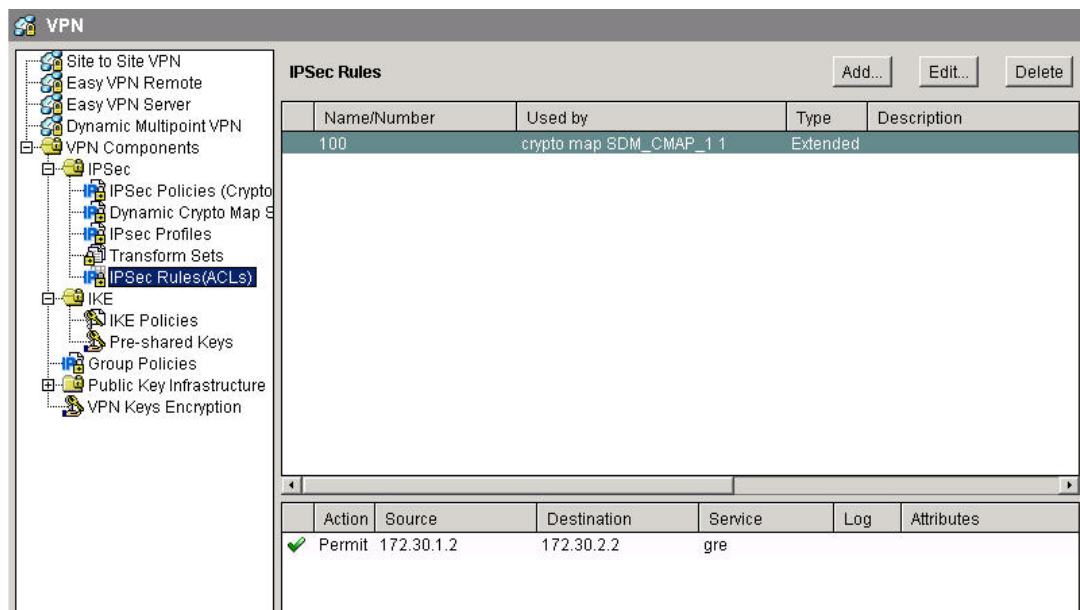
| Status | Interface                 | Description          | IPSec Policy | Serial |
|--------|---------------------------|----------------------|--------------|--------|
| Up     | Tunnel0 / FastEthernet0/1 | Tunnel to 172.30.2.2 | SDM_CMAP_1   | 1      |

- j. This will provide the tunnel status as well as additional information about the VPN tunnel configuration.
- k. Click through the **VPN Components** tree to view the detailed configuration.

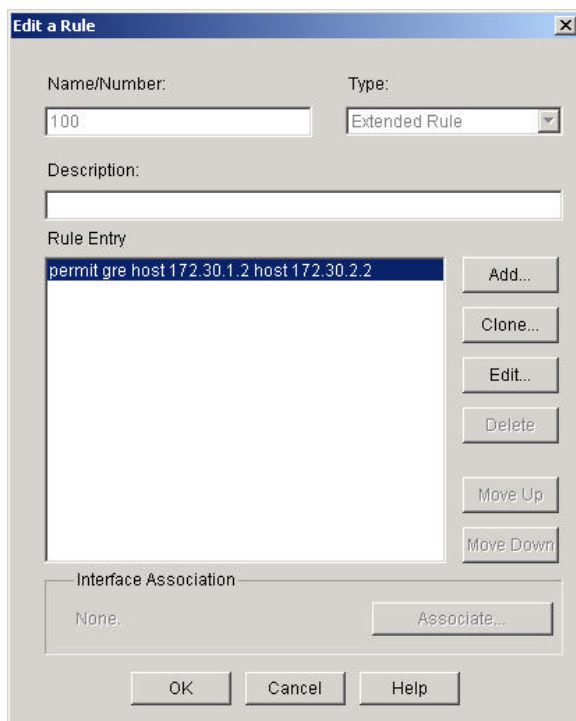
### Step 3 Modify the GRE over IPSec configuration

Work with the members of the pod group to modify the VPN encryption settings

- a. Click on **IPSec Rules(ACLs)** in the VPN Components tree.



- b. Click on the IPsec Rules Number **100**.
- c. Click the **Edit** button.



Notice that the only traffic which is in the GRE over IPsec tunnel is from outside interface of the router to the outside interface of the peer router.

- d. Click the **Add** button to add an ACL to protect LAN to LAN traffic.

**Add an Extended Rule Entry**

Action  
Select an action: Protect the traffic

Description  
LAN to LAN

Source Host/Network  
Type: A Network  
IP Address: 10.0.1.0  
Wildcard Mask: 0.0.0.255  
( Mask bit 0 - Must match )  
( Mask bit 1 - Don't care )

Destination Host/Network  
Type: A Network  
IP Address: 10.0.2.0  
Wildcard Mask: 0.0.0.255  
( Mask bit 0 - Must match )  
( Mask bit 1 - Don't care )

Protocol and Service  
☐ TCP ☐ UDP ☐ ICMP ☒ IP  
IP Protocol  
IP Protocol: ip

☐ Log matches against this entry

OK Cancel Help

This sample shows the ACL added on Router1. Router 2 will have Source/Destination Networks reversed.

- e. Click the **OK** button. The **Edit a Rule** window will appear now with the added ACL entry.

**Edit a Rule**

Name/Number:  Type:

Description:

Rule Entry

|   |           |
|---|-----------|
| permit gre host 172.30.1.2 host 172.30.2.2      | Add...    |
| permit ip 10.0.1.0/0.0.0.255 10.0.2.0/0.0.0.255 | Clone...  |
|   | Edit...   |
|   | Delete    |
|   | Move Up   |
|   | Move Down |

Interface Association

None... Associate...

OK Cancel Help

- f. If the **Command Delivery Status** window appears, click the **OK** button to continue.
- g. Verify that there are now two ACL entries.

|   | Action | Source             | Destination        | Service | Log | Attributes |
|---|--------|--------------------|--------------------|---------|-----|------------|
| ✓ | Permit | 172.30.1.2         | 172.30.2.2         | gre     |     |            |
| ✓ | Permit | 10.0.1.0/0.0.0.255 | 10.0.2.0/0.0.0.255 | ip      |     |            |

- i. Navigate to the **Tools>Ping**.
- h. Ping the inside address of the peer router at 10.0.Q.2 from a source address of 10.0.P.2. 20% may be lost while the tunnel is negotiated for the first time for this traffic.

**Ping**

\* Source:  Destination:

Ping

Sending 5, 100-byte ICMP Echos to 10.0.2.2, timeout is 2 seconds  
 Packet sent with a source address of 10.0.1.2  
 .!!!!  
 Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/12

(\*) Optional Field

Clear Output Close Help