



Lab 4.4.8b Configure Cisco IOS IPSec with Pre-Shared Keys using SDM

Objective

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

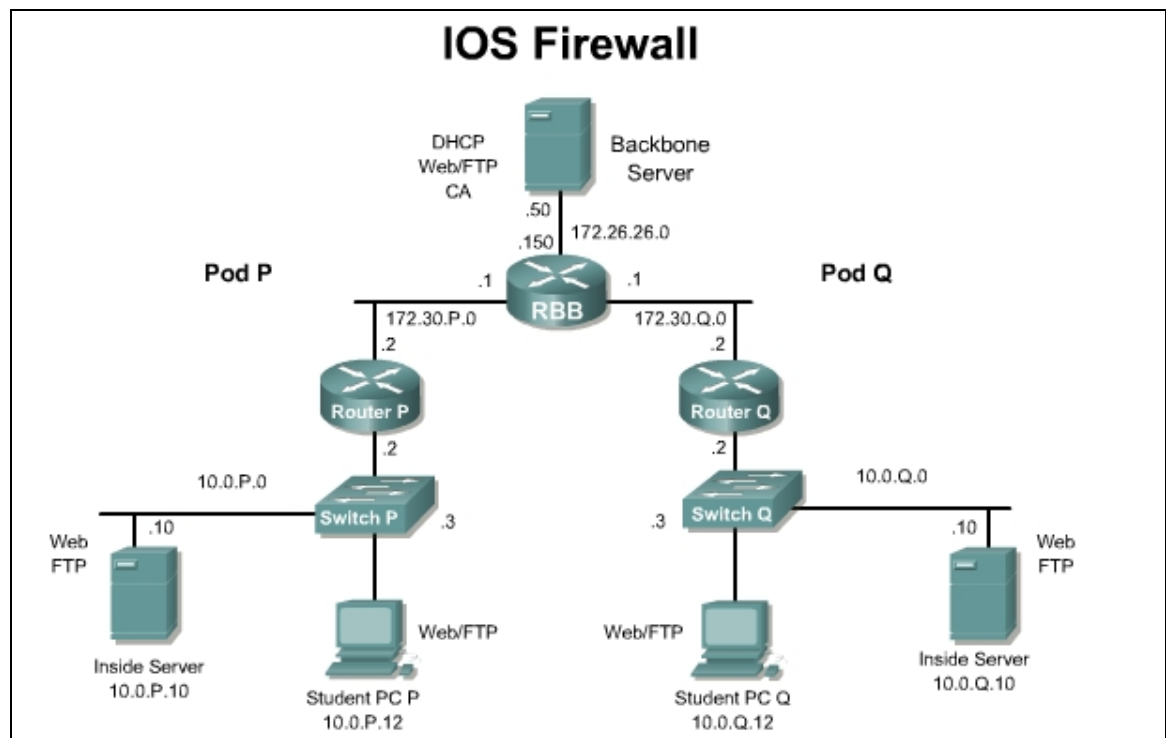
- Prepare to configure Virtual Private Network (VPN) Support
- Configure VPN tunnel using SDM VPN Wizard
- Modify IKE and IP Security (IPSec) configuration
- Verify and test IPSec configuration

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 security policy specifies using IPSec with pre-shared keys for authentication.

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 website:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ddeb.html

Step 1 Prepare to Configure VPN Support

Perform the following steps to prepare for the IPSec configuration:

- Determine the IKE and IPSec policy. In this exercise, use the default values except when directed to enter a specific value. The following are the overall policies used in the lab exercise:
 - IKE policy is to use pre-shared keys.
 - IPSec policy is to use Encapsulating Security Payload (ESP) mode with Advanced Encryption Standard (AES) encryption.
 - IPSec policy is to encrypt all traffic between perimeter routers.
- Verify that connectivity has been established to the peer router. Answer the following question:

`ping 172.30.Q.2`

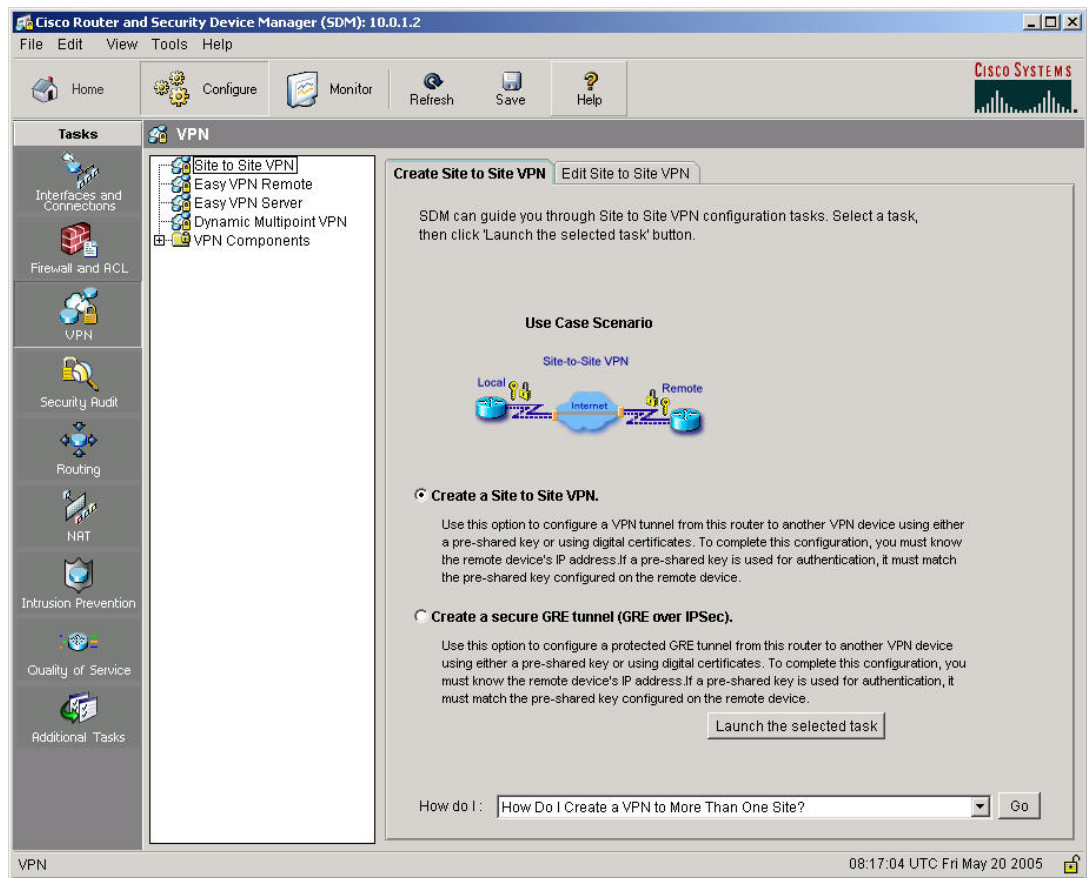
(where Q = peer pod number)

- In a production environment, what other steps would need to be completed at this point?
-

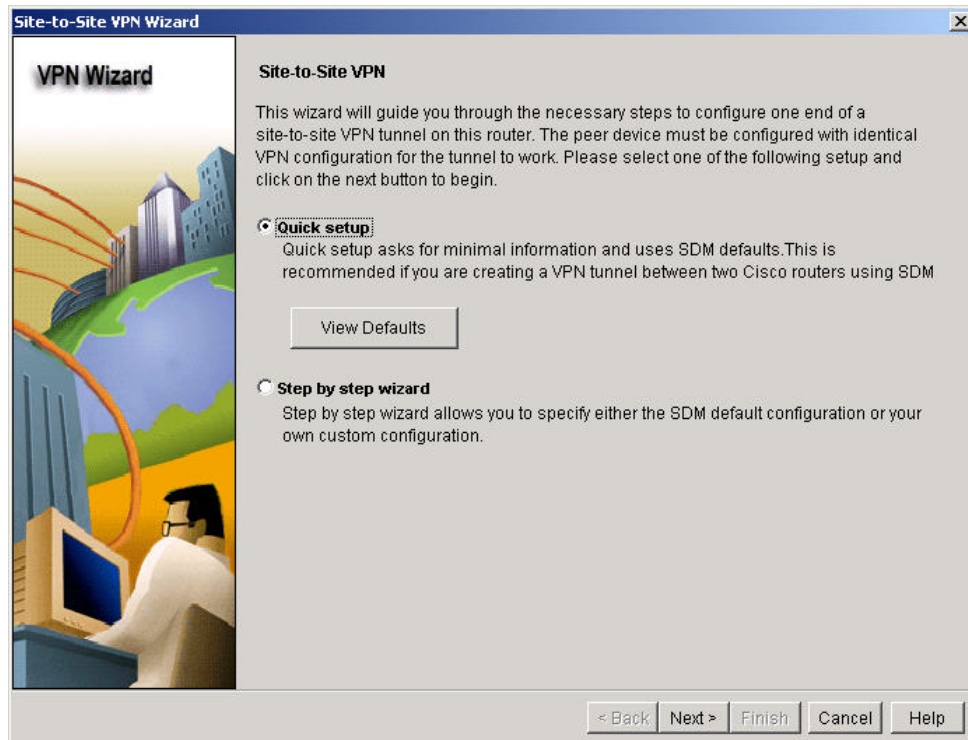
Step 2 Configure VPN Parameters

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 Site to Site VPN**. option from the **Create Site to Site VPN** tab.

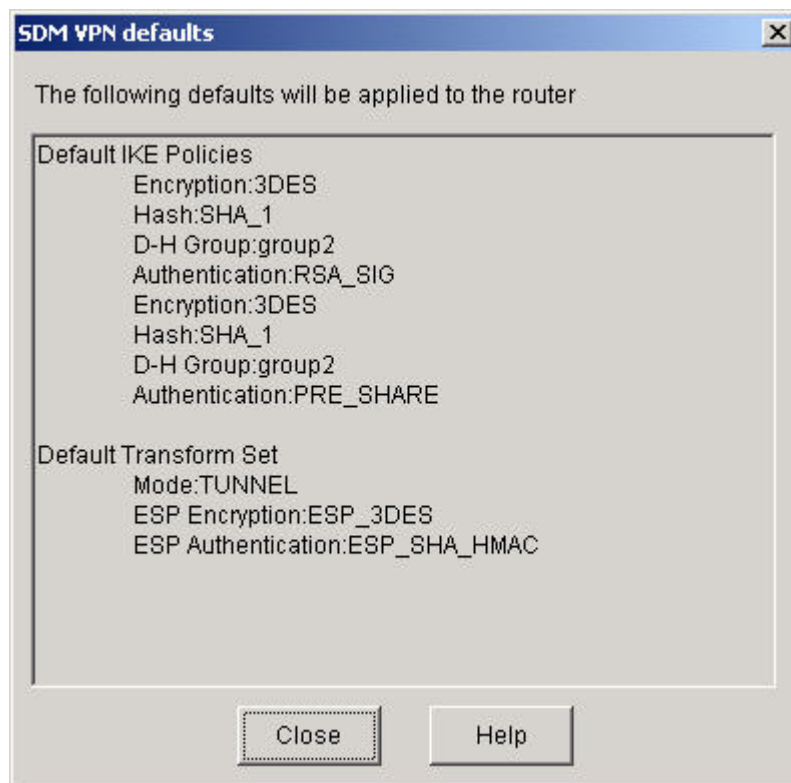


- d. Click **Launch the selected task** button.

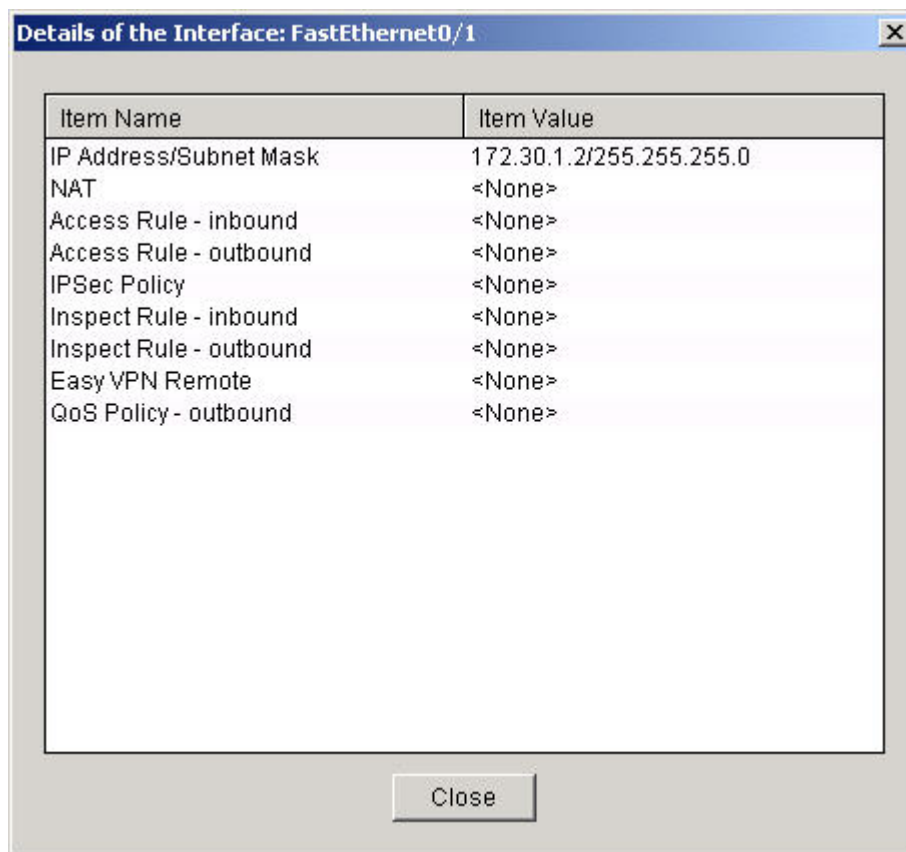


At this point, a choice between one of two options is available. The Quick setup mode or the Step by step wizard can be used. For this lab exercise, use the Quick setup mode.

- e. Click **View Defaults** button to see how the quick setup will configure the VPN.

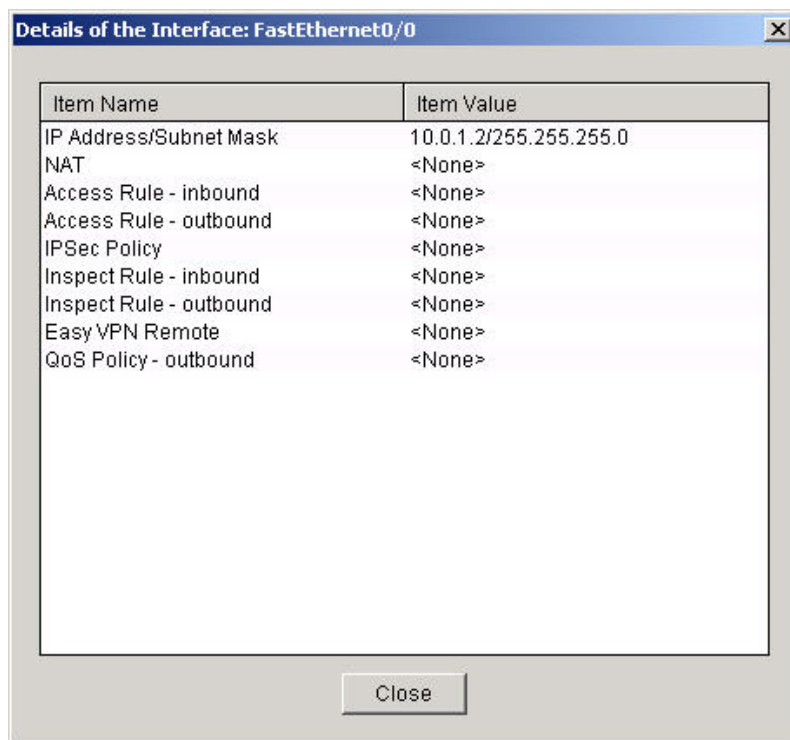


- f. Select **Quick Setup** and click the **Next** button.
- g. Click the **Close** button to return to the Site to Site VPN Wizard.
- h. Select the outside interface (Fa0/1) for the VPN connection.
- i. Click on the **Details** button to verify the proper external address.



The IP address should be **172.30.P.2** (where P = pod number)

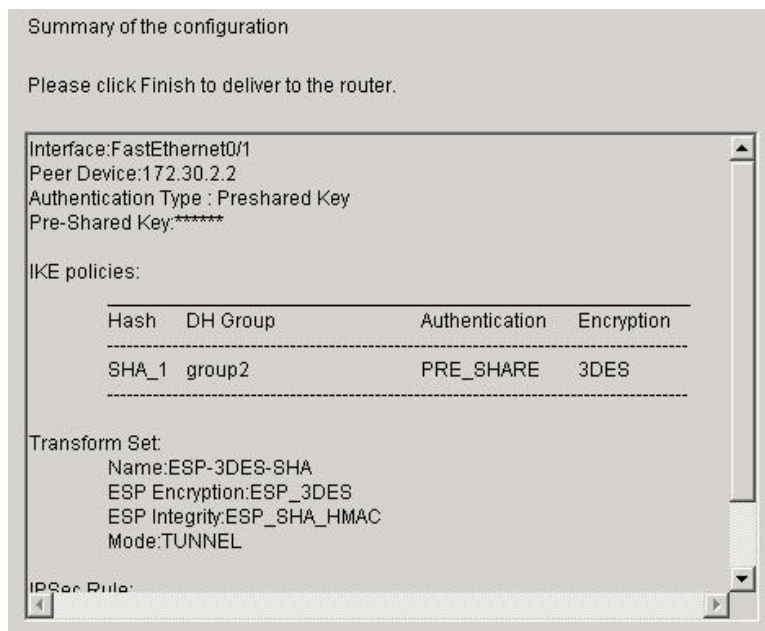
- j. Click the **Close** button to return to the Site to Site VPN Wizard.
- k. Set the Peer Identity as **172.30.Q.2** (where Q = peer pod number).
- l. Enter and confirm a pre-shared to be used for authentication. (make sure the CAPS lock is not on)
cisco1234
- m. Select the inside interface (Fa0/0) where the traffic to be encrypted originates to protect the source traffic.
- n. Click on the **Details** button to verify the address is 10.0.P.2/255.255.255.0 (where P = pod number).



- o. Click the **Close** button to return to the Site to Site VPN Wizard.
- p. Make the appropriate selection for the destination where encrypted traffic terminates to protect all destination traffic.

IP Address: **10.0.Q.0/** (where Q = peer pod number)

Subnet Mask: **255.255.255.0** or **24**
- q. Click the **Next** button. When a message appears stating that IKE is disabled on the router, click the **OK** button.
- r. Verify the configuration summary.



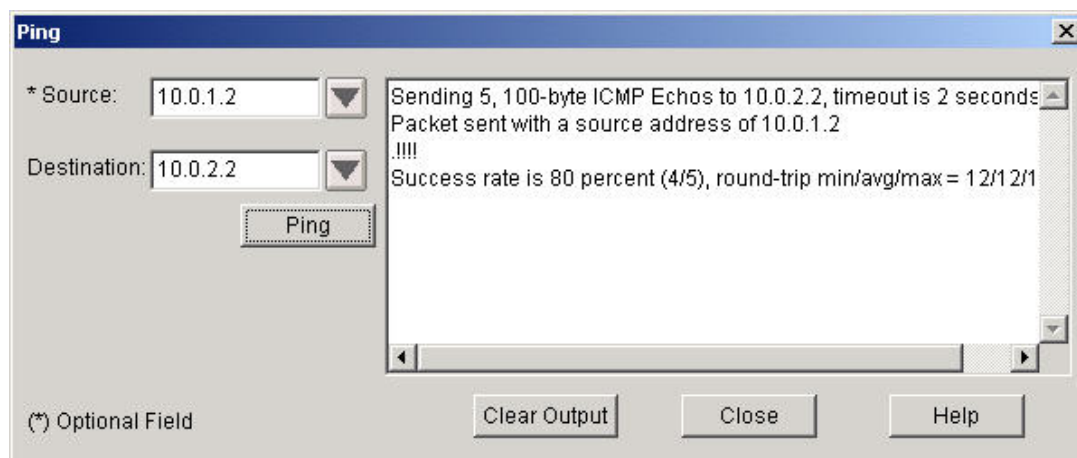
Note which IKE policy and Transform set will be deployed. If there are any mistakes, go back and fix them before proceeding.

- s. Click the **Finish** button to apply this change to the router configuration. Click the **OK** button on the **Command Deliver Status** window to complete the configuration delivery.

Step 3 Verify and Monitor the VPN Tunnel

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

- a. Navigate to the **Tools>Ping**.
- b. Ping the peer's inside router interface address at 10.0.2.2. Make sure the source address is the inside address of the router.10.0.1.2. In the example below, the ping is initiated from Pod 1.



- c. If the ping is less than 100% successful the first time, this is due to the tunnel establishment phase.
- d. Click on the **Clear Output** button and repeat the ping.
- e. The ping should be at 100%.
- f. Click on the **Close** button.
- g. Now click on the **Monitor** button on the top navigation bar.

Resource Status

CPU Usage: 1%

Memory Usage: 13%
Available: 74 MB

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

Interface Status

Total Interface(s) Up: 2 **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

Firewall Status

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

QoS

No. of QoS-enabled Interfaces: 0

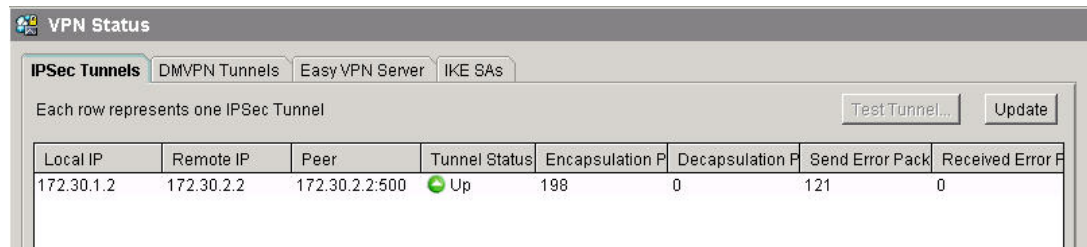
VPN Status

No. of Open IPSec Tunnels: 1
No. of Open IKE SAs: 1

No. of DMVPN Clients: 0
No. of Active VPN Clients: 0

- h. Notice the VPN Status box where one open IKE SA and one open IPSec tunnel are now shown.

- i. 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 Easy VPN Server IKE SAs

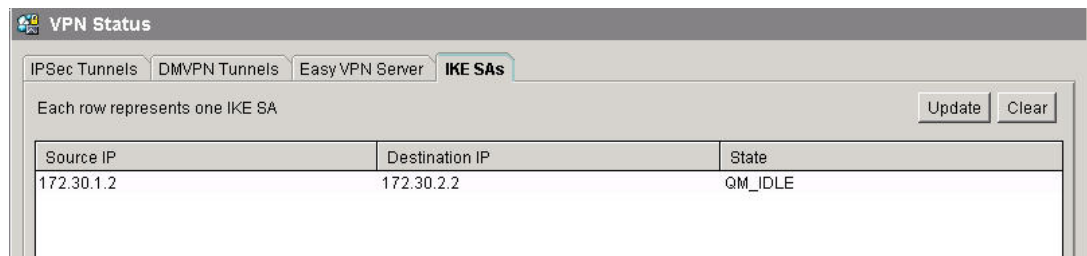
Each row represents one IPsec Tunnel

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

1. What other types of connections can be viewed on this page?

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



VPN Status

IPsec Tunnels DMVPN Tunnels Easy VPN Server IKE SAs

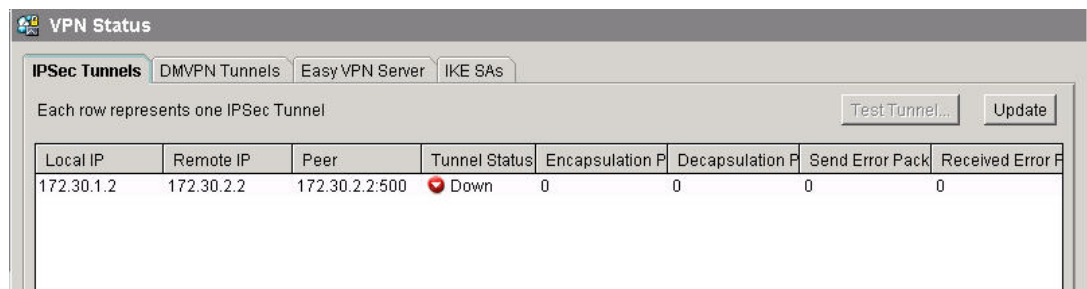
Each row represents one IKE SA

Update Clear

Source IP	Destination IP	State
172.30.1.2	172.30.2.2	QM_IDLE

- k. Click on the **Clear** button. This will delete the IKE SA.
- l. On the router, through the command line, clear the VPN session

```
RouterP#clear crypto session
```
- m. Return back to the **IPsec Tunnels** tab in SDM. Click the **Update** button to update the **IPsec Tunnels** status.



VPN Status

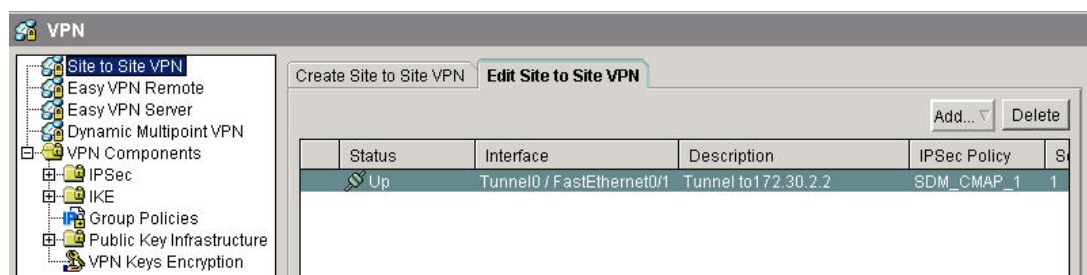
IPsec Tunnels DMVPN Tunnels Easy VPN Server IKE SAs

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	Down	0	0	0	0

- n. The VPN tunnel will show a down state indicated by the red icon.
- o. Repeat the ping as directed, beginning in Step3a to reestablish the tunnel.
- p. Select **VPN** from the **Tasks** panel of the **Configuration** page.



VPN

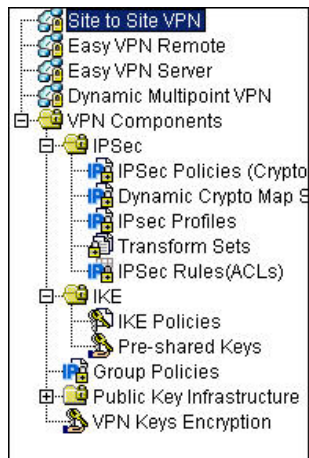
Site to Site VPN Easy VPN Remote Easy VPN Server Dynamic Multipoint VPN VPN Components IPsec IKE Group Policies Public Key Infrastructure VPN Keys Encryption

Create Site to Site VPN Edit Site to Site VPN

Add... Delete

Status	Interface	Description	IPsec Policy	S
Up	Tunnel0 / FastEthernet0/1	Tunnel to 172.30.2.2	SDM_CMAP_1	1

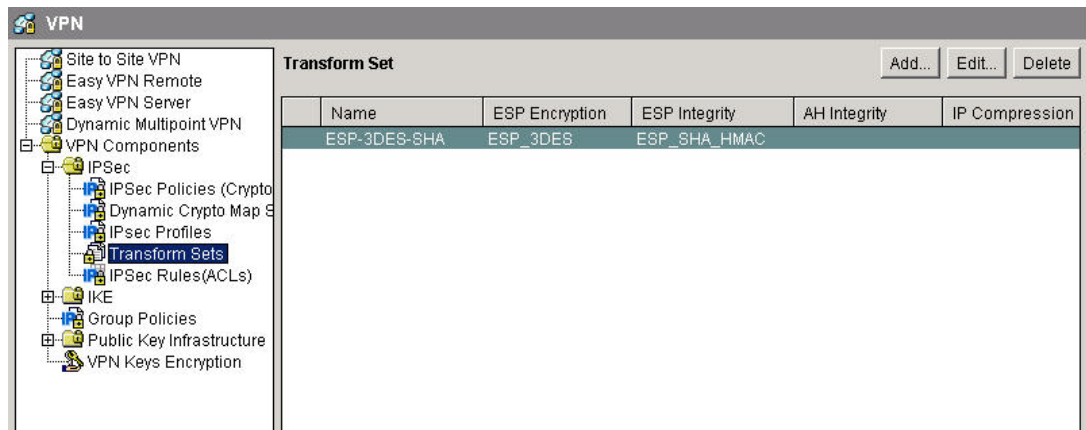
- q. This will provide the tunnel status as well as additional information about the VPN tunnel configuration.
- r. Click through the **VPN Components** tree to view the detailed configuration.



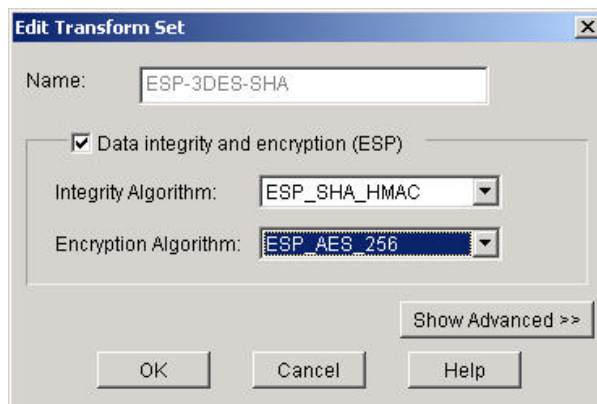
Step 4 Modify the VPN configuration

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

- Navigate to the **Configure>VPN**.
- Click on **VPN Components>IPSec>Transform Sets** in the tree menu.



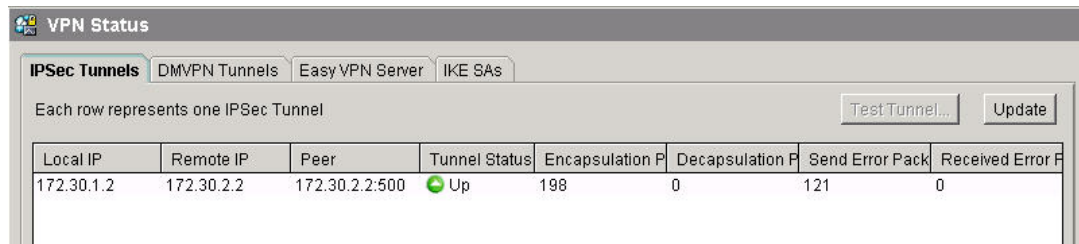
- Click on the **Edit** button
- Change the Encryption Algorithm: to **ESP_AES_256**



- Click **OK**.
- If the **Command Delivery Status** window appears, click the **OK** button to continue.
 - On the router, through the command line, clear the VPN sessions.

```
RouterP#clear crypto session
```

2. Make sure the peer router has changed to ESP_AES256.
- g. Ping the peer as directed, beginning in Step3a. The ping step may have to be repeated a second time.
- h. Navigate to **Monitor>VPN Status>IPSec Tunnels**.
- i. Click the **Update** button. The tunnel should now be up.



VPN Status

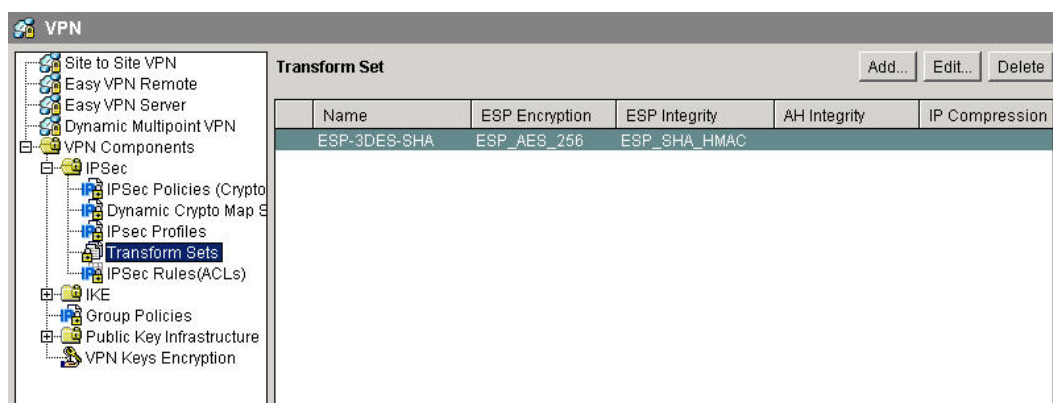
IPSec Tunnels DMVPN Tunnels Easy VPN Server IKE SAs

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

- j. Click the **Configure** button at the top of the SDM window.
- k. Select **VPN** from the **Tasks** panel.
- l. In the tree menu, select **VPN Components>IPSec>Transform Sets**
- m. The transform set ESP_AES_256 should be shown.



VPN

Site to Site VPN
Easy VPN Remote
Easy VPN Server
Dynamic Multipoint VPN
VPN Components
IPSec
IPSec Policies (Crypto)
Dynamic Crypto Map S
IPSec Profiles
Transform Sets
IPSec Rules(ACLs)
IKE
Group Policies
Public Key Infrastructure
VPN Keys Encryption

Transform Set

Add... Edit... Delete

Name	ESP Encryption	ESP Integrity	AH Integrity	IP Compression
ESP-3DES-SHA	ESP_AES_256	ESP_SHA_HMAC		

- n. If desired, change the IKE Policy to AES_256
- o. If desired, change the DH group to Group 5.
- p. If desired, change the Pre-shared Keys.
- q. If desired, change the lifetimes of the IKE and IPSec Policies. Change these to a low value around 2 or 3 minutes. Debug the IPSec output to observe the Tunnel rekey before the time expiration. Also, configure a different lifetime value on the Peer router and observe the Tunnel characteristics at the expiration time.
- r. Enable debug output for IPSec events.


```
RouterP#debug crypto ipsec
```
- s. Enable debug output for ISAKMP events.


```
RouterP#debug crypto isakmp
```

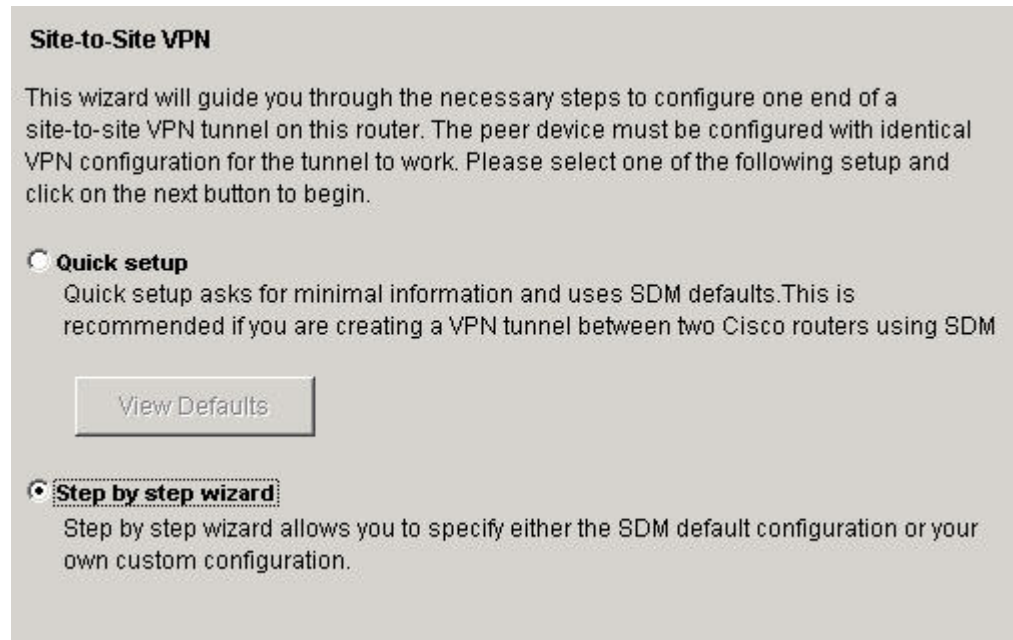
Step 5 Configure VPN Parameters using Step by Step Wizard.(Optional)

Work with the members of the pod group to complete the VPN configuration using the Step by step wizard.

- a. Delete the current VPN.
- b. Select the **VPN** wizard from the category bar.

Figure1

- c. Select the **Create a Site to Site VPN with Pre-Shared Key** option.
- d. Click **Launch the selected task** button.
- e. Choose the **Step by step wizard**.



- f. Continue through the Step by step wizard using the same values that were used in the previous steps.