VPN Configuration for Secure Remote Access using PuTTY with Cisco 2950 Router and Cisco 2600 Switch

1. Introduction Virtual Private Networks (VPNs) provide a secure method for remote access by encrypting data transmitted between remote clients and enterprise networks. This report outlines the configuration of a VPN for secure remote access using PuTTY, a Cisco 2950 router, and a Cisco 2600 switch.

2. Network Topology The setup consists of:

- A Cisco 2950 router as the primary gateway.
- A Cisco 2600 switch for LAN connectivity.
- A remote client using PuTTY for SSH access.
- Internet connectivity for remote access.

3. Prerequisites

- Cisco 2950 router and Cisco 2600 switch with appropriate firmware.
- PuTTY installed on the client machine.
- Basic knowledge of Cisco IOS commands.
- Pre-configured network interfaces.
- VPN software (such as Cisco AnyConnect) if required.

4. Configuring the Cisco 2950 Router for VPN Access

Step 1: Enable SSH for Secure Access

```
Router> enable
Router# configure terminal
Router(config)# hostname VPNRouter
Router(config)# ip domain-name example.com
Router(config)# crypto key generate rsa
Router(config)# username admin privilege 15 secret StrongPassword
Router(config)# line vty 0 4
Router(config-line)# transport input ssh
Router(config-line)# login local
Router(config-line)# exit
Router(config)# ip ssh version 2
Router(config)# exit
Router# write memory
```

Step 2: Configure IPsec VPN

```
Router(config)# crypto isakmp policy 10
Router(config-isakmp)# encryption aes 256
Router(config-isakmp)# hash sha256
Router(config-isakmp)# authentication pre-share
Router(config-isakmp)# group 2
Router(config-isakmp)# exit

Router(config)# crypto isakmp key VPNKey address 0.0.0.0
Router(config)# crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
Router(config)# crypto map VPN-MAP 10 ipsec-isakmp
Router(config-crypto-map)# set peer <Remote-IP>
Router(config-crypto-map)# set transform-set VPN-SET
Router(config-crypto-map)# match address 100
Router(config-crypto-map)# exit

Router(config)# interface FastEthernet0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# crypto map VPN-MAP
Router(config-if)# exit

Router(config)# access-list 100 permit ip 192.168.1.0 0.0.0.255 any
Router(config)# exit
Router# write memory
```

5. Configuring the Cisco 2600 Switch

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname VPN-Switch
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit

Switch(config)# vlan 10
Switch(config-vlan)# name VPN_VLAN
Switch(config-vlan)# exit
Switch(config)# exit
Switch# write memory
```

6. Connecting Remotely using PuTTY

- Open PuTTY on the client machine.
- Enter the router's public IP address.
- Select "SSH" as the connection type.
- Click "Open" and log in using the configured username and password.

7. Testing the VPN Configuration

- Verify IPsec status:

-
  ```
  Router# show crypto isakmp sa
  Router# show crypto ipsec sa
  ```
- Check SSH connectivity using PuTTY.
- Ensure network traffic is encrypted using a packet analyzer.

8. Conclusion This configuration enables secure remote access using VPN and SSH. It ensures encrypted communication between the client and the network while allowing controlled administrative access to the Cisco 2950 router and Cisco 2600 switch.