Name : Muhammad Yaseen

Roll Number 21-Fet/Bsce/F22

Submitted To: Sir. Zahoor Ud Din Shiekh

IPSec VPN Configuration Report

Objective: The goal of this configuration is to establish a secure IPSec VPN tunnel between two routers (R1 and R3) through an ISP, ensuring encrypted communication between two private subnets: 192.168.1.0/24 (R1 LAN) and 192.168.3.0/24 (R3 LAN).

1. Initial Router Configurations:

Each router is configured with appropriate IP addresses on its interfaces, and static routing is implemented to enable communication between networks via the ISP. Below are the configurations:

Router R1:

```
# hostname R1
# interface g0/1
# ip address 192.168.1.1 255.255.255.0
# no shut
# interface g0/0
# ip address 192.168.100.1 255.255.255.0
# no shut
# exit
# ip route 0.0.0.0 0.0.0.0 192.168.100.2
```

ISP Router:

```
# hostname ISP
# interface g0/1
# ip address 192.168.200.2 255.255.255.0
# no shut
# interface g0/0
```

ip address 192.168.100.2 255.255.255.0
no shut
exit

Router R3:

hostname R3
interface g0/1
ip address 192.168.3.1 255.255.255.0
no shut
interface g0/0
ip address 192.168.200.1 255.255.255.0
no shut
exit
ip route 0.0.0.0 0.0.0.0 192.168.200.2

2. Security License Activation:

The security license is enabled on both routers to allow the use of advanced security features, including IPSec:

license boot module c1900 technology-package securityk9

3. IPSec VPN Configuration:

IPSec VPN is configured on R1 and R3 to establish the secure tunnel. The key steps include ISAKMP policy setup, pre-shared key definition, transform-set creation, and applying the crypto map to the outbound interface.

Configuration on R1:

- **ISAKMP Policy:**

crypto isakmp policy 10
encryption aes 256

authentication pre-share

` # group 5

- **Pre-shared Key:**

crypto isakmp key secretkey address 192.168.200.1

- **IPSec Transform Set:**

crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac

- **Crypto Map:**

crypto map IPSEC-MAP 10 ipsec-isakmp

set peer 192.168.200.1

set pfs group5

set security-association lifetime seconds 86400

set transform-set R1-R3

match address 100

- **Apply to Interface:**

interface GigabitEthernet0/0

crypto map IPSEC-MAP

- **Access Control List (ACL):**

access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Configuration on R3:

- **ISAKMP Policy:**

crypto isakmp policy 10

encryption aes 256

authentication pre-share

group 5

- **Pre-shared Key:**

crypto isakmp key secretkey address 192.168.100.1

- **IPSec Transform Set:**

crypto ipsec transform-set R3-R1 esp-aes 256 esp-sha-hmac

- **Crypto Map:**

crypto map IPSEC-MAP 10 ipsec-isakmp

set peer 192.168.100.1

set pfs group5

set security-association lifetime seconds 86400

set transform-set R3-R1

match address 100

- **Apply to Interface:**

interface GigabitEthernet0/0

crypto map IPSEC-MAP

- **Access Control List (ACL):**

access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

4. Summary:

- **ISAKMP Configuration:** AES 256 encryption, pre-shared key authentication, and Diffie-Hellman group 5 are used for Phase 1.
- **IPSec Configuration:** AES 256 for encryption and SHA for hashing ensure data integrity and confidentiality.
- **Access Control:** ACL ensures that only traffic between the two private networks (192.168.1.0/24 and 192.168.3.0/24) is encrypted.
- **Crypto Map Application:** The crypto map binds the IPSec policies to the respective interfaces on R1 and R3.

5. Verification:

After completing the configuration, verify the VPN tunnel status and connectivity using the following commands:

- **ISAKMP Status:**

show crypto isakmp sa

- **IPSec Status:**

show crypto ipsec sa

- **Connectivity:**

ping 192.168.3.1 (from R1) and ping 192.168.1.1 (from R3)

Conclusion:
The IPSec VPN tunnel was successfully configured to provide secure communication between the 192.168.1.0/24 and 192.168.3.0/24 networks. Due to ISAKMP policy and crypto map, the configuration ensured encryption and authentication, meeting the objectives of secure inter-network communication.