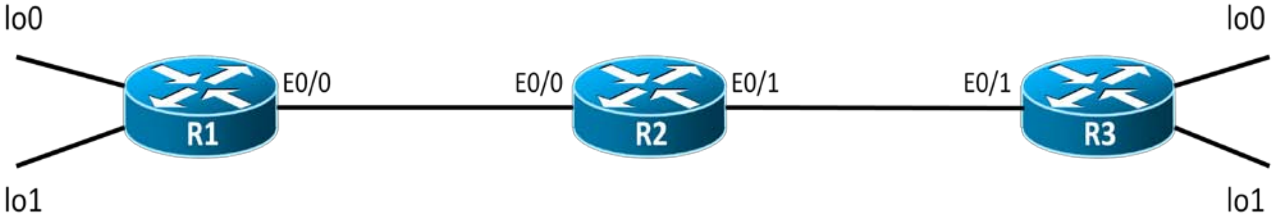
IPSec VPN. GRE tunneling.

1. Topology



2. IP Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	E0/0	192.168.12.1	255.255.255.248
	Lo0	10.1.1.1	255.255.255.0
	Lo1	11.1.1.1	255.255.255.0
R2	E0/0	192.168.12.2	255.255.255.248
	E0/1	192.168.23.2	255.255.255.248
R3	E0/1	192.168.23.3	255.255.255.248
	Lo0	10.3.3.3	255.255.255.0
	Lo1	11.3.3.3	255.255.255.0

3. Objectives

- Configuring and testing all the phases of the implementation of an IPSec Site-to-site VPN
- Capturing traffic from the dynagen interface
- Analyzing traffic with Wireshark
- Configuring and testing a GRE Tunnel

4. IPSec VPN Implementation

4.1 Network connectivity

1. Configure the above topology with the IP addresses shown in the IP Addressing table.
2. Configure EIGRP/OSPF in the above topology in order to have end-to-end connectivity.
3. Test connectivity from router R1's lo0 interface to router R3's lo0 interface using and extended ping.

4.2 Enable IKE

4. Enable IKE (isakmp) on routers R1 and R3

4.3 Configure ISAKMP policy parameters

5. Configure the following ISAKMP policy on both R1 and R3
    - authentication: pre-shared keys
    - encryption: aes 256
    - hashing: sha1
    - diffie-hellman group: 2
    - lifetime: 3600
6. Use the **`show crypto isakmp policy`** command to verify the policy on both ends of the tunnel.

4.4 Configure the authentication of the tunnel peers

7. Configure "srs!@#" as a pre-shared key on both R1 and R3.

4.5 Configure the tunnel transform set

8. Configure the following transform set on both R1 and R3:
    - Tag (name of the transform set): *TS_SRS*
    - Transform set: esp-aes 256 esp-sha-hmac
    - Mode: transport
9. Verify your configuration using the **`sh crypto ipsec transform-set`** command.

4.6 Define interesting traffic

10. The traffic that must be encrypted is traffic flowing between router R1's lo0 interface and router R3's lo0 interface.
11. Construct an access-list that will match the traffic that you want to encrypt. The access-list will have to define both the source and the destination of the traffic. An access-list must be defined on both R1 and R3. **Watch out for the fact that the 2 ACLs must mirror each other.**

12. Verify your configurations using the **`show ip access-lists`** command

4.7 Create and apply a crypto map

13. Create a crypto-map called ***TUNNEL_MAP*** on both R1 and R3.
    - The crypto map must match the ACL that you used to define interesting traffic.
    - The crypto map must set the remote peer for the tunnel. The remote peer is going to be the IP address of the outgoing Ethernet interface of each router.
    - The crypto map must set the transform set to "*TS_SRS*"
14. Apply the crypto map on interface E0/0 of R1 and E0/1 of R3.
15. Verify your configurations using the **`show crypto map`** command.

4.8 Verifying the IPSec VPN in tunnel mode.

16. Type in the command **`show crypto isakmp sa`** on both routers. Why are there no security associations generated ?
17. Ping R3's E0/1 interface from R1. Issue the above show command again. Is anything generated this time? Why?
18. Do an extended ping that will have R1's loopback 0 as a source address and R3's loopback 0 as a destination address.
19. Run the **`show crypto isakmp sa`** command.
20. How many packets got encrypted in the last data transfer? To verify this, run the **`show crypto ipsec sa`** command.

4.9 Verifying that the traffic is encrypted.

21. Use the "capture R2 e0/0 tunnel.cap" command in the dynagen console to start a capture on R2's e0/0 interface
22. Do the extended ping that you performed earlier in order to transmit traffic through the IPSec tunnel.
23. Stop the capture using the "no capture R2 e0/0" command in the dynagen console.
24. Open the tunnel.cap file with Wireshark. Check out the traffic. Is it encrypted or not?
25. If you are using tunnel mode, how come Wireshark only shows one IP header?

5. Implementing a GRE tunnel

One of the limitations of an IPSec VPN is that it cannot send multicast or non-IP traffic. To do this you will have to implement a GRE tunnel.

All the traffic that will be flowing between R1's lo1 interface and R3's lo1 interface is to be encapsulated using the GRE protocol.

26. Configure a GRE tunnel between R1 and R3 using the following parameters:
    - The tunnel's source and destination must be R1 and R3 Ethernet interfaces. Why is this not best practice but does not matter in this current topology ?
    - The network that is to be used on the Tunnel interfaces is 13.13.13.0 /29255
    - The tunnel mode is "gre ip"
27. On R1, direct all the traffic going to network 11.3.3.0 through the GRE tunnel. **Depending on what routing protocol you use, watch out for:**
    - **routes being advertised through the tunnel (including the route towards the tunnel endpoint)**
    - **the subnet mask of dynamic/static routes**
28. On R3, direct all the traffic going to network 11.1.1.0 through the GRE tunnel.

5.1 Verifying the GRE encapsulation

29. Use the "capture R2 e0/0 tunnel.cap" command in the dynagen console to start a capture on R2's e0/0 interface
30. Do an extended from R1's lo1 interface to R3's lo1 interface.
31. Stop the capture using the "no capture R2 e0/0" command in the dynagen console.
32. Open the tunnel.cap file with Wireshark. The traffic must be encapsulated with GRE.