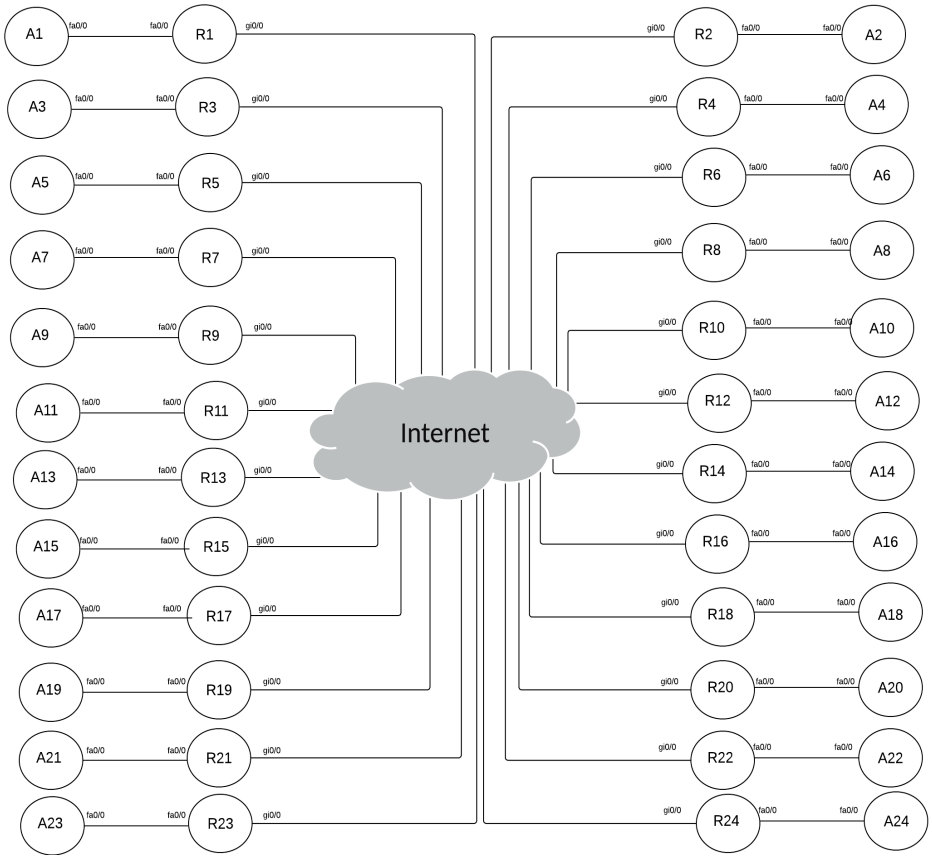
IPSEC Lab

Topology

- In this lab, each participant will be issued a pair of routers Ax and Rx
- The A router is your host that you will be using to test reachability
- The R router is your network edge router
- Each R router is configured with a Basic Nat



Router Assignement

Group	Ax IP	Rx IP
1	192.168.30.254:2031	192.168.30.254:2001
2	192.168.30.254:2032	192.168.30.254:2002
3	192.168.30.254:2033	192.168.30.254:2003
....	.....	.....
....	.....	.....
23	192.168.30.254:2053	192.168.30.254:2023
24	192.168.30.254:2054	192.168.30.254:2024

Note: To access your routers:

```
telnet 192.168.30.254 20XX
```

where XX is your router number (based on the allocation table)

Address Plan

Addresses are based on your group assignment 1-24

Router	Interface	IP Address
A1	fa0/0	100.68.1.1/24
R1	fa0/0	100.68.1.254/24
R1	gi1/0	100.68.0.1/24
A2	fa0/0	100.68.2.1/24
R2	fa0/0	100.68.2.254/24
R2	gi1/0	100.68.0.2/24
....	.....	.....
....	.....	.....
A23	fa0/0	100.68.23.1/24
R23	fa0/0	100.68.23.254/24
R23	gi1/0	100.68.0.23/24
A24	fa0/0	100.68.24.1/24
R24	fa0/0	100.68.24.254/24
R24	gi1/0	100.68.0.24/24

Lab Tasks

You will be setting up a site to site IPsec tunnel between yourself and your neighbours router.
In the examples below we will be using A1 and R1 and establishing a tunnel to R2

First, lets establish that we **can not** see inside our neigbours network.
Log on to your A router and ping your neigbours A router (Below is A1 to A2):

```
A1>en
A1#ping 100.68.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.68.2.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
A1#
```

Can we see our neighbouring R2 router?

```
A1#
A1#ping 100.68.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.68.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/31/40 ms
A1#
```

1. Create ISAKMP Policy: First step to setup an IPSec tunnel is to configure ISAKMP policy parameters.
   There are five policy parameters that need to be defined to each policy entry. Here are those parameters and their default values:
   - IKE policy encryption: Data Encryption Standard (DES) as the default
   - IKE policy hash: Secure Hash Standard-1 (SHA-1) as the default
   - IKE key exchange: Diffie-Hellman Group 1 (768-Bit) as the default
   - IKE lifetime: One-day (86,400 seconds) lifetime as the default
   - IKE authentication: RSA public key as the default

The configuration for R1 would be the following:

```
config t
crypto isakmp policy 10
  encryption aes
  hash sha
  group 5
  authentication pre-share
exit
```

2. Create Pre Shared Key: There are three methods can be used for peer authentication in IPSec VPN.
   I.e.:
   - Pre-shared keys: A secret key configured into each peer manually by the administrator
   - RSA signature: Digital certificate exchanged among the per to authenticate.
   - RSA encrypted nonces: An encrypted random number generated by each IPSec peer then
     exchanged to authenticate. Two nonces are used during the authentication process.

We will be using a symmetric key, which is pre-shared and need to be shared between IPSec peers out of band. Please note the key command below and address is your tunnel destination which is the WAN address of your peer. You need to replace the address with your peer WAN address. Look at the topology diagram above to find your peer WAN address.

Example pre-shared key configuration on R1 connecting to R2:

```
crypto isakmp key Tr@ining123 address 100.68.0.2
```

3. Configure IPSec transform set: IPSec transform sets are exchange between peers during quick mode in phase 2. A transform set is a combination of algorithms and protocol that endorse a security policy for traffic.
   Example transform set configuration for the R1 router:

```
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
```

4. Creating the crypto map: Now need to create a crypto map to glue all those policy together. Please note the peer address which will be your IPSec tunnel destination. Normally WAN address of remote peer.
   Example crypto map configuration for the R1 router connecting to R2:

```
crypto map LAB-VPN 10 ipsec-isakmp
  match address 115
  set transform-set ESP-AES-SHA
  set peer 100.68.0.2
exit
```

5. Configure access-list: As you can see from the previous step there is a `match address 115`. This is telling our crypto map that we want to apply this map to traffic identified in an access list numbered 115. This is the interesting traffic that we want to encrypt and send over our tunnel.
   Here is an example access-list for R1 router send to R2:

```
access-list 115 permit ip 100.68.1.0 0.0.0.255 100.68.2.0 0.0.0.255
```

6. Apply crypto map to an interface: The next step is to apply the crypto map to an outgoing interface.
   Example crypto map configuration for one of the R1 router:

```
 int gigabitEthernet 1/0
  crypto map LAB-VPN
 exit
```

7. Change our NAT Rules: As we are using a basic nat on our WAN interface (Gi1/0) we need to make sure that our interesting traffic does not get sent out with our nat traffic. We do this through the use of a Route map.
   The route map allows us to deny traffic destined for our peers network via the nat yet still allow all other traffic via the nat.
   This is an example access list and route map for R1:

   ```
   access-list 110 deny ip 100.68.1.0 0.0.0.255 100.68.2.0 0.0.0.255
   access-list 110 permit ip 100.68.1.0 0.0.0.255 any
   route-map no-nat permit 10
     match ip address 110
   exit
   ```

   And we also need to modify our NAT rule so that the route-map is applied to our outbound interface.

```
no ip nat inside source list 1 interface GigabitEthernet1/0 overload
ip nat inside source route-map no-nat interface GigabitEthernet 1/0 overload
```

8. Prove that our tunnels are up and sending traffic:
   Lets Ping our Neighboring host, in this case from A1 to A2:

```
A1#
A1#ping 100.68.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.68.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/79/84 ms
A1#
```

9. Verify the IPSec configuration:
   Command to show ISAKMP security associations (SAs) built between peers:

```
show crypto isakmp sa
```

Command to show IPsec SAs built between peers:

```
sh crypto ipsec sa
```

Command to verify ISAKMP peer:

```
sh crypto isakmp peers
```

10. Optional: Try and setup a tunnel with another peer. What elements would you need to change or add?

11. Sample config for R1

```
config t
crypto isakmp policy 10
 encryption aes
 hash sha
 group 5
 authentication pre-share
exit
crypto isakmp key Tr@ining123 address 100.68.0.2
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
crypto map LAB-VPN 10 ipsec-isakmp
 match address 115
 set transform-set ESP-AES-SHA
 set peer 100.68.0.2
exit
access-list 115 permit ip 100.68.1.0 0.0.0.255 100.68.2.0 0.0.0.255
int gigabitEthernet 1/0
 crypto map LAB-VPN
exit
access-list 110 deny ip 100.68.1.0 0.0.0.255 100.68.2.0 0.0.0.255
access-list 110 permit ip 100.68.1.0 0.0.0.255 any
route-map no-nat permit 10
match ip address 110
exit
no ip nat inside source list 1 interface GigabitEthernet1/0 overload
ip nat inside source route-map no-nat interface GigabitEthernet 1/0 overload
exit
wr mem
```

12. Sample config for R2

```
config t
crypto isakmp policy 10
 encryption aes
 hash sha
 group 5
 authentication pre-share
exit
crypto isakmp key Tr@ining123 address 100.68.0.1
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
crypto map LAB-VPN 10 ipsec-isakmp
 match address 115
 set transform-set ESP-AES-SHA
 set peer 100.68.0.1
exit
access-list 115 permit ip 100.68.2.0 0.0.0.255 100.68.1.0 0.0.0.255
int gigabitEthernet 1/0
 crypto map LAB-VPN
exit
access-list 110 deny ip 100.68.2.0 0.0.0.255 100.68.1.0 0.0.0.255
access-list 110 permit ip 100.68.2.0 0.0.0.255 any
route-map no-nat permit 10
match ip address 110
exit
no ip nat inside source list 1 interface GigabitEthernet1/0 overload
ip nat inside source route-map no-nat interface GigabitEthernet 1/0 overload
exit
wr mem
```