Arquitetura de Redes

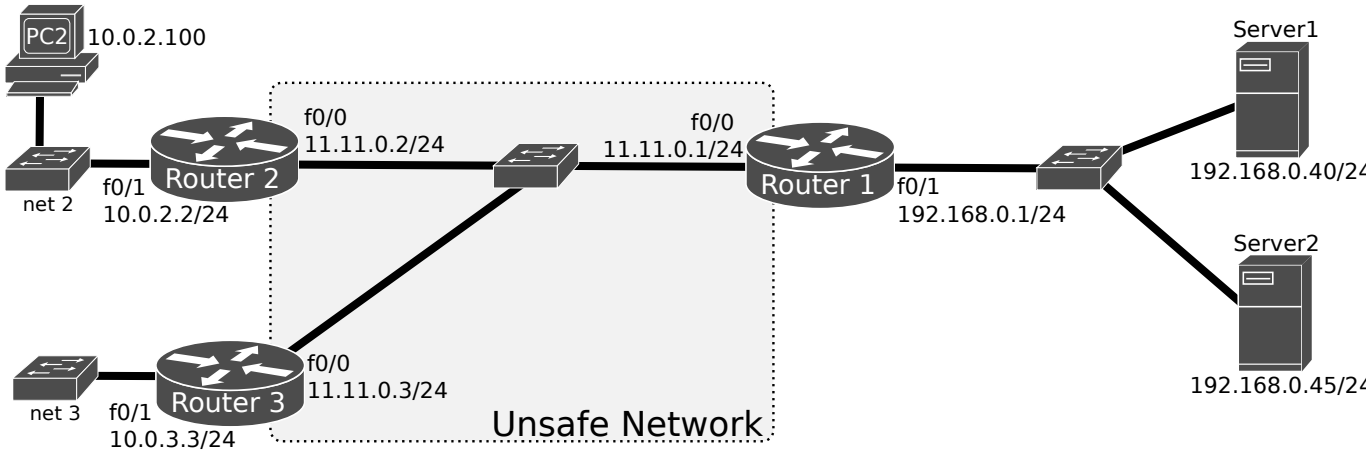
IPSec Tunnels and site-to-site VPNs

Objectives

- IPSec Tunneling
- Policy Based Routing (PBR)
- Site-to-Site IPsec VPNs

IPSec Tunneling

1. Configure the below depicted network (Router 3 is not necessary for now), including IPv4 addresses and IPv4 routing mechanisms (static routes or OSPF). Test for full connectivity. In GNS3, use VPCS to emulate PC and servers.
Warning: Do not use IOS 15.2 as router firmware.



2. Consider that network 11.11.0.0/24 is unsafe. Therefor, all important traffic must be transported securely using an IPSec tunnel. Consider all IP communication between network 10.0.2.0/24 and Server2 as important traffic, all other traffic can be transmitted unencrypted through network 11.11.0.0/24. Router2 configuration (IPSec only) is the following:

```
Router2(config)# crypto isakmp policy 30      ! The number defines the order of preference
Router2(config-isakmp)# authentication pre-share           ! Auth. with password
Router2(config)# crypto isakmp key labcom address 11.11.0.1       ! Passw. with Router1
Router2(config)# crypto ipsec transform-set authT ah-sha-hmac            ! AH
Router2(config)# crypto ipsec transform-set cipherT esp-des              ! ESP with DES
Router2(config)# crypto ipsec transform-set auth_ciphT ah-sha-hmac esp-des     ! AH+ESP
Router2(config)# crypto ipsec profile ARipsec        ! Defines tunnel type/protocols
Router2(ipsec-profile)# set transform-set authT cipherT  auth_ciphT      !Order def. prefs.
---
Router2(config)# interface Tunnel 0
Router2(config-if)# ip unnumbered FastEthernet0/0
Router2(config-if)# tunnel source 11.11.0.2
Router2(config-if)# tunnel destination 11.11.0.1
Router2(config-if)# tunnel mode ipsec ipv4
Router2(config-if)# tunnel protection ipsec profile ARipsec
Router2(config)# ip route 192.168.0.45 255.255.255.255 Tunnel 0       ! Route to Server 2
```

Configure Router1 using a similar and compatible IPsec configuration and define the Tunnel:

```
Router1(config)# interface Tunnel 0
Router1(config-if)# ip unnumbered FastEthernet0/0
Router1(config-if)# tunnel source 11.11.0.1
Router1(config-if)# tunnel destination 11.11.0.2
Router1(config-if)# tunnel mode ipsec ipv4
Router1(config-if)# tunnel protection ipsec profile ARipsec
Router1(config)# ip route 10.0.2.0 255.255.255.0 Tunnel 0         ! Return route
```

Note: the underline words are user-defined names.
Execute (in Router 1 and 2) the commands:

```
show crypto isakmp policy
show crypto ipsec transform-set
show crypto map
```

Explain the information returned by the routers.

3. Disable the IPsec tunnel interface in Router 2:

```
Router2(config)# interface Tunnel0
Router2(config-if)# shutdown
```

Start a capture on network 11.11.0.0/24 and re-enable the IPsec tunnel interface:

```
Router2(config)# interface Tunnel0
Router2(config-if)# no shutdown
```

Analyze the captured ISAKMP packets.

4. Start a capture on network 11.11.0.0/24. From PC2 ping both servers (192.168.0.40 and 192.168.0.45). Explain the differences between the two ICMP flows. Which is the IPSec protection mechanisms (AH, ESP or AH+ESP) been used for the traffic between network 10.0.2.0/24 and Server2?

5. Change the routers configuration (IPSec profiles) in order to use the two remaining protection mechanisms.

```
Router2(config)# crypto ipsec profile ARipsec
Router2(ipsec-profile)# set transform-set cipherT  authT  auth_cipht
------
Router2(ipsec-profile)#set transform-set auth_ciphT  authT  cipherT
```

Clear the tunnel IPsec active connections with commands: `shutdown`, `no shutdown`.

Test the configurations by pinging Server2 from PC2 and capturing the traffic flowing between Router2 and Router1. Explain the differences between the 3 IPSec protection protocols.

Policy Based Routing

6. Start a capture on network 11.11.0.0/24. From Server1, ping PC2. Is the traffic being encrypted (routed by the IPsec tunnel)? Is this correct? Explain why the traffic is being routed by the tunnel, breaking the security/routing policy.

7. To implement Policy Based Routing, disable the OSPF for the private networks and replace the static routes by Route Maps. On Router 2:

```
Router2(config)# no ip route 192.168.0.45 255.255.255.255 Tunnel 0
Router2(config)# access-list 100 permit ip 10.0.2.0 0.0.0.255 host 192.168.0.45
Router2(config)# route-map routeT0 permit 10
Router2(config-route-map)# match ip address 100
Router2(config-route-map)# set interface Tunnel 0
--
Router2(config)#interface FastEthernet0/1
Router2(config-if)#ip policy route-map routeT0       ! IPv4 policy routing activation
```

Perform the equivalent configuration on Router1:

```
Router1(config)# no  ip route 10.0.2.0 255.255.255.0 Tunnel 0
Router1(config)# access-list 100 permit ip host 192.168.0.45 10.0.2.0 0.0.0.255
Router1(config)# route-map routeT0 permit 10
Router1(config-route-map)# match ip address 100
Router1(config-route-map)# set interface Tunnel 0
--
Router1(config)#interface FastEthernet0/1
Router1(config-if)#ip policy route-map routeT0       ! IPv4 policy routing activation
```

Verify the IPv4 routing table (note the absence of routes to the remote private networks). From PC2 ping Server1 and Server2, and vice-versa. Analyze the route-map statistics (`show route-map routeT0`). Analise which traffic is being encrypted (routed by the tunnel). Is the routing policy correct?

Extra: Site-to-Site VPN based on IPSec Tunnels with Dynamic Maps

Disable the previous tunnel interface: `no interface tunnel 0.`

8. In a scenario with multiple IPsec tunnels is advantageous to use dynamic maps which allow the establishment of tunnels from any machine to a central hub (crypto aggregator) without any additional configuration in it. Router 1 will have the role of crypto aggregator, and should process IPsec tunneling requests for new security associations from any remote IP Security peer with correct credentials, even if it does not know all of the crypto map parameters required to communicate with the remote peer and should accept requests for new security associations from previously unknown peers. These requires the usage of dynamic crypto maps.

Router1 configuration (IPSec and DMAP only) is the following:

```
Router1(config)# crypto isakmp policy 20
Router1(config-isakmp)# authentication pre-share
Router1(config)# crypto isakmp key labcom address 0.0.0.0 0.0.0.0
Router1(config)# crypto ipsec transform-set nss-ts esp-3des esp-sha-hmac
Router1(config)# crypto dynamic-map nss-dmap 10
Router1(config-crypto-map)# set transform-set nss-ts
Router1(config-crypto-map)# reverse-route
Router1(config)# crypto map dynamic-map 10 ipsec-isakmp dynamic nss-dmap
Router1(config)# interface FastEthernet0/0
Router1(config-if)# ip address 11.11.0.1 255.255.255.0
Router1(config-if)# crypto map dynamic-map
Router1(config)# ip route 10.0.2.0 255.255.255.0 11.11.0.2
Router1(config)# ip route 10.0.3.0 255.255.255.0 11.11.0.3
---
Router2(config)# crypto isakmp policy 20
Router2(config-isakmp)# authentication pre-share
Router2(config)# crypto isakmp key labcom address 11.11.0.1
Router2(config)# crypto ipsec transform-set nss-ts esp-3des esp-sha-hmac
Router2(config)# crypto map nss-cm 10 ipsec-isakmp
Router2(config-crypto-map)#set peer 11.11.0.1
Router2(config-crypto-map)#set transform-set nss-ts
Router2(config-crypto-map)#match address nss-cm-acl
Router2(config)# interface FastEthernet0/0
Router2(config-if)# ip address 11.11.0.2 255.255.255.0
Router2(config-if)# crypto map nss-cm
Router2(config)# ip access-list extended nss-cm-acl
Router2(config-ext-nacl)# permit ip 10.0.2.0 0.0.0.255 192.168.0.0 0.0.0.255
Router2(config-ext-nacl)# permit ip 10.0.2.0 0.0.0.255 10.0.3.0 0.0.0.255
Router2(config)# ip route 192.168.0.0 255.255.255.0 11.11.0.1
Router2(config)# ip route 10.0.3.0 255.255.255.0 11.11.0.3
---
Router3(config)# crypto isakmp policy 20
Router3(config-isakmp)# authentication pre-share
Router3(config)# crypto isakmp key labcom address 11.11.0.1
Router3(config)# crypto ipsec transform-set nss-ts esp-3des esp-sha-hmac
Router3(config)# crypto map nss-cm 10 ipsec-isakmp
Router3(config-crypto-map)#set peer 11.11.0.1
Router3(config-crypto-map)#set transform-set nss-ts
Router3(config-crypto-map)#match address nss-cm-acl
Router3(config)# interface FastEthernet0/0
Router3(config-if)# ip address 11.11.0.3 255.255.255.0
Router3(config-if)# crypto map nss-cm
Router3(config)# ip access-list extended nss-cm-acl
Router3(config-ext-nacl)# permit ip 10.0.3.0 0.0.0.255 192.168.0.0 0.0.0.255
Router3(config-ext-nacl)# permit ip 10.0.3.0 0.0.0.255 10.0.2.0 0.0.0.255
Router3(config)# ip route 192.168.0.0 255.255.255.0 11.11.0.1
Router3(config)# ip route 10.0.2.0 255.255.255.0 11.11.0.2
```

Using the commands "`show crypto dynamic-map`" and "`show crypto map`" verify the establish secure connections.

Note: To reset the ISAKMP and IPsec SA negotiations use: `clear crypto isakmp` and `clear crypto sa`, respectively.

Start a packet capture at the central network (11.11.0.0/24) and test the IPsec VPN at **Router 2** with the commands:

```
ping 192.168.0.40 source FastEthernet0/1
ping 10.0.3.3 source FastEthernet0/1
```

Check the dynamically created crypto maps in **Router 1**: `show crypto map`

Explain why the second ping didn't succeed.

At **Router 3** perform the following command:

```
ping 10.0.2.2 source FastEthernet0/1
```

It was successful? Why?

Check the dynamically created crypto maps in **Router 1**: `show crypto map`

Re-execute the following command at **Router2**:

```
ping 10.0.3.3 source FastEthernet0/1
```

Check the dynamically created crypto maps in Router 1: `show crypto map`

Explain the results.

What can you conclude how the information is exchanged between routers in this scenario?