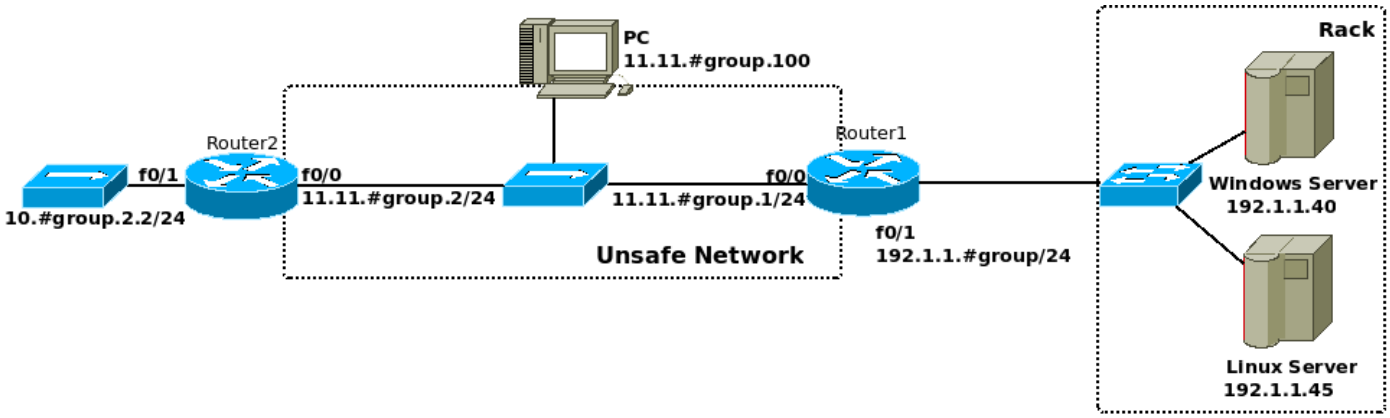
REDES E SERVIÇOS

Objectives

- IPSec Tunneling

IPSec Tunneling

1. Configure an Ethernet network according to the following figure. Assign IP address to all interfaces, configure OSPF in all routers and verify that all equipments have full connectivity.



2. Consider that network 11.11.#group.0 is unsafe. Therefor, all important traffic must be transported securely using an IPSec tunnel. Consider all IP communication between network 10.#group.2.0 and Linux Server as important traffic, all other traffic can be transmitted unencrypted through network 11.11.#group.0. 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.#group.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.#group.2
Router2(config-if)# tunnel destination 11.11.#group.1
Router2(config-if)# tunnel mode ipsec ipv4
Router2(config-if)# tunnel protection ipsec profile ARipsec
Router2(config)# ip route 192.1.1.45 255.255.255.255 Tunnel 0       ! Route to Linux server
```

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.#group.1
Router1(config-if)# tunnel destination 11.11.#group.2
Router1(config-if)# tunnel mode ipsec ipv4
Router1(config-if)# tunnel protection ipsec profile ARipsec
Router1(config)# ip route 10.#group.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
```

At PC start a capture with Wireshark and re-enable the IPsec tunnel interface:

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

Analyze the captured ISAKMP packets.

4. At PC start a capture with Wireshark. From Router2 ping both servers (192.1.1.40 and 192.1.1.45) using the output and f0/1 interfaces as sources:

```
ping 192.1.1.40
ping 192.1.1.45
ping 192.1.1.40 source f0/1
ping 192.1.1.45 source f0/1
```

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 10.10.#group.0.0 and Linux Server?

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 LinuxServer from Router2 and capturing the traffic flowing between Router2 and Router1. Explain the differences between the 3 IPSec protection protocols.