Arquitetura e Gestão de Redes

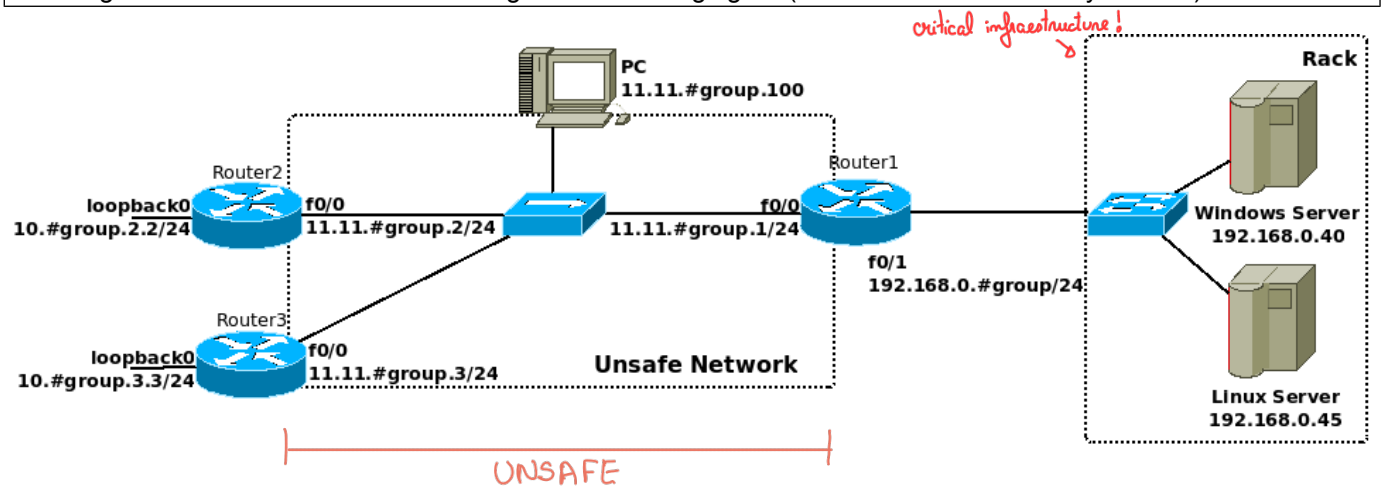
Laboratory Guide

Objectives

- IPSec Tunneling
- Site-to-Site IPsec VPNs

IPSec Tunneling

1. Configure an Ethernet network according to the following figure (Router 3 is not necessary for now).



2. Consider that network 11.11.#group.0 is unsafe. Therefore, 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 11.11.1.2
Router2(config-if)# tunnel destination 11.11.1.1
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
```

Configure Router1 using a similar and compatible IPsec configuration and define th

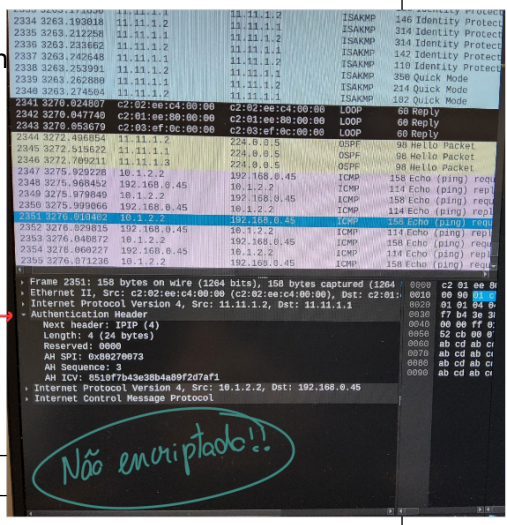
```
Router1(config)# interface Tunnel 0
Router1(config-if)# ip unnumbered FastEthernet0/0
Router1(config-if)# tunnel source 11.11.1.1
Router1(config-if)# tunnel destination 11.11.1.2
Router1(config-if)# tunnel mode ipsec ipv4
Router1(config-if)# tunnel protection ipsec profile ARipsec
Router1(config)# ip route 10.#group.2.0 255.255.255.0 Tunnel 0
```

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.



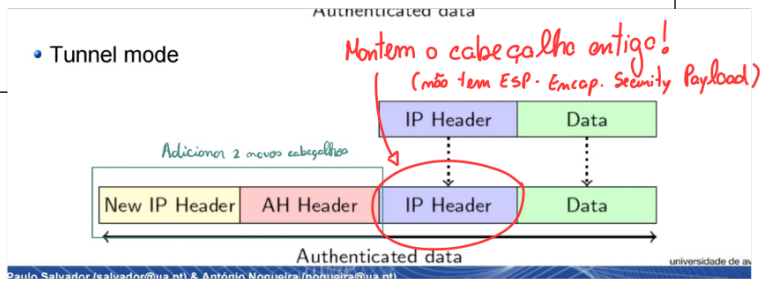
3. Disable the IPsec tunnel interface in Router 2:

```
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.



→ ISAKMP ←

Main Mode: estabelecer a segurança a um canal autenticado

1. Negociação dos regras de segurança
2. Trocar Diffie-Hellman Keys
3. Autenticação e verificação de identidade

Quick Mode: negociar as associações IPsec

1. Estabelecer chaves de sessão (IPsec SA)
   Security Associations

```
1.398640  11.11.1.2  11.11.1.1  ISAKMP  102 Quick Mode
1.434908  11.11.1.1  11.11.1.2  ISAKMP  186 Identity Protection (Main Mode)        (1)
1.470832  11.11.1.2  11.11.1.1  ISAKMP  146 Identity Protection (Main Mode)
1.495801  11.11.1.1  11.11.1.2  ISAKMP  314 Identity Protection (Main Mode)[Malformed Packet]
1.521693  11.11.1.2  11.11.1.1  ISAKMP  314 Identity Protection (Main Mode)[Malformed Packet]  (2)
1.536224  11.11.1.1  11.11.1.2  ISAKMP  142 Identity Protection (Main Mode)
1.546355  11.11.1.1  11.11.1.2  ISAKMP  126 Informational                           (3)
1.556682  11.11.1.1  11.11.1.2  ISAKMP  126 Informational
1.572643  11.11.1.2  11.11.1.1  ISAKMP  110 Identity Protection (Main Mode)
1.587078  11.11.1.1  11.11.1.2  ISAKMP  350 Quick Mode
1.602960  11.11.1.2  11.11.1.1  ISAKMP  214 Quick Mode
                                         102 Quick Mode                            (4)
```

(1)

```
Frame 7: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface -, id 0
Ethernet II, Src: c2:01:ee:80:00:00 (c2:01:ee:80:00:00), Dst: c2:02:ee:c4:00:00 (c2:02:ee:c4:00:00)
Internet Protocol Version 4, Src: 11.11.1.1, Dst: 11.11.1.2
User Datagram Protocol, Src Port: 500, Dst Port: 500
Internet Security Association and Key Management Protocol
  Initiator SPI: 2667615bc356cf71
  Responder SPI: 0000000000000000
  Next payload: Security Association (1)   ← Definir parametros de segurança
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 144
  Payload: Security Association (1)
  Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-07   NAT-traversal
  Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-03   } O que é que ele suporta ??
  Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02\n
```

Allows IPsec to work over NAT

1. Security Association

```
Frame 16: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits) on interface -, id 0
Ethernet II, Src: c2:01:ee:80:00:00 (c2:01:ee:80:00:00), Dst: c2:02:ee:c4:00:00 (c2:02:ee:c4:00:00)
Internet Protocol Version 4, Src: 11.11.1.1, Dst: 11.11.1.2
User Datagram Protocol, Src Port: 500, Dst Port: 500
Internet Security Association and Key Management Protocol
  Initiator SPI: 8e12cce770607df4
  Responder SPI: dd3e083058044e5d
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 272                              DH
  Payload: Key Exchange (4)
  Payload: Nonce (10)
  Payload: Vendor ID (13) : CISCO-UNITY 1.0
  Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
  Payload: Vendor ID (13) : Unknown Vendor ID
  Payload: Vendor ID (13) : XAUTH
  Payload: SA KEK Payload (15)
[Malformed Packet: ISAKMP]
  [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
```

2. Key Exchange

```
Frame 17: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface -, id 0
Ethernet II, Src: c2:01:ee:80:00:00 (c2:01:ee:80:00:00), Dst: c2:02:ee:c4:00:00 (c2:02:ee:c4:00:00)
Internet Protocol Version 4, Src: 11.11.1.1, Dst: 11.11.1.2
User Datagram Protocol, Src Port: 500, Dst Port: 500
Internet Security Association and Key Management Protocol
  Initiator SPI: 2667615bc356cf71
  Responder SPI: ach587568f529d523
  Next payload: Identification (5)   ← Identificação
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x01
  Message ID: 0x00000000
  Length: 68
  Encrypted Data (40 bytes)   ← Vai encriptada !
```

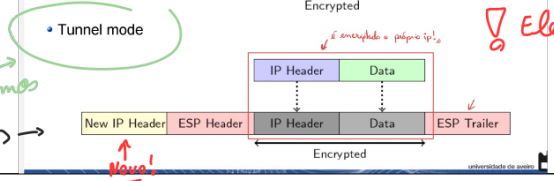
3. Identification

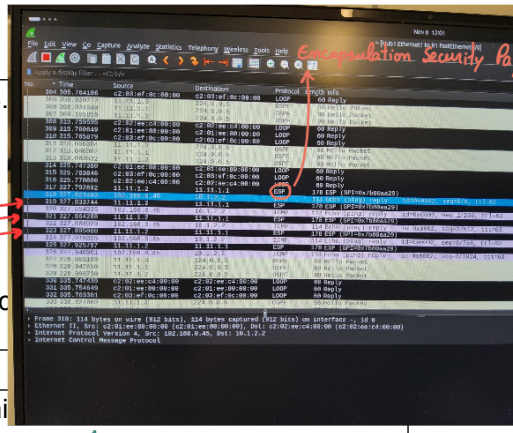
Quick Mode

```
Frame 21: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits) on interface -, id 0
Ethernet II, Src: c2:01:ee:80:00:00 (c2:01:ee:80:00:00), Dst: c2:02:ee:c4:00:00 (c2:02:ee:c4:00:00)
Internet Protocol Version 4, Src: 11.11.1.1, Dst: 11.11.1.2
User Datagram Protocol, Src Port: 500, Dst Port: 500
Internet Security Association and Key Management Protocol
  Initiator SPI: 2667615bc356cf71   } Integridade!
  Responder SPI: ach587568f529d523
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01                       } Negocia novas chaves de sessão
  Message ID: 0xcfc31b4d
  Length: 308
  Encrypted Data (280 bytes)
```

4. Hash

(session Keys)





4. At PC start a capture with Wireshark. From Router2 ping both servers (192.168.
output and loopback interfaces as sources:

```
ping 192.168.0.40
ping 192.168.0.45
ping 192.168.0.40 source Loopback 0
ping 192.168.0.45 source Loopback 0
```

Explain the differences between the two ICMP flows. Which IPSec protection mec
being 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 remaini

```
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 all IPsec active connections with command `clear crypto sa`

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.

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

6. 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.#group.1 255.255.255.0
Router1(config-if)# crypto map dynamic-map

---
Router2(config)# crypto isakmp policy 20
Router2(config-isakmp)# authentication pre-share
Router2(config)# crypto isakmp key labcom address 11.11.#group.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.#group.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.#group.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.#group.2.0 0.0.0.255 192.168.0.0 0.0.0.255
Router2(config-ext-nacl)# permit ip 10.#group.2.0 0.0.0.255 10.#group.3.0 0.0.0.255
---
```

```
Router3(config)# crypto isakmp policy 20
Router3(config-isakmp)# authentication pre-share
Router3(config)# crypto isakmp key labcom address 11.11.#group.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.#group.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.#group.2 255.255.255.0
Router3(config-if)# crypto map nss-cm
Router3(config)# ip access-list extended nss-cm-acl
Router3(config-ext-nacl)# permit ip 10.#group.3.0 0.0.0.255 192.168.0.0 0.0.0.255
Router3(config-ext-nacl)# permit ip 10.#group.3.0 0.0.0.255 10.#group.2.0 0.0.0.255
```

Using the commands "`show crypto dynamic-map`" and "`show crypto map`" verify the established secure connections. Start a packet capture at the central network (11.11.#group.0) and test the IPsec VPN at Router 2 with the commands:

```
ping 192.168.0.#group source Loopback 0
ping 10.#group.3.3 source Loopback 0
```

Explain why the second ping didn't succeed. At Router 3 perform the following command:

```
ping 10.#group.2.2 source Loopback 0
```

It was successful? Why? Re-execute the following command at Router2:

```
ping 10.#group.3.3 source Loopback 0
```

Explain the results.

Check the details of the IPsec ISAKMP SA with:

```
show crypto isakmp sa detail
```

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