Arquitetura de Redes

Access Control (Cisco's Access Lists)
&
IPSec Tunnels and site-to-site VPNs

Objectives

- Access Control (Cisco's Access Lists)
- IPSec Tunneling
- Site-to-Site IPsec VPNs

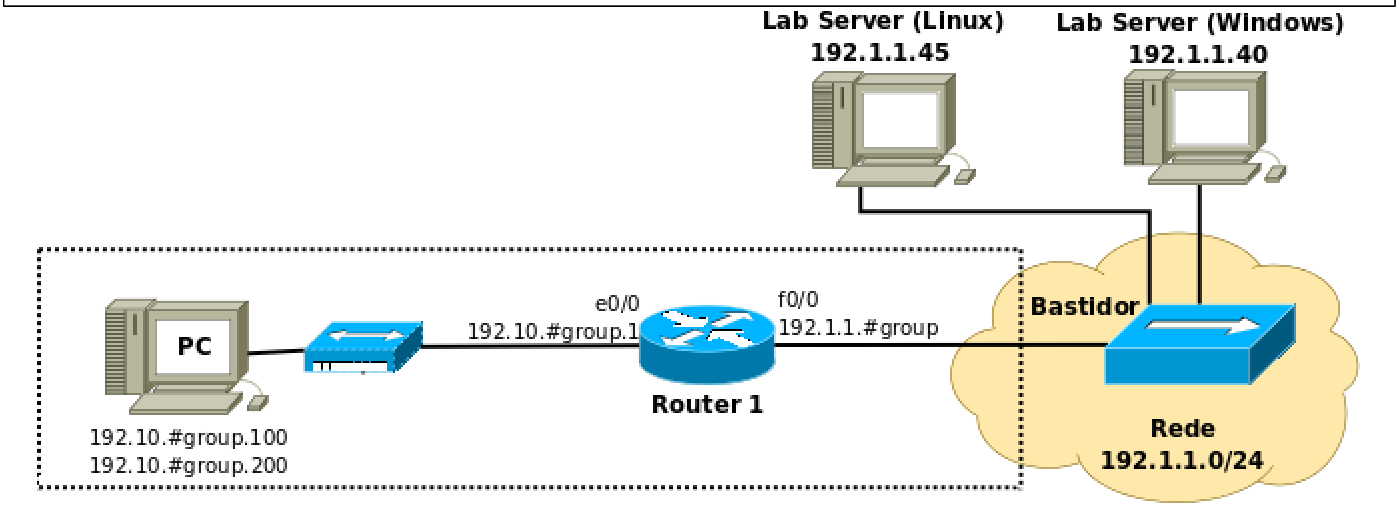
Introduction to Cisco ACLs

1. Start your PC in Linux and configure your network according to the following figure. Use the specified IP addresses with network masks 255.255.255.0. Configure Router1 as the PC's default gateway in order to obtain full connectivity:

```
        PC$ ifconfig eth0 192.10.#group.100/24
        PC$ ifconfig eth0:0 192.10.#group.200/24
        PC$ route add default gw 192.10.#group.1
```

Test the connectivity from the PC to both servers using both IP addresses:

```
        PC$ ping 192.1.1.40 -I 192.10.#group.100
        PC$ ping 192.1.1.45 -I 192.10.#group.100
        PC$ ping 192.1.1.40 -I 192.10.#group.200
        PC$ ping 192.1.1.45 -I 192.10.#group.200
```



2. Configure in Router 1 the following standard ACL:

```
 Router1(config)#access-list 1 permit 192.10.#group.100 0.0.0.0
 ! NOTE: creates a standard ACL that permits only traffic from PC1
 Router1(config)#interface f0/0
 Router1(config-if)#ip access-group 1 out
 ! NOTE: applies the ACL to outgoing traffic at interface f0/0
```

Start a packet capture on the PC and execute connectivity tests (ping) from PC to the servers in network 192.1.1.0. Analyze the captured (ICMP) packets. Explain how this ACL works.

3. Modify the ACL previously created in order to all devices, except the PC, be able to access the servers.

```
 Router1(config)#no access-list 1 permit 192.10.#group.100 0.0.0.0
#NOTE: deletes the previous ACL
 Router1(config)#access-list 1 deny 192.10.#group.100 0.0.0.0
 Router1(config)#access-list 1 permit any
```

Execute connectivity tests (ping) from PC to the servers in network 192.1.1.0. Analyze the captured (ICMP) packets. Explain how this ACL works.

4. Remove the standard ACL in Router 1,

```
Router1(config)#no access-list 1 deny 192.10.#group.100 0.0.0.0
Router1(config)#no access-list 1 permit any
Router1(config)#interface f0/0
Router1(config-if)#no ip access-group 1 out
```

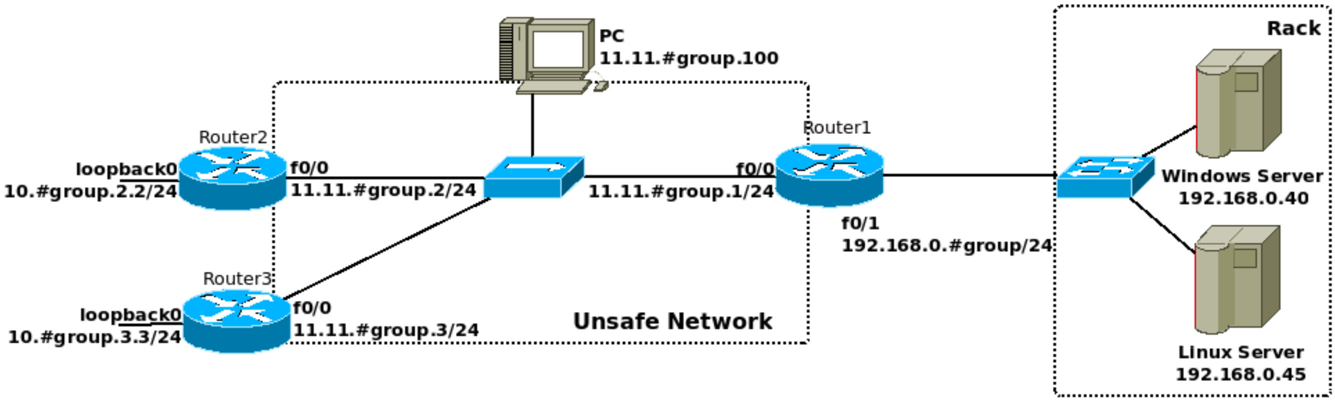
And configure the following extended ACL:

```
Router1(config)#access-list 101 permit tcp host 192.10.#group.100 host 192.1.1.45 eq 80
Router1(config)#access-list 101 permit tcp host 192.10.#group.200 host 192.1.1.45 eq 80
Router1(config)#interface e0/0
Router1(config-if)#ip access-group 101 in
Router1(config-if)#end
```

Execute connectivity tests (ping) from PC to the servers in network 192.1.1.0. Analyze the captured (ICMP) packets. Using a browser access the server 192.1.1.45's web page. Explain how this ACL works.

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. 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 192.168.0.45 255.255.255.255 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 (192.168.0.40 and 192.168.0.45) using the 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 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.

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

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

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.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.#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 establish 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?