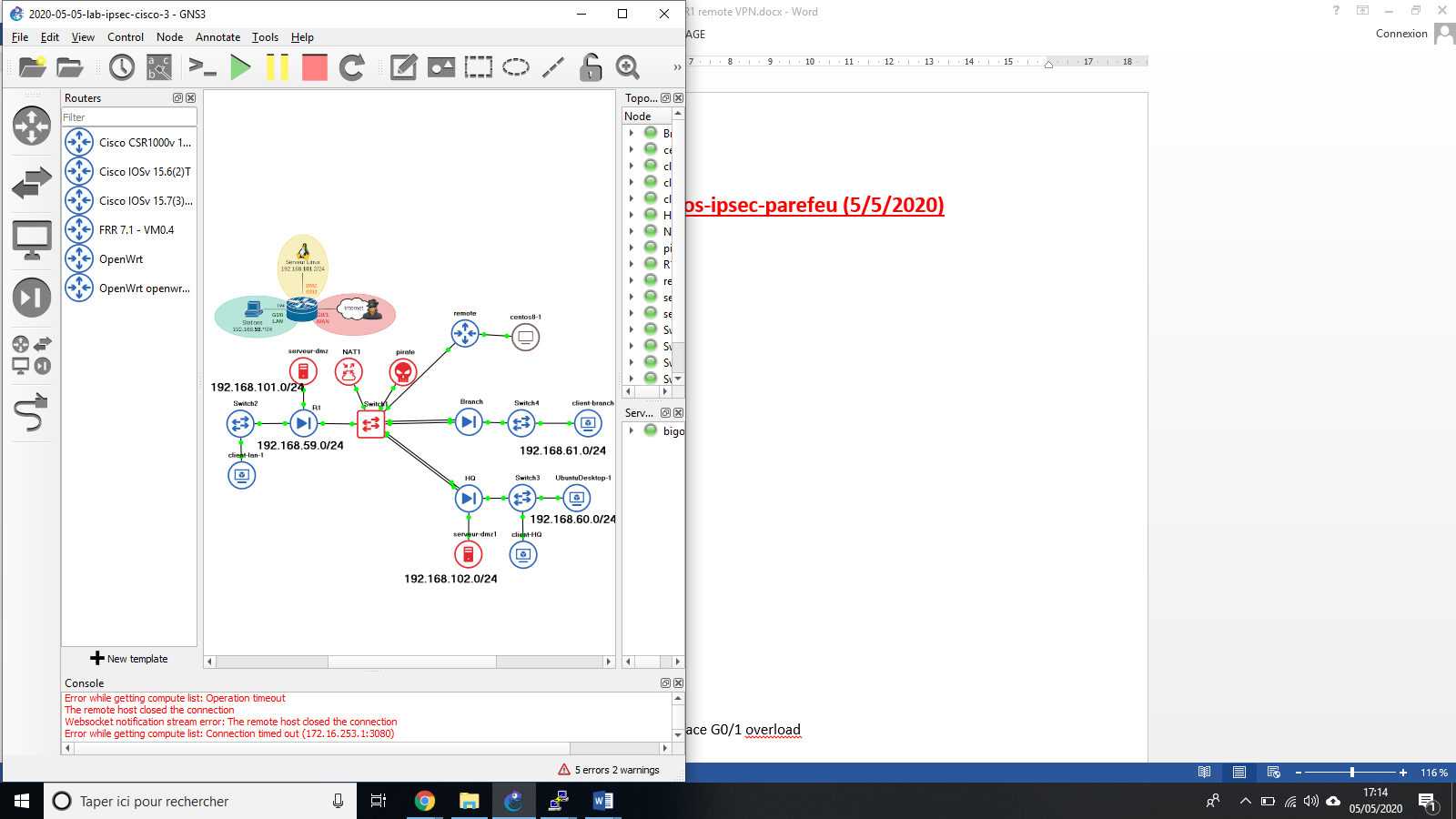
**vpn-04-lab-cisco-ios-ipsec-parefeu (5/5/2020)**



**1-Configuration du remote:**

hostname remote

!

interface G0/0

ip address 192.168.14.1 255.255.255.0

ip nat inside

no shutdown

!

interface GigabitEthernet0/1

ip address dhcp

ip nat outside

no shutdown

!

ip dhcp pool lan

network 192.168.14.0 255.255.255.0

default-router 192.168.14.1

dns-server 1.1.1.1

ip route 0.0.0.0 0.0.0.0 192.168.122.1

ip access-list extended LAN\_REMOTE

permit ip 192.168.14.0 0.0.0.255 any

!

ip nat inside source list LAN\_REMOTE interface G0/1 overload

end

remote#sh ip int brie

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0 192.168.14.1 YES manual up up

GigabitEthernet0/1 192.168.122.207 YES DHCP up up

GigabitEthernet0/2 unassigned YES unset administratively down down

GigabitEthernet0/3 unassigned YES unset administratively down down

NVI0 unassigned YES unset up up

**2-Configuration du vpn sur remote**

crypto isakmp policy 1

encr aes 256

authentication pre-share

group 5

lifetime 7200

!

crypto isakmp key cisco123 address 192.168.122.118

!

crypto ipsec transform-set to-R1-set esp-aes 256 esp-sha-hmac

!

crypto map cm-to-R1 1 ipsec-isakmp

set peer 192.168.122.118

set transform-set to-R1-set

match address crypto-acl

!

interface G0/1

crypto map cm-to-R1

!

ip access-list extended crypto-acl

permit ip 192.168.14.0 0.0.0.255 192.168.59.0 0.0.0.255

!

ip access-list extended LAN\_REMOTE

5 deny ip 192.168.14.0 0.0.0.255 192.168.59.0 0.0.0.255

10 permit ip 192.168.14.0 0.0.0.255 any

!

ip nat inside source list LAN\_REMOTE interface G0/1 overload

end

!

remote#sh access-list

Extended IP access list LAN\_REMOTE

5 deny ip 192.168.14.0 0.0.0.255 192.168.59.0 0.0.0.255

10 permit ip 192.168.14.0 0.0.0.255 any (126 matches)

Extended IP access list crypto-acl

10 permit ip 192.168.14.0 0.0.0.255 192.168.59.0 0.0.0.255

**3- Configuration du vpn sur R1**

hostname R1

crypto isakmp policy 1

encr aes 256

authentication pre-share

group 5

lifetime 7200

!

crypto isakmp key cisco123 address 192.168.122.207

!

crypto ipsec transform-set to-remote-set esp-aes 256 esp-sha-hmac

!

crypto map cm-to-remote 1 ipsec-isakmp

set peer 192.168.122.207

set transform-set to-remote-set

match address crypto-acl

!

interface G0/1

crypto map cm-to-remote

!

ip access-list extended crypto-acl

permit ip 192.168.59.0 0.0.0.255 192.168.14.0 0.0.0.255

!

no ip access-list standard LAN\_NAT

ip access-list extended LAN\_NAT

deny ip 192.168.59.0 0.0.0.255 192.168.14.0 0.0.0.255

permit ip 192.168.59.0 0.0.0.255 any

permit ip 192.168.101.0 0.0.0.255 any

!

End

R1#sh access-list

Extended IP access list LAN\_NAT

10 deny ip 192.168.59.0 0.0.0.255 192.168.14.0 0.0.0.255

20 permit ip 192.168.59.0 0.0.0.255 any (2 matches)

30 permit ip 192.168.101.0 0.0.0.255 any (1 match)

Extended IP access list crypto-acl

10 permit ip 192.168.59.0 0.0.0.255 192.168.14.0 0.0.0.255

Extended IP access list crypto-aclexit

R1#show ip int brie

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0 192.168.59.1 YES NVRAM up up

GigabitEthernet0/1 192.168.122.118 YES DHCP up up

GigabitEthernet0/2 192.168.101.1 YES NVRAM up up

GigabitEthernet0/3 unassigned YES NVRAM administratively down down

NVI0 192.168.59.1 YES unset up up

**4- Adaptation du parfeu R1 :**

ip access-list extended ISAKMP\_IPSEC

permit udp any any eq isakmp

permit ahp any any

permit esp any any

permit udp any any eq non500-isakmp

class-map type inspect match-any vpn-class

match access-group name ISAKMP\_IPSEC

policy-map type inspect to-self-policy

class type inspect vpn-class

inspect

end

**5- Test de la connectivité de bout en bout**

remote#ping 192.168.59.1 source 192.168.14.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.59.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.14.1

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/5 ms

