!

! ============

! R2 - Site B

! ============

hostname R2

!

enable secret cisco

no ip domain-lookup

!

! --- OSPF ---

router ospf 1

network 172.0.0.0 0.255.255.255 area 0

network 10.0.0.0 0.255.255.255 area 0

network 192.168.1.0 0.0.0.3 area 0

log-adjacency-changes

!

interface gi0

description trunk vers sw l2

switchport mode trunk

switchport trunk allowed vlan 10,20,30,40,50,60,70

interface vlan 10

description VLAN 10 - ADMIN

ip address 172.32.10.254 255.255.255.0

ip nat inside

no shutdown

!

interface vlan 20

description VLAN 20 - PERSONNEL

ip address 172.32.20.254 255.255.255.0

ip nat inside

ip helper-address 172.32.10.10

ip access-group RESTRICT\_INTER\_VLAN in

no shutdown

!

interface vlan 30

description VLAN 30 - VIDEO

ip address 172.32.30.254 255.255.255.0

ip nat inside

ip helper-address 172.32.10.10

ip access-group RESTRICT\_INTER\_VLAN in

no shutdown

!

interface vlan 40

description VLAN 40 - PRODUCTION

ip address 172.32.40.254 255.255.255.0

ip nat inside

ip helper-address 172.32.10.10

ip access-group RESTRICT\_INTER\_VLAN in

no shutdown

!

interface vlan 50

description VLAN 50 - DMZ

ip address 172.32.50.254 255.255.255.0

ip nat inside

ip helper-address 172.32.10.10

ip access-group RESTRICT\_INTER\_VLAN in

no shutdown

!

interface vlan 60

description VLAN 60 - WIFI\_PERSONNEL

ip address 172.32.60.254 255.255.255.0

ip nat inside

ip helper-address 172.32.10.10

ip access-group RESTRICT\_INTER\_VLAN in

no shutdown

!

interface vlan 70

description VLAN 70 - WIFI\_INVITE

ip address 172.32.70.254 255.255.255.0

ip nat inside

ip helper-address 172.32.10.10

ip access-group RESTRICT\_INTER\_VLAN in

no shutdown

!

! --- Interface WAN ---

interface GigabitEthernet4

description Connexion WAN / Internet

ip address 10.7.2.1 255.0.0.0

ip nat outside

crypto map GRE-MAP

no shutdown

!

! --- Tunnel GRE over IPsec ---

interface Tunnel0

description Tunnel GRE vers R1 (Site A)

ip address 192.168.1.2 255.255.255.252

tunnel source GigabitEthernet4

tunnel destination 10.7.1.1

no shutdown

!

! --- Routage par défaut / Route statique vers site A ---

ip route 0.0.0.0 0.0.0.0 10.0.0.1

ip route 172.31.0.0 255.255.0.0 192.168.1.1

!

! ===========================================

! 1) ACL pour exclure le trafic inter-sites du NAT

! ===========================================

access-list 101 deny ip 172.31.0.0 0.0.255.255 172.32.0.0 0.0.255.255

access-list 101 deny ip 172.32.0.0 0.0.255.255 172.31.0.0 0.0.255.255

access-list 101 permit ip 172.32.0.0 0.0.255.255 any

!

! ===========================================

! 2) NAT overload

! ===========================================

ip nat inside source list 101 interface GigabitEthernet4 overload

!

! ===========================================

! 3) IPSec pour protéger le GRE

! ===========================================

crypto isakmp policy 10

encr aes

hash sha

authentication pre-share

group 2

!

crypto isakmp key secret\_key address 10.7.1.1

!

crypto ipsec transform-set GRE-IPSec esp-aes esp-sha-hmac

!

access-list 110 permit gre host 10.7.2.1 host 10.7.1.1

!

crypto map GRE-MAP 10 ipsec-isakmp

set peer 10.7.1.1

set transform-set GRE-IPSec

match address 110

!

ip access-list extended RESTRICT\_INTER\_VLAN

permit udp any any eq 67

permit udp any any eq 68

! Permettre tout le trafic depuis VLAN10 (ADMIN)

permit ip 172.32.10.0 0.0.0.255 any

! Bloquer le trafic entre les VLANs 20-70

deny ip 172.32.20.0 0.0.255.255 172.32.20.0 0.0.0.255

deny ip 172.32.20.0 0.0.255.255 172.32.30.0 0.0.0.255

deny ip 172.32.20.0 0.0.255.255 172.32.40.0 0.0.0.255

deny ip 172.32.20.0 0.0.255.255 172.32.50.0 0.0.0.255

deny ip 172.32.20.0 0.0.255.255 172.32.60.0 0.0.0.255

deny ip 172.32.20.0 0.0.255.255 172.32.70.0 0.0.0.255

deny ip 172.32.30.0 0.0.255.255 172.32.20.0 0.0.0.255

deny ip 172.32.30.0 0.0.255.255 172.32.30.0 0.0.0.255

deny ip 172.32.30.0 0.0.255.255 172.32.40.0 0.0.0.255

deny ip 172.32.30.0 0.0.255.255 172.32.50.0 0.0.0.255

deny ip 172.32.30.0 0.0.255.255 172.32.60.0 0.0.0.255

deny ip 172.32.30.0 0.0.255.255 172.32.70.0 0.0.0.255

deny ip 172.32.40.0 0.0.255.255 172.32.20.0 0.0.0.255

deny ip 172.32.40.0 0.0.255.255 172.32.30.0 0.0.0.255

deny ip 172.32.40.0 0.0.255.255 172.32.40.0 0.0.0.255

deny ip 172.32.40.0 0.0.255.255 172.32.50.0 0.0.0.255

deny ip 172.32.40.0 0.0.255.255 172.32.60.0 0.0.0.255

deny ip 172.32.40.0 0.0.255.255 172.32.70.0 0.0.0.255

deny ip 172.32.50.0 0.0.255.255 172.32.20.0 0.0.0.255

deny ip 172.32.50.0 0.0.255.255 172.32.30.0 0.0.0.255

deny ip 172.32.50.0 0.0.255.255 172.32.40.0 0.0.0.255

deny ip 172.32.50.0 0.0.255.255 172.32.50.0 0.0.0.255

deny ip 172.32.50.0 0.0.255.255 172.32.60.0 0.0.0.255

deny ip 172.32.50.0 0.0.255.255 172.32.70.0 0.0.0.255

deny ip 172.32.60.0 0.0.255.255 172.32.20.0 0.0.0.255

deny ip 172.32.60.0 0.0.255.255 172.32.30.0 0.0.0.255

deny ip 172.32.60.0 0.0.255.255 172.32.40.0 0.0.0.255

deny ip 172.32.60.0 0.0.255.255 172.32.50.0 0.0.0.255

deny ip 172.32.60.0 0.0.255.255 172.32.60.0 0.0.0.255

deny ip 172.32.60.0 0.0.255.255 172.32.70.0 0.0.0.255

deny ip 172.32.70.0 0.0.255.255 172.32.20.0 0.0.0.255

deny ip 172.32.70.0 0.0.255.255 172.32.30.0 0.0.0.255

deny ip 172.32.70.0 0.0.255.255 172.32.40.0 0.0.0.255

deny ip 172.32.70.0 0.0.255.255 172.32.50.0 0.0.0.255

deny ip 172.32.70.0 0.0.255.255 172.32.60.0 0.0.0.255

deny ip 172.32.70.0 0.0.255.255 172.32.70.0 0.0.0.255

! Permettre le reste (accès Internet et autres communications non bloquées)

permit ip any any