!

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

! 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

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

no shutdown

!

! --- Tunnel GRE over IPsec ---

interface Tunnel1

description Tunnel GRE vers R1 (Site A)

**ip address 50.50.50.2 255.255.255.0**

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 50.50.50.1**

!

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

R2#sh run

Building configuration...

Current configuration : 3260 bytes

!

! Last configuration change at 07:52:31 UTC Tue Jan 14 2025

!

version 15.8

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R2

!

boot-start-marker

boot-end-marker

!

!

enable secret 5 $1$Dsja$Zmgld2BaS5GDotbQFRlLN1

!

no aaa new-model

!

!

!

!

!

!

!

!

!

!

!

no ip domain lookup

ip domain name societe7.lan

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

!

!

license udi pid C927-4P sn FGL2348L2F5

license boot module c900 technology-package securityk9

!

!

vtp version 2

username remi privilege 15 secret 5 $1$F6uV$3ttxUZjFcLLxRxaa0Zvs90

!

redundancy

!

!

!

!

!

controller VDSL 0

!

!

!

!

!

!

!

!

!

!

!

interface Tunnel1

description Tunnel GRE vers R1 (Site A)

ip address 50.50.50.2 255.255.255.0

tunnel source GigabitEthernet4

tunnel destination 10.7.1.1

!

interface ATM0

no ip address

shutdown

no atm ilmi-keepalive

!

interface Ethernet0

no ip address

shutdown

!

interface GigabitEthernet0

description trunk vers sw l2

switchport mode trunk

no ip address

!

interface GigabitEthernet1

no ip address

!

interface GigabitEthernet2

no ip address

!

interface GigabitEthernet3

no ip address

!

interface GigabitEthernet4

description Connexion WAN / Internet

ip address 10.7.2.1 255.0.0.0

ip nat outside

ip virtual-reassembly in

duplex auto

speed auto

!

interface Vlan1

no ip address

!

interface Vlan10

description VLAN 10 - ADMIN

ip address 172.32.10.254 255.255.255.0

ip nat inside

ip virtual-reassembly in

!

interface Vlan20

description VLAN 20 - PERSONNEL

ip address 172.32.20.254 255.255.255.0

ip access-group RESTRICT\_INTER\_VLAN in

ip helper-address 172.32.10.10

ip nat inside

ip virtual-reassembly in

!

interface Vlan30

description VLAN 30 - VIDEO

ip address 172.32.30.254 255.255.255.0

ip access-group RESTRICT\_INTER\_VLAN in

ip helper-address 172.32.10.10

ip nat inside

ip virtual-reassembly in

!

interface Vlan40

description VLAN 40 - PRODUCTION

ip address 172.32.40.254 255.255.255.0

ip access-group RESTRICT\_INTER\_VLAN in

ip helper-address 172.32.10.10

ip nat inside

ip virtual-reassembly in

!

interface Vlan50

description VLAN 50 - DMZ

ip address 172.32.50.254 255.255.255.0

ip access-group RESTRICT\_INTER\_VLAN in

ip helper-address 172.32.10.10

ip nat inside

ip virtual-reassembly in

!

interface Vlan60

description VLAN 60 - WIFI\_PERSONNEL

ip address 172.32.60.254 255.255.255.0

ip access-group RESTRICT\_INTER\_VLAN in

ip helper-address 172.32.10.10

ip nat inside

ip virtual-reassembly in

!

interface Vlan70

description VLAN 70 - WIFI\_INVITE

ip address 172.32.70.254 255.255.255.0

ip access-group RESTRICT\_INTER\_VLAN in

ip helper-address 172.32.10.10

ip nat inside

ip virtual-reassembly in

!

router ospf 1

network 10.0.0.0 0.255.255.255 area 0

network 172.0.0.0 0.255.255.255 area 0

!

ip forward-protocol nd

no ip http server

no ip http secure-server

!

!

ip route 0.0.0.0 0.0.0.0 50.50.50.1

ip ssh version 2

!

!

!

tftp-server flash:/firmware/vadsl\_module\_img.bin

!

control-plane

!

!

line con 0

line 4

no activation-character

transport preferred none

transport input all

transport output all

stopbits 1

line vty 0 4

login local

transport input ssh

transport output ssh

!

scheduler allocate 20000 1000

!

end