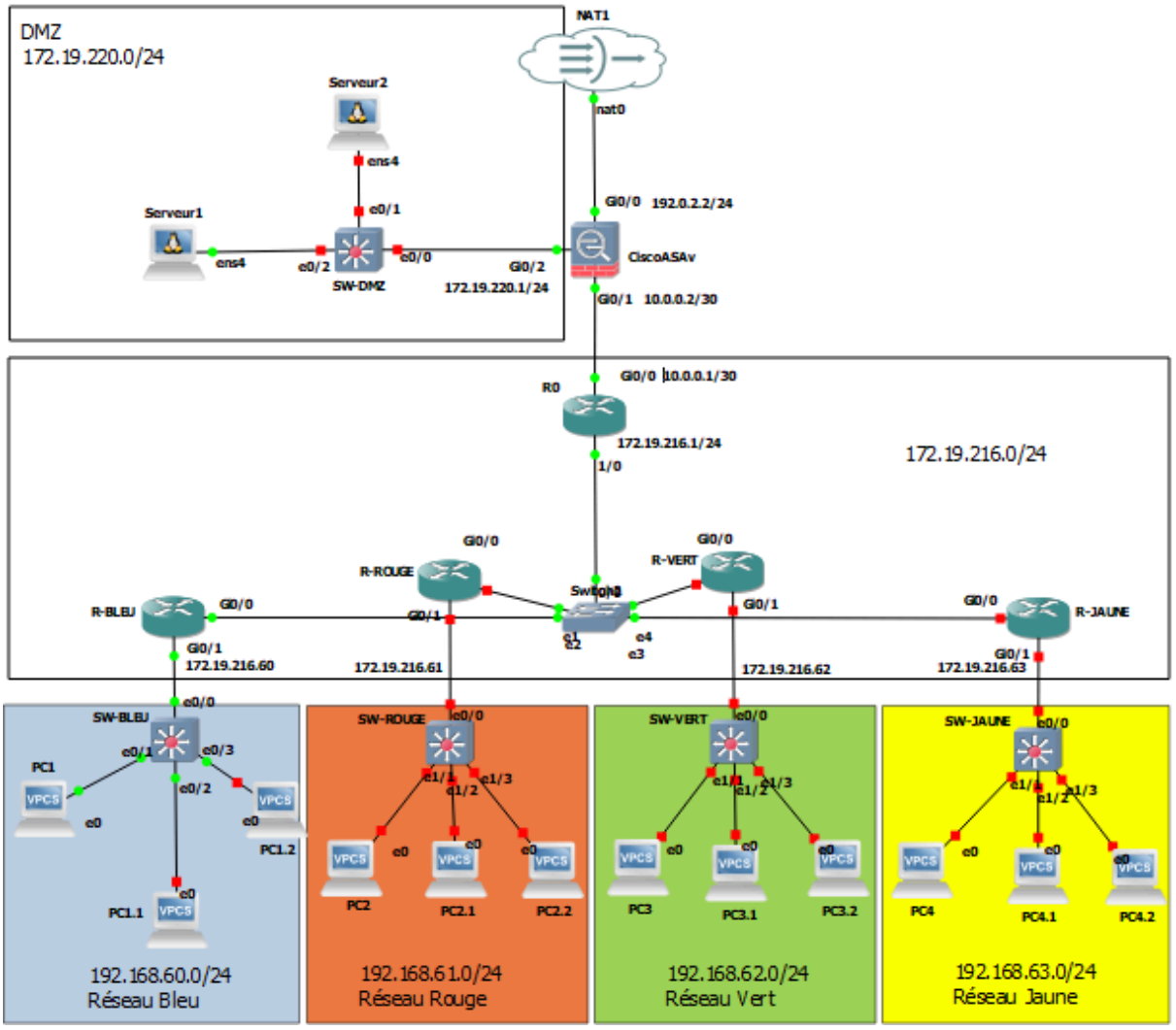
SAE 2.01

Document technique

I- Topologie :



II- Plan d'adressage :

Appliance	Interfaces	Adresse IP	Masque
R-BLEU	G0/0	172.19.216.60	255.255.255.0
	G0/1	192.168.60.1	255.255.255.0
R-ROUGE	G0/0	172.19.216.61	255.255.255.0
	G0/1	192.168.61.1	255.255.255.0
R-VERT	G0/0	172.19.216.62	255.255.255.0
	G0/1	192.168.62.1	255.255.255.0
R-JAUNE	G0/0	172.19.216.63	255.255.255.0
	G0/1	192.168.63.1	255.255.255.0
R-CENTRAL	G0/0	10.0.0.1	255.255.255.252
	G0/1	172.19.216.1	255.255.255.0
Pare-Feu (Cisco ASAv 9.8.1)	G0/0	192.0.2.2	255.255.255.0
	G0/1	10.0.0.2	255.255.255.252
	G0/2	172.19.220.1	255.255.255.0

III- Configuration :

Routeur :

R-CENTRAL :

```
config t
hostname R0
int G0/0
ip addr 10.0.0.1 255.255.255.252
no sh
exit
int G0/1
ip addr 172.19.216.1 255.255.255.0
no sh
exit
ip route 192.168.60.0 255.255.255.0 172.19.216.60
ip route 192.168.61.0 255.255.255.0 172.19.216.61
ip route 192.168.62.0 255.255.255.0 172.19.216.62
ip route 192.168.63.0 255.255.255.0 172.19.216.63
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip route 172.19.220.0 255.255.255.0 10.0.0.2
router ospf 1
network 172.19.216.1 0.0.0.0 area 0
end
wr
```

R-BLEU :

```
config t
hostname R1
int G0/0
ip addr 172.19.216.60 255.255.255.0
no sh
```

```
exit
int G0/1
ip addr 192.168.60.1 255.255.255.0
no sh
exit
ip route 0.0.0.0 0.0.0.0 172.19.216.1
ip route 10.0.0.0 255.255.255.252 172.19.216.1
ip route 172.19.220.0 255.255.255.0 172.19.216.1
router ospf 1
network 172.19.216.60 0.0.0.0 area 0

ip dhcp pool VLAN10
 network 192.168.60.0 255.255.255.0
 default-router 192.168.60.1
 dns-server 8.8.8.8
ip dhcp excluded-address 192.168.60.1 192.168.60.10
ip dhcp excluded-address 192.168.60.101 192.168.60.254
end
copy running-config startup-config
```

R-ROUGE :

```
config t
hostname R2
int G0/0
ip addr 172.19.216.61 255.255.255.0
no sh
exit
int G0/1
ip addr 192.168.61.1 255.255.255.0
no sh
exit
ip route 0.0.0.0 0.0.0.0 172.19.216.1
ip route 10.0.0.0 255.255.255.252 172.19.216.1
ip route 172.19.220.0 255.255.255.0 172.19.216.1
router ospf 1
network 172.19.216.61 0.0.0.0 area 0
ip dhcp pool VLAN20
 network 192.168.61.0 255.255.255.0
 default-router 192.168.61.1
 dns-server 8.8.8.8
```

```
ip dhcp excluded-address 192.168.61.1 192.168.61.10
ip dhcp excluded-address 192.168.61.101 192.168.61.254

end
copy running-config startup-config
```

R-VERT:

```
config t
hostname R3
int G0/0
ip addr 172.19.216.62 255.255.255.0
no sh
exit
int G0/1
ip addr 192.168.62.1 255.255.255.0
no sh
exit
ip route 0.0.0.0 0.0.0.0 172.19.216.1
ip route 10.0.0.0 255.255.255.252 172.19.216.1
ip route 172.19.220.0 255.255.255.0 172.19.216.1
router ospf 1
network 172.19.216.62 0.0.0.0 area 0
ip dhcp pool VLAN30
 network 192.168.62.0 255.255.255.0
 default-router 192.168.62.1
 dns-server 8.8.8.8
ip dhcp excluded-address 192.168.62.1 192.168.62.10
ip dhcp excluded-address 192.168.62.101 192.168.62.254

end
copy running-config startup-config
```

R-JAUNE :

```
config t
hostname R4
int G0/0
```

```
ip addr 172.19.216.63 255.255.255.0
no sh
exit
int G0/1
ip addr 192.168.63.1 255.255.255.0
no sh
exit
ip route 0.0.0.0 0.0.0.0 172.19.216.1
ip route 10.0.0.0 255.255.255.252 172.19.216.1
ip route 172.19.220.0 255.255.255.0 172.19.216.1
router ospf 1
network 172.19.216.63 0.0.0.0 area 0

ip dhcp pool VLAN40
 network 192.168.63.0 255.255.255.0
 default-router 192.168.63.1
 dns-server 8.8.8.8
ip dhcp excluded-address 192.168.63.1 192.168.63.10
ip dhcp excluded-address 192.168.63.101 192.168.63.254

end
copy running-config startup-config
```

Pare-Feu : Cisco ASAv 9.9.2

Activer et nommer les interfaces :

```
enable
conf t

interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address dhcp
 no shutdown

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.0.0.2 255.255.255.252
```

```
 no shutdown

interface GigabitEthernet0/2
 nameif dmz
 security-level 50
 ip address 172.19.220.1 255.255.255.0
 no shutdown
```

Définir les routes vers internet et les sous réseaux

```
route outside 0.0.0.0 0.0.0.0 192.0.122.1
route inside 192.168.60.0 255.255.255.0 10.0.0.1
route inside 192.168.61.0 255.255.255.0 10.0.0.1
route inside 192.168.62.0 255.255.255.0 10.0.0.1
route inside 192.168.63.0 255.255.255.0 10.0.0.1
```

Configuration NAT

```
object network obj-inside
 subnet 10.0.0.0 255.255.255.0
 nat (inside,outside) dynamic interface

object network obj-dmz
 subnet 172.19.220.0 255.255.255.252
 nat (dmz,outside) dynamic interobject network onj-insideface
 nat (inside,dmz) source static obj-inside obj-inside destination static    obj-dmz
obj-dmz no-proxy-arp
 nat (dmz,inside) source static obj-dmz obj-dmz destination static   obj-inside
obj-inside no-proxy-arp

object network obj-60
 subnet 192.168.60.0 255.255.255.0
 nat (inside,outside) dynamic interface

object network obj-61
 subnet 192.168.61.0 255.255.255.0
 nat (inside,outside) dynamic interface

object network obj-62
 subnet 192.168.62.0 255.255.255.0
 nat (inside,outside) dynamic interface
```

```
object network obj-63
 subnet 192.168.63.0 255.255.255.0
 nat (inside,outside) dynamic interface
```

Autoriser le trafic :

```
access-list OUTSIDE-IN extended permit ip any any
access-group OUTSIDE-IN in interface outside

access-list OUTSIDE-IN extended permit icmp any any
access-group OUTSIDE-IN in interface outside

access-list INSIDE_DMZ extended permit icmp any any
access-group INSIDE_DMZ in interface inside
```

Inspection ICMP pour les pings :

```
config t
class-map inspection_default
 match default-inspection-traffic
conf t
policy-map global_policy
 class inspection_default
  inspect icmp
  inspect dns
  inspect http
  inspect ftp
end
wr
```

SW-LAN :

Configuration de VLAN dans le SW-LAN

```
vlan 10
name R-BLEU
vlan 20
name R-ROUGE
vlan 30
name R-VERT
vlan 40
name R-JAUNE


int e1/0
switchport mode access
switchport access vlan 10
int e1/1
switchport mode access
switchport access vlan 20
int e1/2
switchport mode access
switchport access vlan 30
int e1/3
switchport mode access
switchport access vlan 40


end
copy running-config startup-config
```

IV- Fonctionnement de la topologie :

Ping du serveur DNS de google depuis le pare feu :

```
ciscoasa#
ciscoasa# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 90/124/150 ms
ciscoasa#
```

Ping du serveur DNS de google depuis un serveur de la DMZ :

```
debian@debian:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=139 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=127 time=64.6 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=127 time=65.9 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=127 time=81.6 ms
^C
--- 8.8.8.8 ping statistics ---
9 packets transmitted, 4 received, 55.5556% packet loss, time 8120ms
rtt min/avg/max/mdev = 64.571/87.797/139.116/30.378 ms
debian@debian:~$
```

Ping du serveur DNS de google depuis un PCs de mon LAN :

```
PC1.1> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=125 time=99.809 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=125 time=72.902 ms
^C
PC1.1>
```

Fonctionnement du DHCP sur les PCs du LAN :

```
PC1.1> dhcp
DDORA IP 192.168.60.11/24 GW 192.168.60.1
```

Configuration des VLANs :

```
SW-LAN#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/3, Et2/0, Et2/1
                                                Et2/2, Et2/3, Et3/0, Et3/1
                                                Et3/2, Et3/3
10   R-BLEU                           active    Et0/1, Et1/0
20   R-ROUGE                          active    Et0/2, Et1/1
30   R-VERT                           active    Et1/2
40   R-JAUNE                          active    Et1/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```