

Liaison

Switch_1

```
e0/0 vers e0/0 du Switch_L3_4
e0/1 vers e0/1 du Switch_L3_4
e0/2 vers e0/0 du Switch_L3_5
e0/3 vers e0/1 du Switch_L3_5
e1/0 vers VPC en 10.1.10.1/24
e1/1 vers VPC en 10.1.20.1/24
e1/2 vers VPC en 10.1.60.1/24
```

Switch_2

```
e0/0 vers e0/2 du Switch_L3_4
e0/1 vers e0/3 du Switch_L3_4
e0/2 vers e0/2 du Switch_L3_5
e0/3 vers e0/3 du Switch_L3_5
e1/0 vers VPC en 10.1.70.1/24
e1/1 vers VPC en 10.1.80.1/24
```

Switch_3

```
e0/0 vers e1/0 du Switch_L3_4
e0/1 vers e1/1 du Switch_L3_4
e0/2 vers e1/0 du Switch_L3_5
e0/3 vers e1/1 du Switch_L3_5
e1/0 vers VPC en 10.1.90.1/24
e1/1 vers VPC en 10.1.100.1/24
```

Switch_L3_4

```
e0/0 vers e0/0 du Switch_1
e0/1 vers e0/1 du Switch_1
e0/2 vers e0/0 du Switch_2
e0/3 vers e0/1 du Switch_2
e1/0 vers e0/0 du Switch_3
e1/1 vers e0/1 du Switch_3
e1/2 vers port2 du Firewall_8
e1/3 vers port4 du Firewall_9
```

Switch_L3_5

```
e0/0 vers e0/2 du Switch_1
e0/1 vers e0/3 du Switch_1
e0/2 vers e0/2 du Switch_2
e0/3 vers e0/3 du Switch_2
e1/0 vers e0/2 du Switch_3
e1/1 vers e0/3 du Switch_3
e1/2 vers port2 du Firewall_9
e1/3 vers port4 du Firewall_8
```

```
Firewall_8
port2 vers e1/2 du Switch_L3_4
port4 vers e1/3 du Switch_L3_5
port3 vers port3 du Firewall_9 (Ha-Sync)
port1 vers VMnet0 (Internet)
```

```
Firewall_9
port2 vers e1/2 du Switch_L3_5
port4 vers e1/3 du Switch_L3_4
port3 vers port3 du Firewall_8 (Ha-Sync)
port1 vers VMnet0 (Internet)
```

```
Internet(VMnet0)
Internet vers port1 du Firewall_8
Internet vers port1 du Firewall_9
```

Switch_1 En bas a gauche

```
enable
configure terminal
hostname SW1

# VTP client
vtp domain PRINTCORP
vtp mode client
vtp password SecureVTP

# IP de management
interface vlan 200
  ip address 10.1.200.1 255.255.255.0
  no shutdown
exit

ip route 0.0.0.0 0.0.0.0 10.1.200.254
ip routing

# Trunks LACP
interface range e0/0-1
  channel-group 1 mode active
exit

interface Port-channel1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan all
exit
```

```
interface range e0/2-3
  channel-group 2 mode active
exit

interface Port-channel2
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan all
exit

# Ports d'accès
interface e1/0
  switchport mode access
  switchport access vlan 10

interface e1/1
  switchport mode access
  switchport access vlan 20

interface e1/2
  switchport mode access
  switchport access vlan 60
exit

snmp-server group PrintNet_SNMP v3 priv
snmp-server user zabbix PrintNet_SNMP v3 auth sha SNMPPASSWORD123 priv aes 128 M
snmp-server host 10.1.100.20 version 3 priv zabbix
snmp-server enable traps

end
write memory
```

Switch_2 En bas au milieu

```
enable
configure terminal
hostname SW2

# Configuration VTP en mode client
vtp domain PRINTCORP
vtp mode client
vtp password SecureVTP
```

```

interface vlan 200
  ip address 10.1.200.2 255.255.255.0
  no shutdown
exit

ip route 0.0.0.0 0.0.0.0 10.1.200.254
ip routing

# Activation de LACP et configuration des trunks
interface range e0/0-1
  channel-group 1 mode active
exit

interface Port-channel1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan all
exit

interface range e0/2-3
  channel-group 2 mode active
exit

interface Port-channel2
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan all
exit

# Attribution des VLANs aux ports d'accès
interface e1/0
  switchport mode access
  switchport access vlan 70

interface e1/1
  switchport mode access
  switchport access vlan 80
exit

snmp-server group PrintNet_SNMP v3 priv
snmp-server user zabbix PrintNet_SNMP v3 auth sha SNMPPASSWORD123 priv aes 128 M
snmp-server host 10.1.100.20 version 3 priv zabbix
snmp-server enable traps

end
write memory

```

Switch 3 En bas a droite

```
enable
configure terminal
hostname SW3

# Configuration VTP en mode client
vtp domain PRINTCORP
vtp mode client
vtp password SecureVTP

interface vlan 200
  ip address 10.1.200.3 255.255.255.0
  no shutdown
exit

ip route 0.0.0.0 0.0.0.0 10.1.200.254
ip routing

# Activation de LACP et configuration des trunks correctement
interface range e0/0-1
  channel-group 1 mode active
exit

interface Port-channel1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan all
exit

interface range e0/2-3
  channel-group 2 mode active
exit

interface Port-channel2
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan all
exit

# Attribution des VLANs aux ports d'accès
interface e1/0
  switchport mode access
  switchport access vlan 90

interface e1/1
  switchport mode access
  switchport access vlan 100

interface e1/2
  switchport mode access
```

```
switchport access vlan 100

interface e1/3
switchport mode access
switchport access vlan 100

interface e2/0
switchport mode access
switchport access vlan 100
exit

snmp-server group PrintNet_SNMP v3 priv
snmp-server user zabbix PrintNet_SNMP v3 auth sha SNMPPASSWORD123 priv aes 128 M
snmp-server host 10.1.100.20 version 3 priv zabbix
snmp-server enable traps

end
write memory
```

Switch_L3_4 Milieu Gauche VTP SERVER

```
enable
configure terminal
hostname SW_L3_4
vtp domain PRINTCORP
vtp mode server
vtp password SecureVTP
vlan 10
name Administration
vlan 20
name IT-Supervision
vlan 30
name Production-Logistique
vlan 40
name Commercial-Marketing
vlan 50
name Support-Technique
vlan 60
name Invites
vlan 70
name VoIP
vlan 80
name Wifi-Corporate
vlan 90
name Wifi-Invites
vlan 100
name Serveurs-Stockage
```

```
vlan 200
  name Management
exit
interface vlan 10
  ip address 10.1.10.253 255.255.255.0
  standby 10 ip 10.1.10.254
  standby 10 priority 110
  standby 10 preempt
  ip helper-address 10.1.100.10
  ip helper-address 10.1.100.40
  no shutdown
interface vlan 20
  ip address 10.1.20.253 255.255.255.0
  standby 20 ip 10.1.20.254
  standby 20 priority 110
  standby 20 preempt
  ip helper-address 10.1.100.10
  ip helper-address 10.1.100.40
  no shutdown
interface vlan 30
  ip address 10.1.30.253 255.255.255.0
  standby 30 ip 10.1.30.254
  standby 30 priority 110
  standby 30 preempt
  ip helper-address 10.1.100.10
  ip helper-address 10.1.100.40
  no shutdown
interface vlan 40
  ip address 10.1.40.253 255.255.255.0
  standby 40 ip 10.1.40.254
  standby 40 priority 110
  standby 40 preempt
  ip helper-address 10.1.100.10
  ip helper-address 10.1.100.40
  no shutdown
interface vlan 50
  ip address 10.1.50.253 255.255.255.0
  standby 50 ip 10.1.50.254
  standby 50 priority 110
  standby 50 preempt
  ip helper-address 10.1.100.10
  ip helper-address 10.1.100.40
  no shutdown
interface vlan 60
  ip address 10.1.60.253 255.255.255.0
  standby 60 ip 10.1.60.254
  standby 60 priority 110
  standby 60 preempt
  ip helper-address 10.1.100.10
  ip helper-address 10.1.100.40
```

```
no shutdown
interface vlan 70
ip address 10.1.70.253 255.255.255.0
standby 70 ip 10.1.70.254
standby 70 priority 110
standby 70 preempt
ip helper-address 10.1.100.10
ip helper-address 10.1.100.40
no shutdown
interface vlan 80
ip address 10.1.80.253 255.255.255.0
standby 80 ip 10.1.80.254
standby 80 priority 110
standby 80 preempt
ip helper-address 10.1.100.10
ip helper-address 10.1.100.40
no shutdown
interface vlan 90
ip address 10.1.90.253 255.255.255.0
standby 90 ip 10.1.90.254
standby 90 priority 110
standby 90 preempt
ip helper-address 10.1.100.10
ip helper-address 10.1.100.40
no shutdown
interface vlan 100
ip address 10.1.100.253 255.255.255.0
standby 100 ip 10.1.100.254
standby 100 priority 110
standby 100 preempt
no shutdown
interface vlan 200
ip address 10.1.200.4 255.255.255.0
standby 200 ip 10.1.200.254
standby 200 priority 110
standby 200 preempt
no shutdown
interface range e0/0-1
channel-group 1 mode active
exit
interface Port-channel1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan all
exit
interface range e0/2-3
channel-group 2 mode active
exit
interface Port-channel2
switchport trunk encapsulation dot1q
```



```
switchport mode trunk
switchport trunk allowed vlan all
exit
interface range e1/0-1
channel-group 3 mode active
exit
interface Port-channel3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan all
exit
interface e1/2
no switchport
ip address 10.10.10.1 255.255.255.248
no shutdown
interface e1/3
no switchport
ip address 10.10.20.1 255.255.255.248
no shutdown
router ospf 1
network 10.1.10.0 0.0.0.255 area 0
network 10.1.20.0 0.0.0.255 area 0
network 10.1.30.0 0.0.0.255 area 0
network 10.1.40.0 0.0.0.255 area 0
network 10.1.50.0 0.0.0.255 area 0
network 10.1.60.0 0.0.0.255 area 0
network 10.1.70.0 0.0.0.255 area 0
network 10.1.80.0 0.0.0.255 area 0
network 10.1.90.0 0.0.0.255 area 0
network 10.1.100.0 0.0.0.255 area 0
network 10.1.200.0 0.0.0.255 area 0
network 10.10.10.0 0.0.0.7 area 0
network 10.10.20.0 0.0.0.7 area 0
passive-interface Port-channel1
passive-interface Port-channel2
passive-interface Port-channel3
ip routing

ip access-list extended BLOCK_GUEST_TO_SERVER
permit udp any eq bootpc any eq bootps
deny ip 10.1.90.0 0.0.0.255 10.1.100.0 0.0.0.255
deny ip 10.1.60.0 0.0.0.255 10.1.100.0 0.0.0.255
permit ip any any
exit

ip access-list extended BLOCK_PROD_INTERNET
deny ip 10.1.30.0 0.0.0.255 10.0.0.0 0.0.0.255
permit ip any any
exit
```

```

interface vlan 30
  ip access-group BLOCK_PROD_INTERNET in

interface vlan 90
  ip access-group BLOCK_GUEST_TO_SERVER in
exit

interface vlan 60
  ip access-group BLOCK_GUEST_TO_SERVER in
exit

snmp-server group PrintNet_SNMP v3 priv
snmp-server user zabbix PrintNet_SNMP v3 auth sha SNMPPASSWORD123 priv aes 128 M
snmp-server host 10.1.100.20 version 3 priv zabbix
snmp-server enable traps

end
wr

```

Switch_L3_5 Milieu Droite

```

enable
configure terminal
hostname SW_L3_5
#Configuration VTP en mode client
vtp domain PRINTCORP
vtp mode client
vtp password SecureVTP
#Configuration des VLANs avec HSRP (backup)
interface vlan 10
ip address 10.1.10.252 255.255.255.0
standby 10 ip 10.1.10.254
standby 10 priority 100
ip helper-address 10.1.100.10
ip helper-address 10.1.100.40
no shutdown
interface vlan 20
ip address 10.1.20.252 255.255.255.0
standby 20 ip 10.1.20.254
standby 20 priority 100
ip helper-address 10.1.100.10
ip helper-address 10.1.100.40
no shutdown
interface vlan 30
ip address 10.1.30.252 255.255.255.0
standby 30 ip 10.1.30.254
standby 30 priority 100

```

```
ip helper-address 10.1.100.10
ip helper-address 10.1.100.40
no shutdown
interface vlan 40
ip address 10.1.40.252 255.255.255.0
standby 40 ip 10.1.40.254
standby 40 priority 100
ip helper-address 10.1.100.10
ip helper-address 10.1.100.40
no shutdown
interface vlan 50
ip address 10.1.50.252 255.255.255.0
standby 50 ip 10.1.50.254
standby 50 priority 100
ip helper-address 10.1.100.10
ip helper-address 10.1.100.40
no shutdown
interface vlan 60
ip address 10.1.60.252 255.255.255.0
standby 60 ip 10.1.60.254
standby 60 priority 100
ip helper-address 10.1.100.10
ip helper-address 10.1.100.40
no shutdown
interface vlan 70
ip address 10.1.70.252 255.255.255.0
standby 70 ip 10.1.70.254
standby 70 priority 100
ip helper-address 10.1.100.10
ip helper-address 10.1.100.40
no shutdown
interface vlan 80
ip address 10.1.80.252 255.255.255.0
standby 80 ip 10.1.80.254
standby 80 priority 100
ip helper-address 10.1.100.10
ip helper-address 10.1.100.40
no shutdown
interface vlan 90
ip address 10.1.90.252 255.255.255.0
standby 90 ip 10.1.90.254
standby 90 priority 100
ip helper-address 10.1.100.10
ip helper-address 10.1.100.40
no shutdown
interface vlan 100
ip address 10.1.100.252 255.255.255.0
standby 100 ip 10.1.100.254
standby 100 priority 100
no shutdown
```

```
interface vlan 200
  ip address 10.1.200.5 255.255.255.0
  standby 200 ip 10.1.200.254
  standby 200 priority 100
  no shutdown
#Activation de LACP et Trunks vers les autres Switchs
interface range e0/0-1
  channel-group 1 mode active
exit
interface Port-channel1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan all
exit
interface range e0/2-3
  channel-group 2 mode active
exit
interface Port-channel2
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan all
exit
interface range e1/0-1
  channel-group 3 mode active
exit
interface Port-channel3
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan all
exit
interface e1/2
  no sw
  ip address 10.10.10.2 255.255.255.248
  no shutdown
  exit
interface e1/3
  no sw
  ip address 10.10.20.2 255.255.255.248
  no shutdown
  exit
router ospf 1
  network 10.1.10.0 0.0.0.255 area 0
  network 10.1.20.0 0.0.0.255 area 0
  network 10.1.30.0 0.0.0.255 area 0
  network 10.1.40.0 0.0.0.255 area 0
  network 10.1.50.0 0.0.0.255 area 0
  network 10.1.60.0 0.0.0.255 area 0
  network 10.1.70.0 0.0.0.255 area 0
  network 10.1.80.0 0.0.0.255 area 0
  network 10.1.90.0 0.0.0.255 area 0
```

```
network 10.1.100.0 0.0.0.255 area 0
network 10.1.200.0 0.0.0.255 area 0
network 10.10.10.0 0.0.0.7 area 0
network 10.10.20.0 0.0.0.7 area 0
passive-interface Port-channel1
passive-interface Port-channel2
passive-interface Port-channel3
ip routing

ip access-list extended BLOCK_GUEST_TO_SERVER
  permit udp any eq bootpc any eq bootps
  deny ip 10.1.90.0 0.0.0.255 10.1.100.0 0.0.0.255
  deny ip 10.1.60.0 0.0.0.255 10.1.100.0 0.0.0.255
  permit ip any any
exit

ip access-list extended BLOCK_PROD_INTERNET
  deny ip 10.1.30.0 0.0.0.255 10.0.0.0 0.0.0.255
  permit ip any any
exit

interface vlan 30
  ip access-group BLOCK_PROD_INTERNET in

interface vlan 90
  ip access-group BLOCK_GUEST_TO_SERVER in
exit

interface vlan 60
  ip access-group BLOCK_GUEST_TO_SERVER in
exit

snmp-server group PrintNet_SNMP v3 priv
snmp-server user zabbix PrintNet_SNMP v3 auth sha SNMPPASSWORD123 priv aes 128 M
snmp-server host 10.1.100.20 version 3 priv zabbix
snmp-server enable traps

end
wr
```

Firewall_8 Haut gauche

FortiGate-VM64-KVM

```
config system global
set hostname Firewall_8
set admin-port 80
set admin-sport 4443
end

config system ha
set group-name "FortiGate_HA"
set mode a-p
set password "SecureHApass"
set hbdev "port3" 100
set priority 200
set session-pickup enable
set override enable
set monitor "port2" "port4" "port1"
end
```

```
config system dns
set primary 10.1.100.10
set secondary 8.8.8.8
end
```

```
config system snmp community
edit 1
set name "PrintNet_SNMP"
config hosts
edit 1
set ip 10.1.100.20 255.255.255.255
next
end
set events cpu-high mem-low log-full
set status enable
next
end
```

```
config system global
set timezone 26
end
```

```
config system interface
edit "port2"
set vdom "root"
set ip 10.10.10.3 255.255.255.248
set allowaccess ping http https ssh snmp fgfm
next
edit "port4"
set vdom "root"
```

```
set ip 10.10.20.3 255.255.255.248
set allowaccess ping http https ssh snmp fgfm
next
edit "port3"
set alias "HA-Sync"
next
edit "port1"
set mode dhcp
set allowaccess ping ssh fgfm
next
edit "port5"
set vdom "root"
set ip 192.168.99.1 255.255.255.0
set allowaccess ping http https ssh fgfm
set type physical
set alias "TEST-PC-DIRECT"
set role lan
next
end
```

```
config router static
edit 2
set dst 10.1.100.0 255.255.255.0
set gateway 10.1.100.254
set device "port2"
set distance 10
next
edit 3
set dst 10.1.100.0 255.255.255.0
set gateway 10.1.100.254
set device "port4"
set distance 20
next
end
```

```
config router ospf
set router-id 10.10.10.254
set default-information-originate enable
config area
edit 0.0.0.0
next
end
config network
edit 1
set prefix 10.10.10.0 255.255.255.248
set area 0.0.0.0
next
edit 2
```

```
set prefix 10.10.20.0 255.255.255.248
set area 0.0.0.0
next
edit 3
set prefix 10.0.0.0 255.255.255.0
set area 0.0.0.0
next
end
end

config router static
edit 1
set dst 0.0.0.0 0.0.0.0
set gateway 10.0.0.254
set device "port1"
next
end

config firewall address
edit "Zabbix_Server"
set subnet 10.1.100.20 255.255.255.255
next
end

config firewall policy
edit 100
set name "Allow_SNMP_to_Forti"
set srcintf "port2" "port4"
set dstintf "any"
set srcaddr "Zabbix_Server"
set dstaddr "all"
set action accept
set schedule "always"
set service "SNMP"
set logtraffic all
next
end

config webfilter profile
edit "Block_Unwanted_Sites"
config ftgd-wf
config filters
#Drugs
edit 1
set category 1
set action block
next
#Hacking
edit 2
```



```
set category 3
set action block
next
#Illegal or unethical activities
edit 3
set category 4
set action block
next
#Hate or discriminatory content
edit 4
set category 5
set action block
next
#Explicit violence
edit 5
set category 6
set action block
next
#Adult content (forums, images)
edit 6
set category 8
set action block
next
#Gambling
edit 7
set category 11
set action block
next
#Erotic content
edit 8
set category 13
set action block
next
#Pornographic content
edit 9
set category 14
set action block
next
#Weapon sales
edit 10
set category 16
set action block
next
#File sharing / online storage
edit 11
set category 24
set action block
next
#Streaming audio / video
edit 12
```

```
set category 25
set action block
next
#Social networks
edit 13
set category 37
set action block
next
#VPNs and proxies
edit 14
set category 59
set action block
next
#Web chat
edit 15
set category 68
set action block
next
#Instant messaging
edit 16
set category 69
set action block
next
#P2P sharing
edit 17
set category 72
set action block
next
end
end
next
end
```

```
config ips sensor
edit "Detect_Scans"
config entries
edit 1
set location client
set log enable
set action block
set severity high
next
end
next
end
```

```
config firewall policy
edit 2
set name "Allow_Internal_to_Internet"
set srcintf "port2" "port4"
set dstintf "port1"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set nat enable
set logtraffic all
set utm-status enable
set webfilter-profile "Block_Unwanted_Sites"
set ips-sensor "Detect_Scans"
next
end
```

```
config firewall policy
edit 1
set name "Deny_All"
set srcintf "any"
set dstintf "any"
set srcaddr "all"
set dstaddr "all"
set action deny
set schedule "always"
set service "ALL"
set logtraffic all
next
end
```

Firewall_9 Haut Droite

FortiGate-VM64-KVM

```
config system global
set hostname Firewall_9
set admin-port 80
set admin-sport 4443
end

config system ha
set group-name "FortiGate_HA"
set mode a-p
set password "SecureHApass"
```

```
set hbdev "port3" 100
set priority 100
set session-pickup enable
set override enable
set monitor "port2" "port4" "port1"
end
```