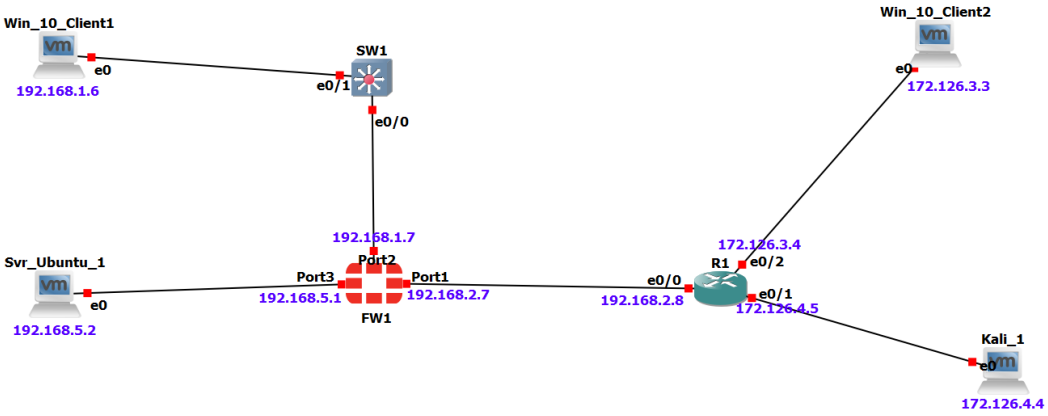
# LAB 1 D'INVESTIGATION NUMÉRIQUE

Auteur : MVONGO MEDJO ORDI FAREL



# TABLEAU D'ADRESSAGE

| Équipements | INTERFACES | Adresses IP | Masques |
|---|---|---|---|
| 3*R1 | e0/0 | 192.168.2.8 | 255.255.255.0 |
| | e0/1 | 172.126.4.5 | 255.255.255.0 |
| | e0/2 | 172.126.3.4 | 255.255.255.0 |
| 3*FW1 | Port1 | 192.168.2.7 | 255.255.255.0 |
| | Port2 | 192.168.1.7 | 255.255.255.0 |
| | Port3 | 192.168.5.1 | 255.255.255.0 |

# Configuration des machines

Rassurez-vous que tous vos machines ont ces configurations :

## Win_10_Client1 :

— IP : 192.168.1.6

— Masque : 255.255.255.0

— Passerelle : 192.168.1.7 (FW1)

### Win_10_Client1 (PowerShell en admin) :

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.1.6 -
   PrefixLength 24 -DefaultGateway 192.168.1.7
```

## Win_10_Client2 :

— IP : 172.126.3.3

— Masque : 255.255.255.0

— Passerelle : 172.126.3.4 (R1)

### Win_10_Client2 :

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 172.126.3.3 -
   PrefixLength 24 -DefaultGateway 172.126.3.4
```

## Kali_1 :

— IP : 172.126.4.4

— Masque : 255.255.255.0

— Passerelle : 172.126.4.5 (R1)

**Kali_1 (terminal) :**

```
sudo ip addr add 172.126.4.4/24 dev eth0
sudo ip route add default via 172.126.4.5
```

## Svr_Ubuntu_1 :

- IP : 192.168.5.2
- Masque : 255.255.255.0
- Passerelle : 192.168.5.1 (FW1)

**Svr_Ubuntu_1 (terminal) :**

```
sudo ip addr add 192.168.5.2/24 dev ens33
sudo ip route add default via 192.168.5.1
```

Une fois l'adressage effectué, on passe à la configuration du routeur :

# Configuration de R1 (Routeur)

```
enable
configure terminal
interface Ethernet0/0
ip address 192.168.2.8 255.255.255.0
no shutdown
exit
interface Ethernet0/1
ip address 172.126.4.5 255.255.255.0
no shutdown
exit
interface Ethernet0/2
ip address 172.126.3.4 255.255.255.0
no shutdown
exit
end
write memory
```

# Configuration des routes statiques sur R1 (Routeur Cisco)

```
enable
configure terminal
# Route vers le r seau 192.168.1.0/24 via FW1 (192.168.2.7)
ip route 192.168.1.0 255.255.255.0 192.168.2.7
# Route vers le r seau 192.168.5.0/24 via FW1 (192.168.2.7)
ip route 192.168.5.0 255.255.255.0 192.168.2.7
# Routes pour les autres r seaux (si n cessaire)
# ip route 0.0.0.0 0.0.0.0 192.168.2.7 # Route par d faut si
    n cessaire
end
write memory
```

### Vérification sur R1 :

```
show ip route
show running-config | include ip route
```

## Configuration de FW1 (FortiGate) via CLI

```
config system interface
edit "port1"
set vdom "root"
set ip 192.168.2.7 255.255.255.0
set allowaccess ping https ssh http
set type physical
next
edit "port2"
set vdom "root"
set ip 192.168.1.7 255.255.255.0
set allowaccess ping https ssh http
set type physical
next
edit "port3"
set vdom "root"
set ip 192.168.5.1 255.255.255.0
set allowaccess ping https ssh http
set type physical
next
end
```

## Configuration des politiques de base (règles de firewall)

```
config firewall policy
edit 1
set name "LAN-to-DMZ"
set srcintf "port2"
set dstintf "port3"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set nat enable
next
edit 2
set name "DMZ-to-LAN"
set srcintf "port3"
set dstintf "port2"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
next
edit 3
```

```
set name "LAN-to-WAN"
set srcintf "port2"
set dstintf "port1"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set nat enable
next
end
```

## Configuration des routes statiques (si nécessaire)

```
config router static
edit 1
set gateway 192.168.2.8
set device "port1"
next
edit 2
set gateway 172.126.3.4
set device "port1"
next
end
```

## Sauvegarde de la configuration

```
execute backup config flash
```

## Vérification de la configuration

```
# V rifier les interfaces
get system interface physical
# V rifier les adresses IP
diagnose ip address list
# V rifier les politiques
get firewall policy list
# V rifier la table de routage
get router info routing-table all
```

## Test de connectivité depuis le FortiGate

```
# Tester la connectivit  vers R1
execute ping 192.168.2.8
# Tester la connectivit  vers le client
execute ping 192.168.1.6
# Tester la connectivit  vers le serveur
execute ping 192.168.5.2
```

## Configuration des routes statiques sur FortiGate (FW1)

```
config router static
# Route vers le r seau 172.126.3.0/24 via R1 (192.168.2.8)
edit 1
set dst 172.126.3.0 255.255.255.0
set gateway 192.168.2.8
set device "port1"
next
# Route vers le r seau 172.126.4.0/24 via R1 (192.168.2.8)
edit 2
set dst 172.126.4.0 255.255.255.0
set gateway 192.168.2.8
set device "port1"
next
# Route par d faut vers R1 (optionnel - si acc s Internet via R1)
edit 3
set dst 0.0.0.0 0.0.0.0
set gateway 192.168.2.8
set device "port1"
next
end
```

## Vérification des routes sur FortiGate

```
# V rifier la table de routage
get router info routing-table all
# V rifier les routes statiques configur es
show router static
# Tester la connectivit
execute ping 172.126.3.3
execute ping 172.126.4.4
execute ping 172.126.3.4
```

## Tableau récapitulatif des routes

| Équipement | Réseau Destination | Masque | Passerelle | Interface |
|---|---|---|---|---|
| **R1** | 192.168.1.0 | 255.255.255.0 | 192.168.2.7 | e0/0 |
| **R1** | 192.168.5.0 | 255.255.255.0 | 192.168.2.7 | e0/0 |
| **FW1** | 172.126.3.0 | 255.255.255.0 | 192.168.2.8 | port1 |
| **FW1** | 172.126.4.0 | 255.255.255.0 | 192.168.2.8 | port1 |

## Tests de connectivité après configuration

### Depuis Win_10_Client1 :

```
ping 192.168.5.2 # Vers Svr_Ubuntu_1
ping 172.126.3.3 # Vers Win_10_Client2
```

### Depuis Kali_1 :

```
ping 192.168.1.6 # Vers Win_10_Client1
ping 192.168.5.2 # Vers Svr_Ubuntu_1
```

Ces routes statiques permettront la communication entre tous les réseaux de la topologie.

Voici la configuration des **services** pour le port **TCP 8000** et **ICMP** sur le FortiGate :

## Création des services sur FortiGate (FW1)

```
config firewall service custom
# Service pour l'application web (TCP 8000)
edit "Web-App-TCP8000"
set category "Custom"
set tcp-portrange 8000
set comment "Service pour l'application web sur Svr_Ubuntu_1"
next
# Service ICMP (pour les tests ping)
edit "ICMP"
set category "Network Services"
set protocol ICMP
set icmptype 8 # Echo Request (ping)
set comment "Service ICMP pour tests de connectivit "
next
end
```

## Mise à jour des politiques firewall pour autoriser le trafic

```
config firewall policy
# Autoriser l'acc s    l'application web depuis le LAN (port2) vers
   DMZ (port3)
edit 4
set name "LAN-to-DMZ-WebApp"
set srcintf "port2"
set dstintf "port3"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "Web-App-TCP8000" "ICMP"
set nat disable
next
# Autoriser l'acc s    l'application web depuis les r seaux derri re
    R1 vers DMZ
edit 5
set name "Remote-to-DMZ-WebApp"
set srcintf "port1"
set dstintf "port3"
set srcaddr "all"
set dstaddr "all"
set action accept
```

```
set schedule "always"
set service "Web-App-TCP8000" "ICMP"
set nat disable
next
end
```

# Configuration optionnelle - VIP (si NAT nécessaire)

Si vous avez besoin de NAT pour exposer l'application web :

```
config firewall vip
edit "Web-App-VIP"
set extintf "port1"
set portforward enable
set extip 192.168.2.7
set mappedip "192.168.5.2"
set extport 8000
set mappedport 8000
set protocol tcp
next
end
# Ajouter une politique pour le VIP
config firewall policy
edit 6
set name "External-to-WebApp"
set srcintf "port1"
set dstintf "port3"
set srcaddr "all"
set dstaddr "Web-App-VIP"
set action accept
set schedule "always"
set service "Web-App-TCP8000"
next
end
```

# Vérification des services et politiques

```
# V rifier les services cr   s
show firewall service custom
# V rifier les politiques
show firewall policy
# V rifier les VIP (si configur s)
show firewall vip
```

# Tests de connectivité

## Depuis Win_10_Client1 (192.168.1.6) :

```
# Test ICMP
ping 192.168.5.2
```

```
# Test application web (si un serveur web coute sur le port 8000)
telnet 192.168.5.2 8000
# Ou avec curl si disponible
curl http://192.168.5.2:8000
```

### Depuis Kali_1 (172.126.4.4) :

```
# Test ICMP
ping 192.168.5.2
# Test application web
nc -zv 192.168.5.2 8000
# Ou
curl http://192.168.5.2:8000
```

## Récapitulatif des services créés

| Nom du Service | Protocole | Port/Type | Description |
|---|---|---|---|
| Web-App-TCP8000 | TCP | 8000 | Application web sur Svr_Ubuntu_1 |
| ICMP | ICMP | Echo Request | Tests de connectivité ping |

Avec cette configuration, l'application web sur le port 8000 sera accessible depuis toutes les autres machines du réseau.