

# RAPPORT DE CONFIGURATION

## DU LAB 1



le cours d'Investigation Numérique

**Auteur :** GHOUMO OLIVIA  
**Établissement :** ENSPY  
**Enseignant :** M. MINKA Thierry

# Table des matières

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	Contexte du laboratoire . . . . .	2
1.2	Objectifs . . . . .	2
<b>2</b>	<b>Architecture du réseau</b>	<b>2</b>
2.1	Topologie . . . . .	2
2.2	Plan d'adressage . . . . .	2
<b>3</b>	<b>Configuration du Routeur R1</b>	<b>2</b>
3.1	Configuration des interfaces . . . . .	2
3.2	Configuration des routes statiques . . . . .	3
<b>4</b>	<b>Configuration du Firewall FortiGate</b>	<b>4</b>
4.1	Configuration des interfaces . . . . .	4
4.2	Configuration du routage . . . . .	4
4.3	Création des services personnalisés . . . . .	5
4.4	Politiques de sécurité . . . . .	5
<b>5</b>	<b>Configuration avancée pour l'application</b>	<b>6</b>
5.1	Service pour le socket TCP 8000 . . . . .	6
5.2	Objet d'adresse pour le serveur Ubuntu . . . . .	6
5.3	Règle d'autorisation spécifique . . . . .	6
5.4	Règle de blocage par défaut . . . . .	7
<b>6</b>	<b>Tests de validation</b>	<b>7</b>
6.1	Tests de connectivité . . . . .	7
6.2	Vérification des routes . . . . .	8
6.3	Vérification des politiques . . . . .	8
6.4	Les configurations sur les équipements : . . . . .	8
6.5	Test de connectivité : . . . . .	10
<b>7</b>	<b>Sécurité et bonnes pratiques</b>	<b>11</b>
<b>8</b>	<b>Dépannage</b>	<b>11</b>
8.1	Problèmes courants et commandes de diagnostic . . . . .	11
<b>9</b>	<b>Conclusion</b>	<b>11</b>
9.1	Compétences acquises . . . . .	12
<b>A</b>	<b>Annexes</b>	<b>12</b>
A.1	Schéma récapitulatif de la topologie . . . . .	12

# 1 Introduction

## 1.1 Contexte du laboratoire

Ce rapport présente la configuration complète d'un laboratoire réseau d'entreprise comprenant plusieurs segments réseau interconnectés par un routeur Cisco et sécurisés par un firewall FortiGate. L'architecture met en œuvre des concepts fondamentaux de routage, de politiques de sécurité et de sécurité des réseaux.

## 1.2 Objectifs

Les objectifs principaux de ce laboratoire sont :

- Configurer une topologie réseau multi-segments
- Mettre en place le routage statique entre les réseaux
- Implémenter des politiques de sécurité avec un firewall
- Permettre la communication sécurisée entre les différents segments
- Configurer un service applicatif sur le port TCP 8000

# 2 Architecture du réseau

## 2.1 Topologie

La topologie du laboratoire comprend les éléments suivants :

- **Routeur R1** : Cisco (interconnexion des réseaux)
- **Firewall FW1** : FortiGate (sécurisation du trafic)
- **4 machines** : 2 clients Windows 10, 1 Kali Linux, 1 serveur Ubuntu

## 2.2 Plan d'adressage

Machine	Adresse IP	Masque	Passerelle
Win_10_Client1	192.168.1.6	255.255.255.0	192.168.1.7 (FW1)
Win_10_Client2	172.126.3.3	255.255.255.0	172.126.3.4 (R1)
Kali_1	172.126.4.4	255.255.255.0	172.126.4.5 (R1)
Svr_Ubuntu_1	192.168.5.2	255.255.255.0	192.168.5.1 (FW1)

TABLE 1 – Plan d'adressage des machines

# 3 Configuration du Routeur R1

## 3.1 Configuration des interfaces

Le routeur R1 dispose de trois interfaces Ethernet configurées comme suit :

Réseau	Adresse	Description
Réseau 1	192.168.1.0/24	Clients internes (via FW1)
Réseau 2	192.168.2.0/24	Interconnexion R1-FW1
Réseau 3	172.126.3.0/24	Clients externes (via R1)
Réseau 4	172.126.4.0/24	Réseau Kali Linux (via R1)
Réseau 5	192.168.5.0/24	Serveurs (via FW1)

TABLE 2 – Segmentation réseau

Listing 1 – Configuration des interfaces du routeur

```

1 enable
2 configure terminal
3
4 interface e0/0
5 ip address 192.168.2.8 255.255.255.0
6 no shutdown
7
8 interface e0/1
9 ip address 172.126.4.5 255.255.255.0
10 no shutdown
11
12 interface e0/2
13 ip address 172.126.3.4 255.255.255.0
14 no shutdown
15
16 do copy running-config startup-config
17 end

```

#### Interfaces R1

- **e0/0** : 192.168.2.8/24 - Connexion vers FW1
- **e0/1** : 172.126.4.5/24 - Connexion réseau Kali
- **e0/2** : 172.126.3.4/24 - Connexion Win\_10\_Client2

## 3.2 Configuration des routes statiques

Pour permettre au routeur de diriger le trafic vers les réseaux derrière le firewall, des routes statiques ont été configurées :

Listing 2 – Routes statiques sur R1

```

1 conf t
2
3 ip route 192.168.1.0 255.255.255.0 192.168.2.7
4 ip route 192.168.5.0 255.255.255.0 192.168.2.7
5
6 do copy running-config startup-config
7 end

```

### Explication des routes

Ces routes indiquent que pour atteindre les réseaux 192.168.1.0/24 et 192.168.5.0/24, le routeur doit transmettre les paquets au firewall (192.168.2.7).

## 4 Configuration du Firewall FortiGate

### 4.1 Configuration des interfaces

Le firewall FW1 possède trois interfaces configurées pour interconnecter les différents segments :

Listing 3 – Configuration des interfaces du firewall

```

1 config system interface
2   edit "port1"
3     set mode static
4     set ip 192.168.2.7 255.255.255.0
5     set allowaccess ping https http ssh
6   next
7   edit "port2"
8     set mode static
9     set ip 192.168.1.7 255.255.255.0
10    set allowaccess ping https http ssh
11  next
12  edit "port3"
13    set mode static
14    set ip 192.168.5.1 255.255.255.0
15    set allowaccess ping https http ssh
16  next
17 end

```

Interface	Adresse IP	Connexion
port1	192.168.2.7/24	Vers routeur R1
port2	192.168.1.7/24	Vers Win_10_Client1
port3	192.168.5.1/24	Vers Svr_Ubuntu_1

TABLE 3 – Interfaces du firewall

### 4.2 Configuration du routage

Les routes statiques sur le firewall permettent d'atteindre tous les réseaux du laboratoire :

Listing 4 – Routes statiques sur le firewall

```

1 config router static
2   edit 1

```

```

3      set dst 0.0.0.0 0.0.0.0
4      set gateway 192.168.2.8
5      set device port1
6  next
7  edit 2
8      set dst 172.126.3.0 255.255.255.0
9      set gateway 192.168.2.8
10     set device "port1"
11  next
12  edit 3
13     set dst 172.126.4.0 255.255.255.0
14     set gateway 192.168.2.8
15     set device "port1"
16  next
17 end

```

### 4.3 Création des services personnalisés

Pour permettre le fonctionnement de l'application sur le port TCP 8000 et autoriser les tests de connectivité ICMP :

Listing 5 – Services personnalisés

```

1 config firewall service custom
2     edit "ICMP_ALL"
3         set protocol ICMP
4     next
5 end
6
7 config firewall service custom
8     edit "TCP_8000"
9         set protocol TCP
10        set tcp-portrange 8000
11    next
12 end

```

### 4.4 Politiques de sécurité

Les politiques de firewall définissent les communications autorisées entre les différentes interfaces :

Listing 6 – Politique Port1 vers Port2

```

1 config firewall policy
2     edit 1
3         set name "Port1 to Port2"
4         set srcintf "port1"
5         set dstintf "port2"
6         set srcaddr "all"
7         set dstaddr "all"

```

```
8      set action accept
9      set schedule "always"
10     set service "ICMP_ALL" "TCP_8000"
11     set logtraffic all
12 next
13 end
```

### Politiques configurées

Au total, 6 politiques bidirectionnelles ont été créées pour permettre la communication entre :

- Port1 ↔ Port2
- Port1 ↔ Port3
- Port2 ↔ Port3

Chaque politique autorise les protocoles ICMP et TCP/8000 avec journalisation complète.

## 5 Configuration avancée pour l'application

### 5.1 Service pour le socket TCP 8000

Un service spécifique a été créé pour l'application :

Listing 7 – Service Allow\_TCP\_8000

```
1 config firewall service custom
2     edit Allow_TCP_8000
3         set tcp-portrange 8000 8000
4     next
5 end
```

### 5.2 Objet d'adresse pour le serveur Ubuntu

Listing 8 – Définition de l'objet Ubuntu\_Server

```
1 config firewall address
2     edit "Ubuntu_Server"
3         set subnet 192.168.5.2 255.255.255.0
4     next
5 end
```

### 5.3 Règle d'autorisation spécifique

Une règle permet explicitement l'accès au serveur Ubuntu sur le port 8000 :

Listing 9 – Autorisation vers Ubuntu sur port 8000

```
1 config firewall policy
2     edit 0
3         set name Allow_to_Ubuntu8000
4         set srcintf "port1"
5         set dstintf "port3"
6         set srcaddr "all"
7         set dstaddr "Ubuntu_Server"
8         set action accept
9         set service "Allow_TCP_8000"
10        set schedule "always"
11        set logtraffic all
12    next
13 end
```

## 5.4 Règle de blocage par défaut

Pour renforcer la sécurité, tout autre trafic vers le serveur Ubuntu est bloqué :

Listing 10 – Blocage du reste du trafic

```
1 config firewall policy
2     edit 0
3         set name Deny_Other_To_Ubuntu
4         set srcintf "port1"
5         set dstintf "port3"
6         set srcaddr "all"
7         set dstaddr "Ubuntu_Server"
8         set action deny
9         set service "ALL"
10        set schedule "always"
11        set logtraffic all
12    next
13 end
```

## 6 Tests de validation

### 6.1 Tests de connectivité

Après la configuration, les tests suivants doivent être effectués :

1. **Test ping entre machines :**
  - Win\_10\_Client1 → Win\_10\_Client2
  - Win\_10\_Client1 → Svr\_Ubuntu\_1
  - Kali\_1 → Svr\_Ubuntu\_1
2. **Test de l'application TCP/8000 :**
  - Démarrer l'application sur Svr\_Ubuntu\_1



- Tenter la connexion depuis les autres machines
- Vérifier les logs du firewall

## 6.2 Vérification des routes

Sur le routeur R1 :

```
1 show ip route
```

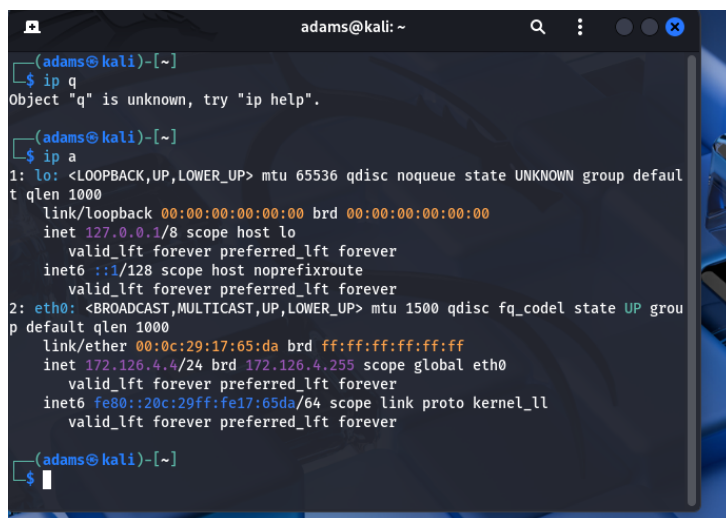
Sur le firewall FW1 :

```
1 get router info routing-table all
```

## 6.3 Vérification des politiques

```
1 diagnose firewall policy list
2 show firewall policy
```

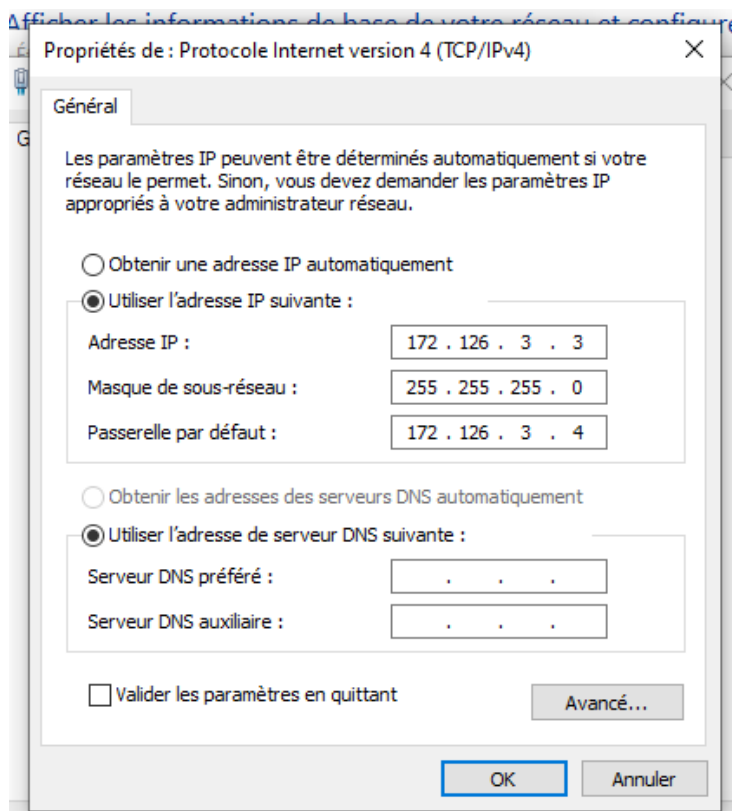
## 6.4 Les configurations sur les équipements :

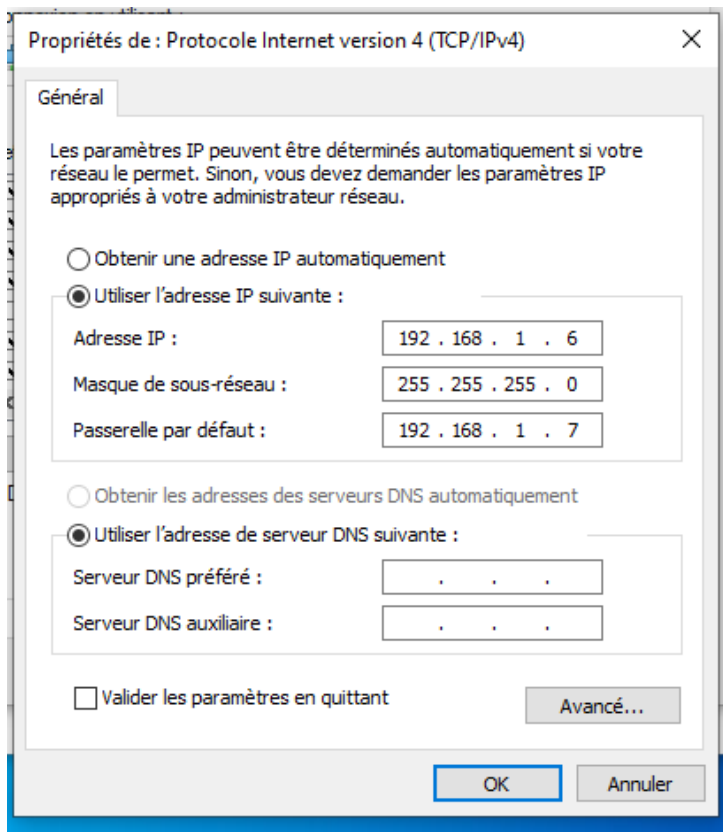


```
(adams@kali)-[~]
$ ip q
Object "q" is unknown, try "ip help".

(adams@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 00:0c:29:17:65:da brd ff:ff:ff:ff:ff:ff
    inet 172.126.4.4/24 brd 172.126.4.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe17:65da/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever

(adams@kali)-[~]
$
```





## 6.5 Test de connectivité :

```
Invite de commandes
Microsoft Windows [version 10.0.19045.4412]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\ADAM'S>ping 192.168.5.2

Envoi d'une requête 'Ping' 192.168.5.2 avec 32 octets de données :
Réponse de 192.168.5.2 : octets=32 temps=5 ms TTL=63
Réponse de 192.168.5.2 : octets=32 temps=4 ms TTL=63
Réponse de 192.168.5.2 : octets=32 temps=3 ms TTL=63
Réponse de 192.168.5.2 : octets=32 temps=4 ms TTL=63

Statistiques Ping pour 192.168.5.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 3ms, Maximum = 5ms, Moyenne = 4ms

C:\Users\ADAM'S>
```

## 7 Sécurité et bonnes pratiques

## 8 Dépannage

### 8.1 Problèmes courants et commandes de diagnostic

Problème	Solution
Pas de connectivité entre réseaux	Vérifier les routes statiques et les passerelles par défaut
Ping fonctionne mais pas TCP/8000	Vérifier les politiques du firewall et les services personnalisés
Configuration non persistante	Utiliser "copy running-config startup-config"
Blocage de tout le trafic	Vérifier l'ordre des politiques (deny avant allow)

TABLE 4 – Guide de dépannage

Listing 11 – Commandes utiles pour le dépannage

```

1 # Sur R1
2 show ip interface brief
3 show ip route
4 ping <destination>
5
6 # Sur FW1
7 get system interface
8 get router info routing-table all
9 diagnose debug flow
10 execute ping <destination>

```

## 9 Conclusion

Ce laboratoire a permis de mettre en œuvre une architecture réseau complète intégrant :

- Le routage inter-réseaux avec Cisco IOS
- La sécurisation du trafic avec FortiGate
- La configuration de services personnalisés
- L'application de politiques de sécurité granulaires

La configuration finale permet une communication contrôlée entre tous les segments réseau tout en maintenant un niveau de sécurité élevé, particulièrement pour le serveur Ubuntu hébergeant l'application critique.

## 9.1 Compétences acquises

- Configuration d'équipements réseau en CLI
- Mise en place de routage statique
- Gestion de politiques de firewall
- Création de services et objets personnalisés
- Dépannage de problèmes de connectivité

## A Annexes

### A.1 Schéma récapitulatif de la topologie

