

RÉPUBLIQUE DU CAMEROUN

Paix - Travail - Patrie

UNIVERSITÉ DE YAOUNDÉ I

ECOLE NATIONALE SUPERIEURE
POLYTECHNIQUE DE YAOUNDE

DÉPARTEMENT DE GENIE

INFORMATIQUE



REPUBLIC OF CAMEROON

Peace - Work - Fatherland

UNIVERSITY OF YAOUNDE I

NATIONAL ADVANCED SCHOOL
OF ENGINEERING OF YAOUNDE

DEPARTMENT OF COMPUTER

ENGINEERING

LAB 1

Configuration d'un Environnement Réseau Fonctionnel et Sécurisé

Option :

Cybersécurité et Investigation Numérique

Rédigé par :

KALDADAK ADAMA, 24P824

Sous l'encadrement de :

M. Minka THierry

Année académique 2025 / 2026

TABLE DES MATIÈRES

Introduction	2
I Architecture du réseau	3
II Configuration du routeur R1	3
III Configuration du pare-feu	4
IV Résultat	8
Conclusion	10

INTRODUCTION

La configuration d'un pare-feu constitue une étape essentielle dans la sécurisation et la gestion du trafic réseau d'une infrastructure informatique. Dans le cadre de ce travail, il s'agit de mettre en place et de configurer un pare-feu FortiGate afin d'assurer la communication et la protection entre plusieurs réseaux interconnectés. L'objectif principal est de définir les interfaces réseau, d'ajouter les routes statiques nécessaires à la connectivité entre les sous-réseaux, puis de créer des services spécifiques permettant le bon fonctionnement des applications, notamment celles utilisant le port TCP 8000 et le protocole ICMP. Enfin, des politiques de filtrage sont établies pour autoriser la communication entre les différentes interfaces (ports 1, 2 et 3) du pare-feu, garantissant ainsi à la fois la connectivité et la sécurité du réseau.

I Architecture du réseau

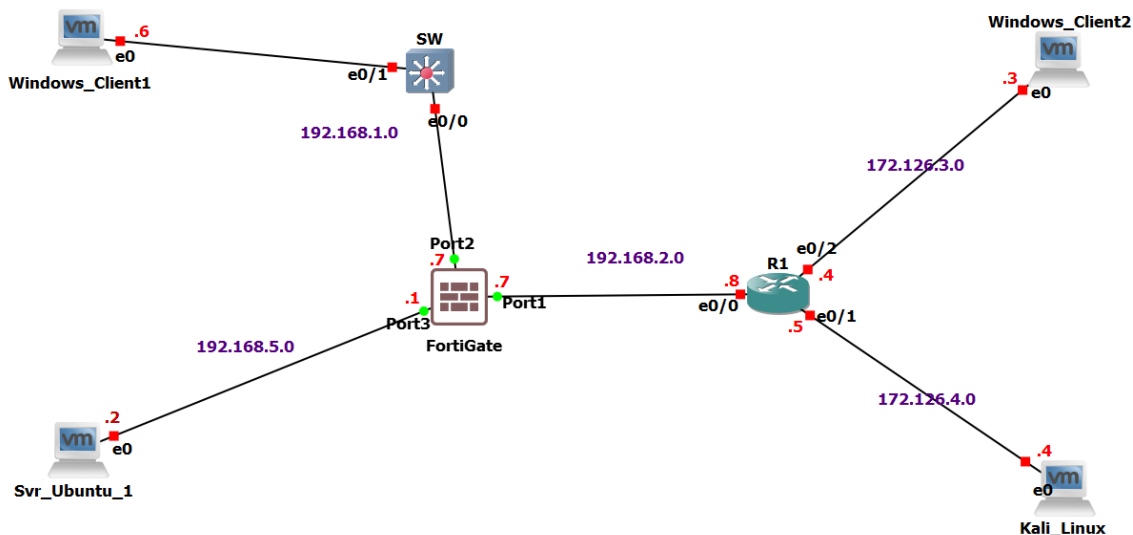


FIGURE 1 – Schéma du réseau utilisé pour les tests

TABLE 1 – Inventaire des équipements réseau

Équipements	Adresses	Ports	Masques	Passerelles
Svr_ubuntu_1 (pwd : Svr_Ubuntu_1)	192.168.5.2	/	255.255.255.0	192.168.5.1 (FW1)
Windows_Client1	192.168.1.6	/	255.255.255.0	192.168.1.7 (FW1)
Windows_Client2	172.126.3.3	/	255.255.255.0	172.126.3.4 (R1)
Kali_Linux (pwd : kali)	172.126.4.4	/	255.255.255.0	172.126.4.5 (R1)
FortiGate (pwd : root)	192.168.2.7 192.165.1.7 192.168.5.1	Port1 Port2 Port3	255.255.255.0	/
R1 (Routeur)	192.168.2.8 172.126.4.5 172.126.3.4	E0/0 E0/1 E0/3	255.255.255.0	/

II Configuration du routeur R1

La première étape consiste à configurer les interfaces réseaux. Il vous suffit d'entrer ces commandes :

```

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

```

Listing 1 – Configuration des interfaces du routeur R1

Ajout des routes statiques

Par la suite, nous procédons à l'ajout des routes statiques :

```

1 conf t
2 ip route 192.168.1.0 255.255.255.0 192.168.2.7
3 ip route 192.168.5.0 255.255.255.0 192.168.2.7
4 ip route 172.126.3.0 255.255.255.0 172.126.4.0
5 ip route 172.126.3.0 255.255.255.0 192.168.1.0
6 ip route 172.126.3.0 255.255.255.0 192.168.2.0
7 ip route 172.126.4.0 255.255.255.0 172.126.3.0
8 ip route 192.158.1.0 255.255.255.0 172.126.4.0
9 ip route 192.168.1.0 255.255.255.0 192.168.2.7
10 ip route 192.168.2.0 255.255.255.0 172.126.3.0
11 ip route 192.168.2.0 255.255.255.0 172.126.4.0
12 ip route 192.168.5.0 255.255.255.0 192.168.2.7
13 ip route 192.168.5.0 255.255.255.0 172.126.4.0
14
15 do copy running-config startup-config
16 end

```

Listing 2 – Configuration des routes statiques

III Configuration du pare-feu

Suivre les commandes ci-dessous pour la configuration du pare-feu FortiGate.

1. Configuration des interfaces du pare-feu

```

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

```

Listing 3 – Configuration des interfaces du pare-feu

2. Configuration des routes statiques

```

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 config router static
8     edit 1
9         set dst 172.126.3.0 255.255.255.0
10        set gateway 192.168.2.8
11        set device "port1"
12    next
13    edit 2
14        set dst 172.126.4.0 255.255.255.0
15        set gateway 192.168.2.8
16        set device "port1"
17    next
18    edit 3
19        set dst 192.168.1.0 255.255.255.0
20        set gateway 192.168.2.8
21        set device "port2"
22    next
23    edit 4
24        set dst 192.168.5.0 255.255.255.0
25        set gateway 192.168.2.8
26        set device "port3"
27    next
28 end

```

Listing 4 – Configuration des routes statiques

3. Création des services TCP 8000 et ICMP

Afin que l'application puisse fonctionner correctement sur les autres machines, il est important de créer un service pour le port TCP 8000.

```
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
```

Listing 5 – Création des services ICMP et TCP 8000

4. Communication entre les ports

```
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"
11        set service "TCP_8000"
12        set logtraffic all
13    next
14
15    edit 2
16        set name "Port2 to Port1"
17        set srcintf "port2"
18        set dstintf "port1"
19        set srcaddr "all"
20        set dstaddr "all"
21        set action accept
22        set schedule "always"
23        set service "ICMP_ALL"
24        set service "TCP_8000"
25        set logtraffic all
26    next
27
28    edit 3
29        set name "Port1 to Port3"
30        set srcintf "port1"
31        set dstintf "port3"
32        set srcaddr "all"
33        set dstaddr "all"
34        set action accept
35        set schedule "always"
```

```

36         set service "ICMP_ALL"
37         set service "TCP_8000"
38         set logtraffic all
39     next
40
41     edit 4
42         set name "Port3 to Port1"
43         set srcintf "port3"
44         set dstintf "port1"
45         set srcaddr "all"
46         set dstaddr "all"
47         set action accept
48         set schedule "always"
49         set service "ICMP_ALL"
50         set service "TCP_8000"
51         set logtraffic all
52     next
53
54     edit 5
55         set name "Port2 to Port3"
56         set srcintf "port2"
57         set dstintf "port3"
58         set srcaddr "all"
59         set dstaddr "all"
60         set action accept
61         set schedule "always"
62         set service "ICMP_ALL"
63         set service "TCP_8000"
64         set logtraffic all
65     next
66
67     edit 6
68         set name "Port3 to Port2"
69         set srcintf "port3"
70         set dstintf "port2"
71         set srcaddr "all"
72         set dstaddr "all"
73         set action accept
74         set schedule "always"
75         set service "ICMP_ALL"
76         set service "TCP_8000"
77         set logtraffic all
78     next
79
80     edit 9
81         set name "Allow Ping"
82         set srcintf "any"
83         set dstintf "any"
84         set srcaddr "all"
85         set dstaddr "all"
86         set action accept
87         set service "PING"
88         set schedule "always"
89     next
90 end

```

Listing 6 – Politiques de communication entre les ports

Une fois toutes ces configurations effectuées, vous pouvez procéder aux tests de **ping** et lancer l'application sur les autres machines.

IV Résultat

Dans l'image ci-dessous, nous montrons comment l'application fonctionne sur le Serveur Ubuntu.

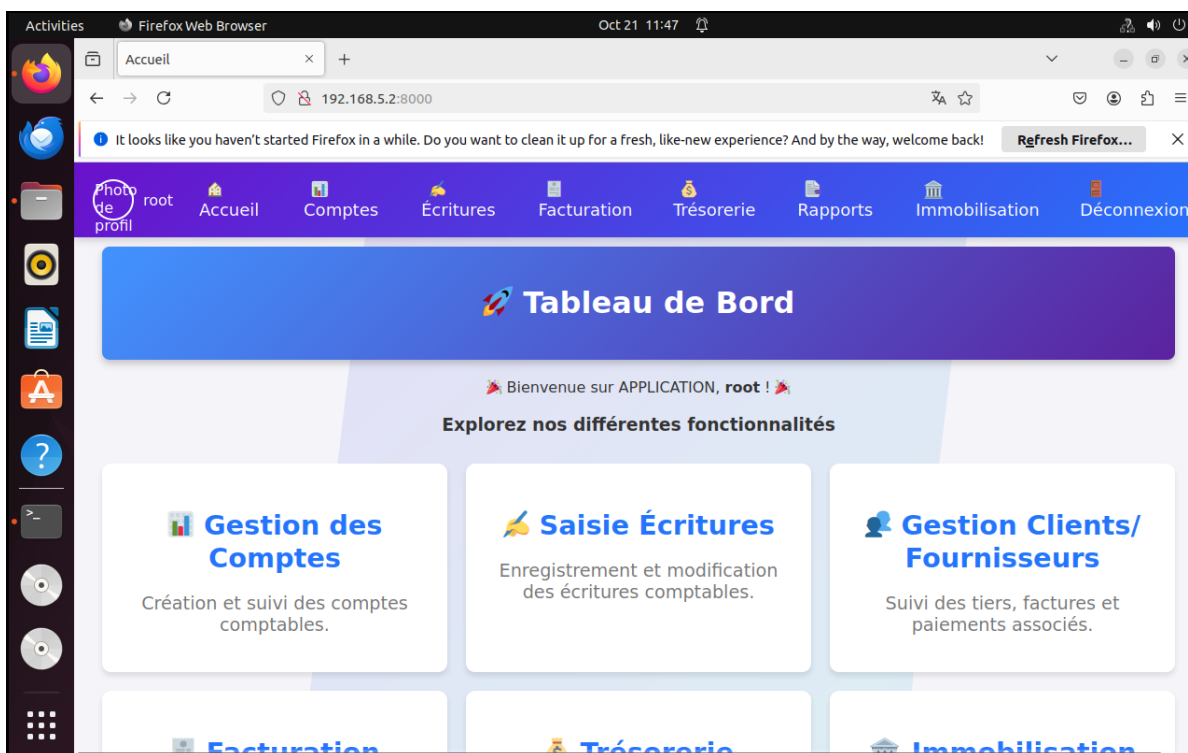


FIGURE 2 – Résultat des tests de fonctionnement du réseau : Serveur Ubuntu

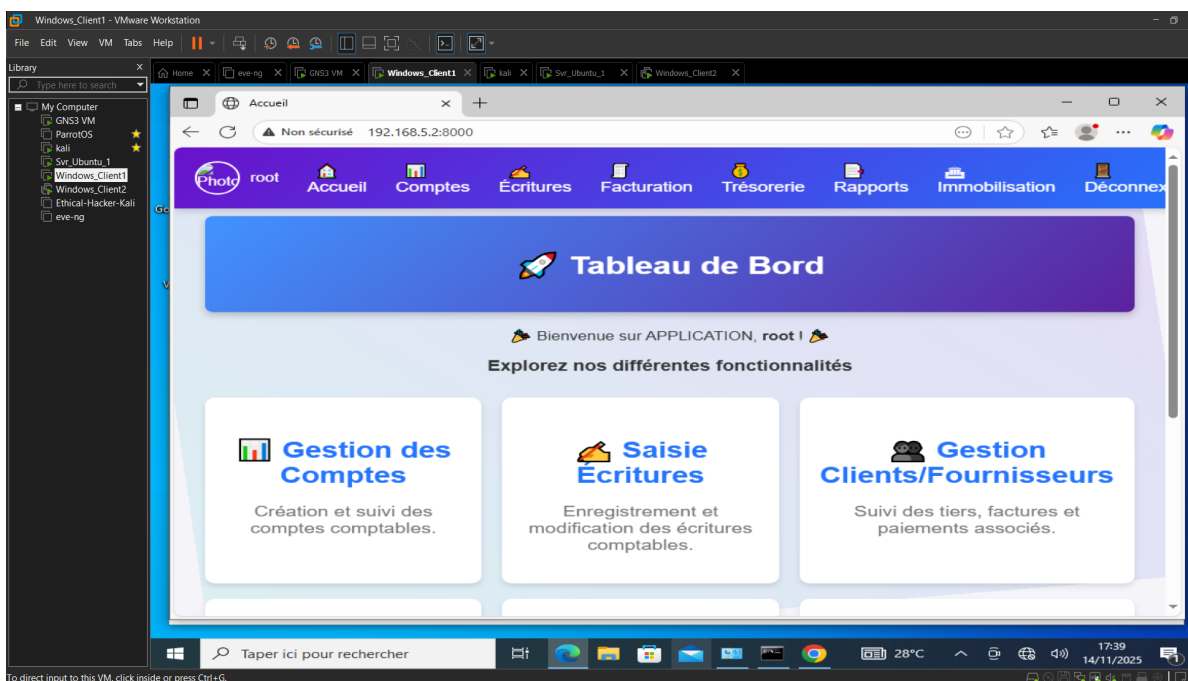


FIGURE 3 – Résultat des tests de fonctionnement du réseau : Client Windows

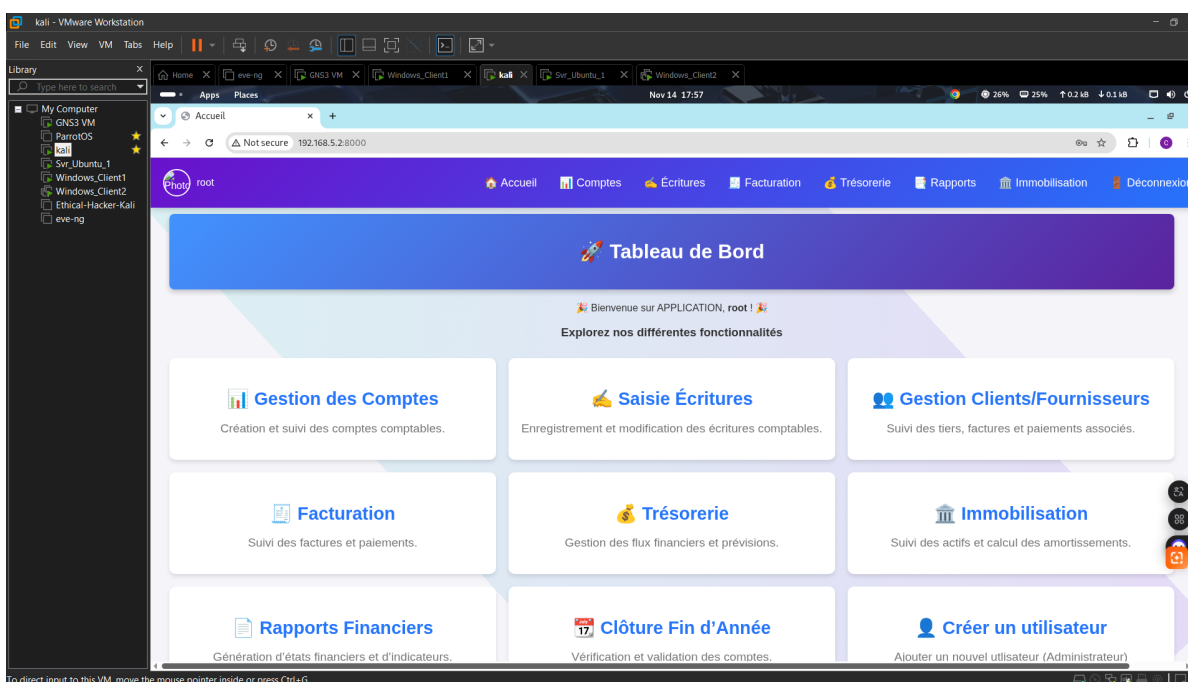


FIGURE 4 – Résultat des tests de fonctionnement du réseau : Kali linux

CONCLUSION

En somme, la configuration effectuée sur le pare-feu FortiGate permet d'assurer une communication fluide et sécurisée entre les différents segments du réseau. Les interfaces ont été correctement paramétrées, les routes statiques définies, et les services nécessaires créés pour permettre le fonctionnement optimal des applications. Grâce aux politiques de sécurité mises en place, les échanges entre les réseaux sont désormais contrôlés et protégés, tout en maintenant la disponibilité des services essentiels tels que le ping et le port TCP 8000. Cette configuration illustre l'importance d'une bonne gestion du pare-feu dans la maîtrise du trafic réseau et la protection de l'infrastructure contre les risques liés aux communications non autorisées.