UNIVERSITÉ DE YAOUNDÉ I
***
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE DE YAOUNDÉ
***
DÉPARTEMENT DE GÉNIE INFORMATIQUE
***
HUMANITÉS NUMÉRIQUES

THE UNIVERSITY OF YAOUNDE I
***
NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE
***
DEPARTMENT OF COMPUTER ENGINEERING
***
DIGITAL HUMANITIES

LAB1

Rédigé par :

FANTA YADON Félicité 22P069

Supervisé par :

M. Thierry MINKA

I Contexte **3**

II Objectif Principal **3**

III Schéma d'Architecture **3**

IV Plan d'Adressage Réseau **4**

V Création des Machines Virtuelles **5**

VI Configuration du Routeur R1 **6**

VII Configuration du Firewall FortiGate **8**

Conclusion **10**

I Contexte

Ce lab pratique s'inscrit dans la première phase des travaux d'investigation numérique , visant à établir une infrastructure réseau complète et sécurisée. Cette infrastructure servira de base isolée pour les simulations d'attaques (ransomware, audit, etc.) dans les Labs suivants.

II Objectif Principal

L'objectif principal du Lab 1 est de configurer une architecture réseau complexe et fonctionnelle dans GNS3, incluant :

- un Routeur frontière,
- un Firewall (FortiGate),
- un Réseau Local (LAN),
- une Zone Démilitarisée (DMZ).

L'accent est mis sur la segmentation réseau, le routage et la mise en place des politiques de sécurité.

III Schéma d'Architecture

L'infrastructure comporte :

- Routeur R1 (équipement de frontière),
- Firewall FortiGate (segmentation LAN/DMZ),
- Serveur web dans la DMZ (Ubuntu),
- Poste utilisateur dans le LAN (Windows 10).

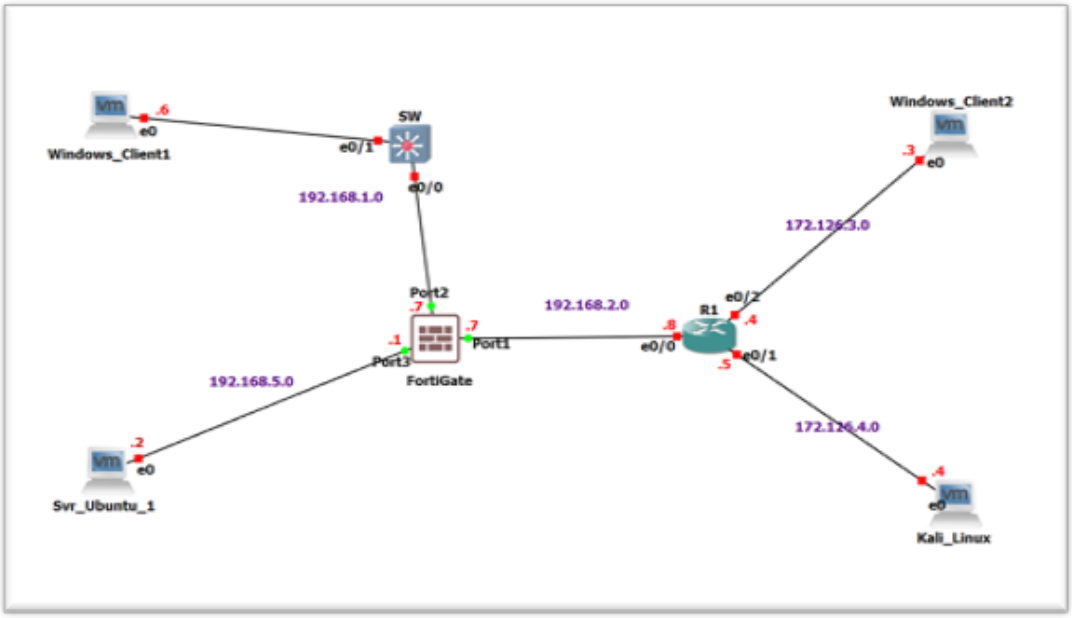


Figure 1: Schéma d'architecture du réseau

IV Plan d'Adressage Réseau

Équipement	Rôle/Réseau	Interface	Adresse IP	Masque	Passerelle
Routeur R1	Frontière	E0/0	192.168.2.8	255.255.255.0	-
FortiGate	WAN	Port1	192.168.2.7	255.255.255.0	-
FortiGate	DMZ	Port3	192.168.5.1	255.255.255.0	-
FortiGate	LAN	Port2	192.168.1.7	255.255.255.0	-
Serveur Ubuntu	Web / DMZ	-	192.168.5.2	255.255.255.0	192.168.5.1
Client Windows	LAN	-	192.168.1.6	255.255.255.0	192.168.1.7

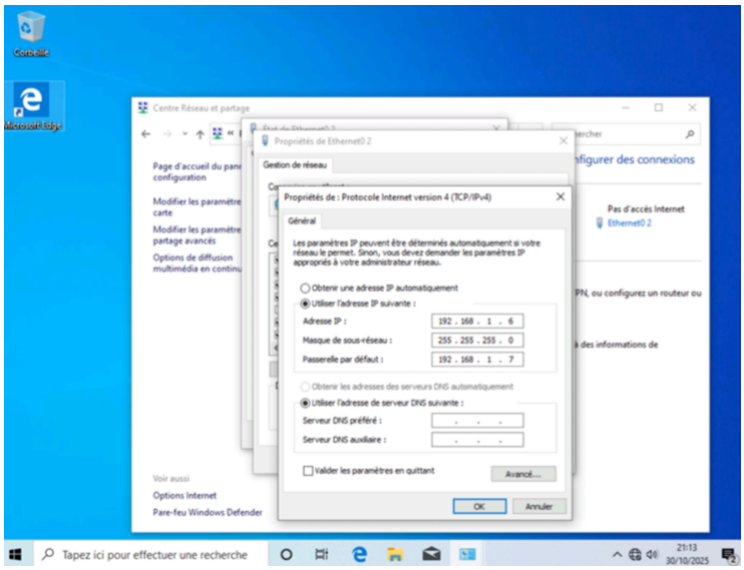
Table 1: Plan d'adressage du Lab 1

- Interconnexion R1–FW1 : 192.168.2.0/24
- LAN : 192.168.1.0/24
- DMZ : 192.168.5.0/24

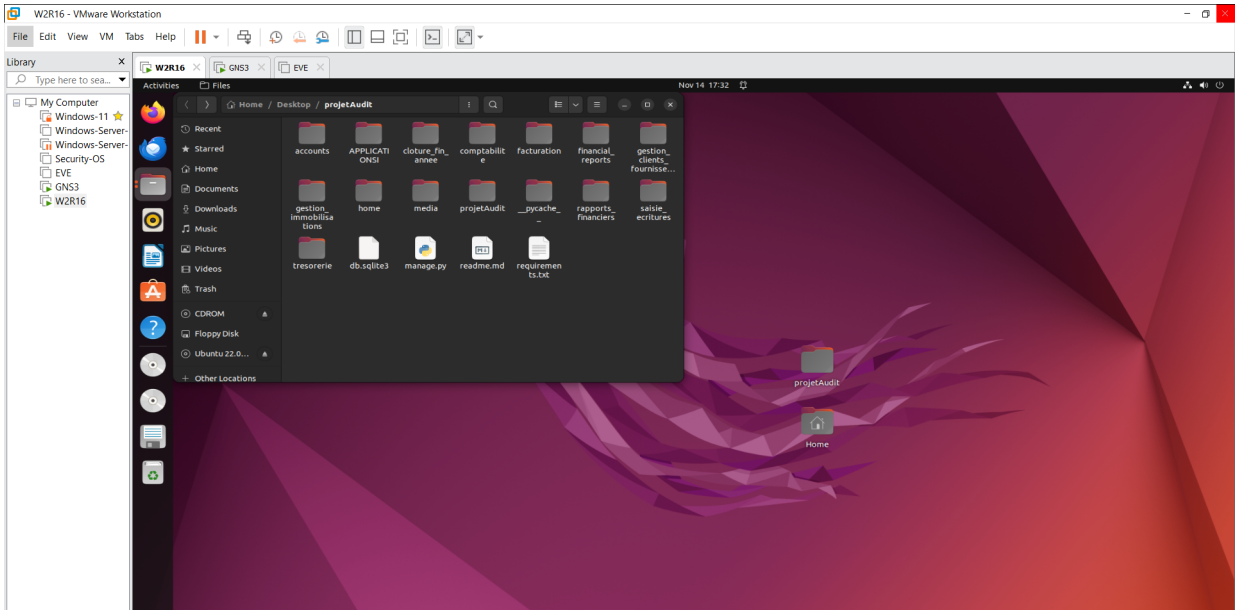
V Création des Machines Virtuelles

Les machines suivantes ont été créées dans GNS3 :

- **Windows_Client1** : Windows 10 avec 2 Go de fichiers dans Documents et Bureau.



- **Svr_ubuntu_1** : Ubuntu configuré comme serveur web (CMS).



0.5

Figure 2: Vue des machines virtuelles dans GNS3

VI Configuration du Routeur R1

Configuration des interfaces

```
enable
configure terminal

interface ethernet0/0
ip address 192.168.2.8 255.255.255.0
no shutdown

interface ethernet0/1
ip address 172.126.4.5 255.255.255.0
no shutdown

interface ethernet0/2
ip address 172.126.3.4 255.255.255.0
no shutdown
```

Routes statiques

```
ip route 192.168.1.0 255.255.255.0 192.168.2.7
ip route 192.168.5.0 255.255.255.0 192.168.2.7
```

Sauvegarde

```
do copy running-config startup-config
```

```
IOU1(config)#hostname R1
R1(config)#enable
% Incomplete command.

R1(config)#configure terminal
                  ^
% Invalid input detected at '^' marker.

R1(config)#
R1(config)#interface e0/0
R1(config-if)#ip address 192.168.2.8 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#interface e0/1
R1(config-if)#ip address 172.126.4.5 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#interface e0/2
R1(config-if)#ip address 172.126.3.4 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#do copy running-config startup-config
Destination filename [startup-config]? end
%Error copying nvram:end (Invalid argument)
R1(config-if)#
*Nov 14 18:53:10.161: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Nov 14 18:53:10.236: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*Nov 14 18:53:10.295: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to up
*Nov 14 18:53:11.185: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to up
*Nov 14 18:53:11.245: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
1, changed state to up
R1(config-if)#
*Nov 14 18:53:11.306: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
2, changed state to up
R1(config-if)#conf t
                ^
% Invalid input detected at '^' marker.

R1(config-if)#ip route 192.168.1.0 255.255.255.0 192.168.2.7
R1(config)#ip route 192.168.5.0 255.255.255.0 192.168.2.7
R1(config)#ip route 172.126.3.0 255.255.255.0 172.126.4.0
R1(config)#ip route 172.126.3.0 255.255.255.0 192.168.1.0
R1(config)#ip route 172.126.3.0 255.255.255.0 192.168.2.0
R1(config)#ip route 172.126.4.0 255.255.255.0 172.126.3.0
R1(config)#ip route 192.158.1.0 255.255.255.0 172.126.4.0
R1(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.7
R1(config)#ip route 192.168.2.0 255.255.255.0 172.126.3.0
R1(config)#ip route 192.168.2.0 255.255.255.0 172.126.4.0
R1(config)#ip route 192.168.5.0 255.255.255.0 192.168.2.7
```

Figure 3: Configuration du routeur R1 dans GNS3

VII Configuration du Firewall FortiGate

Interfaces configurées :

- Port1 : 192.168.2.7 (WAN)
- Port3 : 192.168.5.1 (DMZ)
- Port2 : 192.168.1.7 (LAN)

Politiques de sécurité

- DMZ → LAN : ICMP_ALL, TCP_8000
- LAN → DMZ : ICMP_ALL, TCP_8000
- WAN → DMZ : ICMP_ALL, TCP_8000

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) #     edit "port1"
FortiGate-VM64-KVM (port1) #         set mode static
FortiGate-VM64-KVM (port1) #         set ip 192.168.2.7 255.255.255.0
FortiGate-VM64-KVM (port1) #         set allowaccess ping https http ssh
FortiGate-VM64-KVM (port1) #     next
FortiGate-VM64-KVM (interface) #     edit "port2"
FortiGate-VM64-KVM (port2) #         set mode static
FortiGate-VM64-KVM (port2) #         set ip 192.168.1.7 255.255.255.0
FortiGate-VM64-KVM (port2) #         set allowaccess ping https http ssh
FortiGate-VM64-KVM (port2) #     next
FortiGate-VM64-KVM (interface) #     edit "port3"
FortiGate-VM64-KVM (port3) #         set mode static
FortiGate-VM64-KVM (port3) #         set ip 192.168.5.1 255.255.255.0
FortiGate-VM64-KVM (port3) #         set allowaccess ping https http ssh
FortiGate-VM64-KVM (port3) #     next
FortiGate-VM64-KVM (interface) # end
```

```
FortiGate-VM64-KVM (1) # set logtraffic all

FortiGate-VM64-KVM (1) #     edit 2
Unknown action 0

FortiGate-VM64-KVM (1) #         set name "Port2 to Port1"

FortiGate-VM64-KVM (1) #         set srcintf "port2"

FortiGate-VM64-KVM (1) #         set dstintf "port1"

FortiGate-VM64-KVM (1) #         set srcaddr "all"

FortiGate-VM64-KVM (1) #         set dstaddr "all"

FortiGate-VM64-KVM (1) #         set action accept

FortiGate-VM64-KVM (1) #         set schedule "always"

FortiGate-VM64-KVM (1) #         set service "ICMP_ALL"
entry not found in datasource
```

Figure 4: Politiques FortiGate configurées

Les vérifications suivantes ont été réalisées :

- Ping entre LAN DMZ
- Accès HTTP/TCP 8000 depuis le LAN vers la DMZ

- Vérification du routage via R1

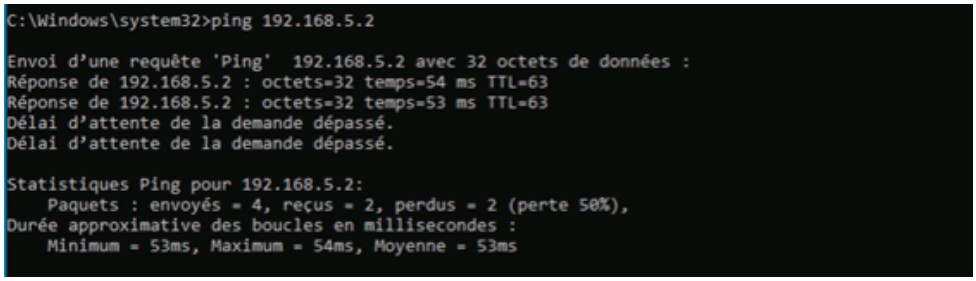


Figure 5: Test de connectivité LAN → DMZ

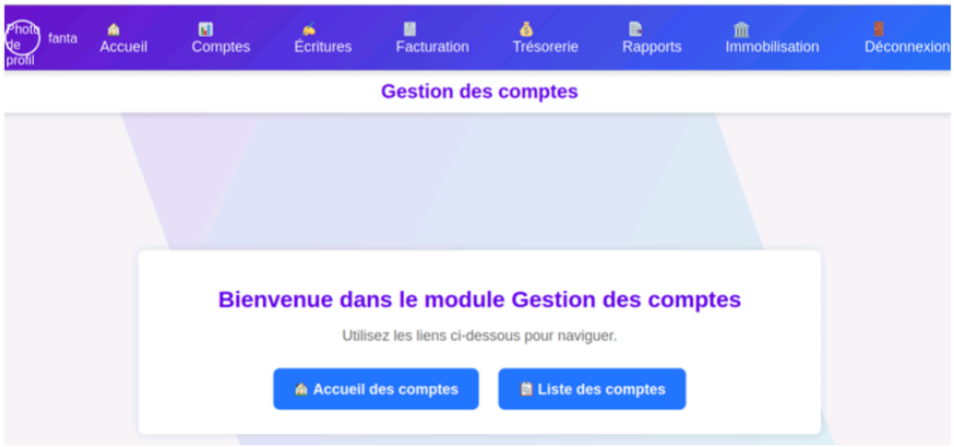


Figure 6: Accès au serveur web depuis Windows_Client1

Conclusion

Le Lab 1 a permis de mettre en place avec succès une infrastructure réseau complète, segmentée et sécurisée incluant :

- un Routeur frontière,
- un Firewall FortiGate,
- un LAN fonctionnel,
- une DMZ hébergeant un serveur web.

La connectivité entre les zones ainsi que les politiques de sécurité ont été validées avec succès. Cette architecture constitue la base pour les futurs Labs (attaque, investigation, audit).