RÉPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie
*****
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
*****
UNIVERSITÉ DE YAOUNDÉ I
*****
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE
*****
DÉPARTEMENT DE GÉNIE INFORMATIQUE
*****

REPUBLIC OF CAMEROON
Peace – Work – Fatherland
*****
MINISTRY OF HIGHER EDUCATION
*****
UNIVERSITY OF YAOUNDE I
*****
NATIONAL ADVANCED SCHOOL OF ENGINEERING
*****
COMPUTER ENGINEERING DEPARTMENT
*****

RAPPORT D'INVESTIGATION NUMÉRIQUE JUDICIAIRE

RAPPORT DU LAB 1

Rédigé par
NZOUCK TOUMPE ERIC - OLIVIER
Matricule : ***22P060***

Sous la supervision de
Thierry MINKA, Eng

Année académique 2025/2026

Contents

INTRODUCTION

L'objectif du Lab 1 est de permettre aux étudiants de concevoir et de configurer un environnement réseau complexe et sécurisé à l'aide de GNS3. Ce projet consiste à mettre en place une architecture complète intégrant un poste client sous Windows, une zone démilitarisée (DMZ) hébergeant un serveur web sous Linux, un pare-feu assurant la sécurité des échanges, ainsi qu'un routeur chargé de la connectivité entre les différentes zones. Ce laboratoire vise à mettre en pratique les principes essentiels de la segmentation réseau, de l'isolation des services critiques et du contrôle du trafic inter-réseaux. Tout au long de ce document, chaque étape de la mise en œuvre sera présentée en détail afin de conduire l'infrastructure jusqu'à un état pleinement fonctionnel et opérationnel.

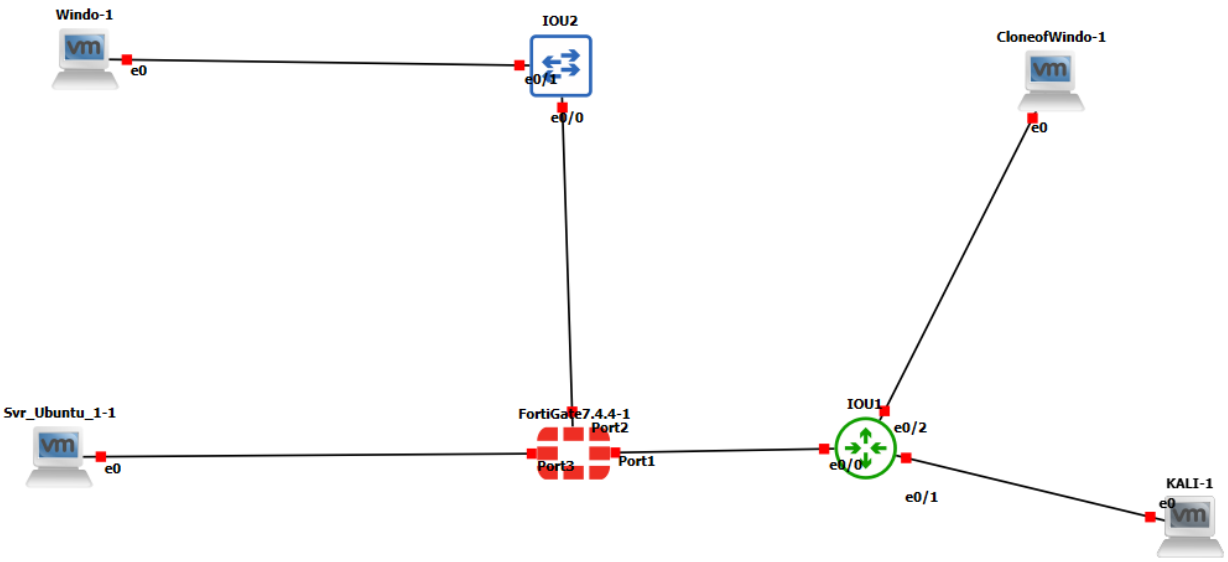
0.1 CONCEPTION

0.1.1 Composition de l'architecture

Notre infrastructure réseau se compose des éléments suivants:

- **Routeur** : il assure la connexion du réseau interne à l'extérieur (*Internet*).
- **Pare-feu FortiGate** : placé en frontière, il protège le réseau interne et contrôle les flux entre *Internet*, la **DMZ** et le réseau local.
- **DMZ (zone démilitarisée)** : elle contient un poste de travail exécutant *Ubuntu*, hébergeant une application web accessible depuis l'extérieur comme depuis l'intérieur du réseau.
- **Poste de travail sur le réseau local** : équipé de *Windows 10* et d'un antivirus, ce poste contient environ 2 Go de données variées, incluant fichiers exécutables, documents *Word*, *PDF* et *Excel*.

0.1.2 Schéma de l'architecture



0.1.3 Plan d'adressage sur GNS3

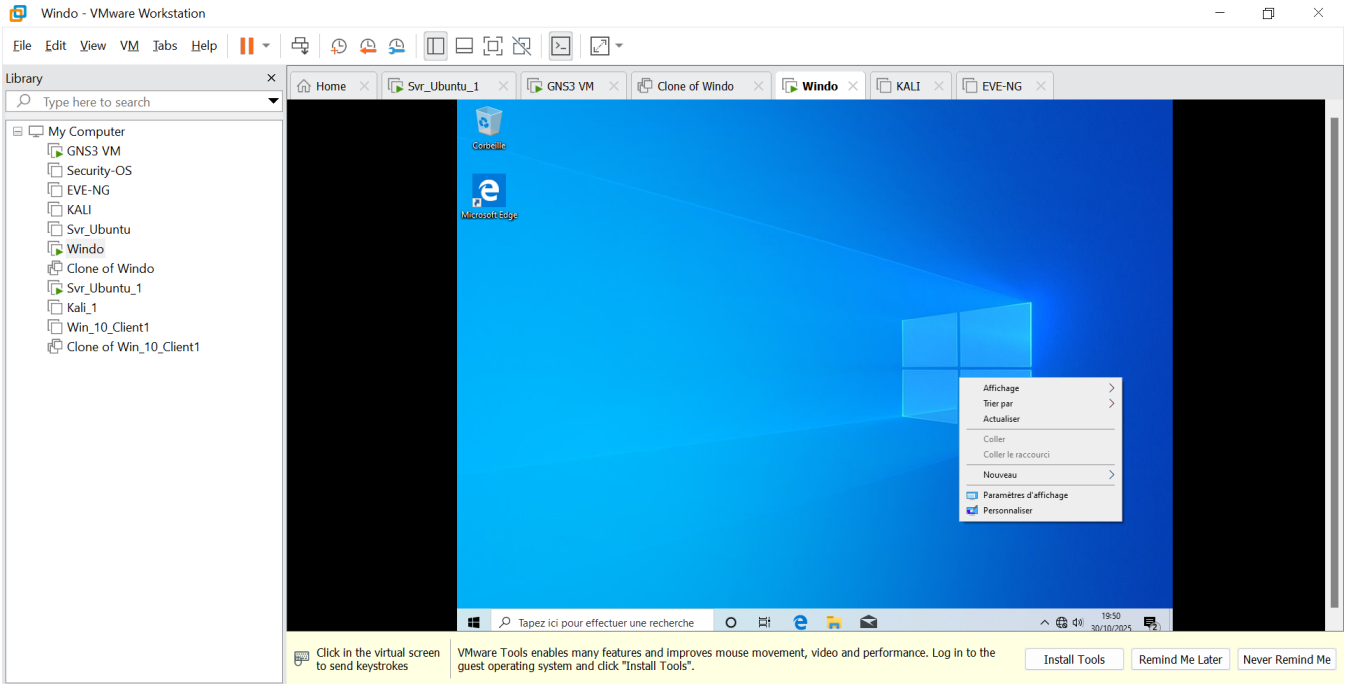
0.2 DÉPLOIEMENT

Pour la mise en place de notre infrastructure réseau, nous avons utilisé VMWare comme logiciel de virtualisation. Cela nous a permis de créer des machines virtuelles configurables et interconnectables facilement au sein de notre environnement réseau.

0.2.1 Machine virtuelle Windows 10

Nous avons créé une machine virtuelle **Windows 10**, qui servira de poste client dans le réseau local. Les caractéristiques minimales configurées sont les suivantes :

- Disque dur : 20 Go
- Mémoire RAM : 2 Go

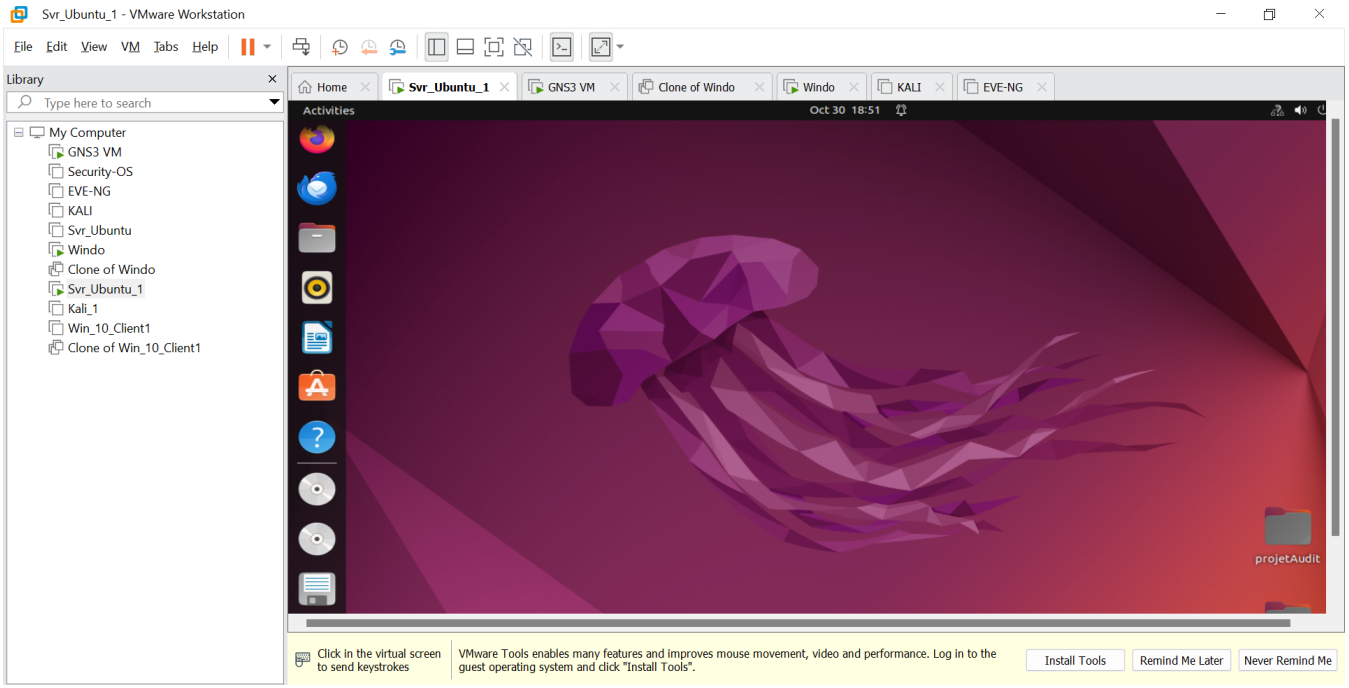


Cette machine permettra de tester la connectivité avec le serveur ainsi que les autres machines du réseau.

0.2.2 Machine virtuelle Linux (serveur web)

Pour la zone DMZ, nous avons créé une machine virtuelle **Ubuntu**, destinée à héberger le serveur web. Ses caractéristiques minimales sont :

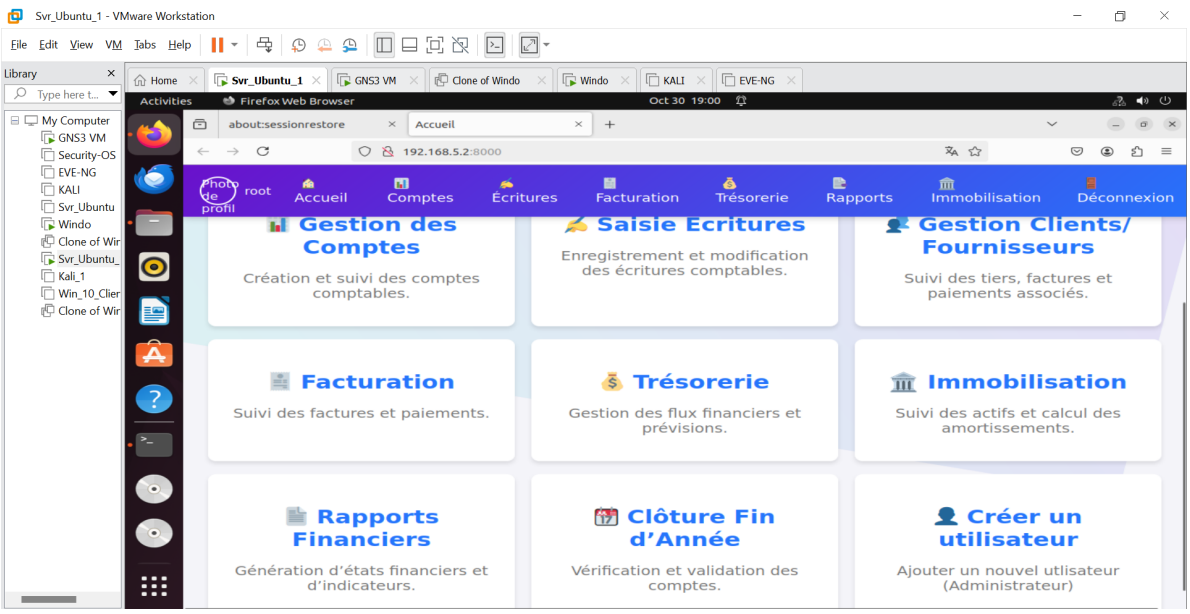
- Disque dur : 20 Go
- Mémoire RAM : 2 Go



Cette machine sert à héberger notre **application web de comptabilité**, accessible depuis les postes clients du réseau interne.

0.2.3 Création de l'application web

Nous avons développé une application web dédiée à la **gestion comptable**, permettant aux utilisateurs d'enregistrer et de consulter des transactions financières de manière sécurisée. L'application est déployée sur le serveur Ubuntu et est accessible via le navigateur des clients.

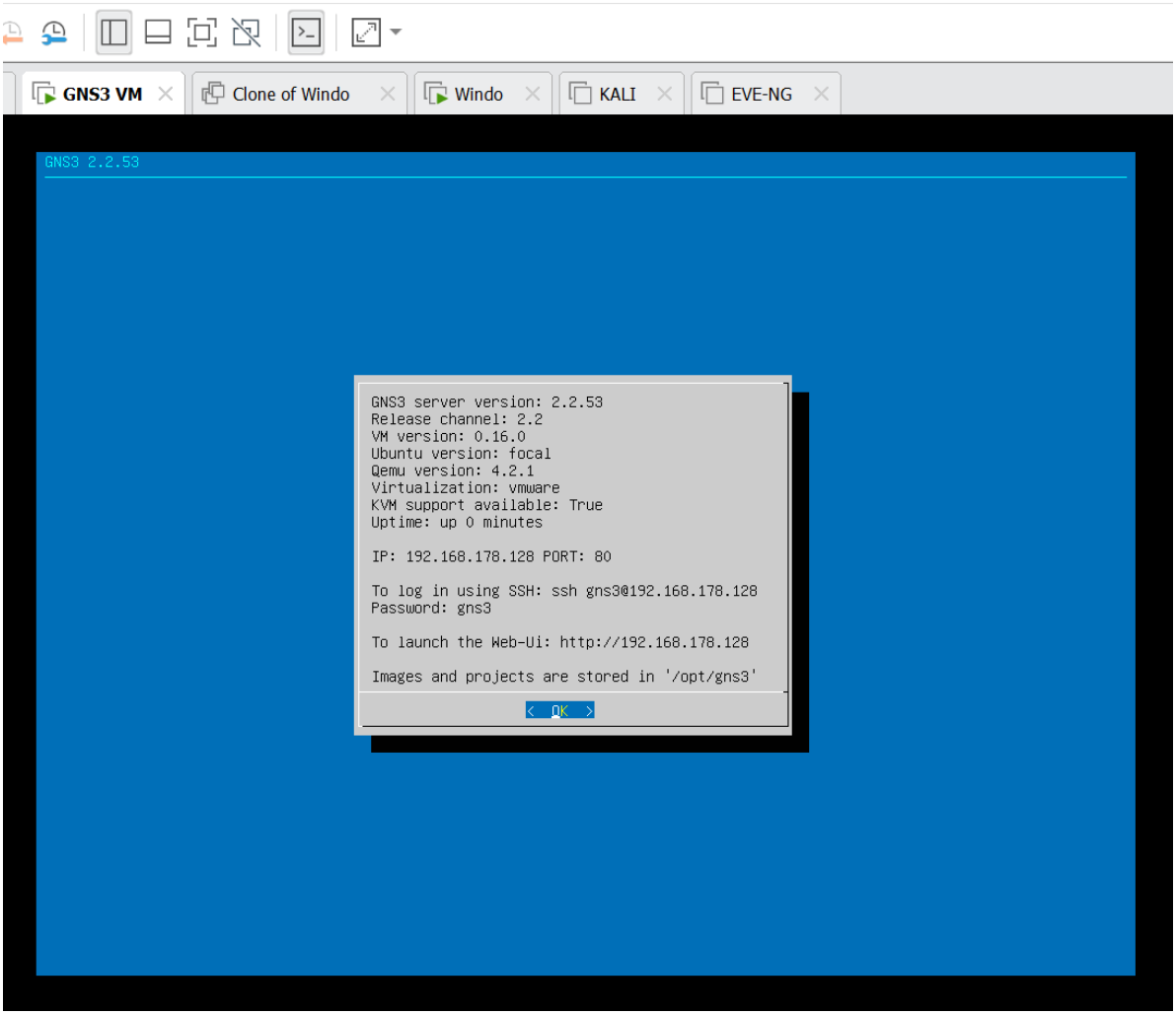


0.2.4 Création de l'infrastructure

Installation de GNS3

L'installation de GNS3 s'est faite en deux temps:

- Installation de la machine virtuelle de GNS3



- Installation et configuration du pare-feu Fortigate: Dans notre architecture, nous avons choisi d'utiliser un pare-feu à notre portée : Fortigate ;la version 7.4.4.Ici il est question de suivre les étapes pas à pas. A la fin du chargement, le pare-feu va redémarrer et l'interface du LAN par défaut va être attribuée de manière statique à l'adresse : 192.168.1.7/24.Il sera question par la suite de se connecter à l'interface graphique via la vm Windows pour assigner les interfaces DMZ et WAN afin de permettre à notre architecture de fonctionner.

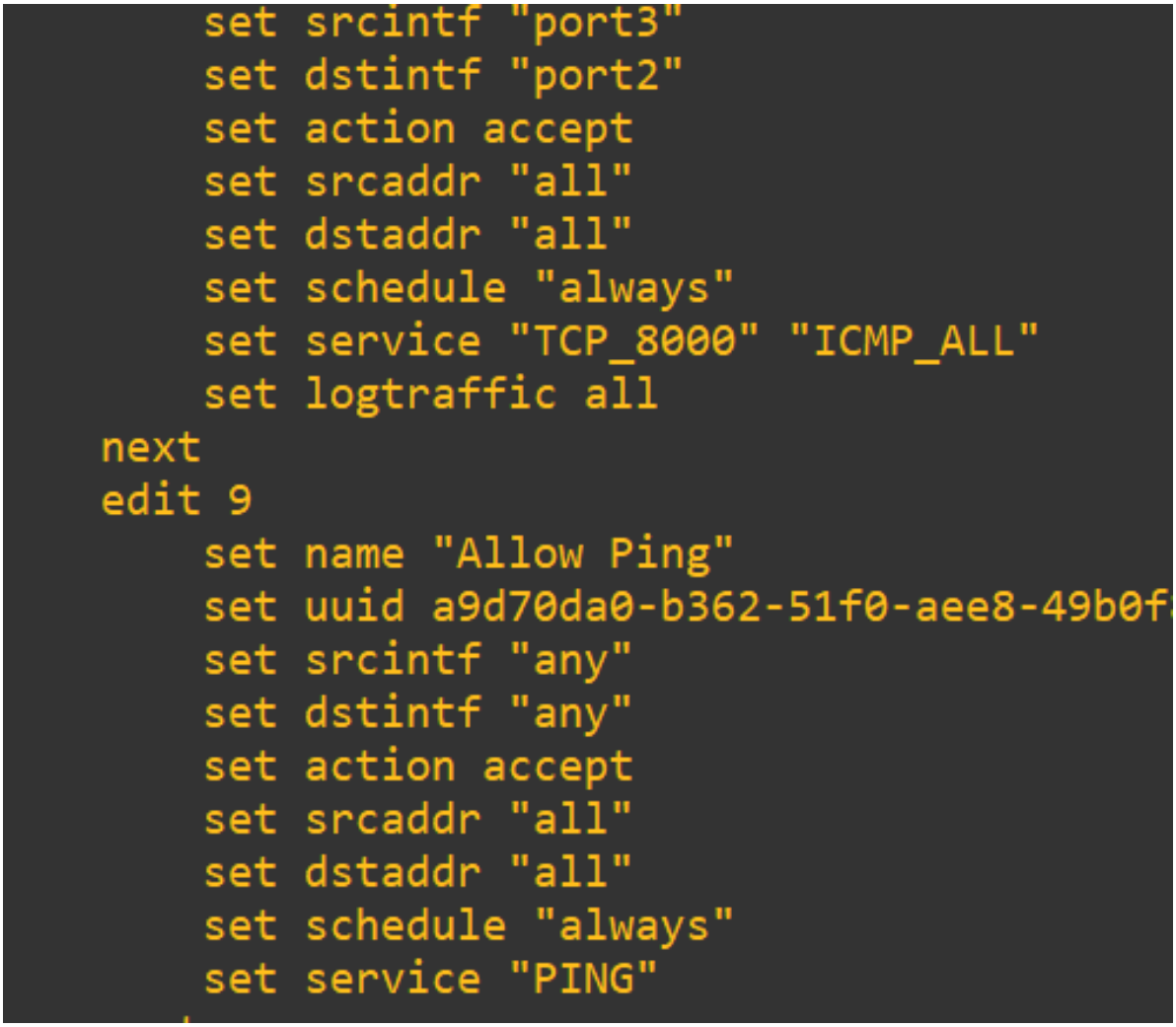
0.3 RÉSULTATS ET ANALYSE

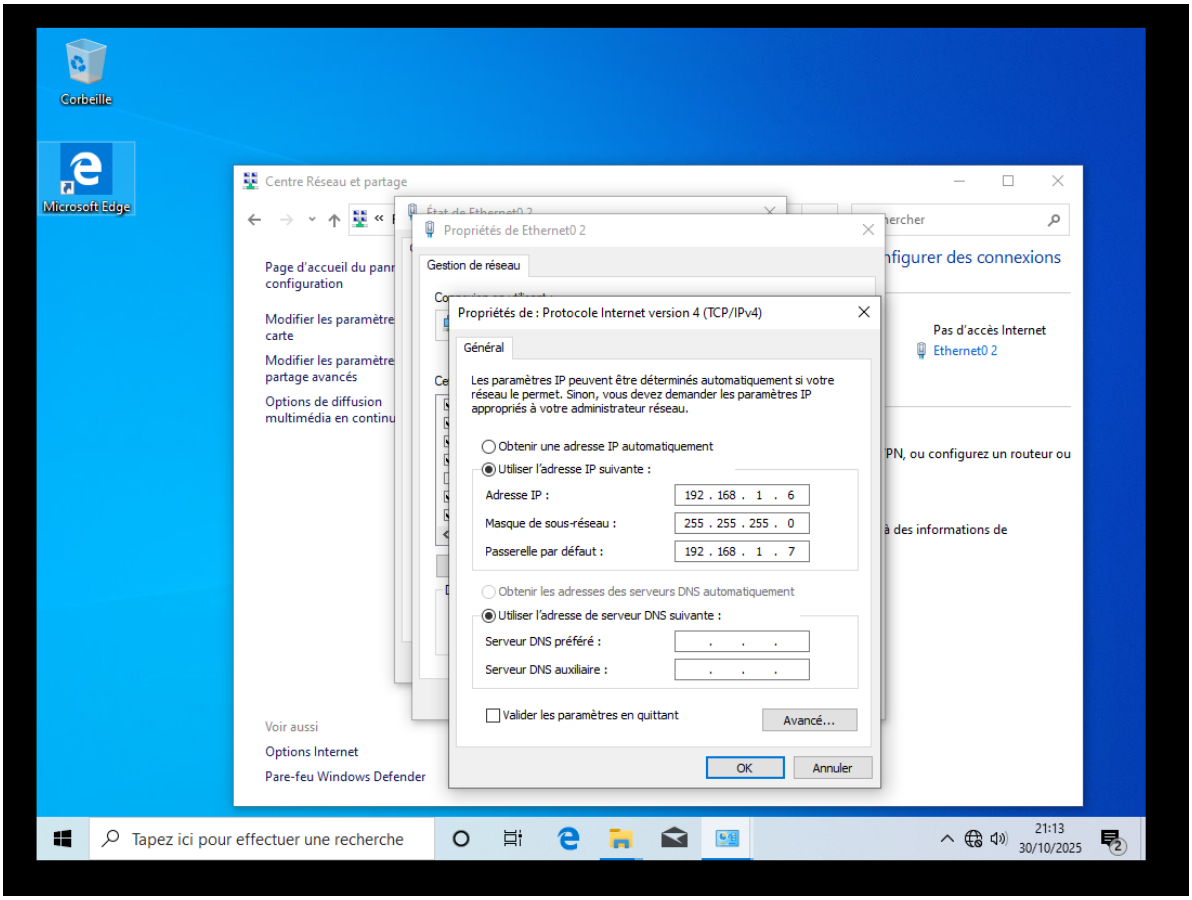
Adressage de la machine Windows et test de ping

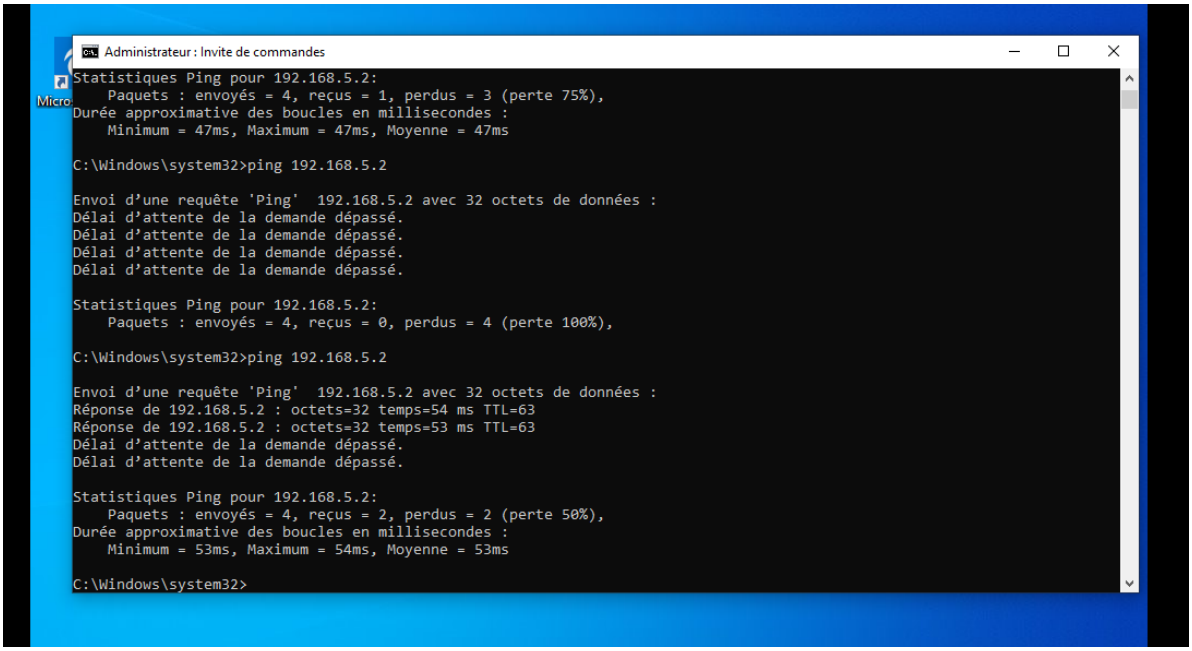
Le test de connectivité révèle que le ping fonctionne normalement depuis Ubuntu vers toutes les machines Windows, mais que, dans le sens inverse, depuis Windows vers Ubuntu, deux requêtes échouent avant que les suivantes aboutissent. Ce comportement indique que la connectivité réseau est globalement opérationnelle, mais qu'un délai initial affecte la réponse d'Ubuntu. Les causes les plus probables sont la résolution ARP initiale, un filtrage partiel des paquets ICMP par le pare-feu d'Ubuntu (ufw ou iptables), ou encore un léger délai introduit par un environnement virtualisé ou une configuration réseau en mode pont/NAT. Après la première communication établie, les réponses deviennent normales, ce qui confirme qu'il ne s'agit pas d'une perte de connectivité, mais d'un léger retard lors de la première phase d'échange réseau.

Appareil	**Interface**	**Adresse IP**	**Masque de sous-réseau**	**Passerelle**
Win_10_Client1	e0	192.168.1.6	255.255.255.0	192.168.1.7 (FW1)
Win_10_Client2	e0	172.126.3.3	255.255.255.0	172.126.3.4 (R1)
Kali_1	e0	172.126.4.4	255.255.255.0	172.126.4.5 (R1)
Svr_Ubuntu_1	e0	192.168.5.2	255.255.255.0	192.168.5.1 (FW1)
Routeur R1	e0/0	192.168.2.8	255.255.255.0	-
Routeur R1	e0/1	172.126.4.5	255.255.255.0	-
Routeur R1	e0/2	172.126.3.4	255.255.255.0	-
Pare-feu FW1	port1	192.168.2.7	255.255.255.0	-
Pare-feu FW1	port2	192.168.1.7	255.255.255.0	-
Pare-feu FW1	port3	192.168.5.1	255.255.255.0	-

Table 1: Plan d'adressage des machines et équipements réseau avec passerelles




Corbeille
Microsoft Edge
Centre Réseau et partage
Propriétés de Ethernet0 2
Gestion de réseau
Propriétés de : Protocole Internet version 4 (TCP/IPv4)
Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP : 192 . 168 . 1 . 6
Masque de sous-réseau : 255 . 255 . 255 . 0
Passerelle par défaut : 192 . 168 . 1 . 7
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré :
Serveur DNS auxiliaire :
Valider les paramètres en quittant
Avancé...
OK
Annuler
Pas d'accès Internet
Ethernet0 2
Voir aussi
Options Internet
Pare-feu Windows Defender
Tapez ici pour effectuer une recherche
21:13
30/10/2025


Administrateur : Invite de commandes
Statistiques Ping pour 192.168.5.2:
Paquets : envoyés = 4, reçus = 1, perdus = 3 (perte 75%),
Durée approximative des boucles en millisecondes :
Minimum = 47ms, Maximum = 47ms, Moyenne = 47ms
C:\Windows\system32>ping 192.168.5.2
Envoi d'une requête 'Ping' 192.168.5.2 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Statistiques Ping pour 192.168.5.2:
Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
C:\Windows\system32>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=54 ms TTL=63
Réponse de 192.168.5.2 : octets=32 temps=53 ms TTL=63
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Statistiques Ping pour 192.168.5.2:
Paquets : envoyés = 4, reçus = 2, perdus = 2 (perte 50%),
Durée approximative des boucles en millisecondes :
Minimum = 53ms, Maximum = 54ms, Moyenne = 53ms
C:\Windows\system32>

0.3.1 Observation des communications

Les communications montrent que les échanges réseau entre les machines sont globalement établis correctement, mais qu'il existe un léger décalage dans la phase initiale de communication lorsque Windows interroge Ubuntu. Ce décalage, visible à travers les deux premiers délais dépassés, traduit un temps d'initialisation de la communication souvent lié à la découverte de l'adresse MAC (résolution ARP) ou à la levée d'un filtrage temporaire par le pare-feu d'Ubuntu. Une fois cette phase passée, les échanges ICMP se déroulent normalement, ce qui confirme que la liaison physique et logique entre les deux hôtes est stable et fonctionnelle.

0.3.2 Analyse du comportement réseau

L'analyse du comportement réseau met en évidence les éléments suivants :

- **Latence :** Une fois la communication établie, la latence observée est normale et stable. Les réponses ICMP sont reçues sans perte après les deux premières requêtes.
- **Délai initial :** Deux requêtes échouent au début du ping depuis Windows vers Ubuntu. Ce délai correspond à une phase d'initialisation du lien, souvent liée à la **résolution ARP** (remplissage de la table ARP lors du premier contact) ou à une légère temporisation du système.
- **Filtrage :** Il est possible qu'un **pare-feu** (UFW ou iptables sur Ubuntu) limite temporairement les paquets ICMP entrants. De même, certaines règles de sécurité ou antivirus sur Windows peuvent introduire un filtrage sélectif.
- **Virtualisation ou économie d'énergie :** Si Ubuntu fonctionne dans un environnement virtualisé ou si la carte réseau gère des modes d'économie d'énergie, un court délai d'activation de l'interface réseau peut également expliquer les deux premières pertes.

  Le comportement observé traduit un réseau fonctionnel, mais avec une légère latence d'initialisation. Après établissement de la communication, les échanges sont stables et continus, confirmant l'absence de perte de connectivité durable.

CONCLUSION

Nous voici arrivés au terme de notre lab, le ping passe entre les différentes machines et l'application web est accessible depuis la vm Windows.