

**REPUBLIQUE DU SENEGAL**



**UN PEUPLE-UN BUT-UNE FOI**

**MINISTERE DE L'ENSEIGNEMENT SUPERIEUR, DE LA RECHERCHE ET DE  
L'INNOVATION**

**DIRECTION GENERALE DE L'ENSEIGNEMENT SUPERIEUR PRIVE**

**INSTITUT SUPERIEUR D'INFORMATIQUE**

**Master 2 Sécurité des Systèmes d'informations**

**Conception et Simulation d'une Infrastructure  
Réseau Sécurisée et Supervisée sous GNS3**

**Présenté par**

**Mlle. Mariama DIACK**

**Sous la direction de :**

**M. Moussa DIEDHIOU**

**Année académique : 2024-2025**

# **PLAN**

- I. Introduction**
- II. Choix des Outils**
- III. Configuration des équipements**
- IV. Conception de l'architecture**
- V. Sécurité et Supervision**
- VI. Conclusion**

**Remarque importante :** Ce projet a été réalisé dans un environnement simulé avec des ressources limitées. Malgré l'usage de technologies comme Docker pour alléger le déploiement, certaines configurations ou scénarios n'ont pas pu être entièrement implémentés ou testés en raison de contraintes matérielles (manque de mémoire RAM, lenteurs sur GNS3, conflits réseau entre Docker et GNS3).

Néanmoins, les éléments essentiels ont été partiellement mis en place et documentés afin de refléter la logique, les objectifs et la structure globale de l'architecture réseau visée.

## I. Introduction

Dans un contexte où la cybersécurité et la supervision des infrastructures informatiques deviennent des enjeux majeurs, il est essentiel de mettre en place des solutions réseau complètes, virtualisées et sécurisées. Le présent projet vise à concevoir, configurer et simuler une architecture réseau réaliste et fonctionnelle à l'aide de l'outil de simulation GNS3, en intégrant des services de sécurité, de supervision et de filtrage web.

Cette infrastructure intègre divers équipements virtuels, tels que des routeurs, switchs, clients (Windows et Kali Linux), ainsi qu'un serveur Debian 12 hébergeant plusieurs services critiques à travers des conteneurs Docker. Parmi ces services, on retrouve notamment :

Wazuh, un SIEM open source pour la détection des menaces et la supervision des hôtes ;

NetAlertX, un outil de surveillance réseau en temps réel ;

Squid et SquidGuard, pour le proxy HTTP et le filtrage de contenu web.

L'objectif principal du projet est de simuler un réseau d'entreprise sécurisé, avec un accès Internet contrôlé, une surveillance active des systèmes, et une capacité de détection des comportements malveillants. L'ensemble de la configuration repose sur un environnement entièrement virtualisé via GNS3, permettant des tests pratiques et une grande flexibilité dans le déploiement.

Ce rapport détaille la démarche suivie pour la conception, la configuration et la validation de cette infrastructure, ainsi que les tests réalisés pour évaluer son efficacité en matière de sécurité et de supervision.

## II. Choix des Outils

Le choix des outils utilisés dans ce projet s'appuie sur des critères de fiabilité, de compatibilité avec la virtualisation, de richesse fonctionnelle et de pertinence pour la supervision et la sécurité réseau. Chacun des éléments retenus joue un rôle clé dans la simulation et l'évaluation de l'architecture réseau.

### \* **GNS3 (Graphical Network Simulator 3)**

GNS3 est un outil incontournable pour la virtualisation et la simulation de réseaux complexes. Il permet d'intégrer à la fois des équipements réseau (routeurs, switchs) et des

machines virtuelles (serveurs, clients). Il facilite la conception visuelle de topologies et le test de scénarios réalistes sans matériel physique.

#### \* **Debian 12**

Le système d'exploitation Debian 12 a été choisi pour sa stabilité, sa sécurité, et sa compatibilité avec Docker. Il sert de base au serveur principal qui héberge les différents services critiques (Wazuh, NetAlertX, Squid).

#### \* **Docker**

Docker permet de déployer rapidement des services isolés dans des conteneurs légers, facilitant la gestion, la configuration et la réutilisabilité. Il est utilisé pour héberger les services Wazuh, NetAlertX et le proxy, tout en évitant les conflits de dépendances.

#### \* **Wazuh**

Wazuh est un système de supervision et de sécurité (SIEM) open source. Il permet la surveillance des hôtes, la détection d'intrusions, l'analyse de logs et la gestion des alertes de sécurité. Son intégration dans le réseau offre une vue centralisée sur l'activité des machines.

#### \* **NetAlertX**

NetAlertX est un outil moderne de monitoring réseau. Il permet de détecter rapidement des anomalies, des déconnexions ou des comportements suspects. Il est complémentaire à Wazuh pour une supervision en temps réel du réseau.

#### \* **Squid & SquidGuard**

Squid est un proxy HTTP permettant de cacher, contrôler et filtrer le trafic web des utilisateurs. SquidGuard agit comme un plugin de filtrage, permettant d'appliquer des règles de contrôle d'accès basées sur des listes (blacklist/whitelist).

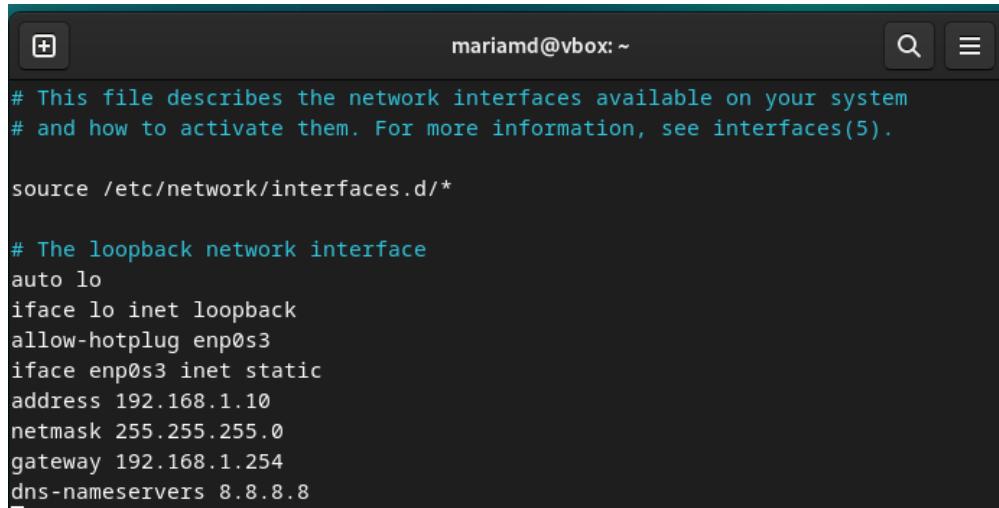
#### \* **Kali Linux & Windows**

Deux types de clients sont utilisés :

Kali Linux, pour les tests d'intrusion, l'analyse de vulnérabilités, et les attaques simulées.

Windows, pour simuler un poste utilisateur classique dans une entreprise.

### III. Configuration des Équipements



```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces/*

# The loopback network interface
auto lo
iface lo inet loopback
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.1.10
netmask 255.255.255.0
gateway 192.168.1.254
dns-nameservers 8.8.8.8
```

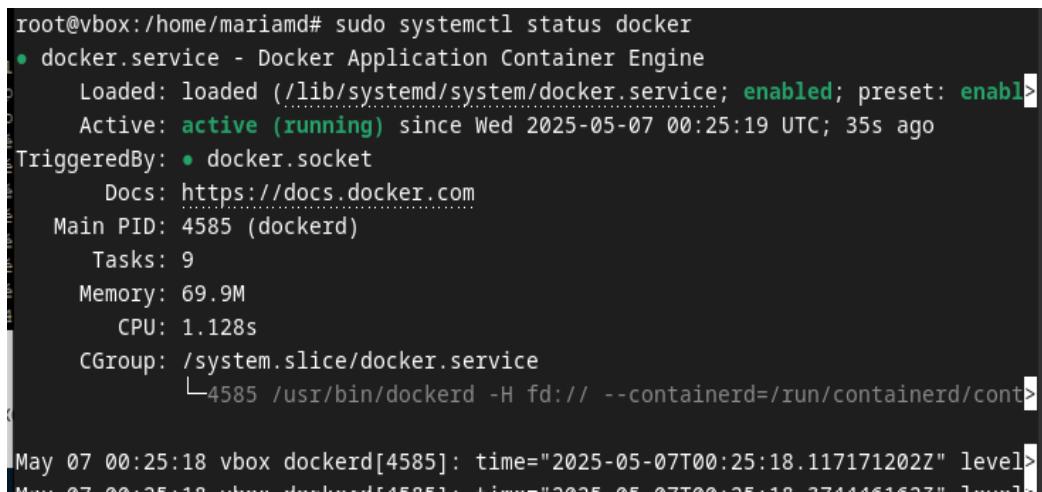
*Figure 1: Configuration réseau*

Il s'agit d'un fichier de configuration réseau Linux (/etc/network/interfaces) avec :

- Interface loopback configurée
- Interface enp0s3 en IP statique (192.168.1.10/24)
- Passerelle 192.168.1.254
- Serveur DNS 8.8.8.8 (Google)

#### A. Configuration Docker

<https://www.it-connect.fr/installation-pas-a-pas-de-docker-sur-debian-11/>



```
root@vbox:/home/mariamd# sudo systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/lib/systemd/system/docker.service; enabled; preset: enabled)
   Active: active (running) since Wed 2025-05-07 00:25:19 UTC; 35s ago
     Tasks: 9
    Memory: 69.9M
      CPU: 1.128s
     CGroup: /system.slice/docker.service
             └─4585 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock

May 07 00:25:18 vbox dockerd[4585]: time="2025-05-07T00:25:18.117171202Z" level=info msg="Containerd version: containerd@vbox:~$
```

*Figure 2: Test Docker*

```

root@vbox:/home/mariamd# docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
e6590344b1a5: Pull complete
Digest: sha256:c41088499908a59aae84b0a49c70e86f4731e588a737f1637e73c8c09d995654
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

```

*Figure 3: Test Docker*

Commande **docker run hello-world** qui montre :

- Docker fonctionne correctement
- Téléchargement de l'image hello-world depuis Docker Hub
- Création d'un conteneur et affichage du message de bienvenue
- Suggestions pour tester des images plus complexes comme Ubuntu

## B. Configuration de Wazuh

<https://www.it-connect.fr/xdr-deploiement-de-wazuh-pour-creer-un-lab-cybersecurite/>

```

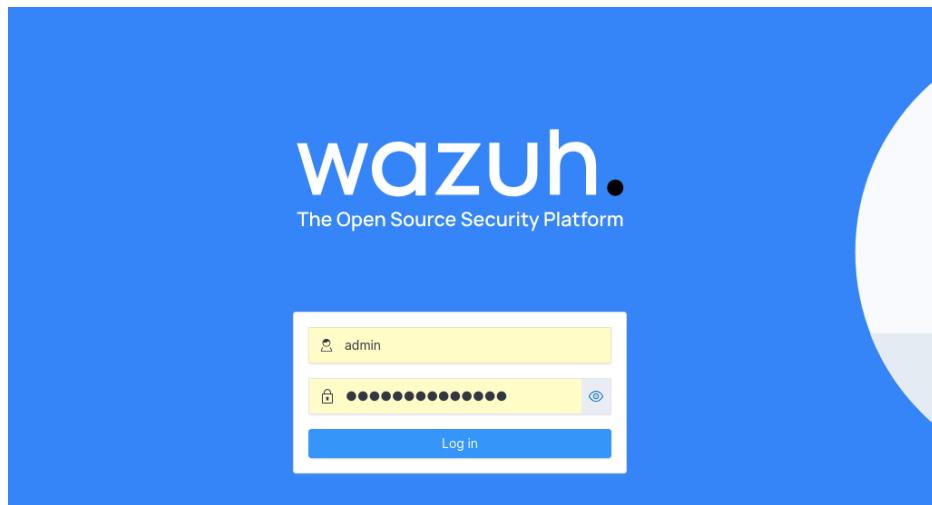
root@vbox:/home/mariamd/wazuh-docker/single-node# docker compose up -d
WARN[0002] /home/mariamd/wazuh-docker/single-node/docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please remove it to avoid potential confusion
WARN[0002] Found orphan containers ([single-node-generator-1]) for this project.
If you removed or renamed this service in your compose file, you can run this command with the --remove-orphans flag to clean it up.
[+] Running 3/3
✓ Container single-node-wazuh.manager-1    Running      0.0s
✓ Container single-node-wazuh.indexer-1    Running      0.0s
✓ Container single-node-wazuh.dashboard-1  Running      0.0s

```

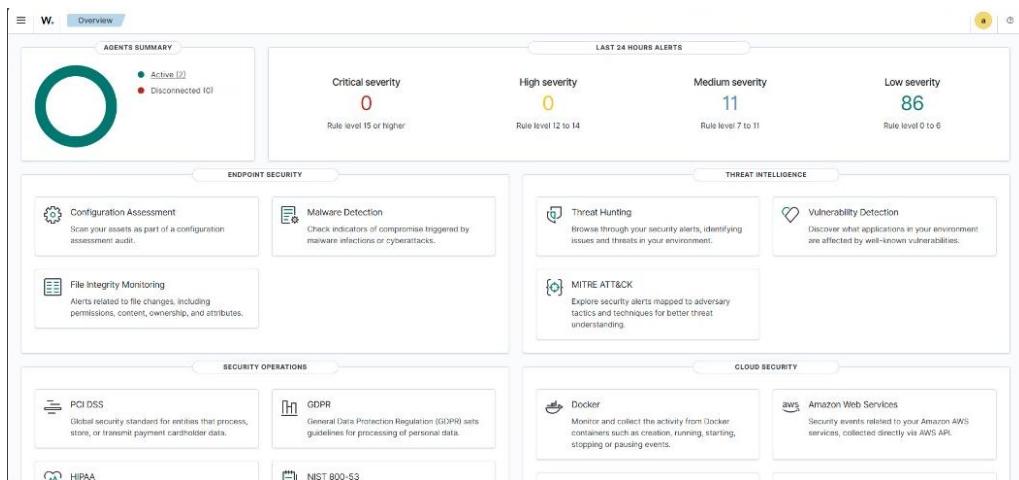
*Figure 4: Déploiement wazuh*

Exécution de **docker compose up -d** pour déployer Wazuh (solution de sécurité) en mode single-node :

- Trois services démarrés avec succès :
  - **Wazuh Manager**
  - **Wazuh Indexer**
  - **Wazuh Dashboard**



**Figure 5: Page de connexion de Wazuh**



**Figure 6: L'interface de wazuh**

L'interface montre le tableau de bord Wazuh avec :

Deux agents enregistrés la machine client Win10 et Wazuh

### Sections principales :

- **Chocolate Security** : Surveillance de configuration, intégrité des fichiers, détection de malware
- **Threat Intelligence** : Chasse aux menaces, cadre MITRE ATT&CK, détection de vulnérabilités

Tableau des alertes par niveau de严重性 (Critical à Low)

### C. Configuration de NetAlertx

<https://www.it-connect.fr/tuto-netalertx-surveillance-reseau-detecter-appareil/>

```

root@vbox:/opt/docker-compose/netalertx# docker compose up -d
[+] Running 8/8
  ✓ netalertx Pulled
    ✓ f18232174bc9 Pull complete   120.7s
    ✓ 3214a9cdd72f Pull complete   8.1s
    ✓ 8a318d0babe7 Pull complete   66.1s
    ✓ fbe43fdcd7ff Pull complete   66.4s
    ✓ 09f197029662 Pull complete   109.7s
    ✓ 6825ededa86 Pull complete   114.7s
    ✓ fe9fcbb62365f Pull complete   114.9s
    ✓ fe9fcbb62365f Pull complete   115.5s
[+] Running 4/4
  ✓ Volume "netalertx_log"        Created   0.1s
  ✓ Volume "netalertx_config"     Created   0.0s
  ✓ Volume "netalertx_db"         Created   0.0s
  ✓ Container netalertx          Started   4.0s
root@vbox:/opt/docker-compose/netalertx#

```

*Figure 7: Déploiement de NetAlertx*

Commande **docker compose up -d** qui :

- Télécharge 8 couches d'images Docker (temps variant de 8.15s à 120.75s)
- Crée 3 volumes (log, config, db)
- Lance le conteneur NetAlertX

The screenshot shows the NetAlertX web application running at [192.168.1.24:15000/devices.php](http://192.168.1.24:15000/devices.php). The interface includes a sidebar with navigation links like Devices, Monitoring, Network, Maintenance, Settings, Integrations, Workflows, and System info. The main dashboard displays various metrics: 2 My Devices, 2 Connected devices, 0 Favorites, 1 New Device, 0 Down devices, and 0 Archived devices. Below this is a chart titled 'Device presence' showing the status of devices over time, with a legend for Online (green), Down (red), Offline (grey), and Archived (light grey). The chart shows a large green bar representing online devices from 23:26. A 'Filters' section allows users to refine the device list by Source Plugin and Type. The 'My Devices' section lists devices with columns for Icon, Name, Type, Last IP, Status, Full MAC, Source Plugin, and Props / Actions.

*Figure 8: Interface de NetAlertx*

NetAlertX est une solution open source de surveillance réseau qui permet :

- La détection des appareils connectés au réseau
- La surveillance de la présence des appareils

- Un système de notifications (email, webhooks)
- L’analyse des vulnérabilités réseau

## Publishers

Load more Publishers with the `LOADED_PLUGINS` setting

@ Email publisher (SMTP)	
A plugin to publish a notification via Email (SMTP) gateway. <a href="#">Read more in the docs.</a>	
When to run <code>SMTP_RUN</code> ⓘ	Enable sending notifications via the Email (SMTP) gateway. disabled
Command <code>SMTP_CMD</code> ⓘ	<code>python3 /app/front/plugins/_publisher_email/email_smtp.py</code>
Run timeout <code>SMTP_RUN_TIMEOUT</code> ⓘ	Maximum time in seconds to wait for the script to finish. If this time is exceeded the script is aborted. 20
SMTP server URL <code>SMTP_SERVER</code> ⓘ	The SMTP server host URL. For example <code>smtp-relay.sendinblue.com</code> . To use Gmail as an SMTP server <a href="#">follow this guide</a> smtp.gmail.com
SMTP server PORT <code>SMTP_PORT</code> ⓘ	Port number used for the SMTP connection. Set to <code>0</code> if you do not want to use a port when connecting to the SMTP server. 587
Skip authentication <code>SMTP_SKIP_LOGIN</code> ⓘ	Do not use authentication when connecting to the SMTP server. <input type="checkbox"/>
<input type="text" value="Filter Settings..."/> <span style="border: 1px solid #ccc; padding: 2px;">X</span> <span style="background-color: green; color: white; padding: 2px 10px; border-radius: 5px;">Save</span>	

**Figure 9: Configuration du Publisher Email SMTP dans NetAlertX**

 Set password	
A simple plugin to set the web ui password on app start. <a href="#">Read more in the docs.</a>	
Enable login <code>SETPWD_enable_password</code> ⓘ	When enabled a login dialog is displayed. If facing issues, you can always disable the login by setting <code>SETPWD_enable_password=False</code> in your <code>app.conf</code> file. <input checked="" type="checkbox"/>
Password <code>SETPWD_password</code> ⓘ	The default password is <code>123456</code> . *****

**Figure 10: Sécurisation de l'accès à l'interface NetAlertX**

When to run <small>SMTP_RUN</small>	Enable sending notifications via the Email (SMTP) gateway.	on_notification	<input type="button" value="▼"/>	<input type="button" value="✖"/>
Command <small>SMTP_CMD</small>	Command to run	python3 /app/front/plugins/_publisher_email/email_smtp.py		
Run timeout <small>SMTP_RUN_TIMEOUT</small>	Maximum time in seconds to wait for the script to finish. If this time is exceeded the script is aborted.	20	<input type="button" value="▼"/>	<input type="button" value="✖"/>
SMTP server URL <small>SMTP_SERVER</small>	The SMTP server host URL. For example <code>smtp-relay.sendinblue.com</code> . To use Gmail as an SMTP server follow this guide	smtp.gmail.com		
SMTP server PORT <small>SMTP_PORT</small>	Port number used for the SMTP connection. Set to <code>0</code> if you do not want to use a port when connecting to the SMTP server.	587	<input type="button" value="▼"/>	<input type="button" value="✖"/>
Skip authentication <small>SMTP_SKIP_LOGIN</small>	Do not use authentication when connecting to the SMTP server.	<input type="checkbox"/>		
SMTP user <small>SMTP_USER</small>	The user name used to login into the SMTP server (sometimes a full email address).	mdiack700@gmail.com		
SMTP password <small>SMTP_PASS</small>	The SMTP server password.	*****		
Do not use TLS <small>SMTP_SKIP_TLS</small>	Disable TLS when connecting to your SMTP server.	<input type="checkbox"/>		
Force SSL <small>SMTP_FORCE_SSL</small>	Force SSL when connecting to your SMTP server.	<input type="checkbox"/>		
Send email to <small>SMTP_REPORT_TO</small>	Email address to which the notification will be send to.	mdiack700@gmail.com		
<input type="button" value="Cancel"/> <input type="button" value="Save"/>				
<input type="text" value="Filter Settings..."/>				

*Figure 11: Configuration SMTP Sécurisée pour NetAlertX*

## D. Configuration de Proxy

<https://www.it-connect.fr/mise-en-place-et-configuration-dun-proxy-avec-squid/>

Dans ce projet, le proxy (Squid + SquidGuard) joue plusieurs rôles essentiels en matière de sécurité, de contrôle d'accès et de supervision réseau. Voici à quoi il sert précisément :

- ❖ Fonctions principales du proxy :

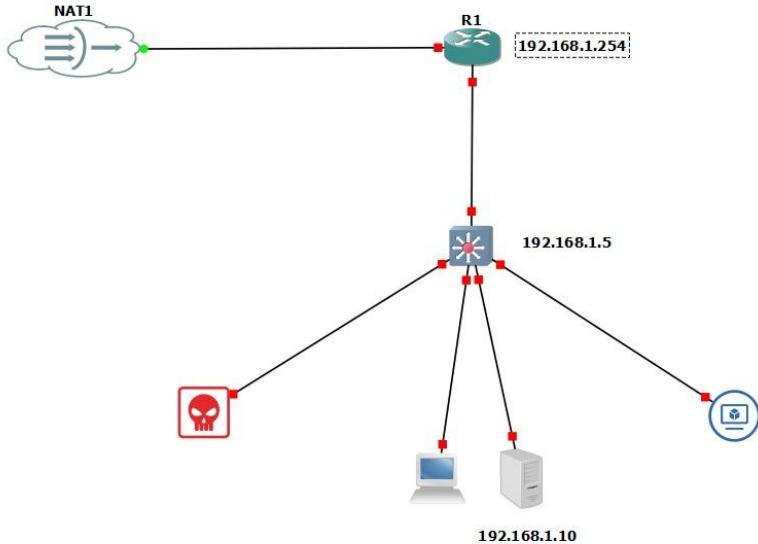
### Filtrage de contenu web

- Grâce à SquidGuard, certains sites sont bloqués (ex. : réseaux sociaux, streaming, contenus inappropriés).
- Cela permet de restreindre les usages non professionnels et de protéger contre les sites malveillants.

### Contrôle de la navigation des utilisateurs

- Les utilisateurs ne peuvent naviguer que via le proxy (accès direct bloqué).
- Cela centralise le trafic HTTP/HTTPS, ce qui facilite l'analyse et le contrôle.

## IV. Conception de l'architecture



*Figure 12: Topologie de l'infrastructure*

Les éléments de la topologie :

❖ **NAT1 :**

- Représente la connexion Internet simulée dans GNS3.
- Permet à la topologie d'accéder à Internet via une interface NAT fournie par la machine hôte.

❖ **R1 (192.168.1.254) :**

- Fait office de passerelle principale pour le réseau local.
- Configure le NAT interne pour permettre aux hôtes de sortir vers Internet.
- Connecté d'un côté à NAT1 (Internet) et de l'autre au switch via l'adresse 192.168.1.254.

❖ **Switch (192.168.1.5) :**

- Interconnecte tous les hôtes internes.
- Pas de configuration IP spécifique (niveau 2), mais central dans le brassage réseau.

❖ **Client Kali :**

- Utilisé pour les tests d'intrusion et d'analyse de sécurité.
- Effectue des scans, des attaques, et génère du trafic à analyser par Wazuh.

❖ **Client Windows :**

- Représente un poste utilisateur typique accédant à Internet via le proxy.
- Utilisé pour les tests d'accès web, de filtrage et de remontée d'événements.

❖ **Serveur Debian (IP : 192.168.1.10) :**

- Héberge plusieurs services critiques via Docker, notamment :
  - Wazuh (supervision SIEM),
  - NetAlertX (monitoring),
  - Squid & SquidGuard (proxy filtrant).
- Joue un rôle central dans la sécurité et la supervision du réseau.

## V. Sécurité et supervision

Élément	Outil utilisé	Fonction assurée
Supervision système	Wazuh	SIEM, détection d'intrusions
Monitoring réseau	NetAlertX	Disponibilité, alertes hôtes
Filtrage web	Squid + SquidGuard	Contrôle d'accès HTTP/HTTPS
Tests de sécurité	Kali Linux	Évaluation des défenses, test des alertes

## VI. Conclusion

Ce projet a permis de concevoir et de simuler une infrastructure réseau sécurisée et supervisée à l'aide d'outils libres et performants. Grâce à GNS3 et Docker, nous avons pu déployer une architecture complète incluant :

- ❖ Un accès Internet contrôlé via un proxy filtrant,
- ❖ Une surveillance centralisée avec Wazuh et NetAlertX,
- ❖ Des tests de vulnérabilité réalistes avec Kali Linux,
- ❖ Une visualisation claire des événements de sécurité.

Les tests ont démontré le bon fonctionnement de l'ensemble, la capacité à détecter des incidents, et la réactivité des outils mis en œuvre. Ce projet a renforcé les compétences en

configuration réseau, supervision, sécurité informatique et déploiement de services en conteneurs.