

Conception et mise en œuvre d'une architecture réseau sécurisée multi- zones avec pfSense

A series of five parallel, light blue diagonal lines that extend from the bottom left towards the top right of the page, positioned behind the footer text.

Juste Fourier ACKO
Formation en réseaux et cybersécurité

Table des matières

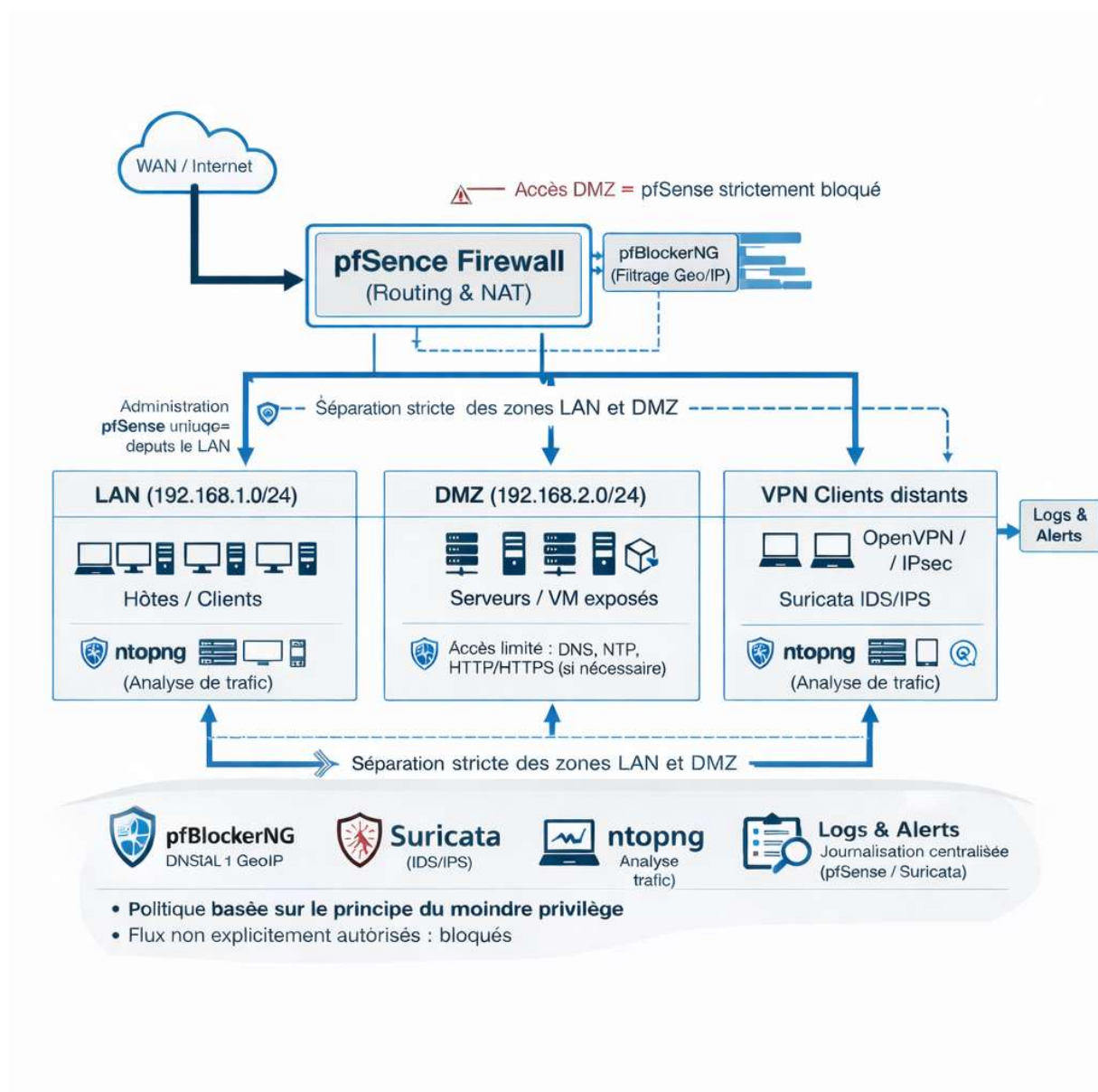
Introduction	2
Architecture globale.....	2
1. Objectif du projet	3
2. Environnement et prérequis	3
2.1 Environnement de virtualisation	3
3. Architecture réseau	3
3.1 Topologie logique.....	3
3.2 Plan d'adressage IP	3
4. Configuration initiale de pfSense	4
4.1. Accès à l'interface Web de pfSense	4
Démarche	4
• Sécurisation de l'accès à l'interface Web (passage HTTP vers HTTPS).....	4
4.2. Assignation des interfaces	5
4.3. Activation des interfaces.....	5
5. Configuration du pare-feu (Firewall)	6
5.1 Règles LAN	6
Objectif.....	6
5.2 Règles DMZ	6
Objectif.....	6
5.3 Règles WAN.....	6
6. Tests de connectivité.....	7
6.1 Tests réalisés	7
6.2 Analyse des logs	7
7. Ajout d'outils de sécurité complémentaires	7
a. Suricata – Système de détection/prévention d'intrusion (IDS/IPS)	7
• Rôle dans le lab	7
• Intégration avec pfSense.....	7
• Configuration mise en place.....	8
b. pfBlockerNG – Filtrage IP et géographique	8
• Rôle dans le lab	8
• Configuration mise en place.....	9
c. ntopng – Supervision et analyse du trafic réseau	9
• Rôle dans le lab	9
• Configuration mise en place.....	9
8. Centralisation des logs et visibilité	10
9. Justification des choix techniques.....	10
Conclusion	11

Introduction

Ce projet présente la conception et la mise en œuvre d'une architecture réseau sécurisée basée sur un pare-feu **pfSense**, destinée à segmenter et protéger un système d'information moderne. L'objectif est de mettre en place une infrastructure intégrant un filtrage avancé (GeoIP), une DMZ pour les services exposés, un accès VPN sécurisé pour les utilisateurs distants, ainsi que des sondes de supervision et de détection d'intrusions (ntopng et Suricata) afin d'améliorer la visibilité, la détection et la réaction face aux menaces.

Cette approche permet d'illustrer des bonnes pratiques de cybersécurité, notamment la séparation des zones (LAN, DMZ, VPN), la centralisation des journaux et le renforcement de la sécurité périmétrique dans un contexte pédagogique et opérationnel.

Architecture globale



1. Objectif du projet

L'objectif de ce laboratoire est de concevoir et déployer une architecture réseau sécurisée multi-zones à l'aide du pare-feu pfSense, intégrant :




- Une séparation logique WAN / LAN / DMZ
- Des règles de filtrage strictes basées sur le principe du moindre privilège
- Des mécanismes de détection et de prévention d'intrusion
- Des outils de filtrage, de supervision et de journalisation

Ce lab a pour but de reproduire une architecture réaliste d'entreprise, exploitable dans un contexte pédagogique, de test ou de démonstration de sécurité.

2. Environnement et prérequis

2.1 Environnement de virtualisation

- Hyperviseur : **Oracle VirtualBox**
- Pare-feu : **pfSense CE**
- Machines virtuelles :

-  pfSense
-  Machine hôte LAN
-  Machine cliente DMZ

3. Architecture réseau

3.1 Topologie logique

Interface pfSense	Mode VirtualBox	Rôle
WAN (em0)	NAT	Accès Internet simulé
LAN (em1)	Host-Only	Réseau interne
DMZ (em2)	Internal Network	Zone serveur isolée

3.2 Plan d'adressage IP

Zone	Adresse IP	Masque
WAN	DHCP (VirtualBox NAT)	-
LAN	192.168.1.1	/24
DMZ	192.168.2.1	/24
Hôte LAN	192.168.1.254	/24
Client DMZ	192.168.2.100	/24

4. Configuration initiale de pfSense

4.1. Accès à l'interface Web de pfSense

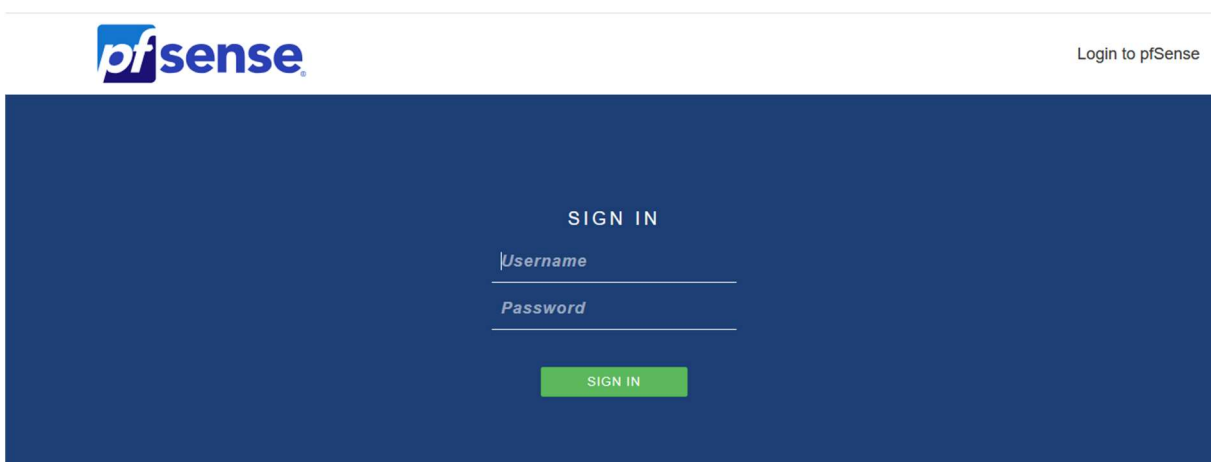
Administrer pfSense via son interface graphique Web.

Démarche

- Depuis la machine hôte LAN
- Accès à l'URL : <http://192.168.1.1>

Une fois connecté :

- Accès à l'interface WebConfigurator
- Visualisation des interfaces, services et règles de sécurité



Sécurisation de l'accès à l'interface Web (passage HTTP vers HTTPS)

Objectif

Sécuriser l'accès à l'interface d'administration de pfSense en chiffrant les échanges entre l'administrateur et le pare-feu.

Démarche

Accès à l'interface WebConfigurator de pfSense

Navigation vers :

- System → Advanced → Admin Access

Activation du protocole HTTPS pour l'interface Web

- Sélection d'un certificat SSL (certificat auto-signé dans le cadre du laboratoire)

Application de la configuration

Une fois la configuration appliquée :

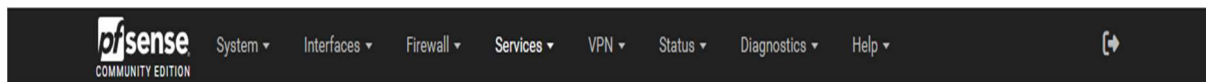
- L'interface Web est accessible uniquement via l'URL : <https://192.168.1.1>

Une alerte de sécurité du navigateur peut apparaître en raison du certificat auto-signé, ce comportement étant normal dans un environnement de test.

Cette étape permet de garantir la confidentialité des identifiants et des échanges lors de l'administration de pfSense, conformément aux bonnes pratiques de sécurité.

4.2. Assignment des interfaces

Associer chaque interface physique détectée par pfSense à une zone logique (WAN, LAN, DMZ).



Démarche :

Depuis la console pfSense :







- Accès au menu **Interfaces**
- Affectation des interfaces :
 - WAN → em0
 - LAN → em1
 - DMZ → em2
- VLAN : **non utilisés**
- Refus de la configuration VLAN (non nécessaire pour ce lab)

Cette étape permet à pfSense de **distinguer les flux entrants selon leur zone d'origine**, principe fondamental du filtrage stateful.

4.3. Activation des interfaces

Pour chaque interface :

- Option **Enable Interface** activée
- Adresse IP statique définie pour LAN et DMZ
- DHCP activé sur LAN et DMZ

Interfaces			
 WAN		1000baseT <full-duplex>	10.0.2.15 fd17:625c:f037:2:a00:27ff:feb7:18c
 LAN		1000baseT <full-duplex>	192.168.1.1
 DMZ		1000baseT <full-duplex>	192.168.2.1

5. Configuration du pare-feu (Firewall)

Le pare-feu pfSense est **stateful** et applique les règles sur l'interface **d'entrée du trafic**.

5.1 Règles LAN

Ordre	Source	Destination	Protocole	Action
1	LAN net	DMZ net	HTTPS	Pass
2	LAN net	WAN net	HTTP / HTTPS	Pass
3	LAN net	WAN net	DNS	Pass
4	LAN net	pfSense	HTTPS	Pass
5	LAN net	any	any	Block

Objectif

- Autoriser l'accès à Internet depuis le réseau interne (LAN) pour les services nécessaires.
- Permettre un **accès contrôlé à la zone DMZ**, limité aux protocoles et services explicitement définis.
- Bloquer par défaut **tout trafic non explicitement autorisé**, conformément au principe du moindre privilège.

5.2 Règles DMZ

Ordre	Source	Destination	Protocole	Action
1	DMZ net	LAN net	any	Block
2	DMZ net	pfSense (LAN address)	any	Block
3	DMZ net	pfSense (LAN address)	DNS	Pass
4	DMZ net	any	NTP	Pass
5	DMZ net	WAN net	HTTP / HTTPS	Pass
6	DMZ net	any	any	Block

Objectif

- Assurer une **isolation stricte** de la DMZ vis-à-vis du LAN et du pare-feu.
- Autoriser uniquement les **services nécessaires** à la DMZ (DNS, NTP, HTTP/HTTPS si nécessaire).
- Bloquer **tout trafic non explicitement autorisé**, garantissant ainsi la sécurité des serveurs exposés.

5.3 Règles WAN

- Politique par défaut : **block all**
- Port forwarding optionnel
- WAN TCP 80 → Serveur DMZ

6. Tests de connectivité

6.1 Tests réalisés

Test	Résultat attendu	Commentaire
Ping LAN → pfSense LAN	OK	L'interface LAN est accessible pour l'administration
Ping LAN → DMZ	Bloqué	ICMP n'est pas autorisé vers la DMZ (selon règles strictes)
LAN → DMZ (HTTP/HTTPS)	OK	Les flux web autorisés passent
DMZ → LAN	Bloqué	Isolation stricte, règle de sécurité essentielle
LAN → Internet (HTTP/HTTPS)	OK	Navigation web autorisée
DMZ → WAN (HTTP/HTTPS, NTP, DNS)	OK	Accès sortant limité aux services autorisés
LAN → DMZ	Bloqué	Vérifie que seuls les services explicitement autorisés passent

6.2 Analyse des logs

- Menu : **Status** → **System Logs** → **Firewall**
- Vérification des règles appliquées (Pass / Block)
- Activation du logging sur certaines règles pour le diagnostic

7. Ajout d'outils de sécurité complémentaires

Afin de renforcer la sécurité du lab et d'élargir les capacités de détection, de prévention et de supervision, plusieurs **outils complémentaires** ont été déployés sur pfSense. Ces outils permettent de couvrir différents axes de la sécurité réseau : **détection d'intrusion, filtrage, visibilité et journalisation**.

a. Suricata – Système de détection/prévention d'intrusion (IDS/IPS)

Suricata est un moteur open-source de **détection et de prévention d'intrusion réseau (IDS/IPS)**.

Il analyse le trafic réseau en temps réel et le compare à des **signatures d'attaques connues**.

Rôle dans le lab

- Détection des scans réseau
- Détection d'attaques applicatives (HTTP, DNS, brute force, etc.)
- Analyse comportementale du trafic LAN et DMZ

Intégration avec pfSense

Suricata a été installé directement via le **gestionnaire de paquets pfSense**, ce qui permet :

- Une intégration native avec les interfaces LAN et DMZ
- Une gestion centralisée des alertes
- Une exploitation conjointe avec le firewall pfSense

Configuration mise en place

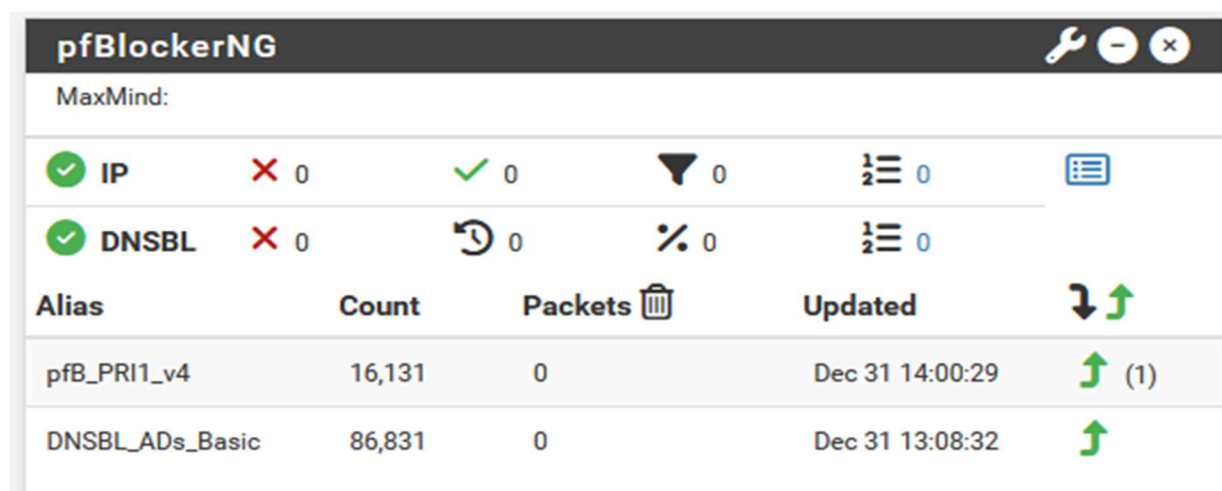
Paramètre	Configuration
Interfaces surveillées	LAN, DMZ
Mode	IDS (détection uniquement)
Jeu de règles	Emerging Threats Open
Protocoles analysés	ICMP, TCP, HTTP, DNS
Journalisation	Activée

Le mode IDS a été privilégié afin d'observer les attaques **sans bloquer automatiquement le trafic**.

b. pfBlockerNG – Filtrage IP et géographique

pfBlockerNG est une extension de pfSense permettant :

- Le **blocage d'adresses IP malveillantes**
- Le **géoblocage**
- Le filtrage DNS (publicités, domaines malveillants)



pfBlockerNG					
MaxMind:					
✓ IP	✗ 0	✓ 0	🔍 0	📋 0	📄
✓ DNSBL	✗ 0	🔄 0	📊 0	📋 0	
Alias	Count	Packets 🗑️	Updated		↕
pfB_PRI1_v4	16,131	0	Dec 31 14:00:29	📈 (1)	
DNSBL_ADs_Basic	86,831	0	Dec 31 13:08:32	📈	

Rôle dans le lab

pfBlockerNG agit comme une **première ligne de défense**, bloquant les connexions indésirables **avant même qu'elles n'atteignent le firewall applicatif**.

Il est principalement utilisé sur l'interface **WAN**.

🔧 Configuration mise en place

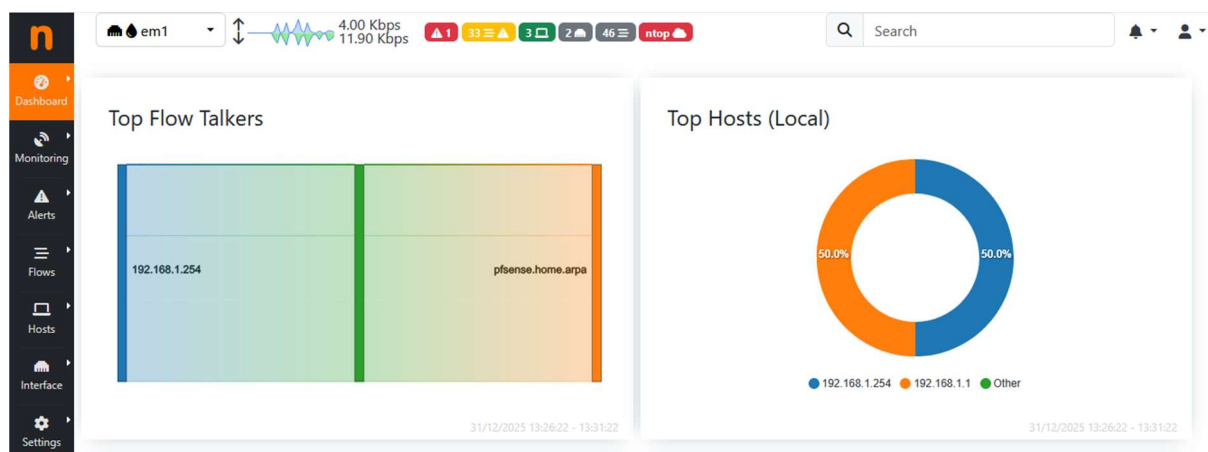
Fonction	État
Listes IP (Threat feeds)	Activées
Blocage WAN entrant	Activé
Journaux	Activés
Mises à jour automatiques	Activées

Ce filtrage réduit significativement l'exposition de l'infrastructure aux sources de trafic malveillant connues.

c. ntopng – Supervision et analyse du trafic réseau

ntopng est un outil de **monitoring réseau avancé**, fournissant :

- Une visibilité temps réel sur les flux
- Des statistiques détaillées par hôte, protocole et interface
- Une aide à la détection d'anomalies



🔧 Rôle dans le lab

ntopng permet :

- De comprendre le comportement du trafic LAN et DMZ
- D'identifier les flux dominants
- De corrélérer des alertes Suricata avec l'activité réseau réelle

🔧 Configuration mise en place

Paramètre	Configuration
Interfaces surveillées	LAN, DMZ
Accès Web	Activé
Collecte des flux	Temps réel
Historique	Activé

8. Centralisation des logs et visibilité

L'ensemble des outils déployés permet une **vision globale de la sécurité** :

Outil	Fonction principale
pfSense Firewall	Filtrage et routage
Suricata	Détection d'intrusion
pfBlockerNG	Blocage préventif
ntopng	Supervision et analyse

Cette complémentarité permet :

- Une meilleure **détection des incidents**
- Une **analyse post-incident** efficace
- Une meilleure compréhension des flux réseau

9. Justification des choix techniques

Besoin	Outil choisi	Justification
Filtrage réseau	pfSense	Pare-feu stateful robuste
IDS	Suricata	Performant et open-source
Blocage préventif	pfBlockerNG	Réduction de surface d'attaque
Supervision	ntopng	Visibilité réseau avancée

L'ajout de ces outils transforme pfSense en une **plateforme de sécurité réseau complète**, capable de :

- Filtrer le trafic
- Détecter les attaques
- Surveiller le comportement réseau
- Fournir des logs exploitables pour l'analyse

Cette approche multicouche est conforme aux **bonnes pratiques de sécurité des systèmes d'information**.

Conclusion

Ce laboratoire a permis de mettre en place une **architecture réseau sécurisée multi-zones** reposant sur pfSense, avec une séparation claire entre les zones **WAN, LAN et DMZ**.

La configuration des **règles de filtrage firewall** a permis d'appliquer une politique de sécurité cohérente basée sur le principe du **moindre privilège**, tout en garantissant le bon fonctionnement des flux légitimes.

Les différents tests de connectivité et l'analyse des journaux ont validé l'**isolation effective entre le LAN et la DMZ**, confirmant la pertinence des choix de configuration. L'intégration de **Suricata** a apporté une capacité de détection d'intrusion, permettant d'identifier des comportements suspects et d'enrichir l'analyse de sécurité du réseau.

Par ailleurs, la mise en place de solutions de **VPN**, telles qu'**OpenVPN ou IPSec**, permet à des clients distants d'accéder de manière sécurisée aux ressources internes du réseau. Ces mécanismes assurent l'authentification des utilisateurs, la confidentialité des échanges et une meilleure traçabilité grâce à la journalisation des connexions.

Enfin, l'ajout d'outils complémentaires tels que **pfBlockerNG** et **ntopng** a renforcé la protection globale et amélioré la visibilité sur le trafic réseau.

Ce lab constitue ainsi une **base solide et réaliste** pour l'apprentissage et la démonstration des mécanismes fondamentaux de sécurité réseau, ainsi que pour de futurs travaux pratiques ou projets avancés.