OFPPT – ISTA TAZA

Infrastructure Digital – Option Systèmes et Réseaux

Rapport de projet fin de formation:

MISE EN PLACE D'UNE INFRASTRUCTURE AZURE SÉCURISÉE ET SUPERVISÉE

Année académique : 2025–2026

Réalisé par : Youssef Kachmar - Driss Jhilal

Encadré par : M. Majid Lamkadam

REMERCIEMENTS

Nous tenons à exprimer nos sincères remerciements à toutes les personnes qui ont contribué à la réalisation de ce projet de fin de formation.

Tout d'abord, nous adressons nos remerciements à M. Majid Lamkadam, et M. Meriem Mengad nos encadrants, pour leur accompagnement, leurs conseils et leur disponibilité tout au long de ce travail. Leur encadrement et leurs orientations ont été essentiels pour structurer le projet, résoudre les difficultés techniques rencontrées et améliorer la qualité des résultats obtenus.

Nous remercions également l'équipe pédagogique de l'OFPPT – ISTA TAZA, ainsi que tous les formateurs de la filière Infrastructure Digital – Option Systèmes et Réseaux, pour les connaissances et les compétences techniques transmises durant notre formation, qui ont constitué la base de ce projet.

Enfin, nous remercions toute personne ayant apporté, de près ou de loin, une aide ou un soutien durant la mise en œuvre de cette infrastructure (conseils, tests, retours, et encouragements).

TABLE DES MATIÈRES

LISTE DES FIGURES

RÉSUMÉ

Ce rapport présente la conception et la mise en place d'une infrastructure Azure sécurisée et supervisée, réalisée dans le cadre d'un projet de fin d'année à l'OFPPT – ISTA TAZA. L'objectif principal est de déployer un environnement cloud cohérent, segmenté et contrôlé, permettant d'héberger des services essentiels tout en garantissant la sécurité, la disponibilité, la traçabilité et la supervision.

L'infrastructure repose sur une architecture réseau segmentée en plusieurs sous-réseaux (Active Directory/DNS, Web, Clients, VoIP, Management). Le routage est maîtrisé via des tables de routage Azure (UDR) afin de forcer le trafic à transiter par une passerelle pfSense, utilisée comme pare-feu central (filtrage LAN/WAN, NAT). Un accès distant sécurisé est assuré grâce à OpenVPN avec une gestion des certificats (CA et certificats client/serveur).

Les services déployés incluent notamment un serveur Web publié via HAProxy en reverse proxy, ainsi qu'un service VoIP basé sur Asterisk, validé par des tests d'appels avec Zoiper. Sur le plan de la sécurité, un dispositif IDS/IPS est mis en place avec Suricata pour la détection d'attaques réseau (ex. scan Nmap). Enfin, l'infrastructure est surveillée et auditée via Zabbix (supervision) et Wazuh (SIEM/HIDS, alertes et vulnérabilités).

Les résultats obtenus démontrent la faisabilité d'un environnement Azure sécurisé et professionnel, capable d'héberger des services tout en offrant une visibilité complète sur l'état, la performance et les événements de sécurité.

INTRODUCTION GÉNÉRALE

Avec l'évolution rapide des technologies cloud, les organisations migrent de plus en plus leurs services vers des plateformes telles que Microsoft Azure, afin de bénéficier de la flexibilité, de la scalabilité et de la disponibilité offertes. Toutefois, cette migration introduit également de nouveaux enjeux, notamment en matière de sécurité, de gestion des accès, de segmentation réseau, de supervision et de détection des menaces.

Dans le cadre de notre formation à l'OFPPT – ISTA TAZA, ce projet de fin d'année a pour objectif de mettre en place une infrastructure Azure sécurisée et supervisée. L'idée principale est de construire un environnement réaliste, proche d'une infrastructure d'entreprise, intégrant des composants essentiels comme un pare-feu central, un VPN, un annuaire Active Directory, un service Web, un service VoIP, ainsi que des outils de monitoring et de sécurité.

Pour répondre à ces objectifs, nous avons adopté une démarche structurée :

analyser le besoin et définir une architecture cible ;
concevoir une segmentation réseau claire via des sous-réseaux dédiés ;
contrôler le routage grâce aux UDR afin d'imposer le passage par la passerelle de sécurité ;
mettre en place des services (AD/DNS, Web, VoIP) et valider leur fonctionnement ;
renforcer la sécurité par l'intégration de Suricata (IDS/IPS) ;
assurer la supervision et la visibilité via Zabbix et Wazuh ;
effectuer des tests afin de confirmer la conformité et la stabilité de l'infrastructure.
Ce rapport est organisé en chapitres décrivant successivement le cadre du projet, l'analyse des besoins, la conception détaillée de l'infrastructure, puis la partie sécurité/supervision et la validation par des tests. L'objectif final est de présenter une solution complète, cohérente et exploitable, mettant en avant les bonnes pratiques en réseau, sécurité et administration système dans un contexte cloud Azure.

CHAPITRE 1 : CADRE DU PROJET

Le déploiement d'une infrastructure cloud sécurisée nécessite une compréhension approfondie des besoins, des contraintes et des objectifs métiers. Dans un contexte réel, une infrastructure cloud doit assurer à la fois la disponibilité des services, la protection des données, le contrôle des accès, ainsi qu'une capacité de supervision permettant de détecter et de corriger rapidement les incidents.

Dans ce chapitre, nous présentons le cadre général du projet, le contexte dans lequel il a été réalisé, ainsi que les objectifs que nous avons cherchés à atteindre à travers la mise en place d'une infrastructure Azure sécurisée et supervisée.

1.1 Contexte du projet

Ces dernières années, le cloud computing est devenu un choix stratégique pour de nombreuses entreprises. Azure permet de déployer rapidement des ressources (réseaux, machines virtuelles, stockage) tout en offrant des services managés facilitant l'exploitation. Cependant, la simplicité de déploiement ne suffit pas : une infrastructure cloud doit être conçue selon des principes de sécurité (segmentation, filtrage, chiffrement, journalisation) et de performance (routage maîtrisé, optimisation des flux).

Dans le cadre de notre projet, nous avons construit une architecture réseau sur Azure en s'appuyant sur :

une segmentation en sous-réseaux dédiés (services, clients, management, VoIP) ;
une passerelle de sécurité pfSense jouant le rôle de pare-feu central ;
un accès distant sécurisé via OpenVPN ;
des services essentiels : Active Directory / DNS, serveur Web, VoIP ;
des outils de sécurité et de supervision : Suricata, Zabbix, Wazuh.

L’objectif est de disposer d’un environnement cohérent, sécurisé et observable, permettant d’illustrer une architecture moderne de type “entreprise” dans le cloud.

1.2 Objectifs du projet

L’objectif global du projet est de mettre en place une infrastructure Azure sécurisée et supervisée, capable d’héberger des services tout en garantissant un haut niveau de contrôle et de visibilité.

Les objectifs spécifiques sont :

- Concevoir une architecture réseau segmentée (VNet + subnets) adaptée aux rôles des machines ;
- Maîtriser le routage au moyen de tables de routage Azure (UDR) afin de forcer le passage par pfSense ;
- Déployer et sécuriser un VPN (OpenVPN) pour l’accès distant ;
- Mettre en place Active Directory / DNS pour la centralisation de l’authentification et la gestion des clients ;
- Publier un service Web en HTTPS via un reverse proxy (HAProxy) ;
- Mettre en œuvre un service VoIP (Asterisk) et le valider par des appels avec Zoiper ;
- Renforcer la sécurité réseau grâce à un IDS/IPS (Suricata) ;
- Assurer la supervision et la journalisation via Zabbix et Wazuh ;
- Valider la solution par une série de tests techniques.

1.3 Étude de l’existant

Avant de concevoir notre solution, il est important d’étudier les approches généralement utilisées pour sécuriser et superviser une infrastructure réseau, ainsi que les limites rencontrées lorsqu’on ne met pas en place une architecture structurée.

Dans de nombreux environnements, on observe :

- des réseaux peu ou pas segmentés (toutes les machines dans le même sous-réseau) ;
- un filtrage insuffisant ou dispersé (règles appliquées machine par machine) ;
- l’absence de VPN sécurisé pour l’administration ;
- un manque d’outils de supervision centralisée ;
- peu de visibilité sur les attaques et événements de sécurité.

1.3.1 Limites d’une infrastructure non segmentée

Lorsque tous les serveurs et clients partagent le même réseau, une compromission sur une machine (ex. poste client) peut faciliter la propagation vers d’autres services critiques (AD, Web, VoIP). L’absence de séparation logique augmente la surface d’attaque et réduit le contrôle sur les flux.

1.3.2 Limites d’une infrastructure sans pare-feu central

Sans passerelle de sécurité centrale (type pfSense/Firewall), le contrôle du trafic devient difficile. Les règles sont souvent réparties, non cohérentes, et difficiles à auditer. Cela entraîne des risques :

- exposition involontaire de services ;
- ports ouverts non maîtrisés ;
- difficulté à appliquer une politique de sécurité homogène.

1.3.3 Limites d’une infrastructure sans supervision et détection

Sans supervision, il est complexe d’anticiper les pannes ou de mesurer les performances. Sans IDS/IPS ni SIEM, les attaques (scans, tentatives d’exploitation) peuvent passer inaperçues. En cas d’incident, l’absence de logs centralisés rend l’analyse et la réponse plus lentes.

1.4 Solution proposée

Pour répondre à ces limites, notre solution repose sur une architecture Azure intégrant :

- **Segmentation réseau :** création d’un VNet et de plusieurs sous-réseaux dédiés (AD/DNS, Web, Clients, VoIP, Management).
- **Routage contrôlé :** mise en place d’UDR afin d’imposer le passage du trafic par pfSense.
- **Pare-feu central :** pfSense assure le filtrage LAN/WAN, NAT, et la centralisation de la politique de sécurité.
- **VPN sécurisé :** OpenVPN avec certificats (CA + certificats client/serveur).
- **Publication sécurisée :** HAProxy pour exposer le service Web en HTTPS.
- **Services métiers :** Active Directory/DNS, serveur Web, VoIP Asterisk.
- Sécurité & supervision : Suricata (IDS/IPS), Zabbix (monitoring), Wazuh (SIEM/HIDS).

Cette approche permet de construire une infrastructure robuste, avec un niveau de sécurité renforcé et une visibilité complète sur l’état des services et les événements de sécurité.

CHAPITRE 2 : ANALYSE DES BESOINS

Dans ce chapitre, nous présentons les besoins nécessaires à la réalisation de notre infrastructure Azure sécurisée et supervisée. Cette étape permet de définir clairement les fonctionnalités attendues, ainsi que les contraintes non fonctionnelles (sécurité, performance, disponibilité, etc.) afin de garantir une conception cohérente et conforme aux objectifs du projet.

2.1 Besoins fonctionnels :

- **Segmentation du réseau (VNet + Subnets) :** Mise en place de plusieurs sous-réseaux afin d'isoler les rôles (AD/DNS, Web, Clients, VoIP, Management) et réduire la surface d'attaque.
- **Routage contrôlé (UDR) :** Définition de tables de routage Azure pour forcer le trafic à transiter par une passerelle de sécurité.
- **Pare-feu central (pfSense) :** Application d'une politique de filtrage (LAN/WAN), gestion du NAT, contrôle des flux entrants et sortants.
- **Accès distant sécurisé (OpenVPN) :** Mise en place d'un VPN chiffré permettant l'administration à distance de manière sécurisée via certificats.
- **Services d'annuaire et de résolution (AD DS + DNS) :** Centralisation de l'authentification, gestion des postes et des utilisateurs, et résolution de noms interne/externe via DNS (forwarders).
- **Publication d'un service Web en HTTPS :** Exposition contrôlée d'un service Web via un reverse proxy (HAProxy) avec accès sécurisé.
- **Service VoIP (Asterisk) :** Mise en place d'un serveur VoIP permettant la communication via un client SIP (Zoiper), avec configuration SIP et validation d'appels.
- **Détection d'intrusion (Suricata) :** Surveillance du trafic, détection d'activités suspectes (ex. scan Nmap) et génération d'alertes.
- **Supervision et visibilité (Zabbix + Wazuh) :** Monitoring de l'état des services/VM et centralisation des événements de sécurité, alertes et vulnérabilités.

2.2 Besoins non fonctionnels :

- **Sécurité :** Chiffrement des accès (VPN), filtrage réseau, segmentation, certificats, journalisation et détection des menaces.

- **Disponibilité :** Les services critiques (pfSense, AD/DNS, Web, VoIP) doivent rester accessibles de manière stable.
- **Performance :** L'architecture doit limiter les latences inutiles et assurer un routage cohérent et efficace.
- **Traçabilité / Audit :** Conservation des logs et alertes pour faciliter l'analyse des incidents et la réponse aux attaques.
- **Maintenabilité :** Configuration claire, documentation et supervision permettant une administration et un dépannage rapides.

CHAPITRE 3 : CONCEPTION DE L'INFRASTRUCTURE

Après l'analyse des besoins, nous passons à la phase de conception. Cette étape consiste à définir l'architecture globale de l'infrastructure Azure, la segmentation réseau, ainsi que les composants de sécurité et de supervision qui assurent la protection et la visibilité sur l'environnement.

3.1 Architecture générale de la solution :

L'infrastructure est déployée sur Microsoft Azure et repose sur les principes suivants :

- ➔ Réseau virtuel (VNet) regroupant plusieurs sous-réseaux (subnets) dédiés selon le rôle des machines.
- ➔ pfSense utilisé comme passerelle de sécurité centrale (pare-feu + NAT + VPN).
- ➔ Active Directory / DNS pour la gestion des identités et la résolution de noms.
- ➔ Serveur Web publié via HAProxy en HTTPS.
- ➔ Service VoIP basé sur Asterisk, avec validation via Zoiper.
- ➔ Suricata pour la détection d'intrusion réseau.
- ➔ Zabbix pour la supervision des ressources et services.
- ➔ Wazuh pour la collecte des logs, alertes sécurité et détection de vulnérabilités.

Cette architecture vise à assurer une séparation claire des rôles, un contrôle strict des flux, et une observation continue de l'état de l'infrastructure.

Figure 1 : Topologie globale de l'infrastructure (Azure VNet + sous-réseaux + rôles)

3.2 Plan d'adressage et segmentation (subnets) :

La segmentation en sous-réseaux permet d'isoler les composants critiques et de limiter la propagation des attaques. Les principaux sous-réseaux sont :

- ➔ Subnet AD/DNS : héberge le contrôleur de domaine et le service DNS.
- ➔ Subnet Web : héberge le serveur Web et les composants associés.
- ➔ Subnet Clients : contient les machines clientes (tests et intégration domaine).
- ➔ Subnet VoIP : héberge le serveur Asterisk et les clients SIP si nécessaire.
- ➔ Subnet Management : réservé à l'administration et aux outils de supervision (Zabbix/Wazuh).
- ➔ La communication entre ces sous-réseaux est contrôlée par le routage et par les règles pfSense.

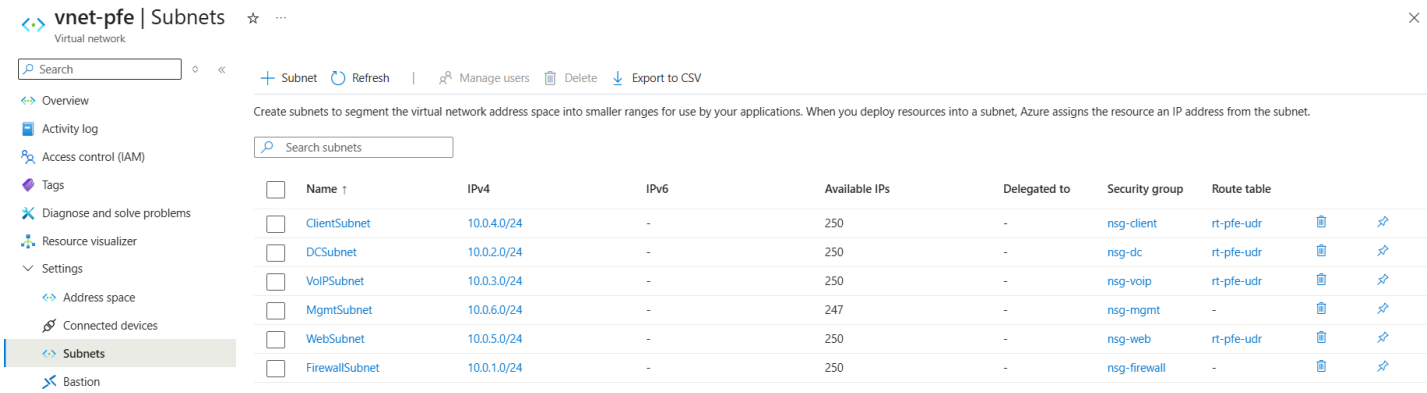

Figure 2 : Sous-réseaux Azure (segmentation)

Subnet	CIDR	Charge(s) / Workload(s)	IP(s) d'exemple	Objectif
DCSubnet	10.0.2.0/26	Windows Server (AD DS / DNS)	10.0.2.10	Identité + DNS (contrôleur de domaine, résolution interne)
VoIPSubnet	10.0.3.0/26	Asterisk PBX	10.0.3.4	Services SIP / RTP (téléphonie IP)
ClientSubnet	10.0.4.0/24	Client Windows	10.0.4.4	Tests / poste intégré au domaine
WebSubnet	10.0.5.0/24	Serveur Web (ex. Nginx)	10.0.5.10	Application Web interne derrière HAProxy
Management	10.0.6.0/24	Jumpbox, Zabbix, Wazuh	10.0.6.5 10.0.6.6 10.0.6.7	Exploitation / administration / supervision / SIEM

Figure 3 : Plan d'adressage du réseau

3.3 Choix technologiques (pfSense, Azure, OpenVPN, etc.)

- **Fournisseur Cloud : Microsoft Azure**

Le choix de Microsoft Azure comme infrastructure IaaS (Infrastructure as a Service) repose sur sa fiabilité, sa scalabilité et ses fonctionnalités réseau avancées. Azure permet une segmentation fine grâce aux VNets et aux Sous-réseaux (Subnets), et offre un contrôle total sur le routage via les UDR (User Defined Routes), ce qui est indispensable pour forcer le trafic à passer par notre pare-feu central.

- **Pare-feu et Routeur central : pfSense**

PfSense, basé sur FreeBSD, a été choisi comme NVA (Network Virtual Appliance) pour centraliser le routage et la sécurité. C'est une solution open-source de classe entreprise extrêmement puissante. Elle a été préférée aux pare-feux natifs d'Azure (comme Azure Firewall) pour des raisons d'optimisation des coûts, mais aussi pour sa richesse fonctionnelle : elle intègre nativement le routage, le VPN, le proxy, et supporte des packages additionnels essentiels (HAProxy, Suricata).

- **Gestion des Identités et DNS : Windows Server Active Directory (AD DS)**

Justification : Active Directory reste le standard incontesté de l'industrie pour la gestion centralisée des identités et des accès (IAM). Couplé à son propre service DNS, il permet une résolution de noms fluide au sein du réseau local et facilite l'application de stratégies de sécurité (GPO) pour les machines clientes.

- **Accès distant sécurisé : OpenVPN**

Justification : Pour l'accès télétravail/administration, OpenVPN a été privilégié par rapport à IPsec pour sa simplicité de déploiement à travers des pare-feux restrictifs (fonctionne via un port unique UDP/TCP) et

sa forte sécurité basée sur SSL/TLS. Son intégration native dans pfSense avec la gestion d'une PKI (Public Key Infrastructure) locale a grandement facilité son choix.

- **Téléphonie sur IP (VoIP) : Asterisk**

Justification : Asterisk est le framework open-source leader mondial pour la création d'applications de communication. Il a été choisi pour sa gratuité, sa stabilité et sa compatibilité totale avec le protocole standard SIP, permettant de créer un central téléphonique (IP-PBX) interne totalement indépendant des fournisseurs externes.

- **Publication Web et Proxy : HAProxy et Nginx**

Justification : Pour exposer de manière sécurisée les services internes vers Internet, Nginx a été choisi comme serveur Web pour sa légèreté et ses hautes performances. Pour le protéger, HAProxy (déployé sur pfSense) agit comme un Reverse Proxy. Ce choix permet de centraliser la gestion des certificats (SSL Offloading) et de cacher la véritable adresse IP des serveurs Web internes.

- **Sécurité et Supervision (Suricata, Zabbix, Wazuh)**

Suricata (IDS/IPS) : Préféré pour sa capacité de traitement multi-thread, assurant une détection des intrusions performante sans ralentir le flux réseau sur pfSense.
Zabbix : Choisi pour la supervision de la disponibilité et des ressources matérielles grâce à son système de gabarits (templates) très flexible.
Wazuh (SIEM/HIDS) : Sélectionné pour sa capacité à analyser les logs en temps réel, détecter les vulnérabilités et assurer la conformité, offrant ainsi un centre de contrôle de sécurité (SOC) complet et open-source.

CHAPITRE 4 : RÉALISATION ET DÉPLOIEMENT

4.1 Déploiement du réseau Azure et routage (UDR)

Pour garantir la centralisation de la sécurité, nous avons mis en place des tables de routage personnalisées, appelées User Defined Routes (UDR), au sein de l'environnement Azure. Celles-ci ont pour rôle de forcer l'ensemble du trafic sortant des différents sous-réseaux à transiter obligatoirement par le pare-feu pfSense pour inspection et filtrage. Cette configuration permet non seulement d'éviter tout accès direct à Internet depuis les machines hébergées dans les sous-réseaux sensibles, mais également de maîtriser finement les flux inter-réseaux. Ainsi, le pare-feu s'impose comme l'unique point de contrôle logique de notre infrastructure.

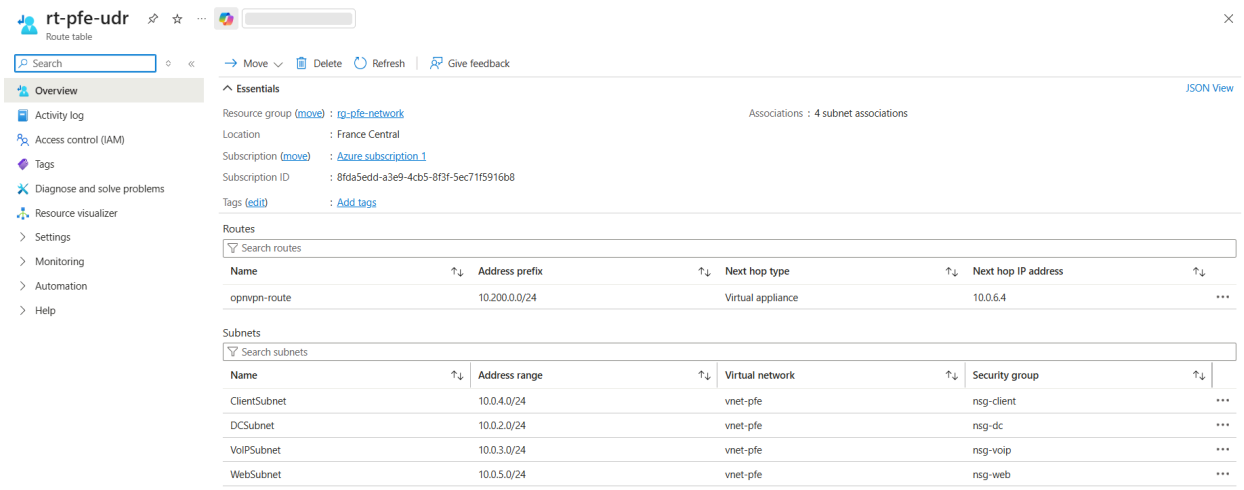

Figure 4 : Table de routage Azure (UDR)

4.2 Configuration du pare-feu central (pfSense)

Véritable cœur de notre architecture sécurisée, le pare-feu pfSense agit comme le point de passage obligatoire pour toutes les communications. Sa configuration a consisté à définir de manière stricte les règles de filtrage entre le réseau interne (LAN) et le réseau externe (WAN). Il prend également en charge la gestion du routage NAT pour autoriser de manière ciblée la publication de certains services indispensables et la sortie des postes vers Internet. L'application de cette politique de sécurité centralisée réduit considérablement l'exposition directe des machines internes et garantit le respect du principe de moindre privilège.

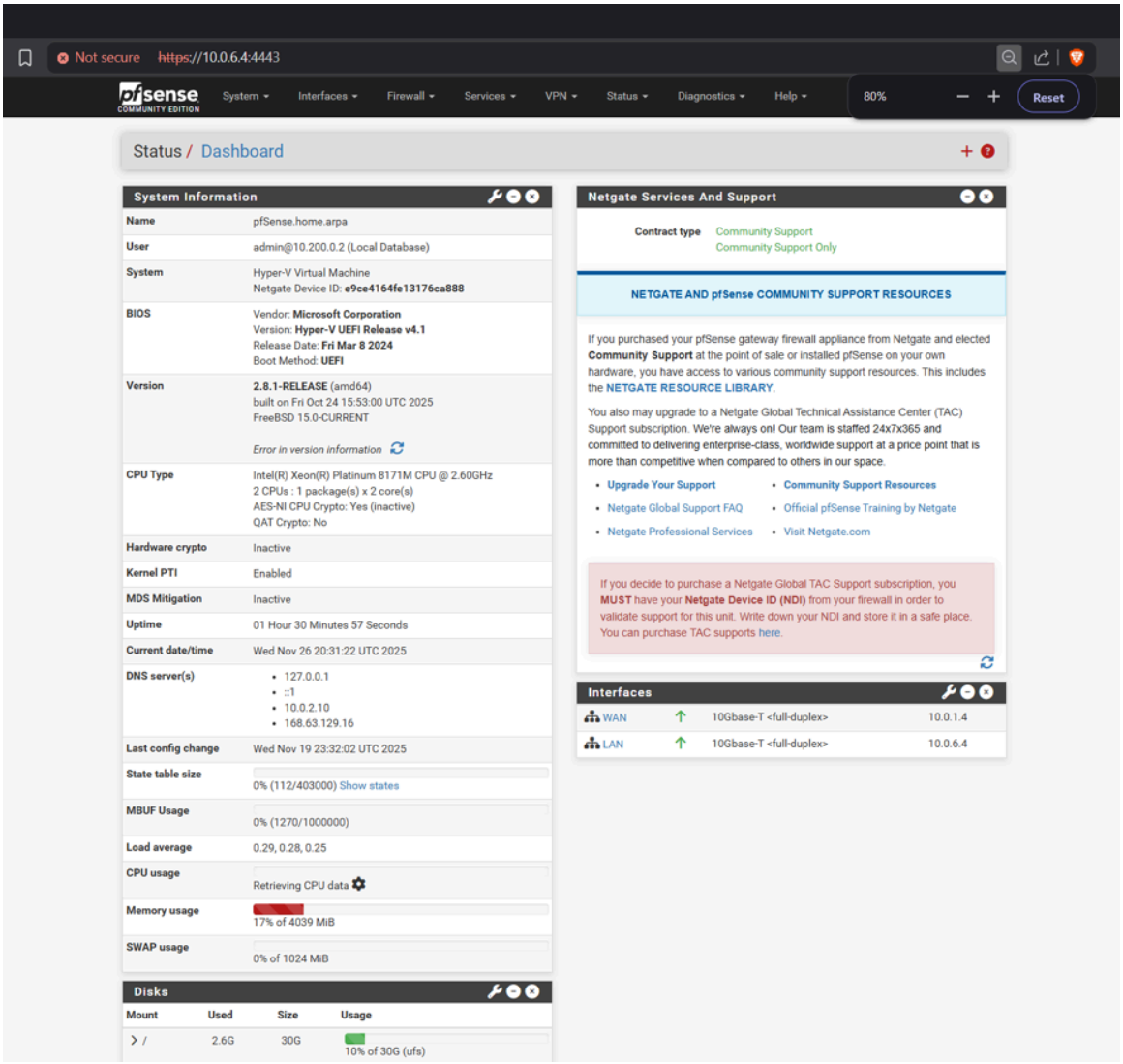

Figure 5 : Tableau de bord pfSense (passerelle)

4.3 Mise en place de l'accès distant (OpenVPN)

Afin d'offrir une administration sécurisée de l'environnement depuis l'extérieur, un serveur OpenVPN a été implémenté directement sur pfSense. La sécurisation de ce tunnel repose sur la création d'une Autorité de Certification (CA) locale, chargée d'émettre et de valider les certificats pour le serveur et les clients. Grâce à cette solution, les administrateurs bénéficient d'un accès chiffré et fortement authentifié aux réseaux internes (notamment le sous-réseau Management), et ce, sans avoir à exposer publiquement les interfaces d'administration des serveurs critiques sur Internet.

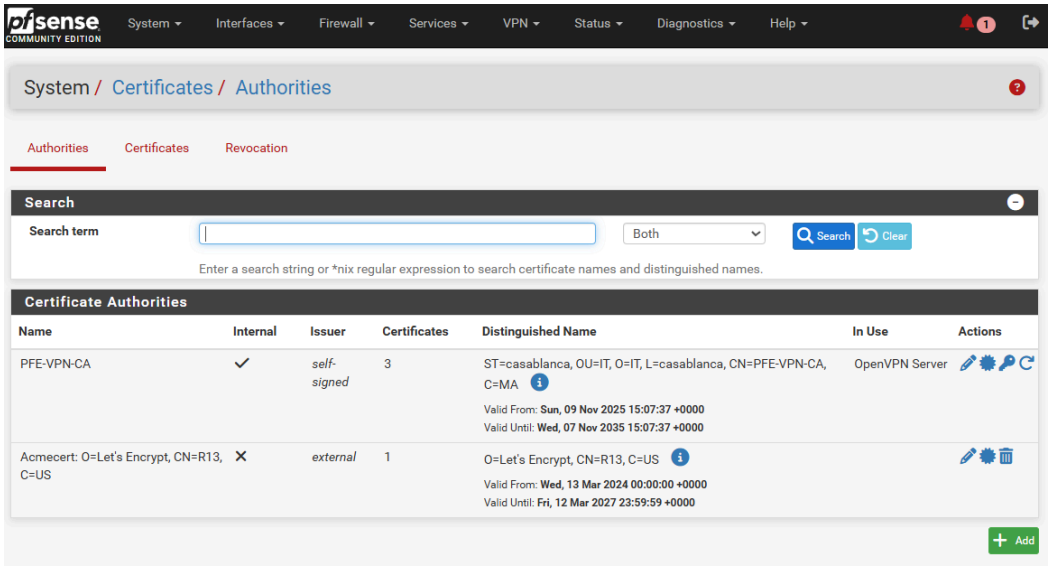

Figure 6: Autorité de certification (CA) OpenVPN

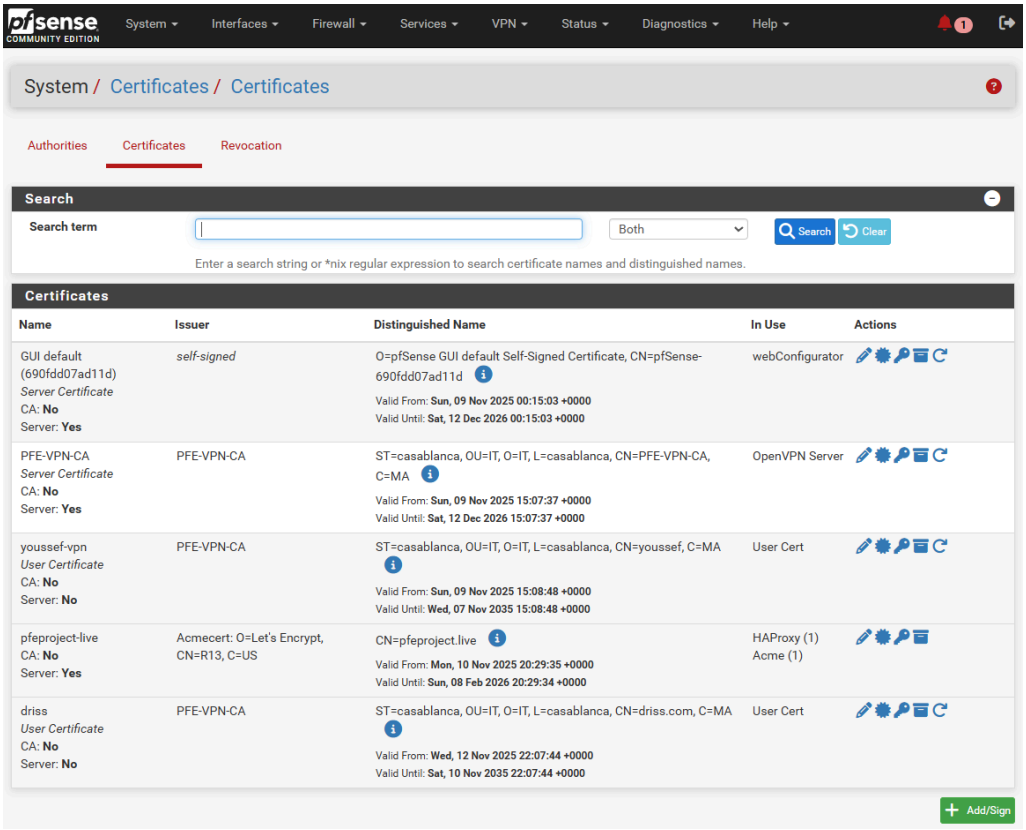

Figure 7 : Certificats OpenVPN (utilisateur/serveur)

4.4 Active Directory & DNS

Afin de centraliser l'authentification et l'administration du parc, un contrôleur de domaine Windows Server a été déployé. Il prend en charge la gestion des utilisateurs, des groupes de sécurité et l'application des stratégies de base. Conjointement, le service DNS a été configuré pour assurer la résolution des noms de domaine en interne. Pour les requêtes pointant vers l'extérieur, des redirecteurs (DNS Forwarders) ont été mis en place. Cela permet aux machines locales d'accéder à Internet tout en maintenant un contrôle total sur les requêtes de résolution de noms.

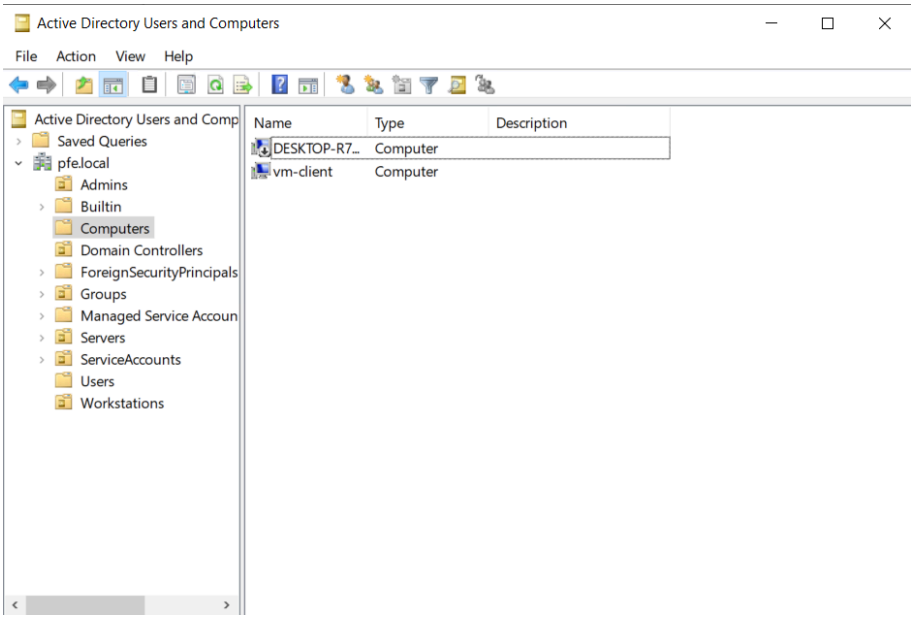

Figure 8 : Active Directory Computers

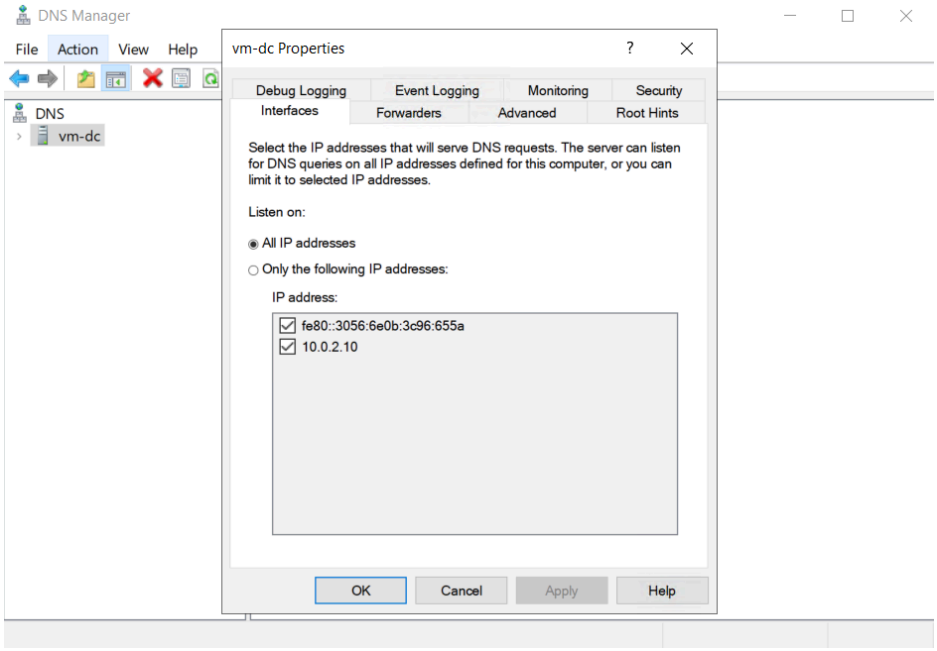

Figure 9 : Interfaces DNS (AD/DNS)

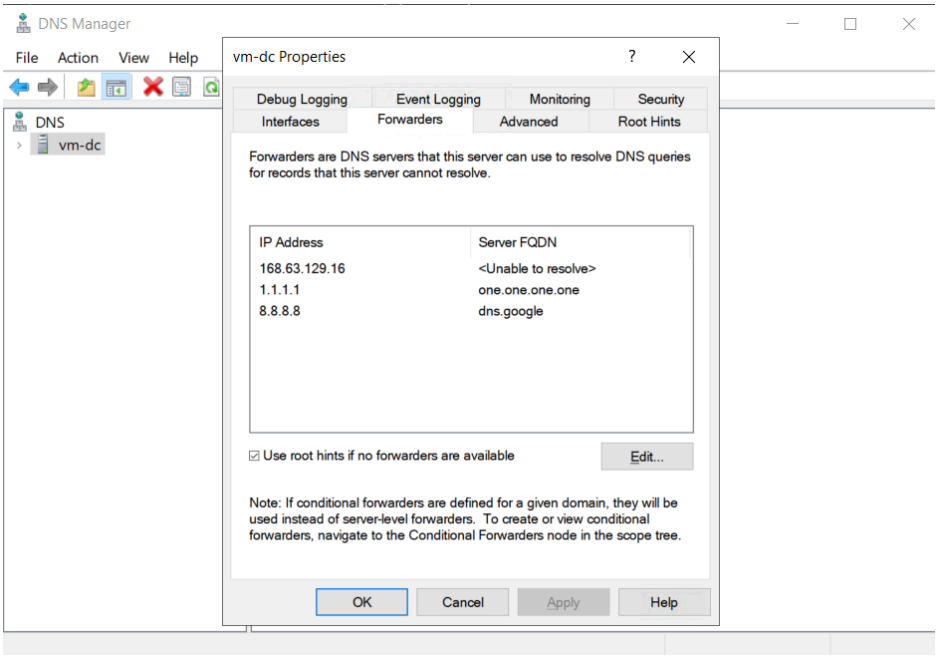

Figure 10 : DNS Forwarders

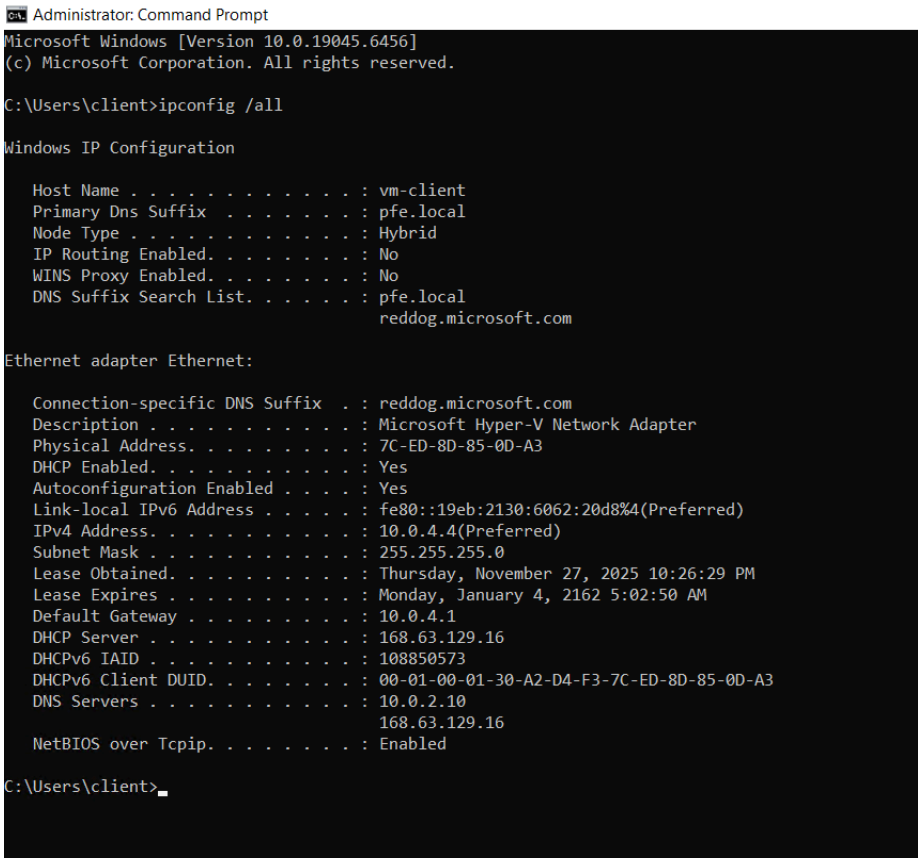

Figure 11 : Configuration IP du client (DNS + Domaine)

4.5 Publication Web sécurisée (HAProxy + HTTPS)

L'exposition de notre service Web interne vers l'extérieur a été réalisée par l'intermédiaire du composant HAProxy, agissant en tant que reverse proxy. Cette méthode permet de centraliser l'accès au service sur un point d'entrée unique, ajoutant ainsi une couche de protection supplémentaire en masquant la topologie réelle du réseau interne. De plus, l'accès au site a été sécurisé en l'associant à un nom de domaine, garantissant ainsi le chiffrement des échanges via l'ajout d'une couche HTTPS.

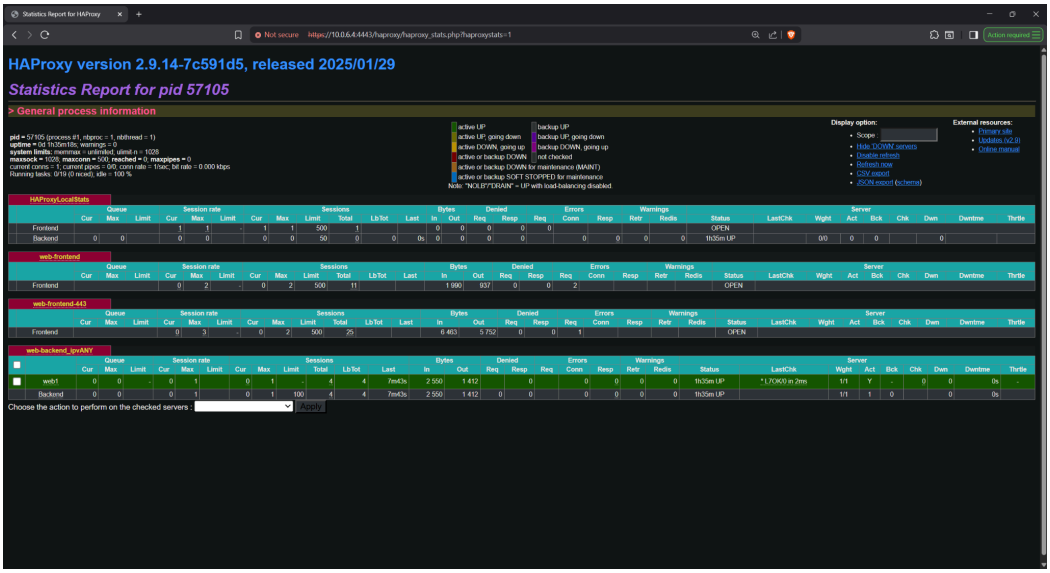

Figure 12 : Statistiques HAProxy (reverse proxy)

4.6 Service VoIP (Asterisk + Zoiper)

Pour la mise en œuvre de la téléphonie sur IP, un serveur Asterisk a été déployé et configuré pour orchestrer la création des comptes SIP et l'établissement des appels. Étant donné que le serveur VoIP est hébergé derrière le pare-feu, une attention particulière a été portée à la configuration du routage. Des règles spécifiques de "NAT Outbound" ont été définies sur pfSense pour empêcher la réécriture stricte des ports, assurant ainsi un acheminement fluide, bidirectionnel et sans coupure du flux audio (protocole RTP). Les validations ont ensuite été effectuées à l'aide du client logiciel Zoiper.

```
voip@vm-voip:/etc/asterisk$ sudo cat extensions.conf
[phones]

exten => 1001,1,Dial(SIP/youssef,20)
 same => n,Voicemail(1001@default,u)
 same => n,Hangup()

exten => 1002,1,Dial(SIP/driss,20)
 same => n,Voicemail(1002@default,u)
 same => n,Hangup()

exten => 500,1,Goto(ivr-menu,s,1)
voip@vm-voip:/etc/asterisk$
```

Figure 13 : Asterisk – Configuration du dialplan (extensions.conf)

```
voip@vm-voip:/etc/asterisk$ sudo cat sip.conf
[general]
context=default
bindport=5060
bindaddr=0.0.0.0
disallow=all
allow=ulaw,alaw
nat=yes

[youssef]
type=friend
secret=youssef.123
host=dynamic
context=phones

[driss]
type=friend
secret=driss.123
host=dynamic
context=phones

voip@vm-voip:/etc/asterisk$
```

Figure 14 : Asterisk – Configuration SIP des comptes (sip.conf)

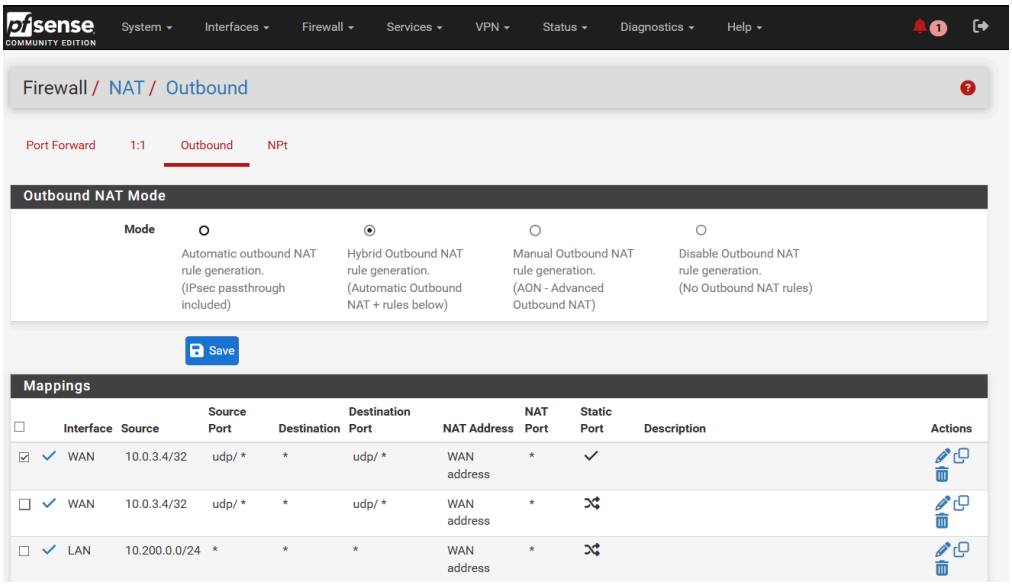

Figure 15 : Règles NAT Outbound

CHAPITRE 5 : SÉCURITÉ ET SUPERVISION

Après la phase de conception et le déploiement opérationnel des différents services, la sécurisation et la supervision de l'infrastructure constituent une étape critique du projet. L'objectif de ce chapitre est de présenter les mécanismes mis en place pour contrôler rigoureusement les flux réseau, détecter de manière proactive les comportements suspects, centraliser les événements de sécurité et assurer un suivi en temps réel de l'état de santé des machines.

5.1 Filtrage réseau et politique de sécurité (pfSense)

pfSense constitue le point central de contrôle. La politique appliquée repose sur :

- L'autorisation uniquement des flux nécessaires (principe du moindre privilège) ;
- La séparation claire entre trafic interne (LAN) et trafic externe (WAN) ;
- La mise en place de règles NAT pour la publication des services indispensables ;
- La limitation de l'exposition des machines internes.

Cette approche permet de réduire la surface d'attaque et de mieux maîtriser les accès.

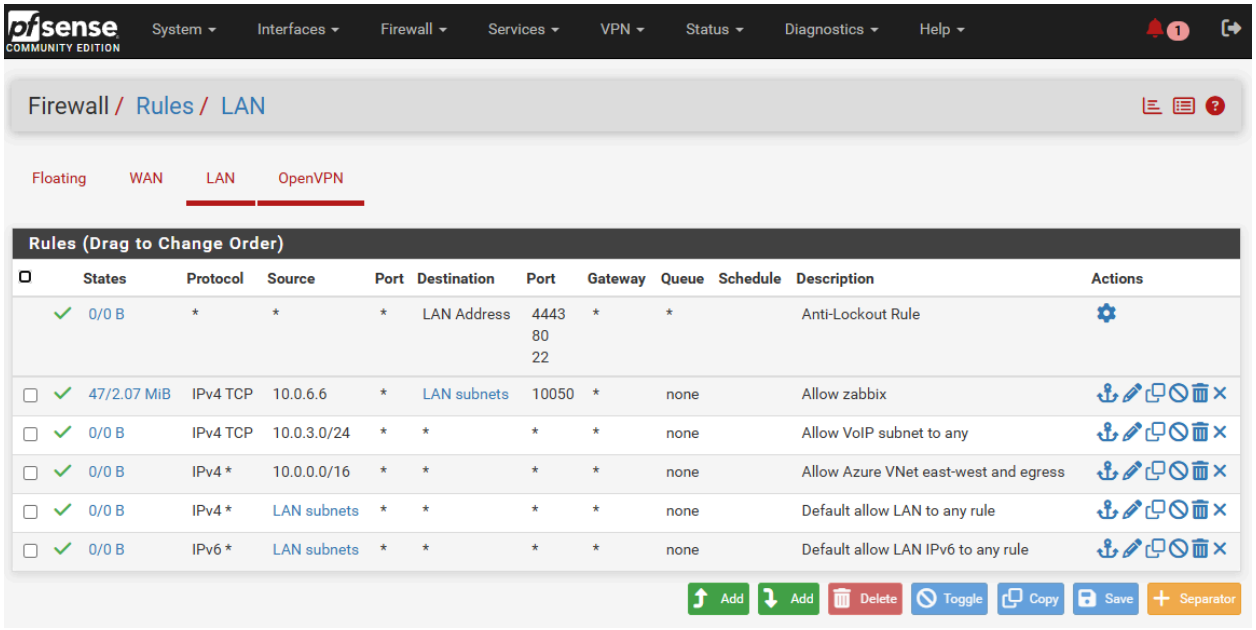

Figure 16 : pfSense – Règles de pare-feu LAN

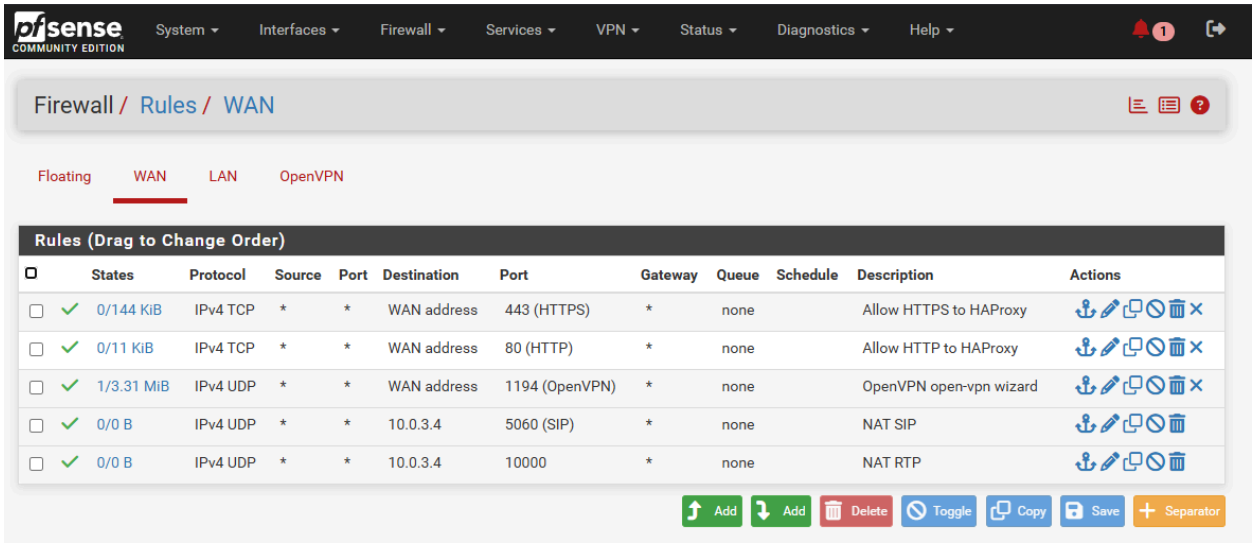

Figure 17 : pfSense – Règles de pare-feu WAN

5.2 VPN sécurisé (OpenVPN):

L'accès distant à l'infrastructure pour des besoins d'administration est exclusivement conditionné par l'utilisation d'un tunnel VPN. Ce mécanisme garantit la confidentialité absolue des communications grâce à un chiffrement robuste. L'authentification des administrateurs est renforcée par l'utilisation de certificats numériques, empêchant ainsi tout accès non autorisé. Ce sas de sécurité offre un accès contrôlé aux réseaux internes (notamment le sous-réseau Management), permettant d'administrer l'environnement de manière totalement transparente sans jamais exposer les services sensibles sur des ports publics.

5.3 Détection d'intrusion réseau (Suricata):

Afin d'ajouter une couche de sécurité dynamique à notre pare-feu, le système de détection et de prévention d'intrusion (IDS/IPS) Suricata a été intégré. Son rôle est d'analyser le trafic réseau en continu pour y déceler des signatures d'attaques connues ou des comportements anormaux, tels que des balayages de ports malveillants. Lorsqu'une menace est identifiée, Suricata génère des alertes détaillées et peut agir de manière proactive en bloquant les adresses IP sources, contribuant ainsi à une réaction rapide et automatisée face aux incidents.

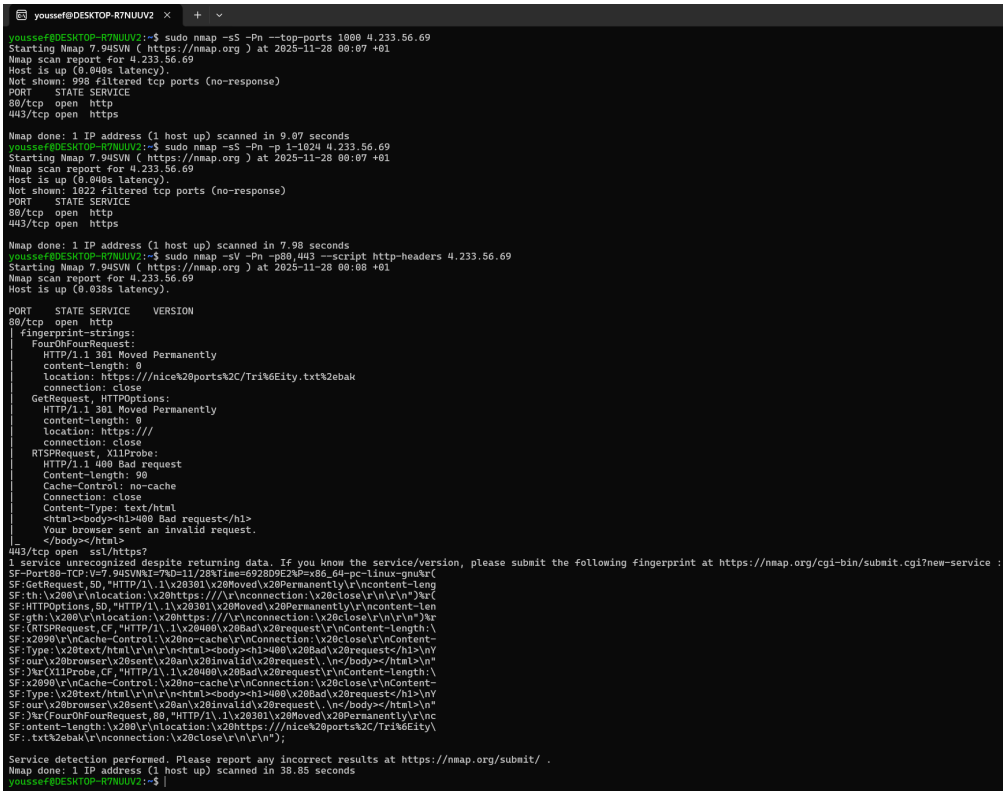

Figure 18 : Suricata – détection Nmap

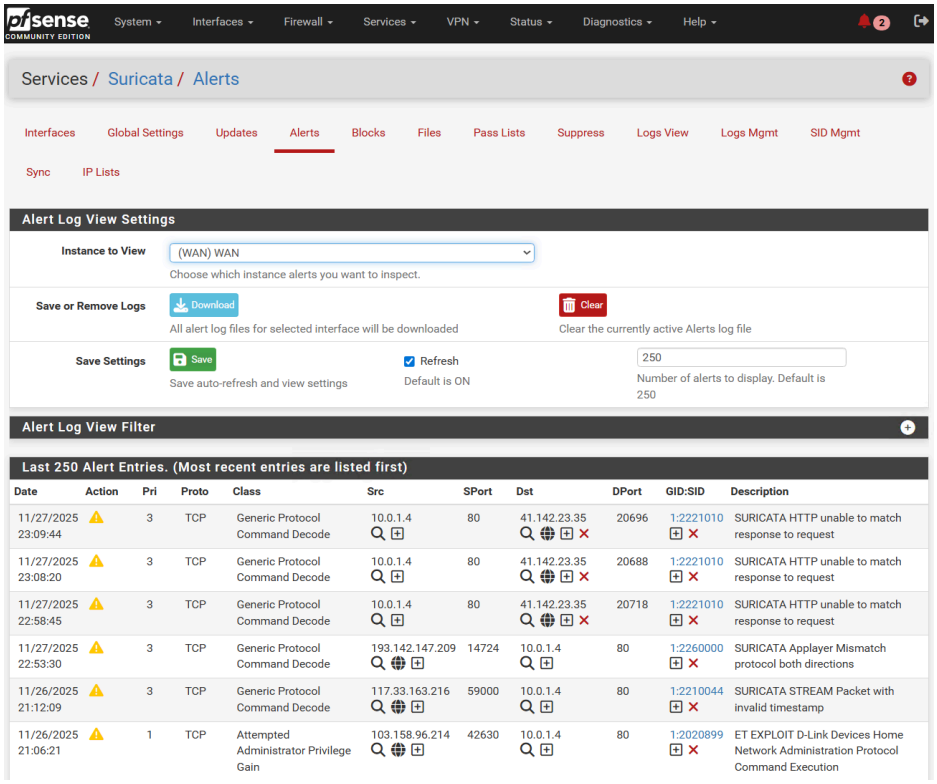

Figure 19 : Suricata – alertes

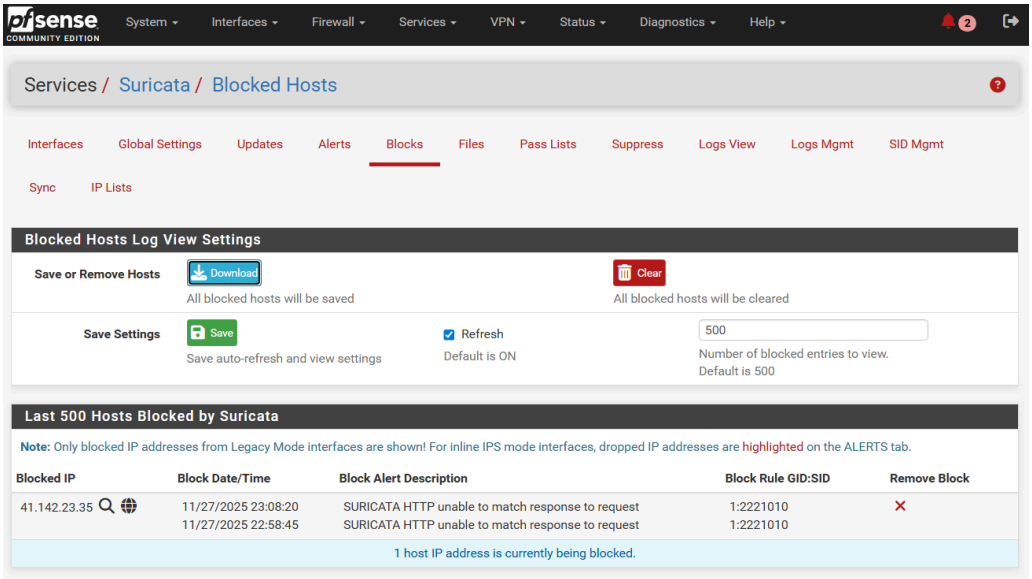

Figure 20 : Suricata – IP bloquée (Blocked Hosts)

5.4 Supervision (Zabbix)

Pour garantir le maintien en conditions opérationnelles de l'infrastructure, la solution Zabbix a été déployée. Cet outil de monitoring technique permet de suivre en temps réel l'état de santé des machines et la disponibilité des services. Il surveille en continu la consommation des ressources matérielles telles que l'utilisation du processeur, de la mémoire RAM et de l'espace disque. Grâce à des tableaux de bord centralisés, les administrateurs peuvent détecter instantanément les anomalies, telles qu'une surcharge ou une panne de service, assurant ainsi une grande réactivité dans le dépannage.

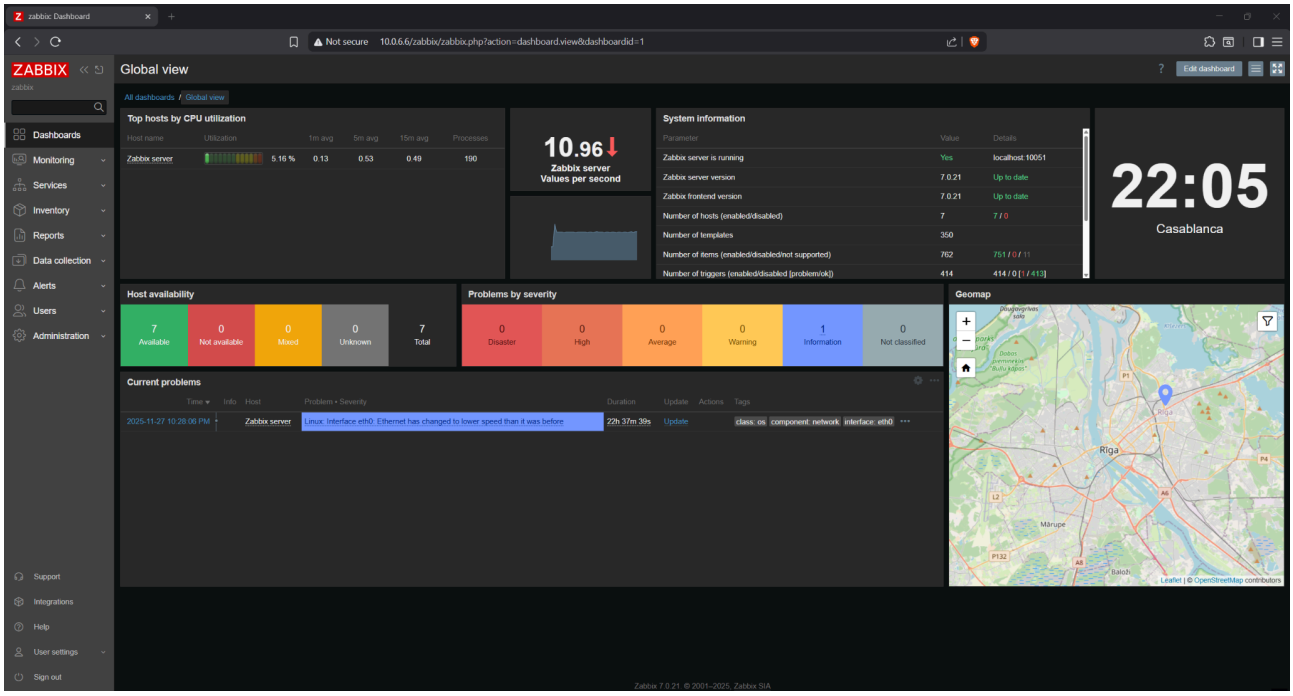

Figure 21 : Tableau de bord Zabbix

5.5 SIEM / HIDS (Wazuh)

En complément de la supervision purement technique, la plateforme Wazuh a été mise en œuvre pour centraliser la gestion des événements de sécurité. Wazuh collecte et analyse les journaux système (logs) en temps réel, offrant une visibilité granulaire sur l'activité des agents déployés sur les différentes machines virtuelles. Il excelle dans la détection de comportements anormaux, la remontée d'alertes de sécurité critiques et l'analyse continue des vulnérabilités liées aux configurations, facilitant grandement les audits de sécurité et la traçabilité globale de l'environnement Azure.

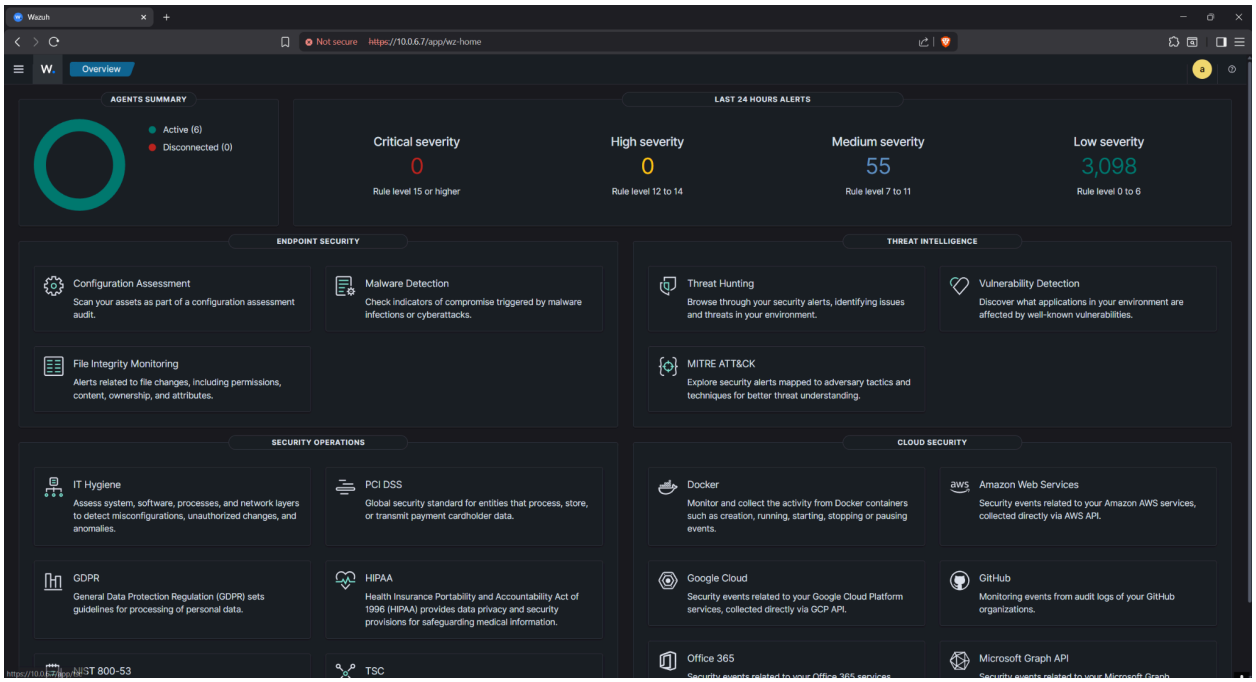

Figure 22 : Tableau de bord Wazuh

5.6 Tests et validation

La phase finale de notre projet a consisté à éprouver l'infrastructure au travers d'une série de tests rigoureux afin de confirmer la conformité des déploiements par rapport aux besoins initiaux. L'objectif était de vérifier que chaque composant interagit de manière cohérente avec le reste du système.

5.6.1 Validation du réseau et du VPN

Nous avons d'abord vérifié l'étanchéité du réseau en testant les communications entre les sous-réseaux et en validant l'application stricte des tables de routage (UDR) forçant le trafic à transiter par pfSense. L'accès distant a également été validé en simulant une connexion depuis un poste externe via OpenVPN, confirmant le bon fonctionnement de l'authentification par certificats et l'accessibilité au réseau de management interne.

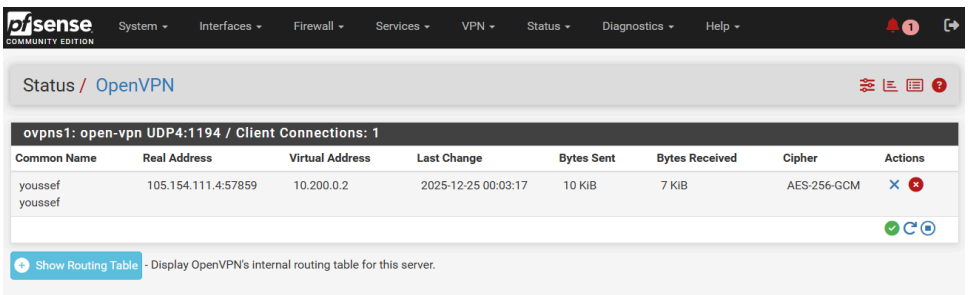

Figure 23 : OpenVPN – Statut des connexions client

5.6.2 Validation des services métiers (Web et VoIP)

Les services hébergés ont été soumis à des tests d'usage réels. Le service Web a été sollicité via un navigateur externe pour confirmer le bon routage du reverse proxy HAProxy, la résolution correcte du nom de domaine et la protection du flux via HTTPS. Concernant la téléphonie, des tests d'enregistrement SIP et d'appels entrants/sortants via le client Zoiper ont prouvé la parfaite stabilité du flux audio et la bonne configuration du NAT au niveau du pare-feu.

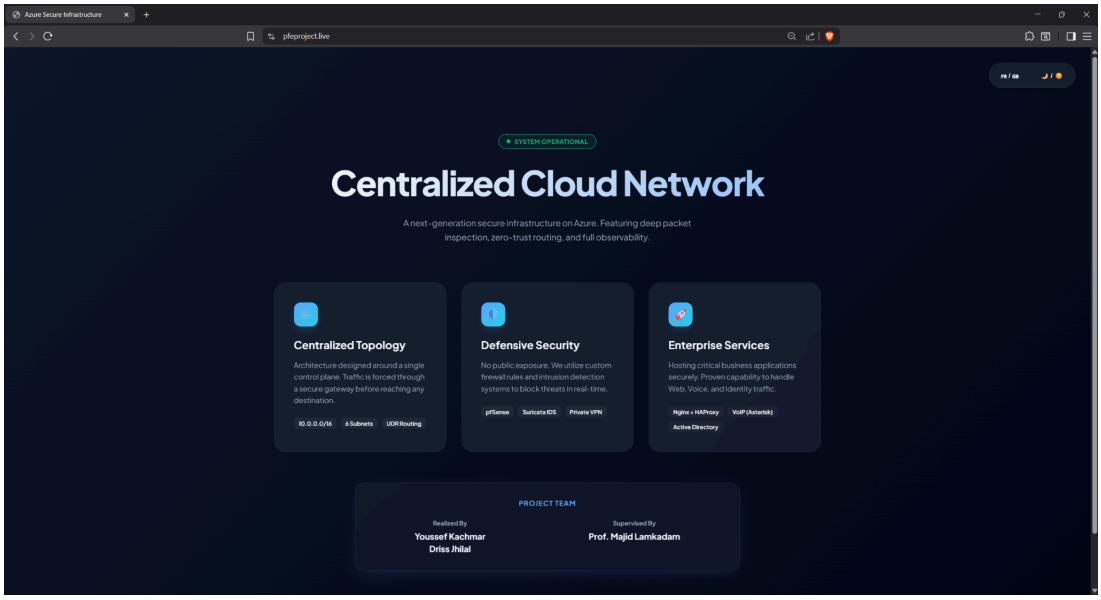

Figure 24 : Site accessible via nom de domaine

5.6.3 Validation de la sécurité et supervision

Enfin, la robustesse de l'environnement a été auditée par l'exécution intentionnelle de scans de ports (via l'outil Nmap) depuis l'extérieur. Ces simulations ont permis de confirmer l'efficacité de Suricata, qui a généré les alertes correspondantes et appliqué les règles de blocage d'IP. Parallèlement, nous avons vérifié que Zabbix et Wazuh remontaient correctement et en temps réel ces événements de sécurité ainsi que les métriques de charge au sein de leurs tableaux de bord, validant ainsi l'opérabilité et la sécurité totales de notre architecture.

CONCLUSION GÉNÉRALE

Ce projet de fin de formation a permis de concevoir, de déployer et de valider une infrastructure cloud sécurisée et supervisée sur Microsoft Azure, répondant en tout point aux exigences d'un environnement d'entreprise moderne. La solution mise en œuvre repose sur une architecture réseau rigoureusement segmentée, où le routage est maîtrisé par des tables personnalisées (UDR) afin de forcer le transit des flux par notre pare-feu central pfSense. Ce dernier a prouvé son efficacité en centralisant le filtrage, la translation d'adresses (NAT) et l'accès distant via un tunnel VPN chiffré.

Au-delà de l'infrastructure réseau, les services métiers essentiels ont été déployés avec succès. L'intégration d'Active Directory et du DNS a permis une gestion centralisée des identités, tandis que la publication d'un service Web via le reverse proxy HAProxy (en HTTPS) et la mise en place d'un central téléphonique VoIP (Asterisk) ont démontré la capacité de l'architecture à héberger des services critiques de manière sécurisée. Sur le plan défensif, le couplage du pare-feu avec l'IDS/IPS Suricata a considérablement renforcé la protection contre les intrusions. Enfin, l'intégration des solutions Zabbix et Wazuh a apporté une visibilité totale et en temps réel sur la santé des ressources et les événements de sécurité, facilitant ainsi l'audit et la réponse aux incidents.
Les objectifs fixés au cahier des charges ont donc été pleinement atteints. L'infrastructure est aujourd'hui fonctionnelle, hautement sécurisée, et les séries de tests réalisés confirment la cohérence globale des choix technologiques adoptés.

Perspectives d'évolution

Bien que cette infrastructure constitue une base solide et opérationnelle illustrant les bonnes pratiques du cloud et de la cybersécurité, plusieurs améliorations peuvent être envisagées pour aller plus loin. Dans une logique de production à grande échelle, il serait pertinent d'intégrer des mécanismes de haute disponibilité (redondance) pour les composants critiques comme le pare-feu ou le contrôleur de domaine. De plus, le durcissement avancé des systèmes (hardening) et la mise en place d'une stratégie de sauvegardes régulières avec un plan de reprise d'activité (PRA) renforceraient la résilience globale. Enfin, l'automatisation complète du déploiement via des outils d'Infrastructure as Code (tels que Terraform ou Ansible) permettrait de standardiser et d'accélérer le provisionnement de cet environnement à l'avenir.

BIBLIOGRAPHIE & WEBOGRAPHIE

Microsoft Azure : https://azure.microsoft.com/

pfSense : https://www.pfsense.org/

OpenVPN : https://openvpn.net/

HAProxy : https://www.haproxy.org/

NGINX : https://nginx.org/

Asterisk : https://www.asterisk.org/

Zoiper : https://www.zoiper.com/

Suricata : https://suricata.io/

Zabbix : https://www.zabbix.com/

Wazuh : https://wazuh.com/

RFC 1918 : https://datatracker.ietf.org/doc/html/rfc1918