الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Université A.MIRA-Béjaia

جامعة عبد الرحمان ميرة - بجاية

Mémoire Fin D'études
En vue d'obtention du diplôme Master en informatique
Option : Administration Sécurité Des Réseaux

Mise en place d'un système de Détection et Prévention (IDS/IPS) dans l'infrastructure réseau de Cevital

Réalisé par :
M. Boudjemia Massinissa
M. Zidouni Walid

Soutenu le 29 Juin 2025 Devant le jury composé de :

Présidente	Dr Bachiri Lina	U. A/Mira Béjaia.
Encadrant	Dr Amroun Kamal	U. A/Mira Béjaia.
Examinateur	Dr Yazid Mohand	U. A/Mira Béjaia.
Examinatrice	Dr Sabri Salima	U. A/Mira Béjaia.
Examinateur	Dr Farah Zoubyr	U. A/Mira Béjaia.

Promotion : 2024/2025

REMIRCIMENTS

Nous tenons à remercier sincèrement les membres du jury pour le temps et l'attention qu'ils ont accordés à l'évaluation de notre travail.
Nous exprimons une gratitude particulière à Monsieur Kamal Amroun , notre encadrant universitaire, pour son suivi rigoureux et ses conseils précieux
Nos remercions également l'encadrant à l'entreprise CEVITAL -BEJAIA, Monsieur Benouaret Nordine pour son accueil et son accompagnement durant notre stage.
Enfin, nous remercions chaleureusement nos enseignants ainsi que nos familles pour leur soutien constant, leur aide et leurs encouragements tout au long de notre parcours .

Table des matières

Table des figures

Liste des acronymes

- **2FA** : Two-Factor Authentication
- **ADSL** : Asymmetric Digital Subscriber Line
- **AES** : Advanced Encryption Standard
- **API** : Application Programming Interface
- **BGP** : Border Gateway Protocol
- **CERT** : Computer Emergency Response Team
- **DDoS** : Distributed Denial of Service
- **FAI** : Fournisseur d'Accès à Internet
- **FTP** : File Transfer Protocol
- **GNS3** : Graphical Network Simulator 3
- **HIDS/HIPS** : Host-based Intrusion Detection/Prevention System
- **HTTP** : HyperText Transfer Protocol
- **HTTPS** : HyperText Transfer Protocol Secure
- **IANA** : Internet Assigned Numbers Authority
- **IEEE** : Institute of Electrical and Electronics Engineers
- **IMAP** : Internet Message Access Protocol
- **IoT** : Internet of Things
- **IPv4** : Internet Protocol version 4
- **IPv6** : Internet Protocol version 6
- **MAC** : Media Access Control
- **MFA** : Multi-Factor Authentication
- **NAS** : Network Attached Storage
- **NFS** : Network File System
- **NTP** : Network Time Protocol

- **OSPF** : Open Shortest Path First
- **PCA** : Plan de Continuité d'Activité
- **PCI-DSS** : Payment Card Industry Data Security Standard
- **POP3** : Post Office Protocol version 3
- **PRA** : Plan de Reprise d'Activité
- **RAID** : Redundant Array of Independent Disks
- **RCE** : Remote Code Execution
- **RIP** : Routing Information Protocol
- **RSA** : Rivest–Shamir–Adleman
- **SCTP** : Stream Control Transmission Protocol
- **SMB** : Server Message Block
- **SMTP** : Simple Mail Transfer Protocol
- **SOC** : Security Operations Center
- **SQL** : Structured Query Language
- **SSH** : Secure Shell
- **SSDP** : Simple Service Discovery Protocol
- **STP** : Shielded Twisted Pair
- **SYN** : Synchronize (paquet de synchronisation TCP)
- **TCP/IP** : Transmission Control Protocol / Internet Protocol
- **TLS** : Transport Layer Security
- **USB** : Universal Serial Bus
- **UTP** : Unshielded Twisted Pair
- **VoIP** : Voice over Internet Protocol
- **Wi-Fi** : Wireless Fidelity

Introduction générale

Avec la montée en puissance des technologies de l'information et de la communication, les entreprises s'appuient de plus en plus sur des infrastructures réseau complexes pour assurer la continuité de leurs activités. Cependant, cette dépendance croissante aux réseaux expose les organisations à des menaces de plus en plus sophistiquées. Les cyberattaques, telles que le piratage, le vol de données et les intrusions non autorisées, représentent aujourd'hui un défi majeur pour la sécurité informatique.

Dans ce contexte, la mise en place de systèmes de sécurité performants est devenue une priorité absolue pour garantir l'intégrité, la disponibilité et la confidentialité des données. Parmi les mécanismes de défense les plus efficaces, les systèmes de détection et de prévention d'intrusion (IDS/IPS) jouent un rôle essentiel en identifiant et en neutralisant les menaces en temps réel.

Le présent travail s'inscrit dans cette démarche en proposant une étude approfondie de la mise en place d'un système de sécurité pour la détection et la prévention des intrusions. Il s'agira d'explorer les concepts fondamentaux des réseaux informatiques et de la sécurité, d'analyser l'existant au sein d'une entreprise spécifique, puis de concevoir et d'implémenter une solution basée sur des technologies éprouvées telles que Snort et PFSense.

Ce mémoire a été réalisé dans le cadre d'un stage au sein de **l'entreprise Cevital**, ce qui a permis de confronter les aspects théoriques de la cybersécurité à un environnement réel. Le travail a consisté à analyser l'architecture réseau de l'entreprise, à identifier ses vulnérabilités, puis à concevoir et déployer une solution de sécurité adaptée, reposant sur la mise en place d'un IDS/IPS intégré dans l'infrastructure existante. Ce stage a ainsi permis de renforcer la sécurité du réseau tout en améliorant la gestion des risques liés aux cybermenaces.

Pour atteindre cet objectif, nous avons structuré cette étude de la manière suivante en Cinq chapitres :

Le premier chapitre : Généralités sur les réseaux informatiques , est consacré aux généralités sur les réseaux informatiques. Nous y abordons les concepts fondamentaux liés aux réseaux, notamment les types de réseaux, leurs topologies, les modèles en couches (OSI et TCP/IP), ainsi que les principaux protocoles de communication. Une compréhension approfondie de ces notions est essentielle pour appréhender les enjeux de la sécurité des infrastructures informatiques.

Le deuxième chapitre : Sécurité informatique. , explore les principes fondamentaux de la sécurité informatique et les différentes menaces qui pèsent sur les réseaux. Nous y analysons les exigences essentielles de la cybersécurité (confidentialité, intégrité, disponibilité), l'étude des risques, les types d'attaques (IP Spoofing, attaques DNS, DHCP, ARP, VLAN, etc.) et les stratégies de protection. Ce chapitre met également l'accent sur l'importance d'une politique de sécurité et des mécanismes de contrôle d'accès.

Le troisième chapitre : IDS/IPS. , est consacré aux systèmes de détection et de prévention des intrusions (IDS/IPS). Nous y expliquons en détail le fonctionnement des IDS et IPS, en mettant l'accent sur l'outil Snort. Nous abordons également les principes de configuration et d'implémentation des IDS/IPS, ainsi que leur intégration avec PFSense pour assurer une protection optimale du réseau.

Le quatrième chapitre : Étude de l'existant , nous réalisons une étude approfondie de l'environnement existant au sein de l'entreprise Cevital. Nous y présentons l'architecture actuelle du réseau, les équipements utilisés, la segmentation VLAN, les serveurs et les applications en place. Nous analysons ensuite les vulnérabilités potentielles de cette infrastructure et proposons des solutions adaptées pour améliorer sa sécurité.

Le cinquième chapitre : Conception et réalisation , est dédié à la conception et à la mise en œuvre de la solution IDS/IPS. Nous y décrivons l'installation et la configuration des outils (GNS3, VMware, PFSense, Snort), la mise en place d'une topologie réseau sécurisée, la définition des règles de détection et la validation du système à travers des tests d'intrusion. Ce chapitre constitue la phase finale de notre travail, aboutissant à une solution opérationnelle capable de détecter et de bloquer les attaques en temps réel.

Chapitre 1

Gnéralités sur les réseaux informatiques

Introduction

Dans ce premier chapitre, nous posons les bases fondamentales nécessaires à la compréhension des réseaux informatiques et de leur fonctionnement. Une bonne maîtrise de ces concepts est essentielle avant d'aborder les aspects de sécurité et de mise en place d'un système IDS/IPS.

1.1 Les réseaux informatiques

Les réseaux informatiques permettent l'échange et le partage d'informations entre différents équipements connectés. Cette section aborde plusieurs aspects fondamentaux :

1.1.1 Terminologie de base des réseaux informatiques

Avant d'explorer les concepts avancés des réseaux informatiques, il est essentiel de comprendre certains termes fondamentaux qui décrivent les éléments clés d'une infrastructure réseau. Voici une explication détaillée des notions principales :

Nœud (Node)

Un nœud est un élément actif d'un réseau capable d'envoyer, de recevoir ou de relayer des données. Il peut s'agir de divers équipements, tels que :
- Ordinateurs (clients et serveurs)
- Routeurs, commutateurs (switches), points d'accès Wi-Fi
- Imprimantes réseau, caméras de surveillance IP, objets connectés (IoT)
- Chaque nœud est généralement identifié par une adresse IP et une adresse MAC pour communiquer efficacement dans le réseau. [1]

Hôte (Host)

Un hôte est tout dispositif capable de communiquer sur un réseau en utilisant une adresse IP unique. Tous les hôtes sont des nœuds, mais tous les nœuds ne sont pas nécessairement des hôtes.

Exemples d'hôtes :

- Un ordinateur connecté à Internet.
- Un serveur web hébergeant un site internet.
- Un smartphone utilisant une connexion Wi-Fi.
- Une machine virtuelle sur un réseau .
- Un commutateur ou un routeur peut être un nœud, mais il n'est généralement pas considéré comme un hôte, car il ne génère pas directement du trafic applicatif.[4]

Routeur (Router)

Un routeur est un équipement réseau qui assure l'acheminement des paquets de données entre plusieurs réseaux. Son rôle principal est de trouver le meilleur chemin pour que les données atteignent leur destination.[1]

Commutateur (Switch)

Un commutateur (ou switch) est un équipement réseau qui connecte plusieurs appareils dans un réseau local (LAN) et permet leur communication. Contrairement à un hub, qui diffuse les données à tous les ports, un switch dirige les paquets uniquement vers le destinataire approprié en fonction de son adresse MAC. .[1]

Serveur (Server)

Un serveur est un ordinateur ou un logiciel spécialisé qui fournit des services aux clients sur un réseau.
Types de serveurs courants :
- Serveur Web (HTTP/HTTPS) : héberge des sites Internet (exemple : Apache, Nginx).
- Serveur de messagerie (SMTP, IMAP, POP3) : gère l'envoi et la réception d'e-mails.
- Serveur de fichiers (FTP, SMB, NFS) : stocke et partage des fichiers.
- Serveur DNS : traduit les noms de domaine en adresses IP.
- Serveur DHCP : attribue automatiquement des adresses IP aux appareils.

Exemple :Lorsque vous consultez un site web, votre navigateur contacte un serveur Web qui lui envoie la page demandée.[1]

Client

Un client est un appareil ou une application qui envoie des requêtes à un serveur pour accéder à des services.
Exemples de clients :
- Un navigateur Web (Chrome, Firefox) qui demande une page à un serveur Web.
- Une application de messagerie qui contacte un serveur e-mail.
- Un ordinateur d'entreprise qui récupère des fichiers sur un serveur NAS.

Dans un modèle client-serveur, le client initie la communication et le serveur répond à ses requêtes. [2]

Bande passante (Bandwidth)

La bande passante représente la capacité maximale d'un réseau à transférer des données sur une période donnée, généralement mesurée en bits par seconde (bps, Mbps, Gbps).

Caractéristiques :

• La bande passante élevée permet des transferts rapides et simultanés (exemple : fibre optique à 1 Gbps).
• Une bande passante faible peut provoquer des ralentissements et de la latence. Les fournisseurs d'accès à Internet (FAI) limitent souvent la bande passante pour certains usages (exemple : streaming vidéo). .[1]

Latence (Latency)

La latence désigne le temps nécessaire pour qu'un paquet de données voyage d'un point A à un point B sur un réseau, mesurée en millisecondes (ms).
Facteurs influençant la latence :
• Distance physique : plus les données doivent parcourir de distance, plus la latence est élevée.
• Type de connexion : la fibre optique a une latence plus faible que le Wi-Fi ou l'ADSL.
• Charge du réseau : un réseau surchargé entraîne des retards de transmission.[2]

1.2 Catégories des réseaux

1.2.1 Selon leur étendue géographique

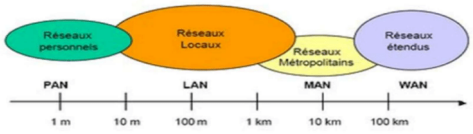

Fig. 1.1: Catégories des réseaux

• LAN (Local Area Network) : Réseau local limité à un périmètre restreint (bureaux, maisons, écoles).
• MAN (Metropolitan Area Network) : Réseau métropolitain couvrant une ville ou une grande zone urbaine.
• WAN (Wide Area Network) : Réseau étendu reliant plusieurs villes, pays ou continents (exemple : Internet).
• PAN (Personal Area Network) : Réseau personnel généralement utilisé pour la communication entre dispositifs d'un individu (exemple : Bluetooth).

1.2.2 Selon la topologie

Topologie en bus

Tous les périphériques sont connectés à un câble principal unique, appelé "bus". Cette configuration est simple et économique, mais une défaillance du câble principal peut entraîner l'arrêt complet du réseau.

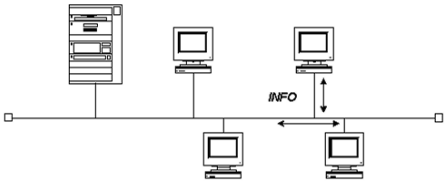

FIG. 1.2: Topologie en bus

Topologie en étoile

Chaque périphérique est relié à un nœud central, tel qu'un commutateur ou un concentrateur. Cette structure facilite la gestion et l'isolation des pannes individuelles ; toutefois, si le nœud central tombe en panne, l'ensemble du réseau est affecté. [15]

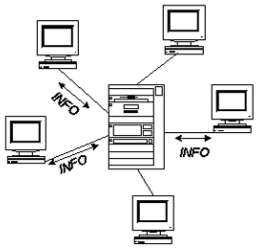

FIG. 1.3: Topologie en étoile

Topologie en anneau

Les périphériques sont connectés en série pour former une boucle fermée. Les données circulent généralement dans une seule direction, passant par chaque nœud jusqu'à atteindre leur destination. Une défaillance dans le circuit peut perturber l'ensemble du réseau. [14]

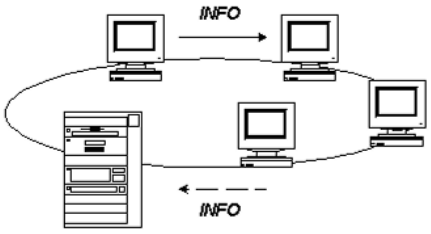

FIG. 1.4: Topologie en anneau

Topologie maillée

Chaque périphérique est connecté à plusieurs autres, offrant ainsi une redondance accrue. Dans une topologie maillée complète, tous les nœuds sont interconnectés, ce qui assure une tolérance aux pannes élevée, mais augmente la complexité et le coût d'installation. [17]

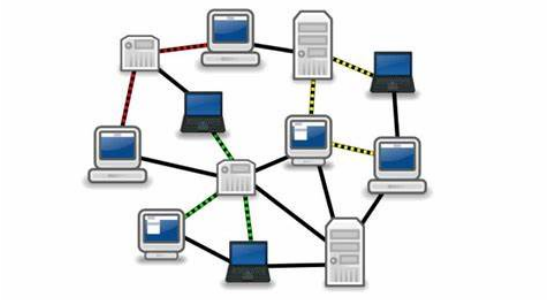

FIG. 1.5: Topologie maillée

Topologie hybride

Cette configuration combine plusieurs topologies de réseau, telles que l'étoile, le bus ou l'anneau, pour répondre aux besoins spécifiques d'une organisation. Elle offre une flexibilité et une évolutivité accrues, mais peut également augmenter la complexité de la conception et de la maintenance du réseau. [16]

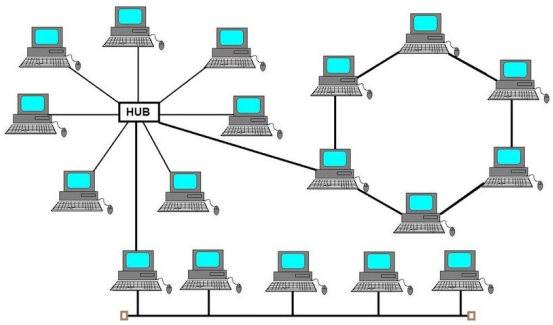

FIG. 1.6: Topologie hybride

1.3 Moyens de transmission

1.3.1 Moyens physiques

- Câble coaxial : Ancien type de câble réseau, utilisé principalement pour la télévision.
- Câble à paires torsadées (UTP, STP) : Plus couramment utilisé pour les réseaux Ethernet.
- Fibre optique : Offre un débit élevé et une transmission sur de longues distances. [14] [3]

1.3.2 Accès sans fil

- Wi-Fi : Technologie de réseau sans fil basée sur les standards IEEE 802.11.
- Bluetooth : Utilisé pour les communications à courte portée.
- Infra-rouge : Moins utilisé aujourd'hui, remplacé par des technologies plus performantes. [14] [3]

1.4 Architecture des réseaux

1.4.1 Modèle OSI (Open System Interconnexion)

Le modèle OSI est un modèle théorique développé par l'ISO (International Organisation for Standardization) en 1984. Il est composé de sept couches, chacune remplissant un rôle précis dans la communication réseau.

Couche physique (Physical Layer)

Transmet les bits bruts sous forme de signaux électriques, optiques ou radio. Exemples : câbles Ethernet, fibre optique, signaux Wi-Fi.[5]

Couche liaison de données (Data Link Layer)

Regroupe les données en trames et assure la communication entre équipements adjacents. Gère l'adresse MAC et la détection des erreurs. Exemples : Ethernet, Wi-Fi (802.11), PPP (Point-to-Point Protocol).

Couche réseau (Network Layer)

Assure le routage des paquets entre différents réseaux. Utilise les adresses IP pour identifier les équipements. Exemples : IPv4, IPv6, ICMP (Ping), RIP, OSPF, BGP. [5]

Couche transport (Transport Layer)

Garantit la transmission fiable des données entre l'expéditeur et le destinataire. Utilise le protocole TCP (connexion fiable, contrôle de flux) ou UDP (sans connexion, rapide, utilisé pour le streaming et la VoIP). Exemples : TCP, UDP, SCTP. [5]

Couche session (Session Layer)

Gère l'établissement, la maintenance et la terminaison des connexions entre applications. Exemples : protocole NetBIOS, RPC (Remote Procedure Call). [5]

Couche présentation (Presentation Layer)

Formate les données pour les rendre compréhensibles par l'application. Gère la compression, le chiffrement (SSL/TLS) et la conversion de formats. Exemples : JPEG, MP3, ASCII, SSL/TLS. [5]

Couche application (Application Layer)

Interface entre l'utilisateur et le réseau. Propose des services comme la navigation Web, la messagerie, le transfert de fichiers. Exemples : HTTP, FTP, SMTP, DNS, SSH. [5]

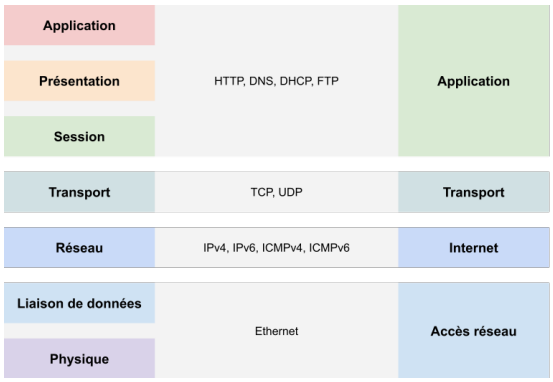

Fig. 1.7: Modèle OSI (Open System Interconnexion)

1.4.2 Modèle TCP/IP

Le modèle TCP/IP est un modèle plus pratique et largement utilisé sur Internet. Il est basé sur quatre couches et regroupe plusieurs fonctionnalités du modèle OSI.

Explication des couches TCP/IP :

Couche Accès Réseau (Network Access Layer)

Cette couche, également appelée couche lien (Link Layer), combine les fonctions des couches physique et liaison de données du modèle OSI. Elle est responsable de la transmission des données sur le support physique, qu'il s'agisse de réseaux câblés comme Ethernet ou de réseaux sans fil comme le Wi-Fi. Elle gère également les aspects liés à l'adressage matériel (adresses MAC) et au contrôle d'accès au média.[37]

Couche Internet (Internet Layer)

Correspondant à la couche réseau du modèle OSI, la couche Internet est chargée de l'adressage logique et du routage des paquets de données à travers des réseaux interconnectés. Elle utilise des adresses IP pour identifier les dispositifs sur le réseau et détermine le chemin que les paquets doivent emprunter pour atteindre leur destination. Exemples de protocoles : IPv4, IPv6, ARP (Address Resolution Protocol), ICMP (Internet Control Message Protocol). [37]

Couche Transport (Transport Layer)

Fournit un transport fiable des données via TCP ou un transport rapide via UDP. Permet le contrôle de flux et la gestion des connexions. [37]

Couche Application (Application Layer)

Cette couche englobe les fonctions des couches application, présentation et session du modèle OSI. Elle fournit des services de réseau directement aux applications de l'utilisateur final, permettant des interactions telles que la navigation web, le transfert de fichiers et la messagerie électronique. Exemples de protocoles : HTTP ,FTP, DNS, SSH.[37]

1.5 Les protocoles réseau

1.5.1 Client/Serveur

Ce modèle repose sur des appareils clients qui envoient des requêtes à un serveur centralisé qui répond aux demandes. Exemples :

- HTTP/HTTPS pour le Web
- FTP pour le transfert de fichiers
- SMTP/IMAP pour les e-mails
- POP utiliser pour recevoir des mails
- Telnet utiliser surtout pour commander des applications côté serveur en lignes de commande . [2]

1.5.2 Poste à poste (Peer-to-Peer - P2P)

Dans ce modèle, chaque machine peut être client ou serveur à la fois. Utilisé pour :

- Partage de fichiers (ex : BitTorrent)
- Réseaux locaux entre ordinateurs sans serveur centralisé.[4]

1.6 Adressage Réseaux

Les adresses IP se présentent sous diverses formes, chacune ayant des objectifs et des fonctions différents au sein d'un réseau. Comprendre ces types d'adresses permet de clarifier la manière dont les appareils se connectent et communiquent à l'échelle locale et mondiale,Il se divise en plusieurs types :

1.6.1 Adressage IPv4

on distingue :

- Adresse IPv4 sur 32 bits, exprimée sous la forme de quatre nombres séparés par des points (ex : 192.168.1.1).
- Classes d'adresses IPv4 : A, B, C, D, E.
- Masque de sous-réseau permettant de définir la partie réseau et hôte.
- Adressage privé et public selon l'IANA.[17]

classe	adresses
A	0.0.0.1 à 126.255.255.254
B	128.0.0.1 à 191.255.255.254
C	192.0.0.1 à 223.255.255.254
D	224.0.0.0 à 239.255.255.255
E	240.0.0.0 à 247.255.255.255

Fig. 1.8: Adressage IPv4

1.6.2 Adressage IPv6

- Adresse IPv6 sur 128 bits, exprimée en notation hexadécimale (ex : 2001:db8::1)
- Simplification de la gestion des adresses et support d'un grand nombre d'appareils. [17]

1.6.3 Adressage MAC

- Adresse unique attribuée à chaque carte réseau
- Utilisée pour l'identification des périphériques dans un réseau local (LAN). [17]

1.6.4 Adresses IP dynamiques

Ces adresses sont attribuées par un serveur DHCP (Dynamic Host Configuration Protocol) et peuvent changer chaque fois qu'un appareil se connecte au réseau. Les fournisseurs d'accès à Internet et les routeurs de réseau utilisent couramment des adresses IP dynamiques car elles sont plus efficaces pour gérer de grandes quantités d'adresses. Les adresses IP dynamiques sont idéales pour un usage général, comme les ordinateurs personnels et les appareils mobiles, où une adresse permanente n'est pas nécessaire. [7][17]

1.6.5 Adresses IP réservées et cas d'utilisation

Certaines adresses IP sont réservées à des fins spécifiques et ne peuvent pas être utilisées pour l'adressage général des appareils :

- Adresses de bouclage : Ces adresses (IPv4 : 127.0.0.1, IPv6 : ::1) sont utilisées par un appareil pour se référer à lui-même, principalement à des fins de test et de diagnostic.
- Adresses de diffusion : Ces adresses (IPv4 : 255.255.255.255) sont utilisées pour envoyer un message à tous les appareils d'un réseau.
- Adresses de multidiffusion : Ces adresses permettent une communication un-à -plusieurs, où un message est envoyé d'un appareil à plusieurs appareils faisant partie d'un groupe de multidiffusion (IPv4 : 224.0.0.0 – 239.255.255.255, IPv6 : ff00::/8). [17] [14]

1.7 Conclusion

À travers ce chapitre, nous avons acquis une compréhension globale des réseaux informatiques, en abordant leurs composants fondamentaux, les différentes topologies, les moyens de transmission, ainsi que les modèles de communication et les types d'adressage. Ces notions sont essentielles pour saisir comment les dispositifs interagissent, échangent des données et assurent la connectivité au sein d'une infrastructure. La maîtrise de ces concepts constitue une base solide pour toute personne souhaitant travailler dans le domaine des réseaux et de leur administration.

Chapitre 2

Sécurité Informatique

Introduction

Avec l'essor des technologies de l'information et la généralisation des communications numériques, la sécurité informatique est devenue un enjeu stratégique pour les entreprises. Les réseaux informatiques sont de plus en plus exposés aux cyberattaques, mettant en péril la confidentialité, l'intégrité et la disponibilité des données. Les menaces exploitant les vulnérabilités des systèmes pour voler des informations, perturber les services ou compromettre des infrastructures critiques. Face à ces risques, il est impératif d'adopter des stratégies de sécurité adaptées, combinant prévention, détection et réponse aux incidents. Ce chapitre explore les principes fondamentaux de la sécurité informatique, les exigences essentielles à respecter, ainsi que les différentes menaces qui ciblent les réseaux et les périphériques. Nous aborderons également les méthodes de protection, notamment la mise en place d'une politique de sécurité et l'implémentation de mécanismes de contrôle d'accès pour restreindre les intrusions et garantir un environnement sécurisé.

2.1 Principes de la sécurité informatique

La sécurité informatique repose sur un ensemble de principes fondamentaux visant à protéger les données, les systèmes et les infrastructures réseau contre les menaces internes et externes. L'objectif est d'assurer un environnement fiable dans lequel les informations restent accessibles aux utilisateurs autorisés tout en étant protégées contre les accès non autorisés et les attaques malveillantes.

Les trois piliers de la sécurité informatique sont souvent désignés sous l'acronyme CIA (Confidentiality, Integrity, Availability), qui correspond aux notions de confidentialité, intégrité et disponibilité. À ces principes de base s'ajoutent des notions complémentaires comme l'authentification, la traçabilité et la non-répudiation.

2.1.1 Confidentialité

La confidentialité garantit que les informations ne sont accessibles qu'aux personnes, systèmes ou processus autorisés. Elle vise à protéger les données sensibles contre tout accès non autorisé, qu'il soit intentionnel (piratage, espionnage) ou accidentel (mauvaise manipulation, erreurs de configuration).[20]

FIG. 2.1: Principes de la sécurité informatique

Mécanismes de protection

- Chiffrement des données : Conversion des informations en un format illisible sans clé de déchiffrement (exemple : AES, RSA, SSL/TLS).
- Contrôle d'accès : Limitation de l'accès aux ressources selon des règles d'authentification et d'autorisation.
- Segmentation du réseau : Isolement des données critiques dans des environnements protégés (exemple : VLANs, zones DMZ).
- Politiques de gestion des accès : Attribution de droits et permissions selon le principe du moindre privilège.

2.1.2 Intégrité

L'intégrité assure que les données ne sont ni modifiées, ni altérées de manière non autorisée, que ce soit en stockage ou en transit. Elle vise à garantir que les informations restent fiables et exactes.[20]

Mécanismes de protection

- Hachage des données : Utilisation de fonctions de hachage (SHA-256, MD5) pour vérifier l'intégrité des fichiers et des transmissions.
- Signatures numériques : Assurer l'authenticité et l'intégrité des messages grâce à des certificats cryptographiques.
- Contrôle de versions et journaux d'audit : Surveillance des modifications apportées aux fichiers et bases de données
- Redondance et sauvegardes régulières : Préservation des données originales en cas de corruption ou d'attaque (exemple : sauvegarde incrémentale et journalière).

2.1.3 Disponibilité

La disponibilité garantit que les ressources informatiques restent accessibles en permanence aux utilisateurs autorisés. Elle vise à éviter les interruptions de service causées par des pannes matérielles, des attaques ou des erreurs humaines.[20]

Mécanismes de protection

- Mise en place de redondance : Utilisation de serveurs de secours, RAID, clusters pour assurer une continuité de service.
- Protection contre les attaques DDoS : Filtrage du trafic malveillant grâce à des pare-feu, systèmes IDS/IPS et services anti-DDoS.
- Plan de reprise d'activité (PRA) : Stratégies de sauvegarde et de récupération rapide après un sinistre.
- Surveillance proactive : Outils de monitoring réseau pour détecter et anticiper les défaillances (exemple : Nagios, Zabbix).

2.1.4 Authentification et Contrôle d'Accès

L'authentification garantit que seuls les utilisateurs ou appareils autorisés peuvent accéder aux ressources du système. Elle repose sur plusieurs facteurs d'identification :

- Quelque chose que l'utilisateur sait : Mot de passe, code PIN.
- Quelque chose que l'utilisateur possède : Carte à puce, token de sécurité.
- Quelque chose que l'utilisateur est : Empreinte digitale, reconnaissance faciale. [19]

L'authentification forte (2FA, MFA) combine plusieurs de ces méthodes pour renforcer la sécurité. Le contrôle d'accès détermine ensuite quels droits un utilisateur authentifié possède sur les ressources du système

- Modèle DAC (Discretionary Access Control) : L'utilisateur propriétaire définit les permissions.
- Modèle MAC (Mandatory Access Control) : Les permissions sont contrôlées par une politique centralisée.
- Modèle RBAC (Role-Based Access Control) : Les droits sont attribués en fonction des rôles des utilisateurs. [21]

2.1.5 Non-répudiation et Traçabilité

La non-répudiation garantit qu'un utilisateur ne peut pas nier une action qu'il a réalisée sur le système. Elle repose sur des mécanismes de journalisation et de signatures numériques. La traçabilité permet de suivre les activités réalisées sur le réseau et les systèmes d'information à travers :

- Les journaux d'audit (logs) : Enregistrement des connexions, modifications et tentatives d'accès.
- Les solutions SIEM (Security Information and Event Management) : Corrélation des événements de sécurité pour détecter les anomalies.

2.2 Exigences fondamentales en sécurité informatique

Exigences fondamentales en sécurité informatique Pour garantir une protection efficace des systèmes d'information, il est essentiel de respecter un ensemble d'exigences fondamentales qui définissent les mesures de sécurité à mettre en place. Ces exigences permettent d'assurer la confidentialité, l'intégrité et la disponibilité des données et des ressources informatiques tout en limitant les risques liés aux cyberattaques. Ces exigences se regroupent en plusieurs catégories : protection des accès, surveillance, résilience des systèmes et conformité réglementaire.

2.2.1 Contrôle des accès et authentification

L'un des premiers objectifs de la sécurité est de s'assurer que seules les personnes autorisées peuvent accéder aux ressources informatiques. Cela passe par plusieurs mécanismes :

A. Identification et authentification des utilisateurs :
- Mise en place de mots de passe robustes et de politiques de renouvellement régulier.
- Utilisation de l'authentification multi-facteurs (MFA) pour renforcer la sécurité.
- Restriction des connexions aux adresses IP autorisées.

B. Gestion des droits et autorisations :
- Application du principe du moindre privilège : chaque utilisateur doit avoir uniquement les accès nécessaires à ses tâches.
- Implémentation du contrôle d'accès basé sur les rôles (RBAC) pour gérer les permissions.
- Segmentation des privilèges entre différents comptes pour éviter les abus (exemple : séparation des rôles administratifs et utilisateurs classiques). [19]

2.2.2 Sécurité des communications et des données

Les données échangées sur un réseau doivent être protégées contre les interceptions et les modifications non autorisées.

A. .Chiffrement des communications :
- Utilisation de protocoles sécurisés (TLS, IPsec, SSH, HTTPS) pour protéger les échanges sur Internet.
- Mise en place du VPN (Virtual Private Network) pour sécuriser les connexions à distance.

B. Protection des données sensibles :
- Chiffrement des fichiers et bases de données stockées sur les serveurs.
- Mise en place de politiques de sauvegarde régulières pour éviter la perte de données.
- Utilisation de solutions DLP (Data Loss Prevention) pour surveiller et empêcher les fuites d'informations sensibles. [18]

2.2.3 Sécurité du réseau et des infrastructures

Un réseau sécurisé empêche les intrusions et limite la propagation des menaces en cas d'attaque.

A. Mise en place de pare-feu (firewall)
- Filtrage des flux réseau pour bloquer les connexions non autorisées.
- Définition de règles d'accès strictes entre les différentes parties du réseau.

B. Utilisation d'un IDS/IPS (Intrusion Détection/Prévention System)
- Détection des activités suspectes grâce à un IDS (exemple : Snort).
- Blocage automatique des attaques avec un IPS.

C. Segmentation du réseau
- Mise en place de VLANs pour séparer les services sensibles.
- Création d'une DMZ (zone démilitarisée) pour isoler les services accessibles depuis l'extérieur (exemple : serveurs Web).

D. Protection contre les attaques DDoS
• Surveillance du trafic pour identifier les pics anormaux.
• Utilisation de services anti-DDoS et de répartiteurs de charge pour absorber les attaques.[18]

2.2.4 Surveillance et détection des incidents

Avoir des mécanismes de surveillance permet d'anticiper et de réagir rapidement en cas d'incident.

A. Supervision des systèmes et logs
• Collecte et analyse des journaux système et réseau pour identifier les anomalies.
• Déploiement d'une solution SIEM (Security Information and Event Management) pour corréler les événements de sécurité.

B. Tests de vulnérabilité et audits réguliers
• Réalisation de tests d'intrusion (pentesting) pour identifier les failles.
• Mise en œuvre de scanners de vulnérabilités pour détecter les logiciels obsolètes et configurations à risque.

C. Réponse aux incidents et plan de reprise
• Élaboration d'un Plan de
Continuité d'Activité (PCA) pour minimiser les interruptions de service.
• Définition d'un Plan de Reprise d'Activité (PRA) pour restaurer rapidement les systèmes après un incident.
• Mise en place d'une équipe de gestion des incidents (SOC, CERT) pour coordonner la réponse aux attaques.

2.2.5 Conformité et réglementation

Les entreprises doivent respecter des normes de sécurité et des obligations légales pour protéger les données de leurs utilisateurs et clients.

A. Respect des normes de cybersécurité
• Mise en conformité avec ISO 27001 pour la gestion de la sécurité de l'information.
• Application des standards de protection des paiements électroniques (PCI-DSS).
• Suivi des recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

B. Protection des données personnelles
• Application des règles du RGPD (Règlement Général sur la Protection des Données) en Europe.
• Respect des obligations de confidentialité et droit à l'oubli des utilisateurs.
• Gestion des notifications en cas de fuite de données auprès des autorités compétentes.

2.3 Type d'attaque

2.3.1 Attaques réseaux

Les attaques réseaux visent à exploiter les vulnérabilités des protocoles de communication et des infrastructures informatiques pour intercepter, manipuler ou perturber le

trafic. Ces attaques peuvent compromettre la confidentialité, l'intégrité et la disponibilité des systèmes.

Dans cette section, nous allons détailler les principales attaques réseau, notamment : IP spoofing, attaques DNS, attaques DHCP, attaques ARP, attaques sur les VLAN, ainsi que d'autres formes d'intrusions courantes.

A.IP Spoofing (Usurpation d'adresse IP)

L'IP spoofing consiste à usurper l'adresse IP d'un périphérique légitime afin de masquer l'identité de l'attaquant ou de tromper les systèmes de sécurité. Cette attaque permet d'envoyer des paquets sous une fausse identité.

Méthodes d'attaque IP Spoofing

- Flooding (Déni de service distribué - DDoS) : L'attaquant envoie un volume massif de paquets en usurpant différentes adresses IP pour saturer le réseau.
- Man-in-the-Middle (MITM) : Usurper l'identité d'un hôte pour intercepter et modifier les communications entre deux parties. [37]

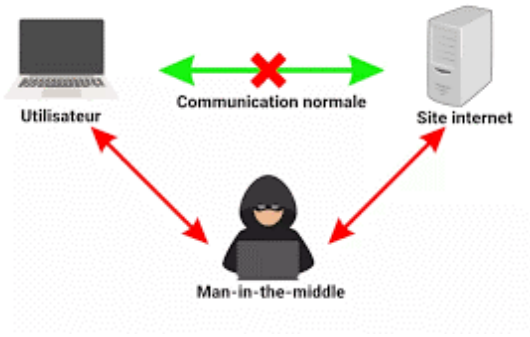

Fig. 2.2: Attaque Man-in-the-Middle

B. Attaques DNS (Domain Name System)

Les attaques DNS visent le système de résolution de noms de domaine qui traduit les noms de domaine (ex. : www.site.com) en adresses IP. Ces attaques peuvent manipuler les requêtes DNS pour rediriger les utilisateurs vers des sites malveillants.

Types d'attaques DNS

- DNS Spoofing (ou Cache Poisoning) : L'attaquant injecte de fausses informations dans le cache DNS, redirigeant l'utilisateur vers un site malveillant.
- DNS Amplification (DDoS) : Utilisation de requêtes DNS volumineuses pour saturer un serveur cible.
- DNS Tunneling : Utiliser les requêtes DNS pour exfiltrer des données en contournant les pare-feu. [22]

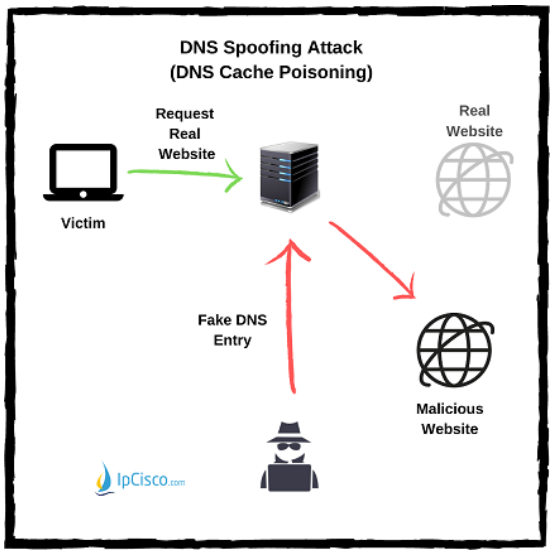

FIG. 2.3: Attaques DNS

C. Attaques DHCP (Dynamic Host Configuration Protocol)

Le DHCP attribue automatiquement des adresses IP aux appareils connectés. Les attaques DHCP visent à manipuler ces attributions pour perturber ou intercepter le trafic.

Types d'attaques DHCP

- DHCP Starvation :
  L'attaquant inonde le serveur DHCP de requêtes falsifiées pour épuiser le pool d'adresses disponibles.
- Rogue DHCP : Mise en place d'un faux serveur DHCP pour attribuer des adresses IP malveillantes et rediriger le trafic vers un attaquant.

D. Attaques ARP (Address Resolution Protocol)

L'ARP Spoofing consiste à empoisonner le cache ARP d'un réseau pour intercepter ou rediriger le trafic. Cette attaque est fréquemment utilisée dans les attaques Man-in-the-Middle (MITM).

Techniques d'ARP Spoofing

- Usurpation ARP : L'attaquant envoie de fausses réponses ARP pour se faire passer pour la passerelle (Gateway).
- MITM via ARP : Capture des données circulant entre deux hôtes du réseau.

E. Attaques sur les VLAN (Virtual Local Area Network)

Les VLAN permettent de segmenter un réseau physique en plusieurs sous-réseaux logiques. Les attaques VLAN visent à traverser ces séparations et accéder à des réseaux restreints.

Techniques d'attaques sur les VLAN

- VLAN Hopping : Exploitation des trames 802.1Q pour accéder à d'autres VLAN.
- Double Tagging : L'attaquant insère un second tag VLAN pour contourner les restrictions.

F.Attaques par déni de service (DoS/DDoS)

Saturer un réseau ou un service en inondant de requêtes massives. DDoS Amplification : Exploitation des protocoles UDP (DNS, NTP, SSDP) pour amplifier l'attaque.

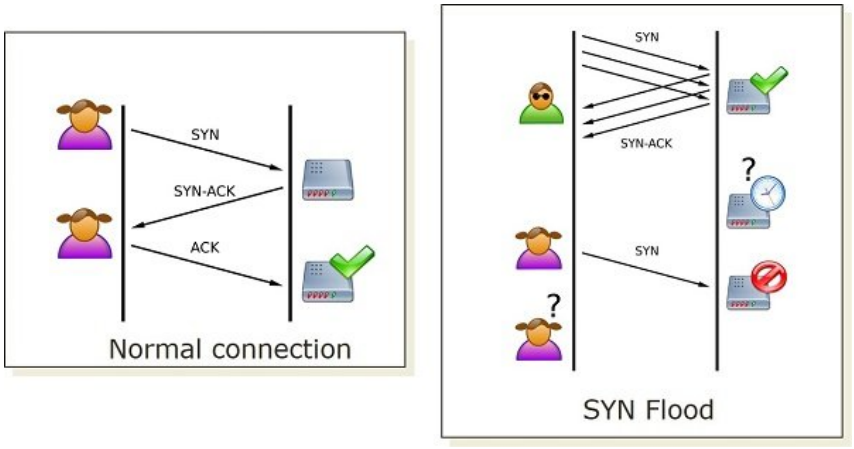

FIG. 2.4: Attaque DOS,sous une attaque potentielle d' inondation SYN(SYN flood attack)

G. Attaques de type Sniffing

Surveillance passive du trafic réseau pour collecter des informations sensibles.

H. Attaques par Injection (SQL, XSS)

Exploiter des failles applicatives pour exécuter du code malveillant.

2.3.2 Principales attaques des périphériques finaux

Les périphériques finaux (ordinateurs, smartphones, tablettes, objets connectés) constituent une cible privilégiée pour les cyberattaquants, car ils sont souvent moins sécurisés que les serveurs et les infrastructures réseau. Ces attaques visent à compromettre l'utilisateur, voler des informations sensibles ou prendre le contrôle du système pour l'exploiter à des fins malveillantes.

A. Attaques par malware

Les malwares (logiciels malveillants) sont des programmes conçus pour endommager, espionner ou prendre le contrôle d'un système.

Types de malwares :

- Virus : Se propage en infectant d'autres fichiers exécutables.

• Cheval de Troie (Trojan) : Se cache dans un programme légitime et permet un accès distant.
• Ransomware : Chiffre les fichiers et exige une rançon pour les débloquer.
• Spyware : Espionne l'utilisateur (enregistre les frappes clavier, capture les écrans).
• Rootkit : Se dissimule profondément dans le système pour échapper aux antivirus.[37]

B.Attaques par phishing et ingénierie sociale

Le phishing est une technique qui vise à tromper l'utilisateur pour lui faire divulguer des informations sensibles (identifiants, mots de passe, données bancaires).
Méthodes d'attaque :
• E-mails frauduleux imitant des services officiels (banques, entreprises, réseaux sociaux).
• Sites Web piégés demandant des informations confidentielles.
• Appels téléphoniques où un faux support technique demande des accès.

C . Attaques par exploitation de vulnérabilités logicielles

Les vulnérabilités logicielles sont des failles présentes dans les systèmes d'exploitation et applications qui peuvent être exploitées pour exécuter du code malveillant.
Exemples d'exploitations :
• Zero-Day Exploit : Attaque utilisant une faille non encore corrigée par le fabricant.
• Exécution de code à distance (RCE) : Prise de contrôle du système via une application vulnérable.
• Failles sur les navigateurs Web (extensions malveillantes, plugins obsolètes).[37]

D. Attaques sur les périphériques USB et supports amovibles

Les clés USB infectées sont un vecteur courant de propagation de malwares. Une clé compromise peut automatiquement exécuter un programme malveillant dès son insertion.
Types d'attaques USB :
• USB Rubber Ducky : Une clé programmée pour exécuter des commandes malveillantes.
• BadUSB : Exploite des vulnérabilités pour transformer une clé en périphérique d'attaque.
• AutoRun Malware : Exécution automatique d'un virus à l'insertion de la clé.

E.Attaques sur les connexions Wi-Fi

Les périphériques finaux connectés à des réseaux Wi-Fi publics ou non sécurisés peuvent être interceptés par des attaquants via des techniques de piratage réseau.
Types d'attaques sur Wi-Fi :
• Attaque Evil Twin : Création d'un faux point d'accès Wi-Fi pour intercepter les communications.
• Décrytage WPA/WPA2 : Exploitation de failles pour obtenir la clé Wi-Fi.
• Sniffing et interception de données : Surveillance du trafic non chiffré.

F. Keyloggers

Les keyloggers sont des logiciels ou dispositifs qui capturent toutes les frappes clavier, tandis que les screenloggers enregistrent l'écran de l'utilisateur.

Objectif des keyloggers :

- Voler les identifiants et mots de passe.
- Espionner les communications confidentielles.
- Enregistrer des transactions bancaires. [37]

G. Botnets

Un botnet est un réseau de périphériques infectés contrôlés par un pirate à distance. Les machines zombies sont utilisées pour lancer des attaques DDoS, miner des crypto-monnaies ou propager des malwares.

Comment un périphérique devient un bot ?

- Infection via pièces jointes ou liens piégés.
- Installation d'un logiciel infecté.
- Exploitation d'une faille de sécurité.

2.4 Étude des risques en sécurité informatique

L'étude des risques en sécurité informatique permet d'identifier, d'analyser et d'évaluer les menaces potentielles qui pèsent sur les systèmes d'information. L'objectif est de détecter les vulnérabilités, d'anticiper les attaques et de mettre en place des mesures de protection adaptées. L'approche repose sur plusieurs étapes : identification des actifs critiques, évaluation des menaces, analyse des vulnérabilités, estimation des impacts et définition des stratégies d'atténuation des risques.[15]

2.4.1 Identification des actifs critiques

Avant d'évaluer les risques, il est essentiel de déterminer quels actifs informatiques doivent être protégés. Ces actifs peuvent être :

- Les données sensibles : informations clients, bases de données financières, secrets industriels.
- Les infrastructures réseau : serveurs, routeurs, commutateurs, équipements de sécurité.
- Les applications critiques : logiciels métiers, services en ligne, messagerie d'entreprise.
- Les utilisateurs et identités : comptes administrateurs, employés, partenaires.
- La protection de ces actifs est une priorité absolue, car leur compromission pourrait avoir des conséquences graves sur l'entreprise. [15]

2.4.2 Identification des menaces et des vulnérabilités

Une menace est un événement ou une action malveillante qui peut exploiter une vulnérabilité et causer un dommage à un actif informatique.

A. Types de menaces courantes

1. Menaces internes
- Mauvaises configurations ou erreurs humaines.
- Employés malveillants ou négligents.
- Perte ou vol d'appareils contenant des données sensibles.
2. Menaces externes
- Cyberattaques : malware, ransomware, phishing.
- Espionnage industriel : vol d'informations stratégiques.
- Attaques réseau : déni de service (DDoS), intrusion via vulnérabilités.

B. Identification des vulnérabilités

Les vulnérabilités sont des failles qui peuvent être exploitées par des attaquants. Elles peuvent être :
- Techniques : failles logicielles, mises à jour non appliquées, mots de passe faibles.
- Organisationnelles : absence de politique de sécurité, formation insuffisante du personnel.
- Physiques : accès non sécurisé aux équipements informatiques. L'identification des vulnérabilités peut être réalisée via des audits de sécurité, des tests d'intrusion et des analyses de conformité.[37]

2.4.3 Analyse et estimation des risques

Une fois les menaces et vulnérabilités identifiées, il faut évaluer leur impact potentiel sur l'organisation.

A. Méthodes d'évaluation des risques

- Matrice de risque : évaluation basée sur deux critères :
1. Probabilité d'occurrence (faible, moyenne, élevée).
2. Impact potentiel (mineur, modéré, critique).
- Analyse qualitative : basée sur l'expérience et l'expertise des responsables sécurité.
- Analyse quantitative : calcul des pertes financières potentielles en cas d'attaque.[14]

Menace	Probabilité	Impact	Niveau de risque
Ransomware	Élevée	Critique	Élevé
Phishing	Moyenne	Modéré	Moyen
Intrusion réseau	Faible	Critique	Moyen

FIG. 2.5: Comparaison entre les menaces (Ransomware/phishing/intrusion réseau)

2.4.4 Stratégies d'atténuation des risques

Une fois les risques évalués, il est possible de définir les actions à mettre en place pour réduire les menaces.
- Élimination du risque : suppression complète d'une vulnérabilité (exemple : désactiver

un service non sécurisé).

• Réduction du risque : mise en place de mécanismes de protection (firewalls, IDS/IPS, sauvegardes régulières).

• Transfert du risque : souscription à une cyberassurance pour couvrir les pertes financières.

• Acceptation du risque : lorsque le coût de la mitigation est supérieur aux dommages potentiels.[14]

2.5 Établissement d'une politique de sécurité

L'établissement d'une politique de sécurité est une étape clé pour garantir la protection des systèmes d'information et la gestion des risques liés aux cyberattaques. Une politique de sécurité définit un ensemble de règles, procédures et bonnes pratiques que les employés, les administrateurs et les utilisateurs doivent suivre pour sécuriser les infrastructures informatiques et les données sensibles. Une politique de sécurité bien conçue permet de :

Prévenir les menaces en limitant les vulnérabilités.

Standardiser les bonnes pratiques en cybersécurité.

Sensibiliser les employés aux risques et aux responsabilités.

Réagir efficacement aux incidents de sécurité.[29]

2.5.1 Définition des objectifs et du périmètre

Avant de rédiger une politique de sécurité, il est essentiel de déterminer son périmètre et ses objectifs.

• Quels systèmes sont concernés ? (réseaux, serveurs, applications, bases de données).

• Qui est soumis à cette politique ? (employés, prestataires, administrateurs).

• Quels sont les principaux risques à couvrir ? (intrusions, fuite de données, attaques malveillantes).

• Quels sont les niveaux de contrôle et d'accès aux informations ?

L'objectif est de définir une politique qui s'adapte aux besoins et à l'environnement de l'entreprise tout en garantissant un niveau de sécurité optimal.[8]

2.5.2 Audit et mise à jour de la politique de sécurité

Une politique de sécurité doit être révisée régulièrement pour s'adapter aux nouvelles menaces et évolutions technologiques.

Bonnes pratiques d'audit

Contrôles de conformité pour s'assurer que les règles sont bien appliquées.

Tests d'intrusion (pentesting) pour identifier les failles de sécurité.

Mise à jour des stratégies en fonction des incidents rencontrés.[8]

2.6 Conclusion

Les attaques informatiques évoluent constamment et ciblent aussi bien les infrastructures réseau que les périphériques finaux, exploitant diverses vulnérabilités techniques et humaines. Pour protéger efficacement les systèmes d'information, il est essentiel d'identifier les risques, d'évaluer leur impact et de mettre en place des stratégies adaptées, notamment à travers une politique de sécurité claire et régulièrement mise à jour. La sensibilisation et la prévention restent des piliers indispensables pour limiter les menaces et garantir la sécurité globale. Dans le chapitre suivant, nous aborderons divers concepts liés aux systèmes de détection et de prévention d'intrusions (IDS/IPS), des outils indispensables pour sécuriser les réseaux d'entreprise face aux menaces informatiques modernes.

Chapitre 3

Systèmes IDS/IPS

3.1 Introduction

Dans un environnement numérique en constante évolution, la sécurité des réseaux d'entreprise est devenue une priorité absolue. Les menaces informatiques, qu'elles proviennent de l'extérieur ou de l'intérieur, représentent un risque majeur pour l'intégrité, la confidentialité et la disponibilité des systèmes . Pour répondre à ces défis, les systèmes de détection d'intrusions (IDS) et de prévention d'intrusions (IPS) jouent un rôle essentiel. Ces outils permettent non seulement de détecter les activités malveillantes, mais aussi de les bloquer avant qu'elles ne causent des dommages . Ce chapitre se concentre sur l'étude approfondie de ces systèmes, en mettant l'accent sur leur fonctionnement, leur mise en œuvre et leur intégration dans un environnement réseau d'entreprise. Ce chapitre sera consacré exclusivement pour définir, expliquer le fonctionnement et démontrer comment se fais la détection et la prévention des intrusions au sein du réseau d'une entreprise, Premièrement, nous examinerons en détail les systèmes de détection (IDS) et de prévention (IPS), en expliquant comment ces outils surveillent le trafic réseau et les journaux système pour détecter les signes d'intrusions. Nous discuterons également des stratégies de prévention, telles que la configuration de pare-feu, l'utilisation de politiques de sécurité robustes, ainsi que le rôle crucial des IDS/IPS dans le blocage des attaques connues et le renforcement de la sécurité des systèmes. Nous aborderons également le système Snort, un outil populaire dans le domaine de la sécurité informatique. Nous explorerons son histoire, son évolution et son mode de fonctionnement, en détaillant ses mécanismes avancés de détection des intrusions, qui le rendent particulièrement efficace dans la protection contre les cybermenaces, enfin nous concluant ce chapitre par la présentation générale du Pfsense en abordant son histoire et évolution ces fonctionnalité principale puis comment le teste et le connecte

3.2 IDS (Intrusion Détection Systems) et IPS (Intrusion Prévention Systems)

3.2.1 Introduction

Dans un contexte de multiplication des menaces informatiques, la mise en place de systèmes de détection (IDS) et de prévention (IPS) des intrusions est devenue indispensable. Ce mémoire explore les étapes pratiques d'implémentation des IDS/IPS en entreprise,

tout en identifiant les principaux défis techniques et organisationnels.

3.2.2 Étapes d'Implémentation

A. Analyse du Réseau

Avant tout déploiement, il est essentiel d'avoir une cartographie claire du réseau :
- Identifier les segments critiques (serveurs, bases de données, DMZ, etc.).
- Évaluer le volume et la nature du trafic.[24]

B. Choix des Emplacements Stratégiques

- En périphérie : surveiller le trafic entrant/sortant (firewall/routeur).
- Au cœur du réseau : observer les échanges internes (entre VLAN ou services).
- Dans les zones sensibles : ex. : bases de données clients, applications métiers critiques.[14]

C. Sélection de la Technologie

- IDS/IPS réseau (ex : Snort, Suricata, Zeek).
- IDS/IPS hôte (HIDS/HIPS) pour surveiller les systèmes individuels (ex : OSSEC, Wazuh).

Critères de choix : scalabilité, compatibilité, capacité de détection, coût.

D. Configuration et Intégration

- Mise en place des règles de détection (signatures ou comportements).
- Connexion avec les pare-feu, antivirus et autres outils de sécurité[25]

3.2.3 Objectifs IDS (Intrusion Détection Systems) et IPS (Intrusion Prévention Systems)

1-Surveiller ce qui se passe sur le réseau et les ordinateurs :

Pour repérer rapidement tout comportement inhabituel ou suspect, comme une tentative d'accès non autorisée ou un virus.[24]

2- Agir dès qu'un problème est détecté :

Bloquer automatiquement une attaque en cours ou alerter les responsables pour qu'ils puissent intervenir à temps.[23]

3- Limiter les dégâts :

en détectant les attaques dès leur début, on peut éviter qu'elles causent des pertes de données, des pannes ou d'autres conséquences graves[37]

4- Renforcer la sécurité à long terme :

en apprenant des incidents passés, on peut améliorer les protections existantes et éviter que les mêmes problèmes se reproduisent.[23]

3.2.4 Défis Courants

Quand on installe un système de détection ou de prévention d'intrusion (IDS/IPS), tout ne fonctionne pas toujours parfaitement dès le départ. Voici quelques problèmes fréquents qu'on a distinguer après notre étude analytique : Faux Positifs et Faux Négatifs

- **Faux positifs :**

Ce sont des alertes qui se déclenchent alors qu'il n'y a pas réellement de menace. Par exemple, un employé qui fait une action normale sur le réseau peut être pris pour un pirate informatique.

Résultat : ça fait perdre du temps à vérifier des fausses alertes.[13]

- **Faux négatifs :**

Là, c'est l'inverse : une attaque réelle passe inaperçue. Le système ne la détecte pas, donc elle peut faire des dégâts sans qu'on s'en rende compte.[13]

Impact sur les Performances

Un autre problème, c'est que ces systèmes peuvent ralentir le réseau s'ils ne sont pas bien réglés.

• Par exemple, si l'IPS vérifie chaque paquet de données de manière trop rigide, cela peut ralentir la connexion internet ou faire buguer certains services.[23]

Maintenance et Mises à Jour

Un IDS/IPS n'est pas un outil qu'on installe une fois pour toutes. Il doit être suivi et mis à jour régulièrement.

• Les signatures (règles qui permettent de reconnaître les attaques) doivent être souvent mises à jour, car les pirates trouvent sans cesse de nouvelles façons d'attaquer.

• Il faut aussi surveiller l'efficacité des règles en place pour s'assurer qu'elles fonctionnent toujours bien[13]

3.2.5 Outils de détection et de prévention (IDS/IPS)

Il existe plusieurs outils fiables et largement utilisés pour mettre en place un système IDS ou IPS. Chacun a ses particularités, ses avantages et parfois ses limites, on peut distinguer :

1. Suricata :

Similaire à Snort, mais avec de meilleures performances sur les réseaux rapides. Il peut analyser plusieurs flux de données en même temps (multithreading). Très rapide, supporte plusieurs protocoles, compatible avec les règles Snort. Fournit aussi des informations contextuelles très utiles pour les analystes[31]

2. SIEM (Security Information and Event Management) :

Ces plateformes collectent et analysent les journaux d'événements provenant de diverses sources, y compris les IDS/IPS, pour fournir une vue d'ensemble de la sécurité du réseau.[30]

3.Snort :

C'est l'un des outils les plus populaires pour détecter les intrusions. Il analyse le trafic réseau en temps réel à l'aide de règles (ou signatures) personnalisables. Gratuit, flexible, largement documenté, Peut être utilisé comme IDS ou comme IPS selon la configuration.

C est cette outils qu'on va entame dans notre partie pratique du mémoire[32]

3.2.6 Technologies de détection et de prévention des intrusions

Les technologies de détection et de prévention des intrusions jouent un rôle clé. Elles permettent d'identifier les menaces, d'y réagir rapidement et de limiter les dommages potentiels, se basent sur plusieurs approches, chacune ayant ses avantages et ses limites on rappelle :

1. Détection par signatures :

Cette méthode compare le trafic réseau ou les activités système à une base de données contenant les "empreintes" connues des attaques (appelées signatures).[9]

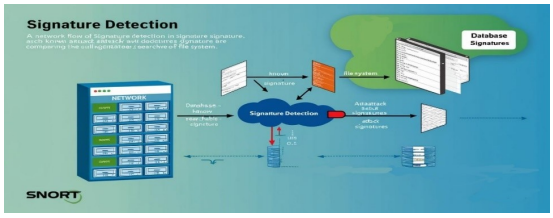

Fig. 3.1: Détection par signatures

2. Détection comportementale (anomalie) :

Cette méthode observe le comportement normal d'un réseau ou d'un système. Toute activité considérée comme "anormale" est signalée comme potentiellement malveillante.[6]

3. Filtrages des paquets :

Le filtrage des paquets par un système de prévention d'intrusion (IPS) est une méthode visant à analyser le trafic réseau entrant et sortant pour détecter et bloquer les activités malveillantes ou suspectes. Ya le Filtrage simple, dynamique et applicatif[11]

4. Le contrôle d'accès :

est une technologie essentielle en cybersécurité, permettant de réguler qui peut accéder à quelles ressources au sein d'un système informatique ou d'un réseau.
Il existe plusieurs modèles de contrôle d'accès, chacun adapté à des besoins spécifiques :

A. Contrôle d'accès discrétionnaire (DAC) : les propriétaires des ressources déterminent
qui a accès.

B. Contrôle d'accès obligatoire (MAC) : les accès sont régis par des règles strictes définies par l'administrateur système.

C. Contrôle d'accès basé sur les rôles (RBAC) : les permissions sont attribuées en fonction des rôles des utilisateurs au sein de l'organisation.

D. Contrôle d'accès basé sur les attributs (ABAC) : les décisions d'accès sont prises en
fonction d'attributs spécifiques des utilisateurs, des ressources et de l'environnement.[12]

5. Détection basée sur l'hôte (HIDS) :

Au lieu de surveiller l'ensemble du réseau, ces systèmes surveillent l'activité sur une machine spécifique :serveur, poste de travail, Fichiers système ,Journaux d'événements (logs).Tentatives de connexion.[10]

6. Analyse des journaux (Log Analysis) :

Exploite les logs générés par les systèmes, les applications ou les pare-feu pour détecter des schémas d'attaque ou des erreurs. Recherche de signes d'intrusion passés ou d'activités suspectes.[28]

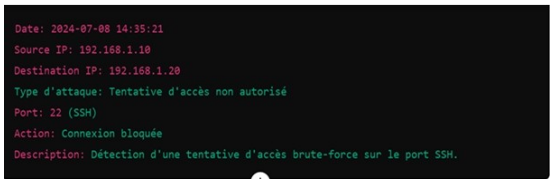

FIG. 3.2: Analyse des journaux

3.2.7 Intégration avec d'autres technologies de sécurité

L'intégration des technologies de sécurité, telles que les systèmes de détection et de prévention des intrusions (IDS/IPS), avec d'autres outils de cybersécurité, est essentielle pour renforcer la protection des réseaux d'entreprise. Cette approche permet une surveillance centralisée, une détection plus rapide des menaces et une réponse coordonnée aux incidents.[37]

3.2.8 Mise en œuvre de l'intégration

Pour réussir l'intégration des IDS/IPS avec d'autres technologies de sécurité :
1. Évaluation des besoins : Identifier les objectifs de sécurité et les systèmes existants.
2. Choix des outils compatibles : Opter pour des solutions qui offrent des interfaces d'intégration (API) et des standards ouverts.
3. Planification de l'intégration : Définir les processus de corrélation des données et les actions automatisées en réponse aux alertes.
4. Formation du personnel : Assurer que les équipes de sécurité comprennent le fonctionnement des systèmes intégrés et peuvent les gérer efficacement.[27]

3.2.9 Avantages de l'intégration des technologies de sécurité

• Détection améliorée : La corrélation des données entre différents systèmes permet d'identifier des schémas d'attaque plus sophistiqués.
• Réduction des faux positifs : En croisant les informations, il est possible de filtrer les alertes non pertinentes et de se concentrer sur les véritables menaces.
• Réponse rapide aux incidents : Une intégration efficace permet une automatisation des réponses, comme le blocage automatique d'une adresse IP suspecte.
• Conformité réglementaire : Les solutions intégrées facilitent la génération de rapports et la conformité aux normes de sécurité, telles que l'ISO/CEI 27001.[23]

3.3 Snort

3.3.1 Histoire et évolution de Snort

Snort est un système de détection d'intrusion open source largement utilisé dans le domaine de la sécurité informatique. Il fournit une solution puissante pour détecter et avertir des activités suspectes et des tentatives d'intrusion dans les réseaux informatiques. Snort utilise des règles de détection flexibles et personnalisables pour analyser le trafic réseau en temps réel, ce qui lui permet de repérer rapidement les comportements anormaux et les signatures d'attaque connues. Snort a une architecture modulaire qui peut être facilement déployée et intégrée à d'autres systèmes de sécurité. Il peut être utilisé à la fois comme IDS (Intrusion Détection System) pour détecter les activités malveillantes et générer des alertes, et comme IPS (Intrusion Prévention System) pour prendre des mesures préventives en bloquant ou en neutralisant les attaques en cours. Snort offre une grande flexibilité en termes de configuration des règles de détection, ce qui permet de l'adapter aux besoins spécifiques de l'environnement réseau. Il dispose également d'une communauté active qui développe régulièrement de nouvelles règles et des mises à jour pour contrer les nouvelles menaces de sécurité. En choisissant Snort comme système de détection d'intrusion pour ce projet, nous bénéficions D'un outil robuste, largement éprouvé et hautement personnalisable pour renforcer la sécurité du réseau de l'entreprise.[32]

3.3.2 Architecture de Snort

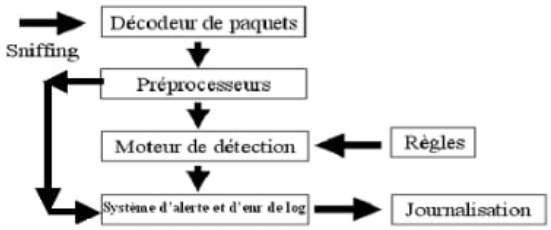

Fig. 3.3: Architecture de Snort

Snort est structuré en plusieurs modules interconnectés :
1. Capture de paquets : ces captures conçus pour intercepter le trafic réseau.
2. Préprocesseurs : Préparent les données pour l'analyse en normalisant et en filtrant le trafic.
3. Moteur de détection : Compare les paquets aux règles définies pour identifier les comportements malveillants.
4. Moteur d'alerte : Génère des notifications en cas de détection d'une menace.
5. Enregistrement des paquets : Stocke les données pour une analyse ultérieure.

Cette architecture modulaire permet une grande flexibilité et une adaptation aux besoins spécifiques des réseaux surveillés.[32]

3.3.3 Fonctionnalités principales

• Analyse en temps réel : Snort inspecte chaque paquet de données dès qu'il transite sur le réseau, permettant une détection rapide des anomalies.

• Détection basée sur des règles : Le système utilise un ensemble de règles définies par l'utilisateur ou la communauté pour identifier des signatures d'attaques spécifiques.
• Flexibilité : Les utilisateurs peuvent personnaliser les règles en fonction des besoins spécifiques de leur réseau.[32]

3.3.4 Mode de fonctionnement

Snort, un système de détection et de prévention d'intrusions (IDS/IPS) open-source, offre plusieurs modes de fonctionnement adaptés à divers besoins en matière de surveillance et de sécurité réseau. Voici une explication détaillée de ses principaux modes :

1. Mode Sniffer (Analyse en temps réel)

Dans ce mode, Snort agit comme un analyseur de paquets réseau. Il capture le trafic en temps réel et affiche les informations des paquets directement sur la console.
Ce mode est principalement utilisé pour :
• Observer le trafic réseau en direct.
• Diagnostiquer des problèmes de réseau.
• Analyser les en-têtes des paquets pour des vérifications rapides.[32]

2. Mode Logger (Enregistrement des paquets)

Le mode Logger permet à Snort de capturer le trafic réseau et de l'enregistrer sur le disque pour une analyse ultérieure.
C'est particulièrement utile pour :
• Effectuer des analyses post-incident.
• Conserver des traces pour des audits de sécurité.
• Étudier des comportements réseau suspects sur une période donnée.[32]

3. Mode IDS/IPS (Détection et prévention des intrusions)

Ce mode est le cœur de la fonctionnalité de Snort. Il analyse le trafic réseau en temps réel en le comparant à un ensemble de règles prédéfinies pour détecter des activités malveillantes. Selon la configuration :
• IDS (Intrusion Détection System) : Snort détecte les intrusions et génère des alertes sans intervenir sur le trafic.
• IPS (Intrusion Prévention System) : Snort détecte et bloque activement les paquets malveillants, empêchant ainsi les attaques de se propager. Ce mode est essentiel pour protéger les réseaux contre des menaces telles que les attaques par déni de service, les tentatives d'exploitation de vulnérabilités ou les intrusions non autorisées.[32]

3.3.5 Règles de détection Snort

La configuration des règles de détection est essentielle pour optimiser la surveillance du réseau et minimiser les faux positif, L'une des étapes clés de la mise en œuvre consiste à configurer les règles de détection de Snort. Cela implique d'identifier le comportement et les signatures des attaques, et de définir les actions à entreprendre lorsque une activité suspecte est détectée. alors pour cela on parle d'abord sur la structure dune règle de détection.

A-Structure d'une règle de détection Snort

Une règle Snort se compose de deux parties principales :
1. En-tête : Définit les conditions de base telles que le protocole, les adresses IP et les ports.
2. Options : Spécifie les critères supplémentaires à vérifier dans le paquet, comme des motifs spécifiques ou des flags TCP.

B-Création et test des règles

1. Identifier les besoins : Déterminez les types de trafic ou d'activités que vous souhaitez surveiller.
2. Écrire la règle : Utilisez la syntaxe appropriée pour définir les critères de détection.
3. Tester la règle : Avant de la déployer en production, testez-la dans un environnement contrôlé pour vérifier son efficacité et éviter les faux positifs.
4. Déployer et surveiller : Une fois validée, intégrez la règle dans votre configuration Snort et surveillez les alertes générées pour ajustements si nécessaire.

Pour mieux comprendre le principe on a illustre des exemple de règle qui font La surveillance toute activité ICMP inhabituelle (comme un scan par ping), et un trafic web spécifique sur un port non standard (8001), ce qui pourrait indiquer une activité suspecte, voici ce capture [32]

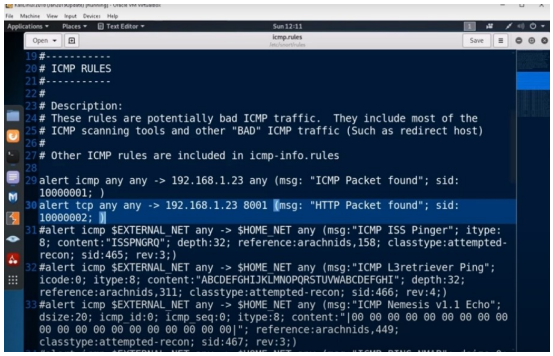

Fig. 3.4: Création et test des règles

3.3.6 Avantages de Snort

• Open-source : Gratuit et soutenu par une large communauté, ce qui facilite les mises à jour et l'ajout de nouvelles fonctionnalités.
• Personnalisable : Les règles peuvent être adaptées aux besoins spécifiques de chaque organisation.
• Large compatibilité : Fonctionne sur plusieurs systèmes d'exploitation, notamment Linux et Windows.
• Communauté active :Une vaste communauté d'utilisateurs et de développeurs contribue à l'amélioration continue du logiciel.
[32]

3.3.7 Limites de Snort

- Faux positifs :

Comme tout système basé sur des signatures, Snort peut générer des alertes pour des activités légitimes mal interprétées comme malveillantes.

- Maintenance des règles :

Nécessite une mise à jour régulière des règles pour rester efficace contre les nouvelles menaces.

- Performance : Sur des réseaux très volumineux, Snort peut nécessiter des ressources matérielles importantes pour fonctionner efficacement.[32]

3.4 PFSense

3.4.1 Introduction

reconnu pour sa robustesse comme pare-feu open-source, peut être encore renforcé en y intégrant un système de détection d'intrusions comme SNORT. Cette combinaison permet d'avoir une sécurité centralisée, intelligente et réactive. Dans cette section, nous allons découvrir c'est quoi PFSense , comprendre ces fonctionnalités principales et son avantages combinés et voir comment cela améliore la réactivité face aux incidents.

3.4.2 Présentation pfsesne

pfSense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD, il utilise le pare-feu à états Packet Filter ainsi que des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. pfSense convient pour la sécurisation d'un réseau domestique ou d'entreprise. Après l'installation manuelle nécessaire pour assigner les interfaces réseaux, il s'administre ensuite à distance depuis l'interface web. pfSense gère nativement les VLAN (802.1q). Comme sur les distributions Linux, pfSense intègre aussi un gestionnaire de paquets pour installer des fonctionnalités supplémentaires, comme un proxy ou un serveur de voix sur IP[2][33]

3.4.3 Histoire et évolution de pfSense

L'aventure pfSense débute en 2004. C'est une évolution du projet m0n0wall, développé par Manuel Kasper. Chris Buechler et Scott Ullrich lancent alors pfSense pour répondre aux besoins des entreprises. Le projet visait à déployer un pare-feu puissant mais accessible. Au fil des années, pfSense s'est enrichi de nombreuses fonctionnalités. La version 2.0, sortie en 2011, marque un tournant majeur. Elle apporte une interface moderne et de nouvelles options de sécurité. Aujourd'hui, pfSense est maintenu par Netgate et bénéficie d'une large communauté active.[14]

3.4.4 Fonctionnalités principales pfSense

Le cœur de pfSense est son pare-feu stateful. Il analyse chaque paquet réseau en temps réel. Cette surveillance constante protège contre les intrusions et les attaques. Le système

inclut aussi un détecteur d'intrusion (IDS/IPS) performant. La solution propose des fonctions VPN intégrées. Elles permettent de mettre en place des tunnels sécurisés entre différents sites. OpenVPN et IPsec sont nativement supportés, Il filtre le trafic internet et bloque les menaces. Les employés peuvent accéder aux ressources internes via VPN. Le système génère des rapports détaillés sur l'utilisation du réseau. Ces outils facilitent le travail à distance en toute sécurité. Les entreprises utilisent pfSense pour filtrer les contenus web. Le portail captif intégré gère l'authentification des utilisateurs. Les administrateurs contrôlent la bande passante par service. Ils peuvent bloquer certaines applications ou sites inappropriés. L'interface web de pfSense est intuitive et complète, offre un tableau de bord personnalisable, affichant des informations en temps réel sur l'état du système, l'utilisation de la bande passante, les connexions actives, etc. La configuration des différentes fonctionnalités se fait aisément via cette interface, rendant pfSense accessible même aux utilisateurs moins expérimentés.. Elle permet de configurer facilement :

- Les règles de pare-feu
- Le routage réseau
- La qualité de service (QoS)
- Les certificats SSL
- La surveillance du trafic [33]

3.4.5 Testé et vérifié

Une fois configuré, des tests sont effectués pour évaluer l'efficacité de Snort dans la détection des attaques. Lancez une attaque simulée pour vérifier que Snort génère les alertes appropriées et que les actions préventives sont correctement déclenchées.

En suivant ces étapes, nous nous sommes assurés que Snort était correctement configuré et en cours d'exécution, prêt à détecter et à prévenir les intrusions dans le réseau d'entreprise de Cevital. Les exemples de test vérifieront si Snort peut identifier les attaques internes et externes, afin d'assurer la sécurité des données et des services du réseau.[34]

3.5 Conclusion

Ce chapitre a permis d'explorer en détail les systèmes de détection et de prévention d'intrusions (IDS/IPS), des outils indispensables pour sécuriser les réseaux d'entreprise face aux menaces informatiques modernes. À travers l'étude de SNORT, nous avons vu comment cet outil open-source utilise des règles de détection pour identifier les activités malveillantes avec précision et flexibilité. L'implémentation des IDS et IPS a été abordée sous un angle pratique, en mettant en lumière les étapes clés pour déployer ces systèmes dans un environnement réseau. La configuration des règles de détection a été un point central, démontrant comment des règles bien conçues peuvent améliorer l'efficacité des IDS/IPS. Enfin, l'intégration de PFSense avec SNORT a été présentée comme une solution robuste pour combiner les fonctionnalités de pare-feu et de détection d'intrusions. En résumé, les IDS/IPS, lorsqu'ils sont correctement configurés et intégrés, constituent un pilier essentiel de la sécurité des réseaux d'entreprise. Ils offrent une protection proactive contre les cybermenaces, tout en s'adaptant aux besoins spécifiques de chaque organisation. Les connaissances acquises ici serviront de base pour approfondir les stratégies de sécurité dans le prochain chapitre, nous détaillerons les étapes de déploiement et de simulation de la solutions, Snort, au sein de l'architecture réseau proposée pour l'entreprise Cevital BEJAIA. Cette étape permettra de mettre en pratique les concepts abordés et d'évaluer leur efficacité dans un environnement simulé, contribuant ainsi à renforcer la posture de sécurité de l'entreprise.

Chapitre 4

Présentation de l'organisme d'accueil et étude de l'existant

4.1 Introduction

Ce chapitre sera réservé à la présentation du l'organisme cevital où nous effectuons notre stage. Dans un premier temps, nous aborderons un bref aperçu de l'entreprise pour mieux comprendre sa structure et ses objectifs. Nous étudierons ensuite l'architecteur réseau de cette entreprise et ses composantes afin de pouvoir suggérer d'éventuelles améliorations.

4.2 Présentions de l'entreprise « cevital »

4.2.1 Création et évolution

Cevital est une Société par Actions au capital privé de 68 ,760 milliards de DA. Elle a été créé en Mai 1998. Elle est implantée à l'extrême –Est du port de Bejaia. Elle est l'un des fleurons de l'industrie agroalimentaire en Algérie qui est constituée de plusieurs unités de production équipées de la dernière technologie et poursuit son développement par divers projets en cours de réalisation. Son expansion et son développement durant les 5 dernières années, font d'elle un important pourvoyeur d'emplois et de richesses. CEVITAL Food est passé de 500 salariés en 1999 à 3850 salariés en 2021

Où SOMMES NOUS ?

A l'arrière port de Béjaia à 200 M du quai : Ce terrain à l'origine marécageux et inconstructible a été récupéré en partie d'une décharge publique, viabilisé avec la dernière technologie de consolidation des sols par le système de colonnes ballastées (337 KM de colonnes ballastées de 18 M chacune ont été réalisées) ainsi qu'une partie à gagner sur la mer.

A Béjaia :

Nous avons entrepris la construction des installations suivantes :
-Raffinerie Huile
-Margarinerie

-Silos portuaires
-Raffinerie de sucre

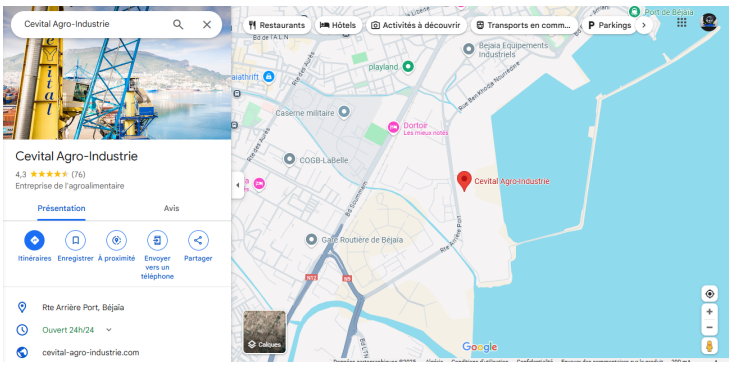

FIG. 4.1: Localisation cevital BEJAIA

A El Kseur :

Une unité de production de jus de fruits cojek a été rachetée par le groupe Cevital dans le cadre de la privatisation des 'entreprises publiques algériennes en novembre 2006.

Un immense plan d'investissement a été consentie visant à moderniser l'outil de production de jus de fruits Cojek...

Sa capacité de production est de 14 400 T par an. Le plan de développement de cette unité portera à 150 000/an en 2010.

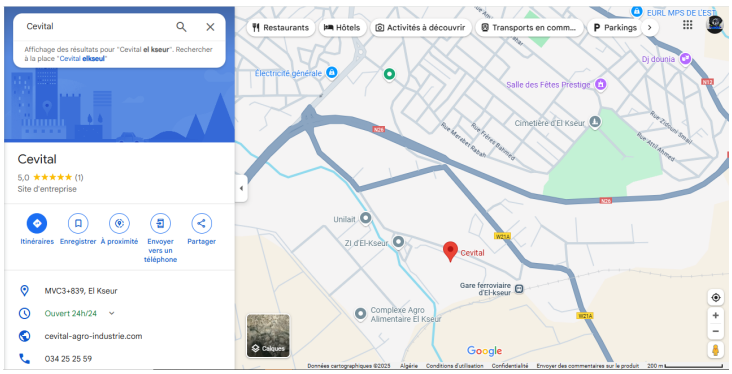

FIG. 4.2: Localisation cevital EL-KSEUR

A Tizi Ouzou :

A Agouni Gueghrane : au cœur du massif montagneux du Djurdjura qui culmine à plus de 2300 mètres : L'Unité d'Eau Minérale Lalla Khedidja a été inaugurée en juin 2007

4.2.2 Historique de l'entreprise

Historique de l'entreprise
1998 : Création de Cevital SPA industrie agro-alimentaire,
2006 : Acquisition de COJEK.
2007 : Création de MFG (VERRE PLAT),

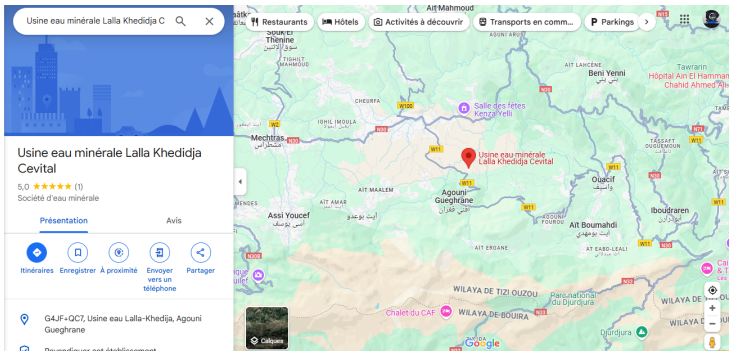

Fig. 4.3: Localisation cevital TIZI-OUZOU

2008 : Création de NUMILOG, 2013 : Acquisition de OXXO.

Cevital est un Groupe familial qui s'est bâti sur une histoire, un parcours et des valeurs qui ont fait sa réussite et sa renommée. Première entreprise privée algérienne à avoir investi dans des secteurs d'activités diversifiés, elle a traversé d'importantes étapes historiques pour atteindre sa taille et sa notoriété actuelle. Industrie agroalimentaire et grande distribution, électronique et électro-ménager, sidérurgie, industrie du verre plat, construction industrielle, automobile, services, médias...

Le Groupe Cevital s'est construit, au fil des investissements, autour de l'idée forte de constituer un ensemble économique. Porté par 18 000 employés répartis sur 3 continents, il représente le fleuron de l'économie algérienne, et œuvre continuellement dans la création d'emplois et de richesse.

4.2.3 Organigramme

La figure qui suit présente l'organigramme générale de Cevital.

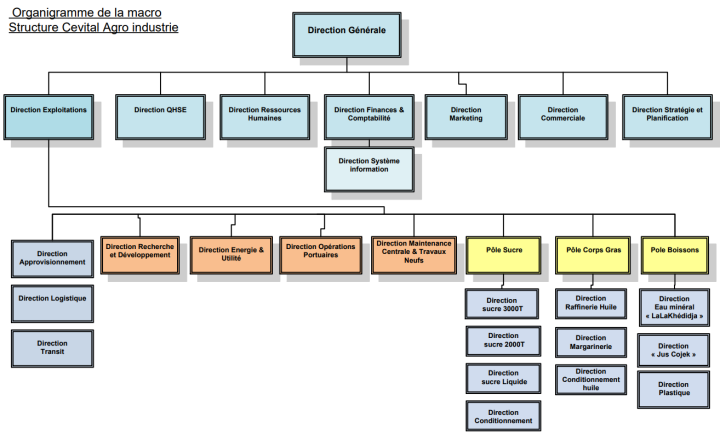

Fig. 4.4: Organigramme du groupe Cevital

4.2.4 Missions de l'entreprise

Le Complexe Agro-alimentaire comprend plusieurs unités de production, telles que la fabrication d'huiles végétales à base de tournesol, soja et palme avec une capacité de production de 828 000 tonnes/an et une part de marché nationale de 70 pour 100, la margarinerie et les graisses végétales produisant des margarines riches en vitamines A, D, E avec une capacité de production de 180 000 tonnes/an et une part de marché nationale de 30 pour 100, le raffinage du sucre roux de canne pour produire du sucre blanc conditionné en sachets de 50 kg et en morceaux, avec une capacité de production de 2 340 000 tonnes/an et une part de marché nationale de 85 pour 100, la production de sucre liquide avec une capacité de production de 219 000 tonnes/an, les silos portuaires offrant une capacité de stockage de 120 000 tonnes avec un projet d'extension en cours pour atteindre 200 000 tonnes, et enfin la production d'eau minérale, de jus de fruits et de sodas avec une capacité de production de 3 000 000 bouteilles par jour pour l'eau minérale "Lalla Khedidja" et la réhabilitation de l'unité de production de jus de fruits "EL KSEUR".

4.2.5 Structures de l'entreprise

L'entreprise Cevital Agro-industrie, créée en 1998 et située au port de Bejaïa, est dotée de plusieurs unités de production ultramodernes, dont deux raffineries de sucre, une unité de sucre liquide, une raffinerie d'huile, une margarinerie, une unité de conditionnement d'eau minérale à Tizi Ouzou, une unité de fabrication et de conditionnement de boissons rafraîchissantes à EL-Kseur, et une conserverie. Avec plusieurs silos portuaires et un terminal de déchargement d'une capacité de 2000 tonnes/heure, Cevital possède le premier terminal de déchargement portuaire en Méditerranée.

4.3 État des lieux

4.3.1 La direction Système d'informations

Elle définit, également, dans le cadre des plans pluriannuels les évolutions nécessaires en fonction des objectifs de l'entreprise et des nouvelles technologies.

Elle assure la mise en place des moyens des technologies de l'information nécessaires pour supporter et améliorer l'activité, la stratégie et la performance de l'entreprise, elle doit ainsi veiller à la cohérence des moyens informatiques et de communication mises à la disposition des utilisateurs, à leur mise à niveau, à leur maîtrise technique et à leur disponibilité et opérationnalité permanente et en toute sécurité.

4.3.2 Équipements informatique

Voici une présentation hardware et software de l'environnement de Cevital :

Equipement	Modèle	illustration
Model switch d'accès	Cisco WS-C2960X	
Switch distribution	Cisco WS-C3850	
Switch core	Cisco C6807-XL	
Switch intermédiaire / interconnexion	Cisco WS-2960C	
Switch DMZ	Cisco WS-C2960X	
Router WAN	Cisco2911	
Router internet (distant)	Cisco2811 + Cisco1900	
Firewall fortinet	Fortigate	

FIG. 4.5: Les équipements informatique de l'entreprise

4.3.3 Réseaux internes de l'entreprise

Cevital dispose d'un réseau interne assez vaste permettant de relier les différents bâtiments, unités de production et direction du complexe. Le réseau est composé de plusieurs équipements dont la plupart sont de marque Cisco (Switch, Catalyst, Routeur) interconnectés entre eu grâce à la fibre optique, ou cuivre.

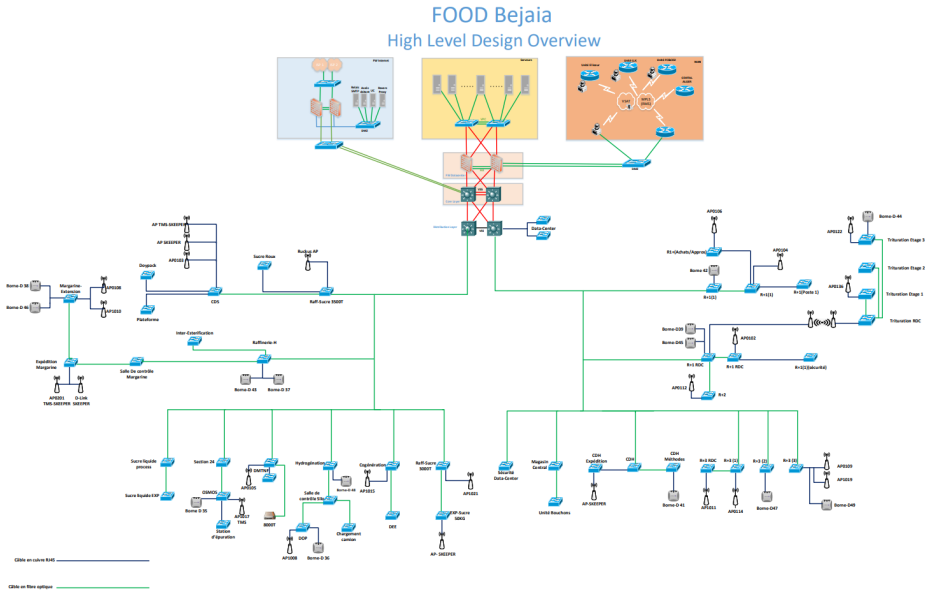

FIG. 4.6: Architecture du réseau informatique de Cevital

4.4 Conclusion

Dans ce chapitre, nous avons donné un aperçu de l'infrastructure de l'entreprise cevital bejaia fournie, identifiant un problème crucial qui a nécessité la recherche et la mise en œuvre d'une nouvelle architecture de réseau sécurisé.

Chapitre 5

Conception et réalisation

Introduction

Ce chapitre présente la mise en œuvre technique d'une solution de sécurité réseau plus performante et adaptée aux besoins spécifiques de Cevital. L'objectif principal est de concevoir et déployer un système de détection et de prévention des intrusions (IDS/IPS), reposant sur des outils open-source fiables comme PFSense pour le pare-feu et Snort pour la détection d'intrusions. Avant toute mise en œuvre, une phase d'étude et d'analyse de l'infrastructure informatique actuelle de l'entreprise Cevital a été réalisée. Cette étape essentielle a permis d'identifier les principales faiblesses du système en place, de mieux comprendre les besoins réels de l'entreprise en matière de sécurité, et de poser les bases pour la conception d'une solution adaptée et efficace.

5.1 Étude et analyse des besoins

5.1.1 Problématique

L'analyse de l'infrastructure informatique actuelle de l'entreprise Cevital a révélé plusieurs faiblesses qui compliquent la détection et la gestion des attaques informatiques. parmi eux Nous allons en présenter :

— La diversité des équipements et des logiciels rend la gestion de la sécurité complexe, ce qui augmente les risques de failles et de mauvaises configurations.
— L'absence d'une visibilité globale et en temps réel sur les systèmes et réseaux empêche une détection rapide des incidents.
— L'entreprise est de plus en plus exposée à des attaques ciblées et sophistiquées, qui échappent souvent aux protections classiques.
menaces ralentit la réactivité de l'entreprise face aux cyberattaques.
— Risque d'accès non autorisés aux systèmes et aux informations sensibles, ce qui peut mettre en péril la sécurité .

Ces problématiques freinent la capacité de Cevital à protéger efficacement son système d'information. Il devient donc essentiel de mettre en place une stratégie de sécurité plus intégrée, intelligente et adaptée aux menaces actuelles. Grâce aux suggestions des membres du personnel qui nous ont accompagnés pendant le stage, nous avons réussi à trouver une solution qui implique la mise en place d'un pare-feu Pfsense pour protéger le réseau et surveiller le trafic entrant et sortant. en adaptant un système de sécurité pour la détection

et la prévention d'intrusions sur le réseau informatique de l'entreprise Cevital, adapté à ses besoins spécifiques.

5.1.2 Objectifs

Objectifs visés :
1-Assurer une visibilité globale et en temps réel de l'infrastructure réseau
2-Assurer la confidentialité et l'intégrité des informations échangées au sein du réseau.
3-Mettre en place un système de détection précoce des tentatives d'intrusion.
4-Mettre en œuvre des mécanismes de prévention pour stopper les attaques en cours.
5-Améliorer la résilience du réseau face aux menaces et aux attaques de plus en plus sophistiquées.
6-Réduire les coûts associés à la perte de données et à l'interruption de l'activité du réseau.
7-Respecter les règles et normes de sécurité en vigueur.
Ces objectifs orientent la mise en place d'un système de sécurité solide, capable de détecter et de prévenir les intrusions pour assurer un environnement réseau sûr et fiable.

5.1.3 Propositions

Dans le but de résoudre ses défis, nous avons proposé un déploiement d'IDS/IPS (Système de Détection et de Prévention d'Intrusion) qui nécessite :

—Surveillance continue du réseau et des systèmes pour détecter les intrusions et les tentatives accès non autorisées.
—Blocage automatique des activités malveillantes et des comportements suspects.
—Intégration avec le SNORT pour une vue ensemble et une réponse coordonnée aux menaces.

5.1.4 Cahier de charge

Projet : Implémentation d'un système de détection

d'intrusion (IDS) et de prévention d'intrusion (IPS) sur le pare-feu pfSense

Organisation d'acceuille

Groupe Cevital

5.1.5 Livrables attendus

-Configuration du pare-feu pfSense avec les règles de sécurité appropriées pour détecter et prévenir les intrusions.
-Rapports détaillés sur les tests effectués, les résultats obtenus et les recommandations pour améliorer la sécurité du réseau.

5.1.6 Planning prévisionnel :

Étapes du projet :

-Étude et analyse des besoins.
-Configuration et implémentation de l'IDS/IPS sur pfSense.
-Tests et vérifications du système IDS/IPS.
-Documentation des résultats obtenus.

Durée prévue pour chaque étape :

-Étude et analyse des besoins : 2 semaines.
-Configuration et implémentation de l'IDS/IPS : 3 semaines.
-Tests et vérifications : 1 semaine.
-Documentation des résultats : 1 semaine.

Ressources nécessaires :

-Accès aux équipements informatiques et logiciels requis.
-Accès aux systèmes et réseaux de Cevital pour la configuration

5.1.7 Environnement de travail

5.1.8 Outils de travail :

Matériel :

Ordinateur : équipé minimum d'un processeur Intel Core i5 , 8 Go de RAM et un disque dur SSD. Le système d'exploitation utilisé est Windows 10 en version 64 bits.

Logiciels :

GNS3 :

Est une plateforme de virtualisation réseau open source qui permet de créer et de simuler des réseaux virtuels complexes. Il offre un environnement de laboratoire virtuel pour concevoir, configurer et tester des topologies réseau en utilisant des périphériques réseau virtuels. Pour ce projet, la version utilisée est GNS3 v2.2.38. Cette version spécifique de GNS3 propose des fonctionnalités avancées et des améliorations pour la création et la gestion des réseaux virtuels. Elle permet d'intégrer différents types de périphériques réseau, tels que des routeurs, des commutateurs, des pare-feu, etc., pour construire une topologie réseau réaliste.

En utilisant GNS3 v2.2.38, l'environnement de travail pour ce projet bénéficie d'une plateforme fiable et performante pour la simulation de réseaux virtuels. Il permet de configurer les périphériques réseau virtuels, de définir les paramètres de connectivité et de tester les fonctionnalités du système de détection d'intrusion IDS/IPS (Snort) en interagissant avec les machines virtuelles utilisées dans VMware. GNS3 facilite également la gestion des configurations et des connexions réseau, et offre des fonctionnalités avancées telles que la capture de paquets, l'analyse du trafic réseau et le débogage. En intégrant GNS3 avec VMware Workstation 17 Pro, il est possible de créer un environnement de test complet et réaliste pour l'implémentation et les tests du système IDS/IPS, en simulant

FIG. 5.1: Version de GNS3

l'architecture réseau de Cevital et en évaluant son efficacité face aux attaques internes et externes.

PFsense :

PfSense est une distribution logicielle open source basée sur FreeBSD, qui transforme un ordinateur standard en un puissant pare-feu et routeur. Il offre une gamme de fonctionnalités avancées de sécurité réseau et de routage, ce qui en fait un choix populaire pour la protection des réseaux d'entreprise. Pour ce projet, la version utilisée de pfSense est la dernière version stable disponible. pfSense permet de déployer un pare-feu robuste et personnalisable, capable de filtrer le trafic réseau, de créer des règles de sécurité avancées et de détecter les intrusions grâce à des fonctionnalités IDS/IPS telles que Snort. L'implémentation de pfSense dans l'environnement de travail du projet permet de créer un pare-feu virtuel sur lequel le système IDS/IPS Snort sera configuré et déployé. Cela offre un contrôle granulaire sur les flux de trafic réseau, la gestion des adresses IP, la création de règles de pare-feu et l'analyse du trafic. En utilisant pfSense, l'environnement de travail bénéficie d'un pare-feu puissant et flexible pour protéger le réseau de Cevital. Il permet de définir des politiques de sécurité adaptées, de détecter les intrusions et de prévenir les attaques en utilisant Snort, et de mettre en place des mécanismes de filtrage et de blocage pour protéger les ressources et les données de l'entreprise. La configuration et les tests réalisés sur pfSense fourniront des résultats précis sur l'efficacité du système IDS/IPS dans la détection et la prévention des intrusions.

VMware :

Est un logiciel de virtualisation qui permet de créer et de gérer des machines

virtuelles sur un seul ordinateur physique. Il permet de faire fonctionner simultanément plusieurs systèmes d'exploitation et applications sur une même machine, sans avoir besoin de plusieurs ordinateurs physiques. VMware offre un environnement isolé et sécurisé pour exécuter des systèmes d'exploitation virtuels, ce qui facilite le déploiement, les tests et la gestion des environnements de travail virtuels. Pour ce projet, la version utilisée est VMware® Workstation 17 Pro. Cette version professionnelle de VMware offre des fonctionnalités avancées pour la création et la gestion des machines virtuelles. Elle permet une intégration étroite avec GNS3 et offre des performances élevées pour exécuter simultanément plusieurs machines virtuelles. Avec VMware Workstation 17 Pro, il est possible de configurer les paramètres des machines virtuelles, d'effectuer des snapshots pour

sauvegarder l'état des machines virtuelles à un instant précis, et de gérer les ressources système allouées à chaque machine virtuelle.

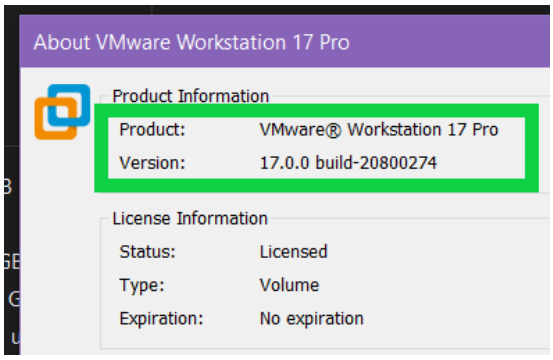

Fig. 5.2: Version de VMware

Dans l'environnement de travail, les logiciels utilisés dans VMware sont les suivants :

1. VM de GNS3 : Il s'agit d'une machine virtuelle spécialement configurée pour exécuter GNS3, une plateforme de virtualisation réseau. Cette machine virtuelle permet de simuler les périphériques réseau nécessaires pour le projet, tels que des routeurs, des commutateurs, etc. Elle offre un environnement virtuel réaliste pour la mise en place de la topologie réseau de Cevital. De plus, elle est connectée à VMware pour faciliter l'intégration des machines virtuelles supplémentaires.

2. Kali Linux 2025 : Cette distribution Linux est largement utilisée dans le domaine de la sécurité informatique. Elle est spécialement conçue pour les tests de sécurité et les audits de pénétration. Dans le cadre du projet, Kali Linux est utilisé pour effectuer des tests d'intrusion dans le réseau de Cevital, afin d'évaluer la résistance du système IDS/IPS (Snort) et de détecter d'éventuelles vulnérabilités. Cette machine virtuelle est également connectée à GNS3 pour permettre la communication avec les autres périphériques virtuels.

3.Windows 7 : Une machine virtuelle Windows 7 est utilisée dans l'environnement de travail pour la configuration et les tests supplémentaires. Windows offre une plateforme familière pour effectuer la configuration de PFsense avec un navigateur web, ainsi que pour vérifier la compatibilité et les performances du système IDS/IPS. Elle est également connectée à GNS3 pour permettre l'échange de données avec les autres machines virtuelles et périphériques réseau.

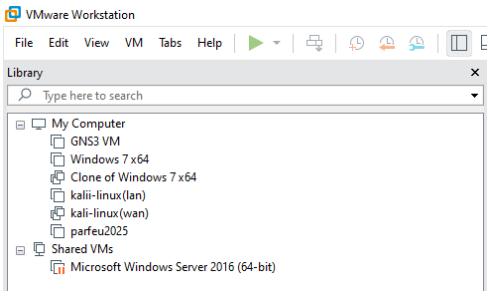

Fig. 5.3: Machines installée sur VMware

En utilisant ces logiciels dans VMware et en les connectant à GNS3, il est possible de créer un environnement virtuel complet et réaliste, où les machines virtuelles interagissent avec les périphériques réseau simulés. Cela permet une intégration fluide entre les différents composants du système de détection d'intrusion IDS/IPS (Snort) et facilite les tests et les analyses approfondis. Note : Les détails spécifiques sur l'installation et la configuration des logiciels et machines seront abordés dans la deuxième partie pratique du mémoire.

5.1.9 Architecture utilisée :

Pour simplifier la simulation du réseau de Cevital en raison des performances de l'ordinateur personnel, nous utiliserons une architecture simplifiée sur GNS3. Cela permettra néanmoins de tester efficacement l'implémentation de l'IDS et de l'IPS sur le pare-feu pfSense.

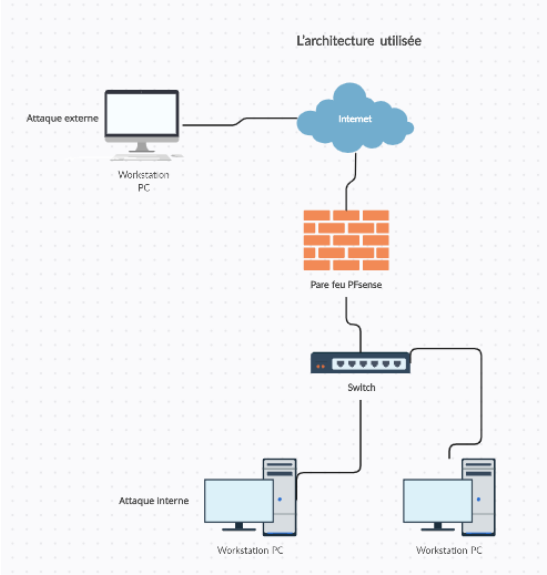

FIG. 5.4: Architecture utilisée

5.2 réalisation

5.2.1 Installation et configuration de GNS3 :

téléchargement de GNS3 :

- Rendez-vous sur le site officiel de GNS3 (https ://www.gns3.com/) et accédez à la section de téléchargement

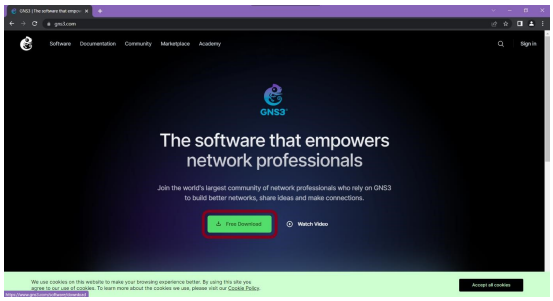

FIG. 5.5: Version de GNS3

• Sélectionnez la version de GNS3 compatible avec votre système d'exploitation (Windows, macOS, Linux) et téléchargez le fichier d'installation.

FIG. 5.6: Téléchargement de la version gns3 compatible

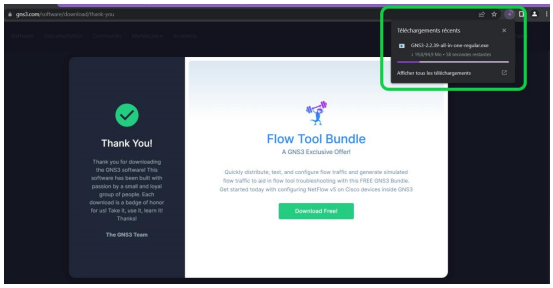

FIG. 5.7: Téléchargement de la version gns3 compatible

Installation de GNS3 :

• Exécutez le fichier d'installation téléchargé et suivez les instructions à l'écran pour installer GNS3 sur votre ordinateur.

Une fois téléchargé, lancez le fichier d'installation. Cliquez sur « Suivant » sur la première fenêtre puis acceptez les conditions d'utilisation sur la suivante. Pour les fonctionnalités, il y en a plusieurs comme par exemple wireshark ou putty, je vous conseille de laisser par défaut afin d'avoir ces outils à disposition pour la suite.

FIG. 5.8: Exécutez le fichier d'installation GNS3

- Choisissez les options d'installation appropriées en fonction de vos besoins.

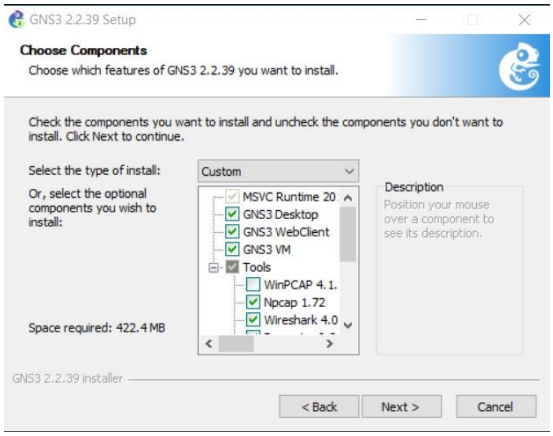

FIG. 5.9: Choisissez les options d'installation appropriées GNS3

Nous avons fini la partie installation une fois cliquer sur « Installer ».

Configuration des paramètres réseau :

- Lancez GNS3 après l'installation et accédez à l'interface utilisateur.
- Allez dans le menu "Préférences" ou "Options" (selon votre système d'exploitation) pour accéder aux paramètres de configuration.
- Configurez les paramètres réseau en fonction de votre environnement. Cela peut inclure la sélection de l'adaptateur réseau à utiliser, la définition des plages d'adresses IP disponibles pour les périphériques virtuels, etc.
- Assurez-vous que les paramètres réseau de GNS3 correspondent à ceux de votre réseau physique pour permettre une connectivité adéquate entre les périphériques virtuels et réels.

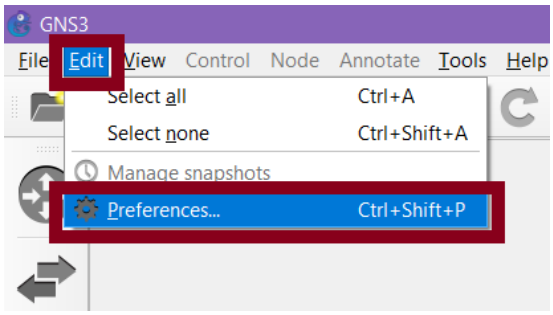

FIG. 5.10: Configuration réseau GNS3

importer des périphériques et des images dans GNS3 :

| 1 | Assurez-vous d'avoir téléchargé les images d'IOS Cisco, ainsi que les images des autres systèmes d'exploitation réseau que vous souhaitez utiliser, en respectant les licences requises.
| 2 | Lancez GNS3 sur votre ordinateur. Assurez-vous d'avoir correctement configuré les paramètres réseau nécessaires dans GNS3.
| 3 | Dans l'interface GNS3, cliquez sur "Edit" (Éditer) dans la barre de menu supérieure, puis sélectionnez "Preferences" (Préférences).

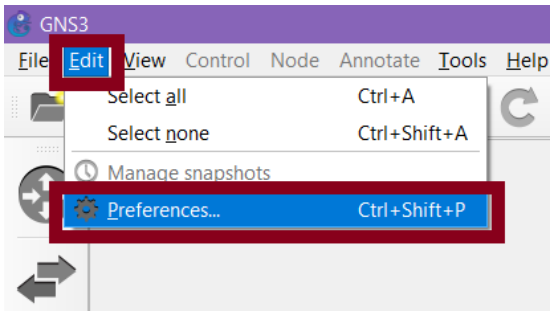

FIG. 5.11: Étape 1 pour importer des images dans GNS3

| 4 | Dans la fenêtre des préférences, sélectionnez l'onglet "IOS routers" (Routeurs IOS) ou l'onglet approprié pour le système d'exploitation que vous souhaitez importer.
| 5 | Cliquez sur le bouton "New" (Nouveau) pour ajouter un périphérique virtuel.

| 6 | Dans la fenêtre qui s'ouvre, donnez un nom au périphérique et sélectionnez le type de périphérique approprié dans le menu déroulant.
| 7 | Cliquez sur "Browse" (Parcourir) pour sélectionner l'image d'IOS ou du système d'exploitation que vous souhaitez importer.

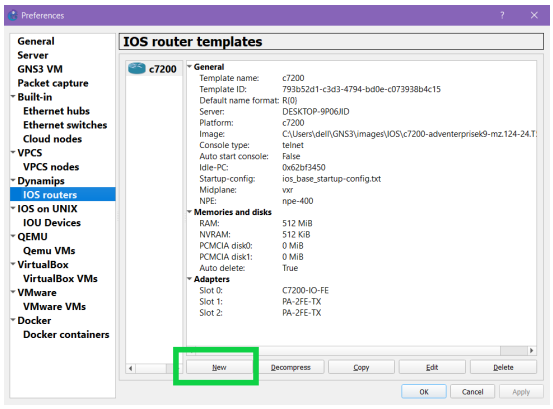

FIG. 5.12: Étape 2 pour importer des images dans GNS3

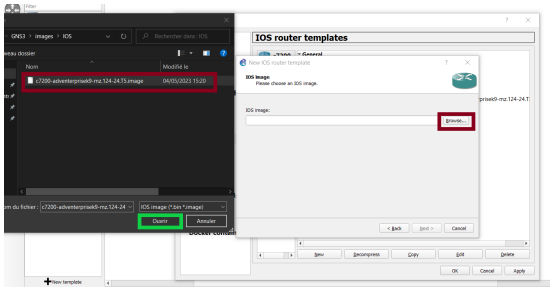

FIG. 5.13: Étape 3 pour importer des images dans GNS3

| 8 | Sélectionnez l'image appropriée dans la liste et cliquez sur "OK" pour l'importer.
| 9 | Répétez les étapes 5 à 8 pour importer tous les périphériques et images nécessaires à votre topologie réseau.
| 10 | Une fois les périphériques et les images importés, vous pouvez les utiliser dans vos topologies en les faisant glisser depuis la fenêtre "Devices" (Périphériques) vers l'espace de travail.

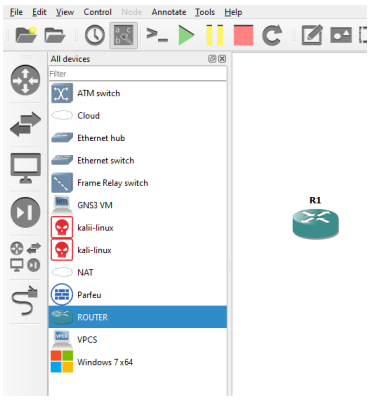

FIG. 5.14: Périphérique est bien importé

Assurez-vous de respecter les licences des images d'IOS et des systèmes d'exploitation que vous importez, et suivez les instructions spécifiques fournies par GNS3 pour importer les périphériques et les images correctement.

5.2.2 Configuration des machines virtuelles VMware :

Téléchargement et installation de VMWare :

- Rendez-vous sur le site officiel de VMware
(https ://www.vmware.com) et recherchez
la version appropriée de VMware pour votre système d'exploitation.

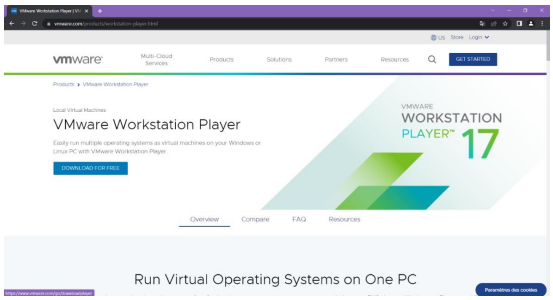

FIG. 5.15: Site de VMware

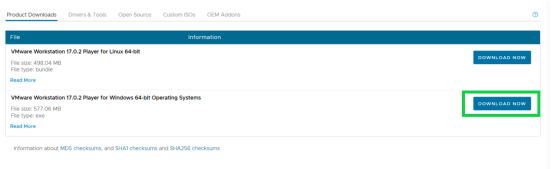

FIG. 5.16: Télécharger VMware

- Téléchargez le programme d'installation de VMware sur votre ordinateur.
- Double-cliquez sur le fichier d'installation téléchargé pour lancer le processus d'installation.
- Suivez les instructions à l'écran pour accepter les conditions de licence, sélectionner le dossier d'installation et choisir les fonctionnalités à installer.
Assurez-vous de sélectionner toutes les fonctionnalités nécessaires pour
votre utilisation, telles que
VMware Workstation ou VMware Player.
- Attendez que l'installation soit terminée. Cela peut prendre quelques minutes en fonction de la vitesse de votre ordinateur.

Configurez les paramètres réseau des machines virtuelles pour les connecter à la topologie réseau créée dans GNS3 :

Création des machines virtuelles :

- Lancez VMware et créez une nouvelle machine virtuelle pour chaque équipement réseau que vous souhaitez représenter (par exemple, pfSense, Kali Linux, Windows).
- Suivez les étapes du processus de création de la machine virtuelle, y compris la sélection du système d'exploitation approprié et la configuration des paramètres de stockage (taille du disque dur virtuel, emplacement du fichier image, etc.).

Configuration des paramètres réseau :

- Pour chaque machine virtuelle, accédez aux paramètres réseau de la machine virtuelle dans VMware.
- Sélectionnez l'option de configuration réseau appropriée pour votre réseau.
- Assurez-vous de sélectionner l'adaptateur réseau correct pour chaque machine virtuelle et associez-le à une interface réseau disponible sur votre système physique.

Pour mieux comprendre ses étapes voici l'Installation et configuration de la machine virtuelle (VM) Kali linux sur GNS3 :

1.Accès au site officiel de Kali Linux :

-Rendez-vous sur le site officiel de Kali Linux à l'adresse https ://www.kali.org/downloads/ pour télécharger la machine virtuelle préconfigurée.

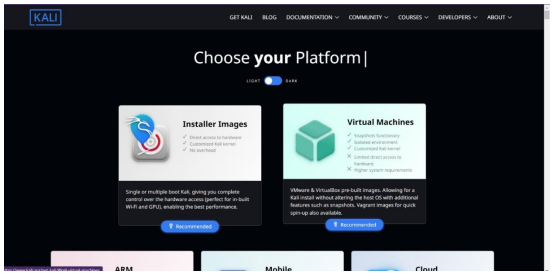

FIG. 5.17: Site de Kali Linux

FIG. 5.18: VMware

2.Téléchargement de la machine virtuelle de Kali Linux :

-Sur la page de téléchargement de Kali Linux, recherchez la section ”VM Images” (Images de machines virtuelles) et sélectionnez la version de Kali Linux que vous souhaitez utiliser (Dans notre cas ”VMware”).

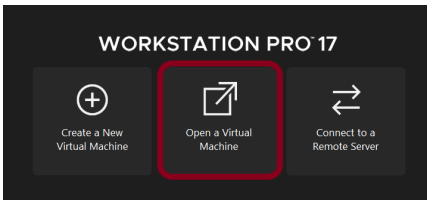

FIG. 5.19: Ouvrir une machine virtuel

Cliquez sur le lien de téléchargement correspondant à votre logiciel de virtualisation.

3.Préparation de la machine virtuelle :

-Créez une nouvelle machine virtuelle en sélectionnant l’option d’importation ou de création à partir d’un fichier image.
-Parcourez votre système de fichiers et sélectionnez le fichier de machine virtuelle (fichier avec une extension. ova ou .vmx) que vous avez téléchargé précédemment.

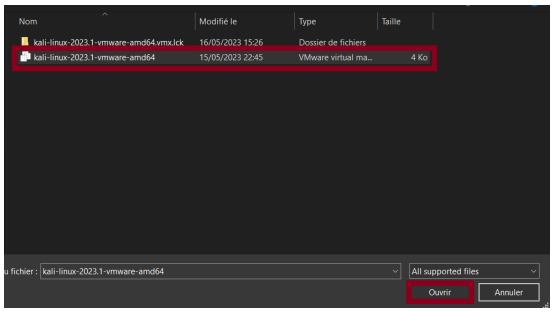

FIG. 5.20: Importer la machine Kali Linux

Une fois clicker sur « Open a Virtual machine » nous allons importez dans le dossier télecharger la VM

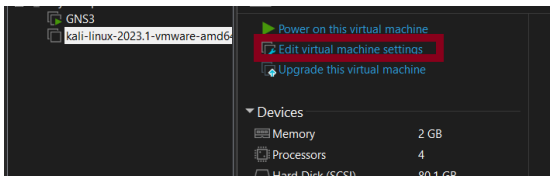

FIG. 5.21: Configuration de la machine virtuelle

4.Configuration de la machine virtuelle :

-Mettez sa carte réseau sur la VMnet1 :
"Edit virtual machine" cliquez sur "Network adapter", séléctionnez "Custom" spécifiez la VMnet1

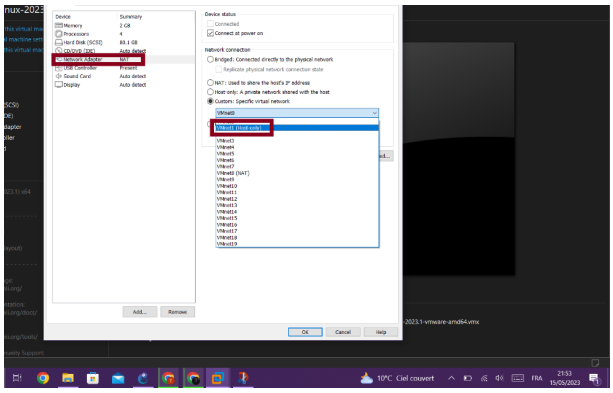

FIG. 5.22: Étape 1 de la configuration de Kali Linux

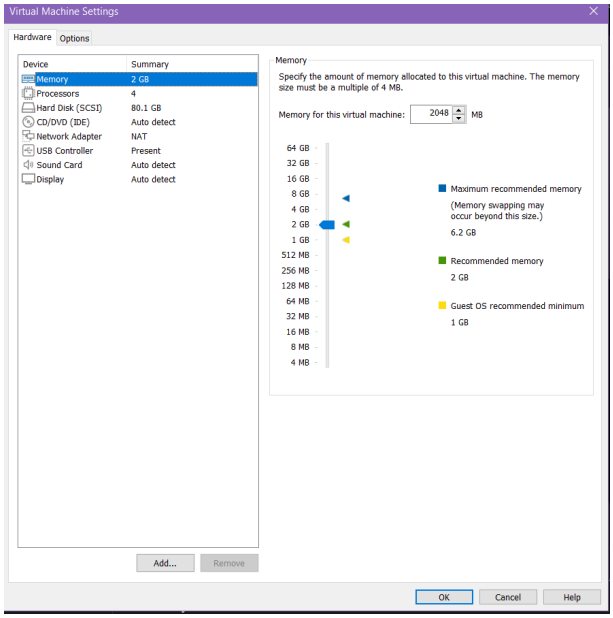

FIG. 5.23: Étape 2 de la configuration de Kali Linux

5.Finalisation de la configuration :

Vérifiez les paramètres de la machine virtuelle et cliquez sur "Terminer" ou "Importer" pour lancer le processus d'importation de la machine virtuelle. Attendez que l'importation se termine. Cela peut prendre quelques minutes en fonction des performances de votre ordinateur.

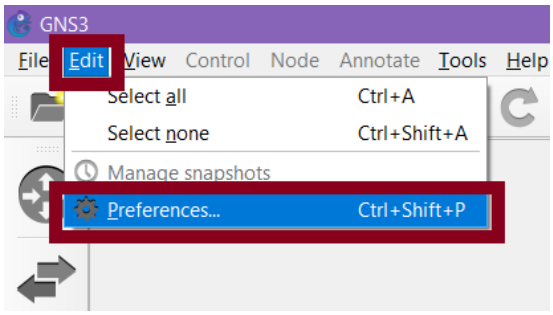

FIG. 5.24: Étape 3 de la configuration de Kali Linux

6.Ajout de la machine virtuelle à la topologie GNS3 :

- Configuration de GNS3 pour l'intégration de VMware :

-Lancez GNS3 et ouvrez votre projet existant ou créez-en un nouveau. -Cliquez sur "Edit" (Modifier) dans la barre de menu supérieure, puis sélectionnez "Preferences" (Préférences).

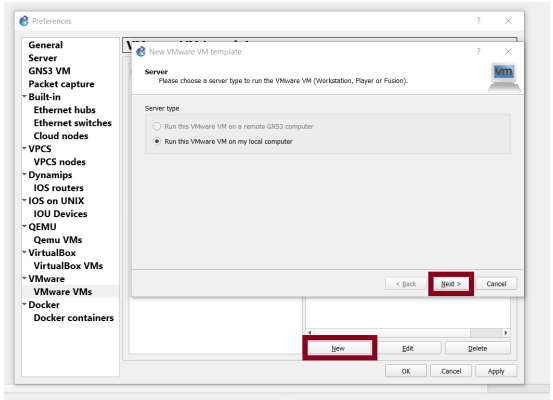

FIG. 5.25: Ajouter la VM a GNS3 Étape 1

-Dans la fenêtre des préférences, cliquez sur "Virtualization" (Virtualisation) puis sur "VMware" dans le menu déroulant.
-Assurez-vous que la case "Enable VMware Workstation/Fusion support" (Activer la prise en charge de VMware Workstation/Fusion) est cochée.
-Spécifiez le chemin d'accès au dossier contenant vos fichiers de machine virtuelle de Kali Linux (.vmx, .vmdk, etc.).
-Cliquez sur "OK" pour enregistrer les modifications.

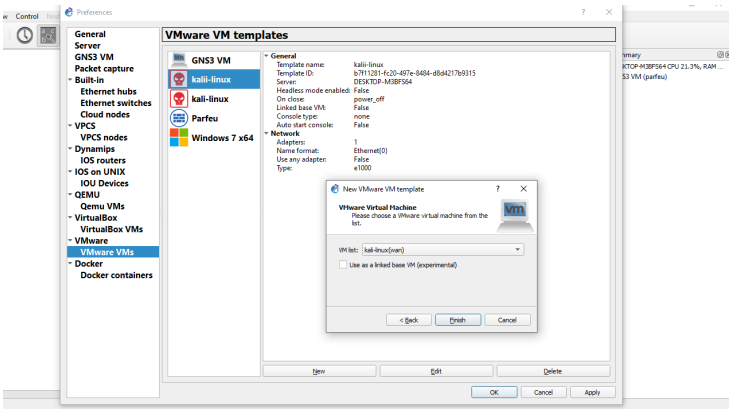

Fig. 5.26: Ajouter la VM a GNS3 Étape 2

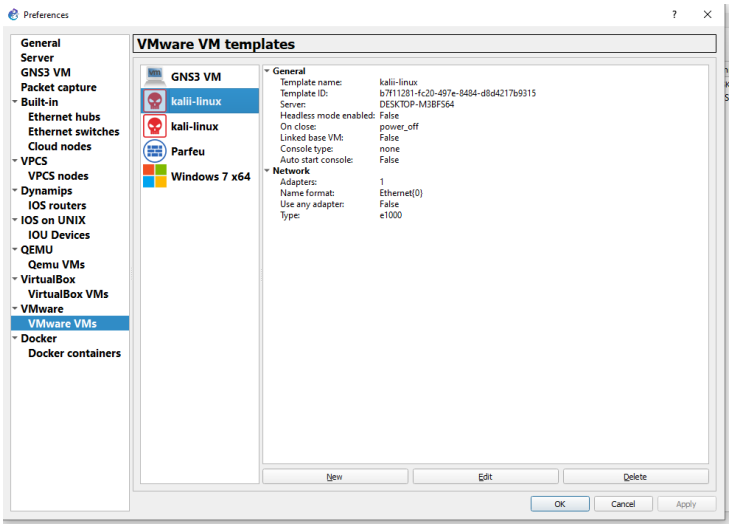

Fig. 5.27: Ajouter la VM a GNS3 Étape 3

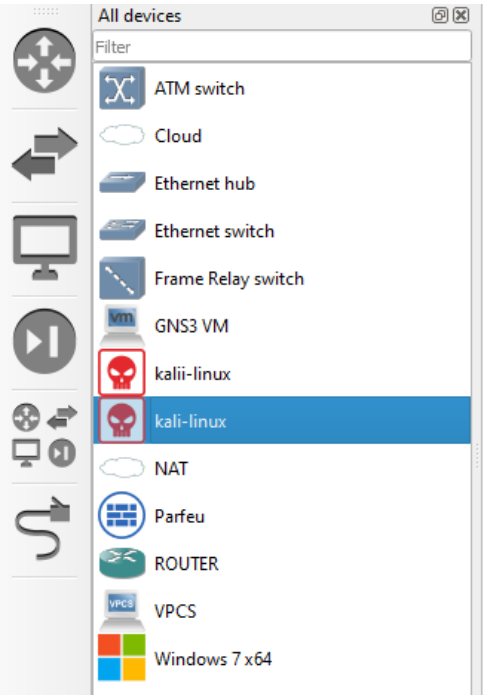

FIG. 5.28: Ajouter la VM a GNS3 Étape 4

5.2.3 Configuration de pfSense :

Téléchargez l'image ISO de pfSense à partir du site officiel et installez-la sur une machine virtuelle :

- Accédez au site officiel de pfSense (https ://www.pfsense.org) et téléchargez l'image ISO correspondant à la version souhaitée de pfSense.

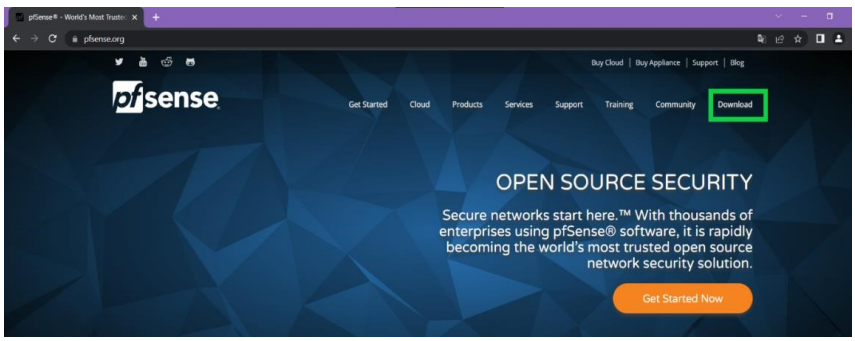

FIG. 5.29: Site offciel Pfsense

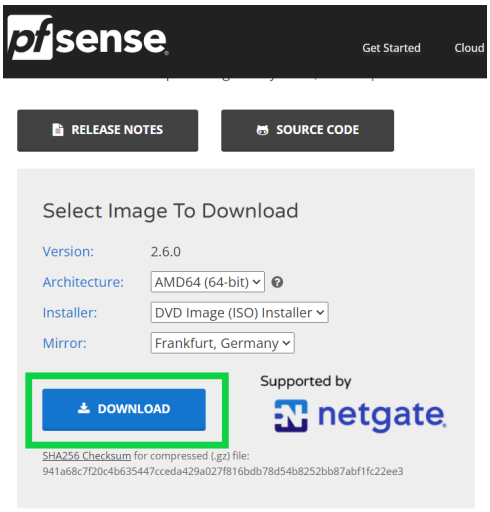

FIG. 5.30: Télécharger PFsense

• Lancez GNS3, cliquez sur l'option "Import appliance" (ou une option similaire) pour importer l'ISO de pfSense.

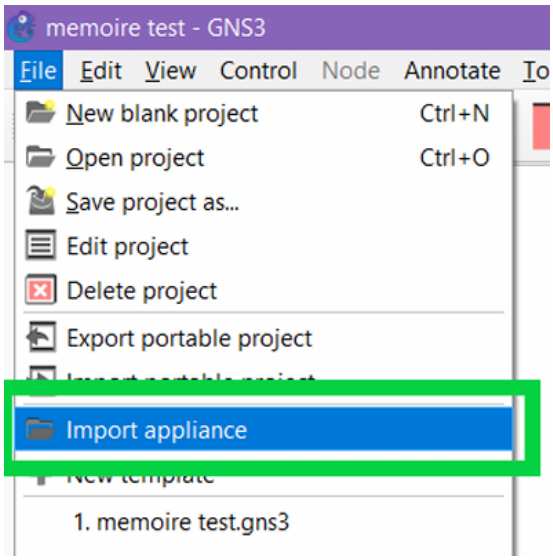

FIG. 5.31: Importer PFsense sur GNS3

• Sélectionnez l'ISO de pfSense que vous avez téléchargée à l'étape 1 et suivez les instructions pour l'importer dans GNS3.

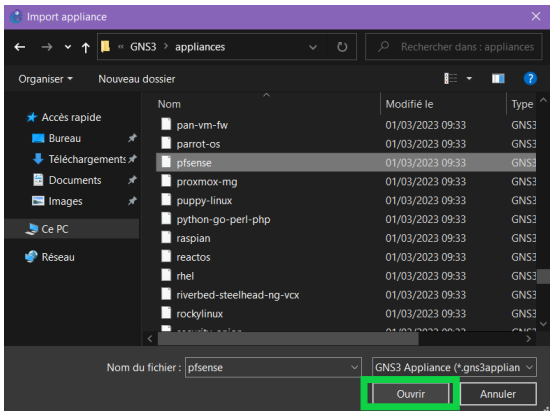

Fig. 5.32: Importer l'image ISO de PFsense

• Après l'importation de l'ISO, GNS3 créera automatiquement un appareil virtuel représentant pfSense dans votre topologie réseau.

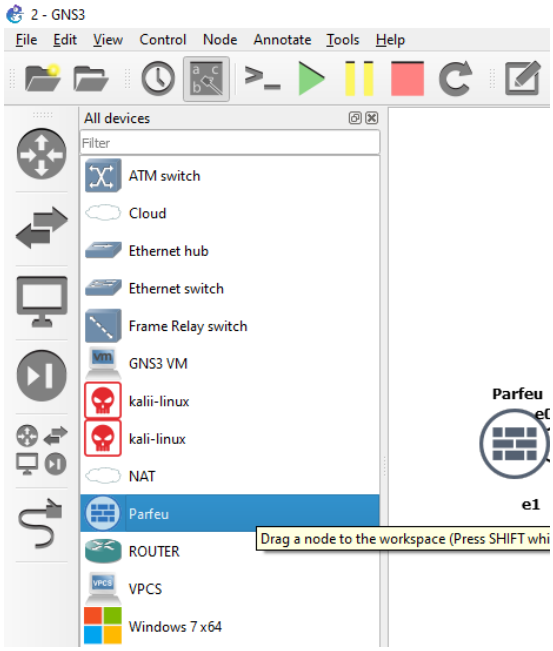

Fig. 5.33: PFsense a était bien importer sur GNS3

• Cliquez avec le bouton droit de la souris sur l'appareil pfSense dans la topologie et sélectionnez l'option "Configure" (ou une option similaire) pour ouvrir les paramètres de configuration.
• Dans les paramètres de configuration de pfSense, configurez les interfaces réseau en fonction de votre topologie réseau dans GNS3. Assurez-vous de mapper correctement les interfaces réseau virtuelles de pfSense avec les interfaces réseau virtuelles dans GNS3.

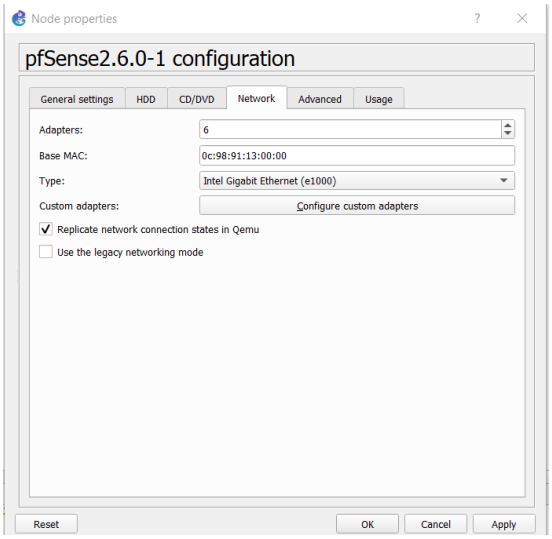

FIG. 5.34: Configurer la template de PFsense sur GNS3

- Une fois l'installation terminée, pfSense sera opérationnel dans votre topologie GNS3. Vous pourrez accéder à l'interface de gestion web de pfSense en utilisant l'adresse IP assignée à l'interface WAN de pfSense.
- Démarrez l'appliance pfSense dans GNS3 en cliquant avec le bouton droit de la souris sur l'appliance et en sélectionnant "Console" pour ouvrir la console de pfSense.
- À partir de la console, vous verrez le menu de démarrage de pfSense. Appuyez sur "Enter" pour démarrer le système.
- Le système démarre et vous présente un menu d'options de configuration. Appuyez sur "entrer" pour lancer l'assistant de configuration initiale.

La configuration initiale de pfSense :

Suivez les étapes de configuration initiale jusqu'à ce que vous atteigniez l'option "Set Disk Partition" (Définir la partition du disque).

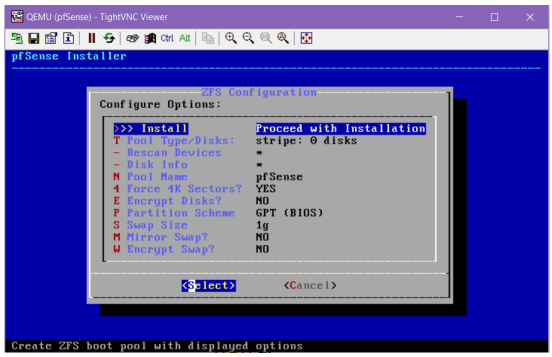

FIG. 5.35: Configuration initiale de PFsense Étape 1

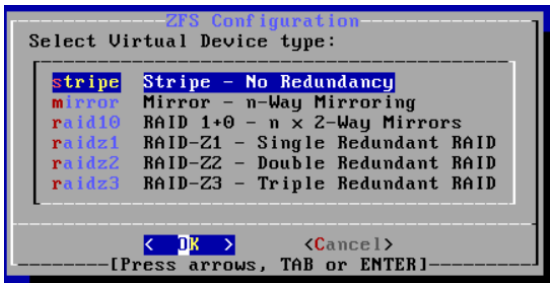

FIG. 5.36: Configuration initiale de PFsense Étape 2

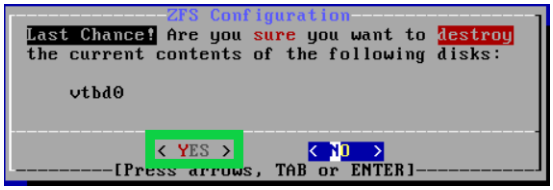

FIG. 5.37: Configuration initiale de PFsense Étape 3

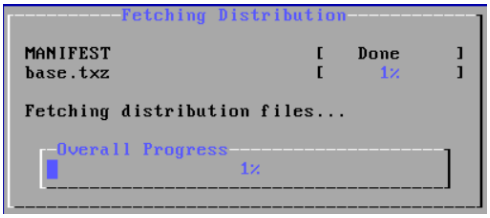

FIG. 5.38: Configuration initiale de PFsense Étape 4

- Dans l'option "Set Disk Partition", sélectionnez "Auto (ZFS)" pour créer automatiquement une partition ZFS sur le disque.
-Vous serez invité à confirmer la création d'une partition ZFS. Appuyez sur "Enter" pour confirmer.
-L'assistant va créer une partition ZFS sur le disque. Une fois terminé, il affichera un résumé des configurations effectuées.
Le système redémarrera pour appliquer les configurations.

Configuration des interfaces réseaux de PFsense :

Le système démarre et affiche un menu avec plusieurs options. Appuyez sur "2" pour configurer les interfaces réseaux
Nous allons commencer par l'interface WAN don nous mettons « 1 »

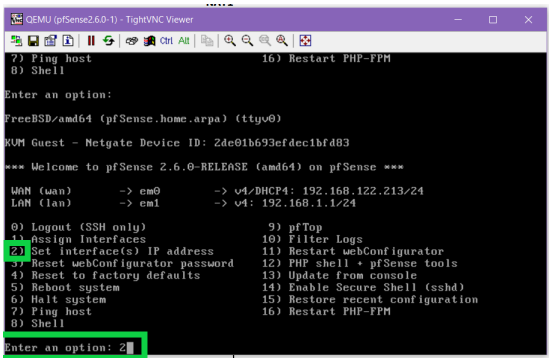

FIG. 5.39: Configuration des interfaces réseaux de PFsense Étape 1

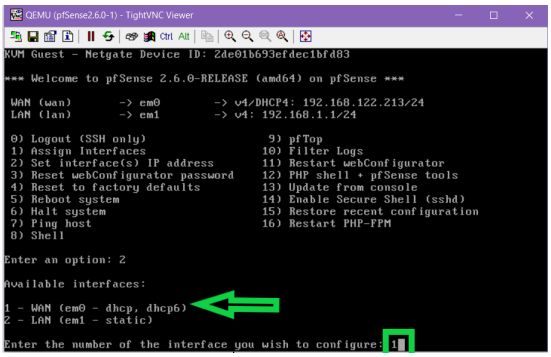

FIG. 5.40: Configuration des interfaces réseaux de PFsense Étape 2

Pour l'interface Wan nous allons mettre une adresse IP statique

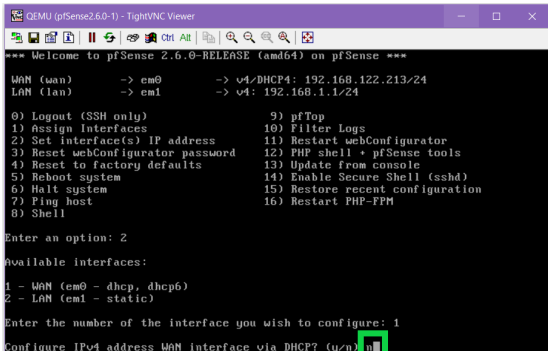

FIG. 5.41: Configuration des interfaces réseaux de PFsense Étape 3

Pour l'interface WAN nous allons lui configurer :
Unes adresse IP : 192.168.11.178
On va attribue un masque de /24
Une adresse de passerelle : 192.168.11.2

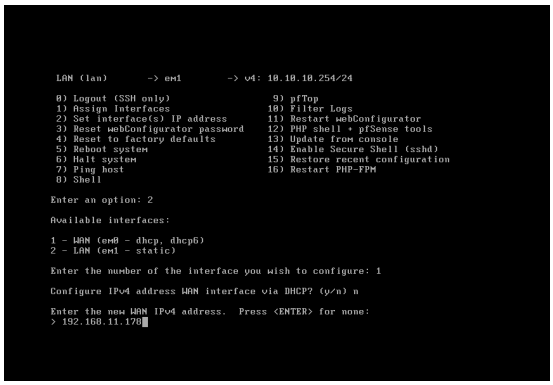

FIG. 5.42: Configuration des interfaces réseaux de PFsense Étape 4

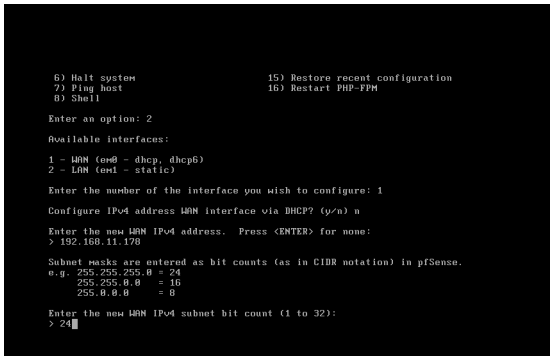

FIG. 5.43: Configuration des interfaces réseaux de PFsense Étape 5

Une fois la configuration de l'interface WAN est terminer, nous passons à l'interface LAN :

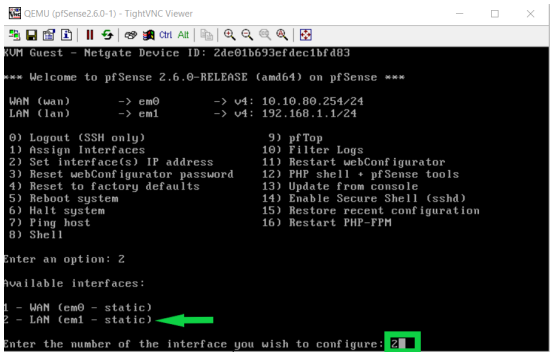

FIG. 5.44: Configuration des interfaces réseaux de PFsense Étape 6

Pour l'interface Lan nous allons lui attribuer ces adresses suivantes :
Adresse IP : 10.10.10 .254/24

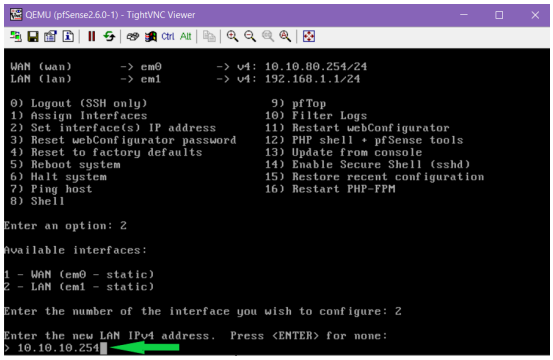

Fig. 5.45: Configuration des interfaces réseaux de PFsense Étape 7

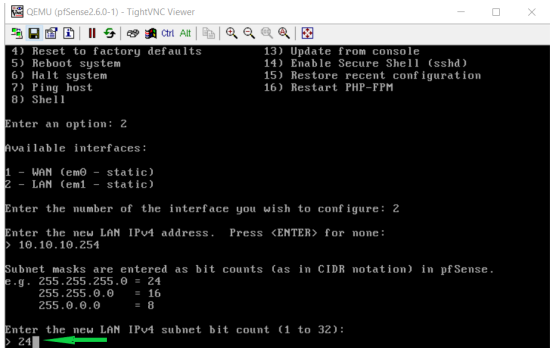

Fig. 5.46: Configuration des interfaces réseaux de PFsense Étape 8

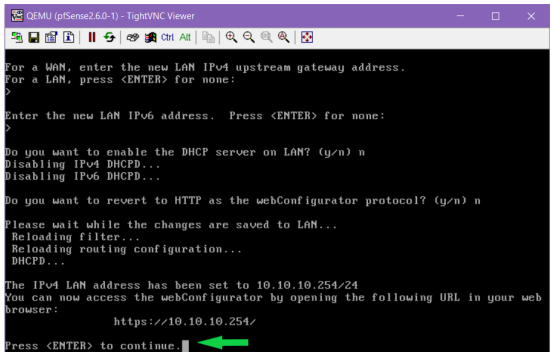

Fig. 5.47: Configuration des interfaces réseaux de PFsense Étape 9

La capture d'image suivante démontre que les interfaces WAN et Lan sont bien configurer

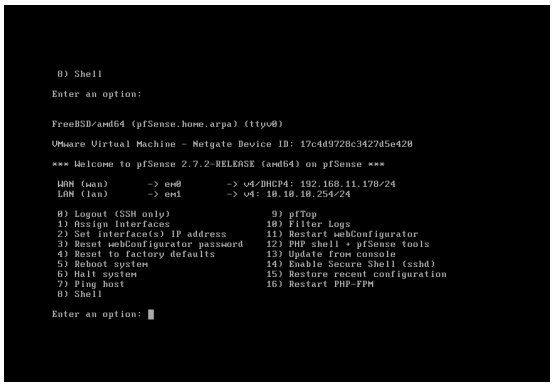

FIG. 5.48: Les interfaces LAN et WAN sont bien configurés

Une fois que PfSense a redémarré, nous pouvons accéder à son interface Web en ouvrant un navigateur et en saisissant l'adresse IP attribuée à l'interface LAN qui est 10.10.10.254. À partir de là, nous pouvons continuer la configuration de pfSense via l'interface Web.

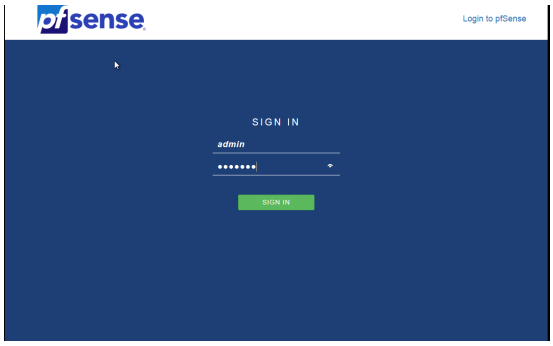

FIG. 5.49: Interface Web de PFsense

Et avec les identifiant par défaut (admin) et mots de passe (pfsense) que nous allons avoir accès à l' Étape suivante qui est la configuration de PFsense

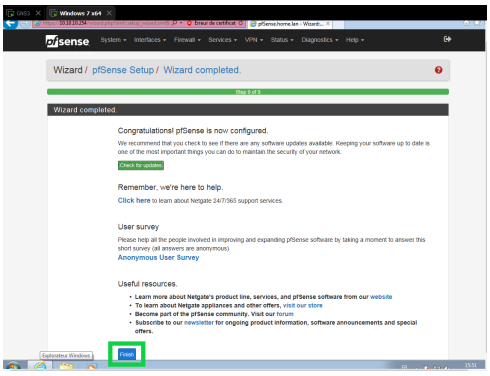

FIG. 5.50: Configuration complétée

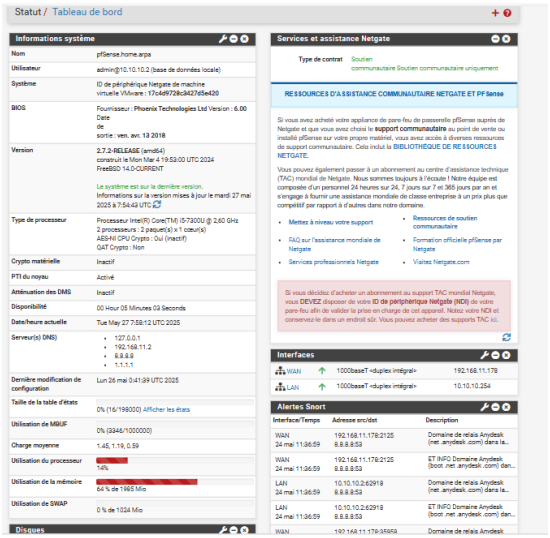

FIG. 5.51: Tableau de bord de PFsense

5.2.4 Configurer la topologie :

Après avoir installé les différents appareils virtuels tels que le parefeu PFsense, Kali-Linux , et la machine Windows dans GNS3, nous pouvons procéder à la mise en place de la topologie réseau :

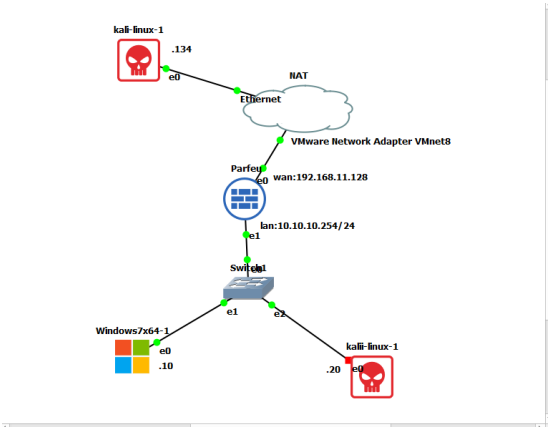

FIG. 5.52: Topologie sur GNS3

Configuration du réseau :

La configuration du réseau a été réalisée en utilisant les commandes appropriées pour chaque composant du réseau. Les adresses IP et les passerelles par défaut ont été attribuées en conséquence pour assurer la connectivité et le routage efficaces entre les sous-réseaux.

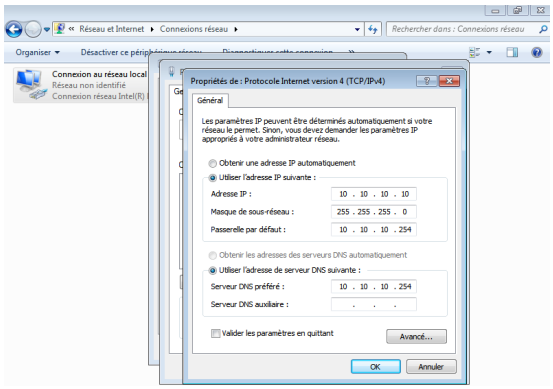

FIG. 5.53: Configuration réseau windows 7

5.2.5 Installation et configuration de SNORT :

Création d'un compte PFsense :

Rendez-vous sur le site snort.org et cliquez sur "Sign up" (S'inscrire) pour créer un nouveau compte. Remplissez les informations requises, acceptez les termes et conditions, puis cliquez sur "Create Account" (Créer un compte).

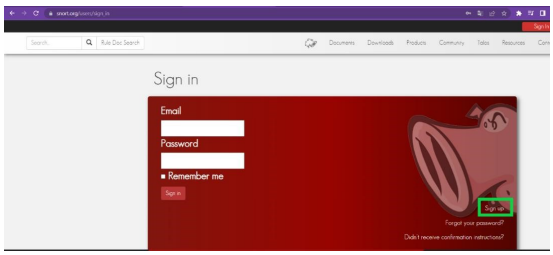

FIG. 5.54: Interface Web SNORT

Dans cette section, vous trouverez généralement un code d'abonnement ou un code de téléchargement. Ce code est unique à votre compte et est nécessaire pour activer les fonctionnalités complètes de Snort sur pfSense.

-Ce code d'abonnement est nécessaire pour les étapes suivantes copier-le en le sélectionnant et en utilisant la fonction de copier-coller ou en notant le code sur un support fiable.

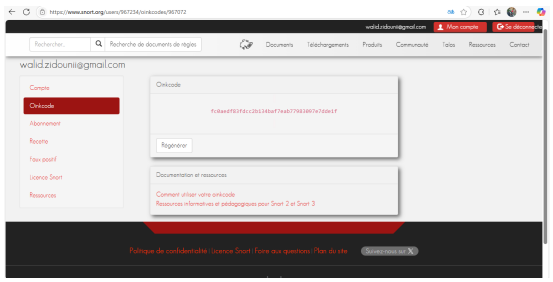

FIG. 5.55: CODE SNORT

Installation du package SNORT :

Pour installer le package Snort faudra se rendre dans « système » et ensuite sur « Package Manager »

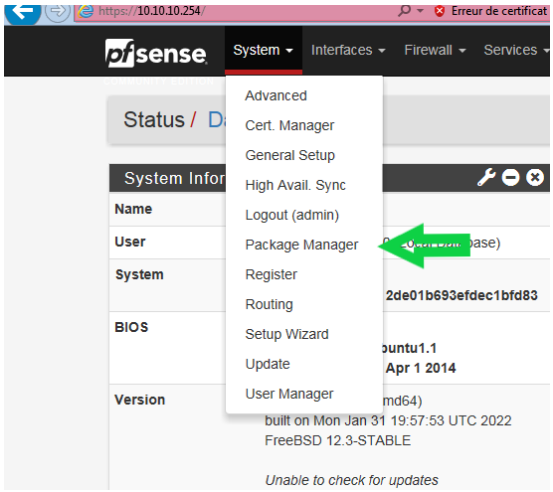

FIG. 5.56: Installation du package SNORT Étape 1

-Tout d'abord faudra se rendre sur « Available Packages » pour importer et installer le package de SNORT et une fois que s'est fait on retrouvera le package de SNORT bien installé sur « Installed packages »

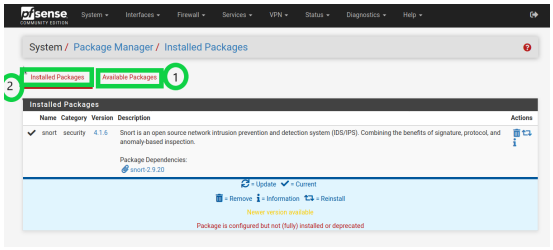

FIG. 5.57: Installation du package SNORT Étape 2

Pour vérifier l'ajout du service SNORT entrez sur le package SNORT

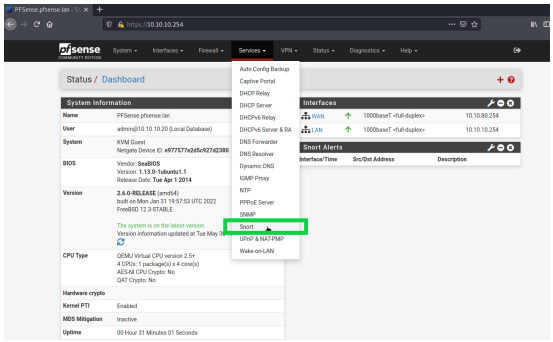

FIG. 5.58: L'ajout du service SNORT

Configuration de SNORT :

Rendez-vous sur "General Settings" : Cette section vous permet de spécifier le comportement global de Snort, comme l'activation/désactivation des règles, l'activation des fonctionnalités d'IPS (Intrusion Prévention System) ou d'IDS (Intrusion Détection System), la spécification des actions en cas de correspondance de règles, etc.

Parcourez les différentes sections et configurez les paramètres selon vos besoins. Vous pouvez activer ou désactiver les options en cochant ou en décochant les cases appropriées, et saisir les valeurs requises dans les champs de texte.

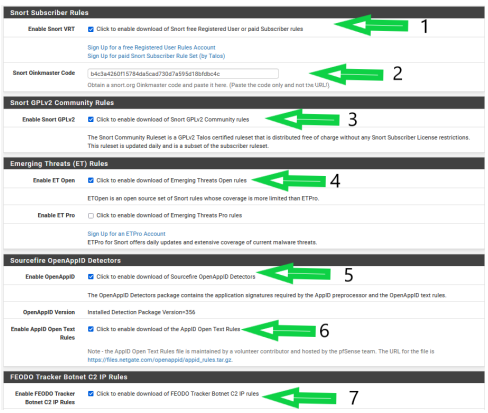

Fig. 5.59: Configuration de SNORT Étape 1

1 : Activé pour l'enregistrement de SNORT en ligne
2 : Clé API « Snort Oinkmaster Code » à récupérer depuis le site de snort.
3 : Activer « Enable snort VRT » (Télécharger les règles gratuites fournies par Snort.
4 : Activer « Enable Snort GPLv2 (Télécharger les règles communautaires).
5 : Activer « Enable OpenAppID » (OpenAppID est une technologie qui permet d'identifier et de contrôler les applications utilisées sur le réseau en analysant les flux de trafic).
6 : Activer « Enable AppID Open Text Rules » (permet d'activer les règles textuelles OpenAppID).
7 : Activer « FEODO Tracker Botnet C2 IP Rules » (sont des règles spécifiques dans Snort qui permettent de détecter et bloquer les communications entre des machines infectées par le botnet FEODO et leurs commandes et contrôles (C2).

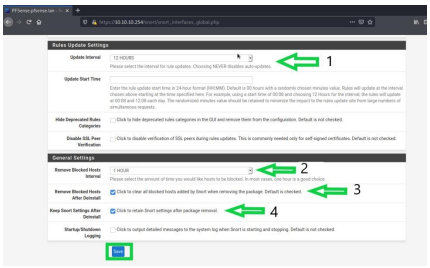

Fig. 5.60: Configuration de SNORT Étape 2

1 : Mettre l'intervalle de mise à jour toutes les 12 Heures.
2 : Mettre les hôtes qui seront bloqués sur 1H.

3 : Supprimer tous les hôtes ajouter par Snort lors de la désinstallation de package.
4 : Garder la configuration de Snort même après la désinstallation.

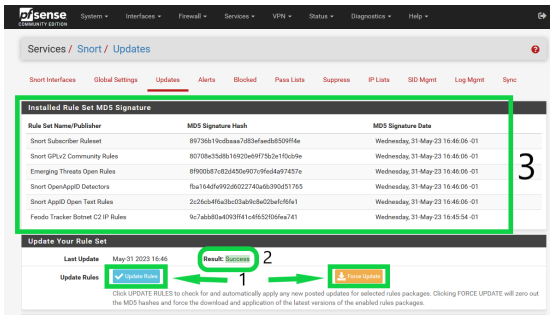

Fig. 5.61: Configuration de SNORT Étape 3

1 : Clickez sur « Uptade rules » pour importer les regles ou bien sur « Force updates » pour forcer l'importation.
2 : « Résultat : Success » donc les règles ont était bien importer
3 : Les règles importer sont afficher

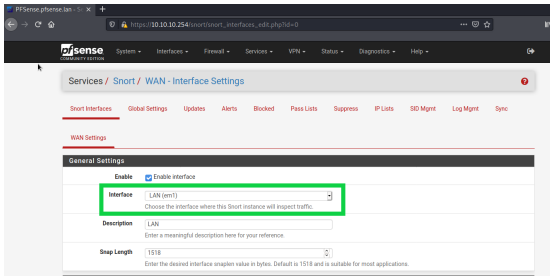

Fig. 5.62: Configuration de SNORT Étape 4

- SNORT / SNORT INTERFACES : Ajouter une interface de surveillance. / LAN /

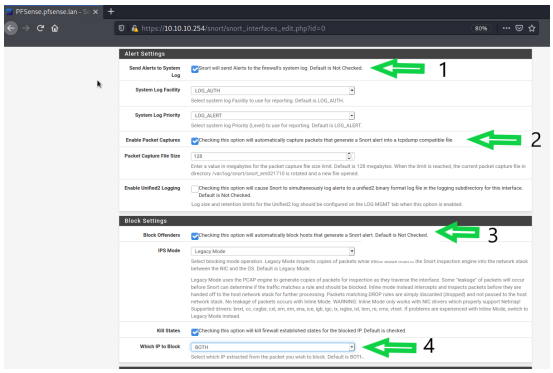

Fig. 5.63: Configuration de SNORT Étape 5

1 : Activer « Send alerts to system log ».
2 : Activer « Enable Packet Captures ».
3 : Activer « Block Offenders ». Bloquer les différentes machines qui peuvent poser problème/ hôtes potentiellement malicieux. Mettre Snort depuis un IDS à un IPS.
4 : Activer « Kill states ».
Save.

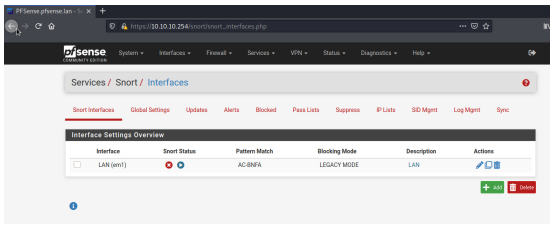

Fig. 5.64: Configuration de SNORT Étape 6

L'interface LAN a était ajouter, l'étape suivante explique comment la configurer

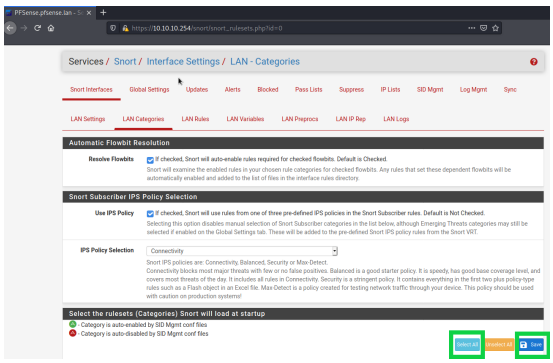

Fig. 5.65: Configuration de SNORT Étape 7

Dans : SNORT / Snort interfaces / LAN catégories : Activer la fonctionnalité « Use IPS Policy ».

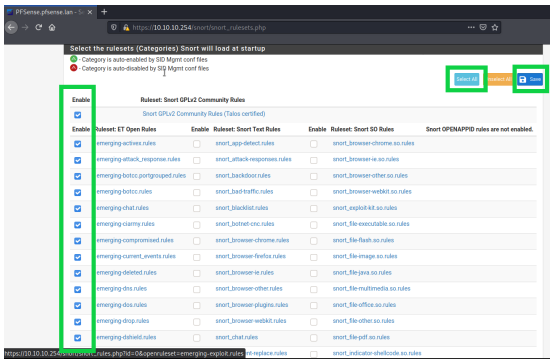

FIG. 5.66: Configuration de SNORT Étape 8

- SNORT / Snort interfaces / LAN catégories : Select All.
- SNORT / Snort interfaces / LAN RULES : Enable All.

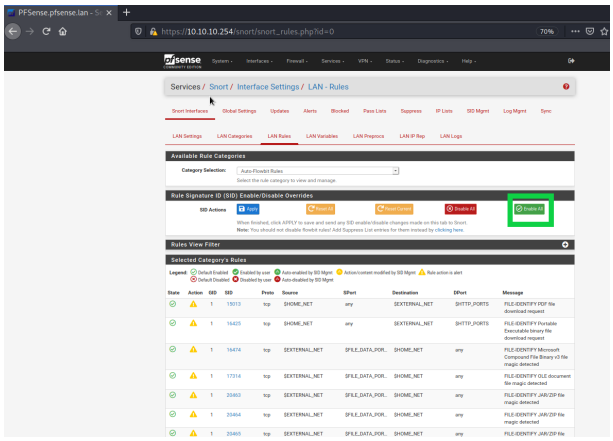

FIG. 5.67: Configuration de SNORT Étape 9

-Clicker sur « Enable all »

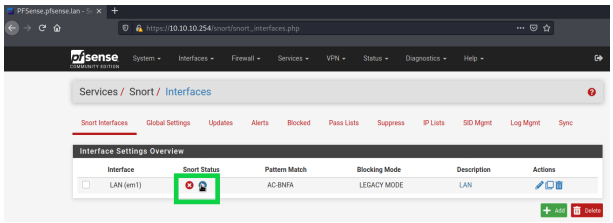

FIG. 5.68: Configuration de SNORT Étape 10

-Lancement de la sonde de surveillance de l'interface LAN

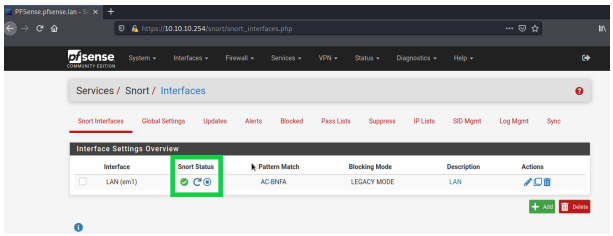

FIG. 5.69: Configuration de SNORT Étape 11

-La sonde de surveillance est activée/ Fonctionnelle.

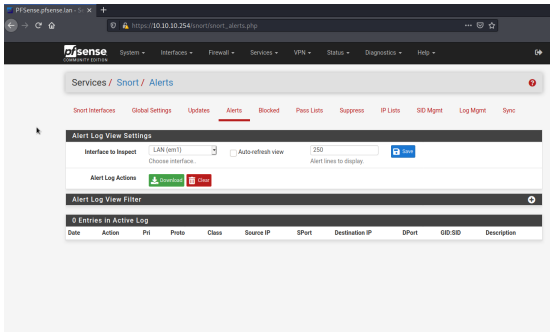

FIG. 5.70: Configuration de SNORT Étape 12

Suivez les mêmes étapes pour le « WAN »

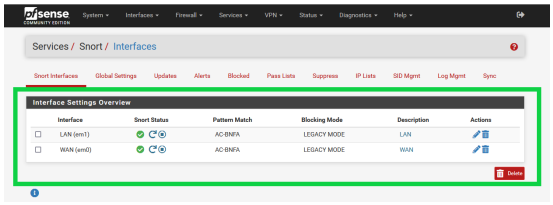

FIG. 5.71: Configuration de SNORT Étape 13

La capture précédente démontre que les deux sondes de surveillance LAN et WAN sont bien configuré.

Remarques :

Les règles à appliquer sur l'interface WAN doivent être plus strictes par rapport à l'interface LAN, en raison du nombre de menaces qui peuvent provenir d'Internet tout en respectant les règles spécifiées approprié à la politique de sécurité de l'entreprise.

5.3 Tests et vérifications :

Dans le cadre de cette étude, on a entamer des tests approfondis afin d'évaluer l'efficacité de Snort lorsqu'il est déployé sur pfSense. Ces tests incluaient des scans de ports, des tentatives d'intrusion, ainsi que des attaques ciblées exécutées à l'aide de la distribution Kali Linux de cote WAN,et une machine windows en réseau LAN. Les résultats ont démontré que Snort, une fois correctement configuré sur pfSense, était capable de détecter, alerter, et bloquer ces attaques, renforçant ainsi sa crédibilité comme solution de sécurité réseau robuste.

5.3.1 Réception des alertes sur la sonde WAN :

Lors de la phase de test, des alertes ont été générées par Snort sur l'interface LAN suite à deux attaques exécutées depuis la machine Kali Linux,connectée sur le réseau WAN, avec l'adresse IP 192.168.11.134 , La cible était l'interface du pare-feu, identifiée par l'adresse 10.10.10.254

Deux types d'attaques ont été menés :

A-scan SYN ("SYN stealth") :

Le scan SYN est une méthode de scan de ports utilisée pour déterminer quels ports TCP sont ouverts, fermés ou filtrés sur une machine cible.Il est appelé "stealth" (furtif) parce qu'il n'établit jamais de connexion TCP complète, ce qui le rend plus difficile à détecter par certains systèmes.

commande : nmap -sS 10.10.10.254
nmap : outil de scan de ports.
-sS : indique un scan SYN (appelé aussi SYN stealth scan).
10.10.10.254 : l'adresse IP de la cible à scanner.

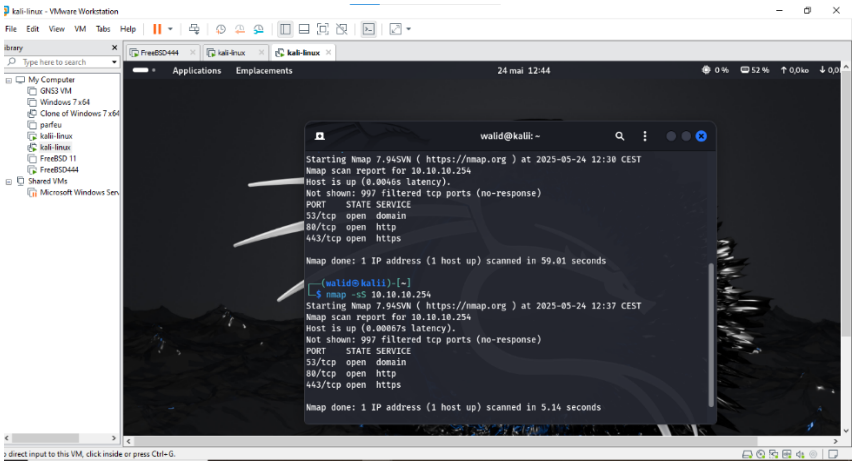

Fig. 5.72: Simulation de l'attaque ("SYN stealth")

Fonctionnement technique du scan SYN :

Nmap envoie un paquet TCP avec le drapeau SYN à un port de la cible (c'est la première étape d'une connexion TCP normale, aussi appelée demande de poignée de main).

-Si le port est ouvert, la cible répond avec un SYN-ACK.

-Au lieu de compléter la connexion (avec un ACK final), Nmap envoie un RST (Reset) pour annuler la connexion immédiatement.

-Si le port est fermé, la cible répond avec un RST.

-Si aucun paquet n'est reçu ou un filtre est en place, le port est considéré comme filtré

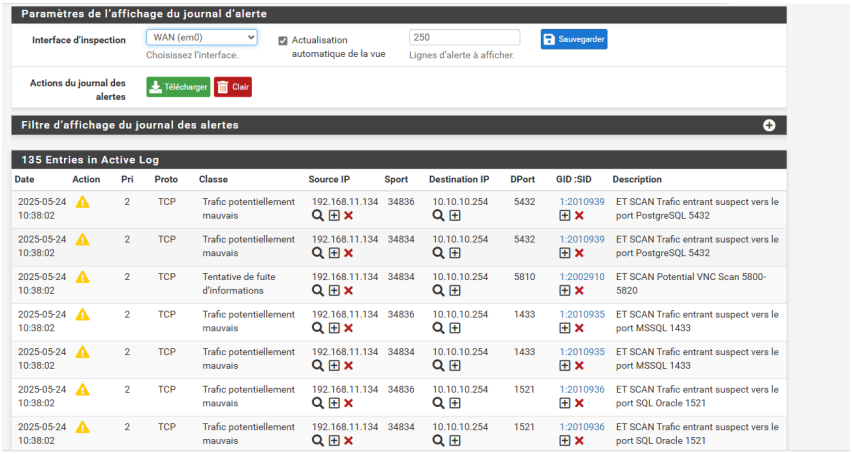

FIG. 5.73: Réception des alertes sur la sonde WAN

on a bien généré une attaque réseau nmap depuis Kali, et Snort a détecté l'activité anormale sur l'interface WAN (em0). Les ports comme 5432, 1433, 1521, etc. sont souvent visés dans les scans car utilisés par des bases de données :

- 5432 = PostgreSQL
- 1433 = Microsoft SQL Server
- 1521 = Oracle
- 5810 = Port VNC (accès bureau à distance)

B-Scan Web

Nikto est un scanner de vulnérabilités pour serveurs web. Il est conçu pour détecter automatiquement :

-Fichiers/dossiers dangereux ou accessibles publiquement.

-Failles connues dans les logiciels web et applications .

-Mauvaises configurations de sécurité et obtention d'informations.

Commande : nikto -h http ://10.10.10.254

nikto : outil open-source de scan de vulnérabilités web.

-h : spécifie la cible (dans ce cas, http ://10.10.10.254).

Cela signifie que tu scannes l'interface Web de pfsense.

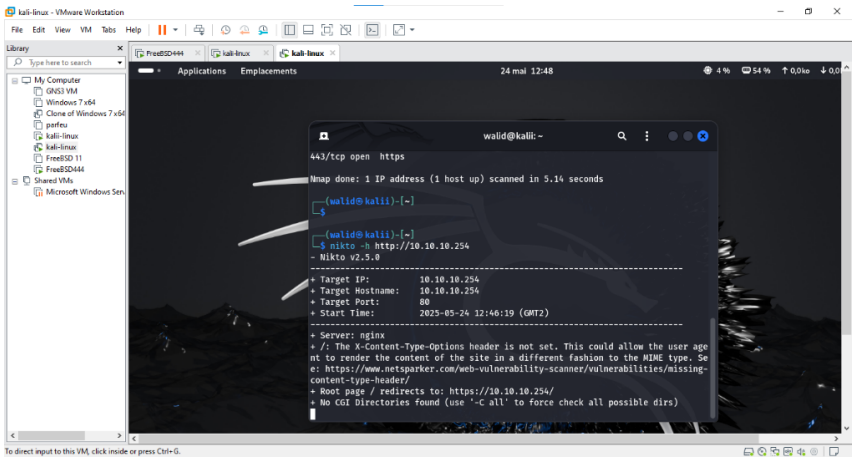

FIG. 5.74: Simulation de l'attaque Nikto

Fonctionnement du scan avec Nikto :

Lorsqu'on lance la commande :

Nikto va : Envoyer des centaines de requêtes HTTP/HTTPS à l'interface web de la cible,et Vérifier la version du serveur Web (Apache, nginx, etc.),puis Rechercher dans sa base de données de signatures les vulnérabilités connues associées à cette version ,pour Tester l'accès à des URL sensibles ou vulnérables comme :/admin/, /phpmyadmin/, /cgi-bin/. /test.php, /robots.txt, /server-statusFailles connues : injection de code, XSS, path traversal, enfin Rapporter tous les comportements suspects, fichiers accessibles, ou signatures de failles connues.

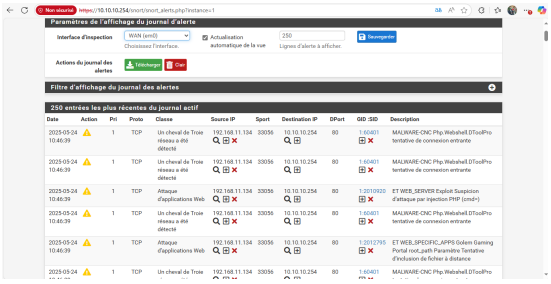

FIG. 5.75: Réception des alertes sur la sonde WAN

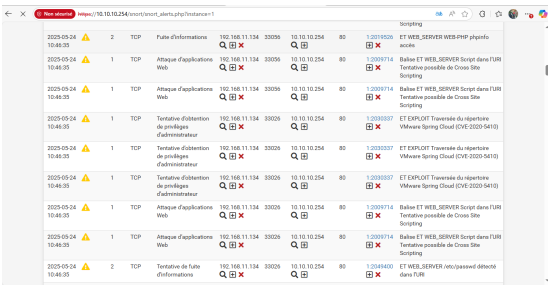

FIG. 5.76: Réception des alertes sur la sonde WAN

On voit bien qu'on est en train de simuler des attaques réalistes, et le pare-feu les intercepte : il a détecté des menaces de haut niveau (priorité 1) comme des tentatives d'injection web, chevaux de Troie etc

5.3.2 Réception des alertes sur la sonde LAN :

Lors de la phase de test, des alertes ont été générées par Snort sur l'interface LAN, à la suite d'activités considérées comme suspectes. Ces alertes ont permis d'identifier une tentative de connexion distante provenant d'une machine Windows sur le réseau interne, équipée du logiciel AnyDesk, utilisé pour l'accès à distance.

L'adresse IP source de la machine initiant la connexion était 10.10.10.2 (poste Windows).

Cest quoi ANYDESK ?

AnyDesk est un logiciel de bureau à distance qui permet de voir l'écran d'un autre ordinateur et de le contrôler comme si on était devant, en toute sécurité et en temps réel.

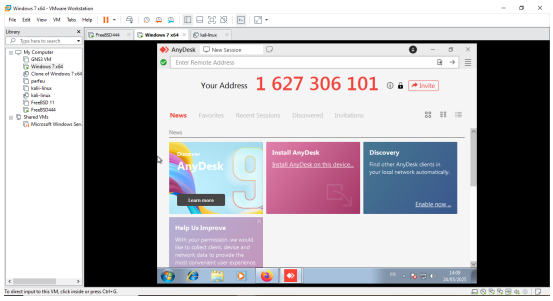

FIG. 5.77: Interface du logiciel AnyDesk sur une machine Windows

Snort a notamment détecté :

- Des connexions réseau inhabituelles sur des ports dynamiques utilisés par AnyDesk.

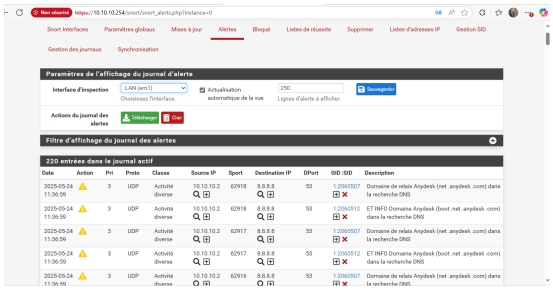

FIG. 5.78: Réception des alertes sur la sonde LAN

5.3.3 Blocage d'une attaque sur le par-feu du coté WAN :

Grâce à la configuration en mode de blocage hérité de Snort sur pfSense, les hôtes à l'origine d'activités suspectes sont immédiatement bloqués dès la détection d'un comportement malveillant. Comme illustré dans la capture, l'adresse IP 192.168.11.134 a été automatiquement inscrite sur la liste noire de Snort suite à une série d'alertes critiques.

Parmi ces alertes figuraient des scans de ports vers des services sensibles (MySQL, Oracle, MSSQL, PostgreSQL), des tentatives d'exploitation Web, ainsi que des attaques potentielles liées à des vulnérabilités connues (ex. : QNAP Shellshock, Bash CGI injection, TRACE HTTP).

Chaque alerte a été enregistrée avec une horodatation précise, démontrant l'efficacité en temps réel du mécanisme de détection et de réponse de Snort. Ce blocage automatique permet de protéger activement le réseau contre les tentatives d'intrusion, sans nécessiter d'intervention manuelle immédiate de l'administrateur. Ainsi, tout comportement suspect provenant d'une machine du réseau interne est non seulement signalé, mais aussi neutralisé instantanément, garantissant une réactivité optimale en matière de sécurité réseau.

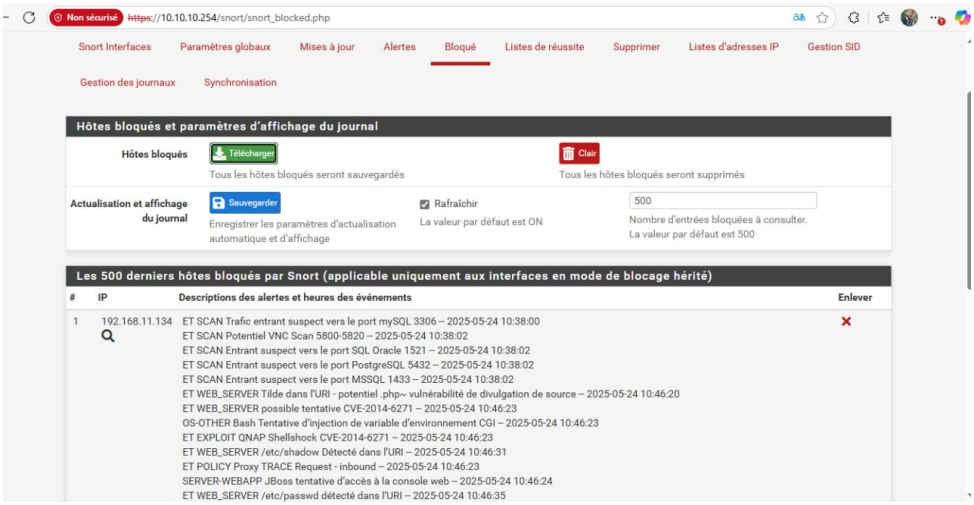

FIG. 5.79: Blocage d'une attaque sur le par-feu du coté WAN

5.4 Conclusion

Finalement, ce chapitre décrit la mise en place et la configuration de l'outil Snort sur notre pare-feu pfSense, dans le cadre du renforcement de la sécurité de notre infrastructure réseau. Nous avons présenté les étapes d'installation et de paramétrage de Snort afin de permettre la surveillance en temps réel du trafic réseau. Grâce à cette solution, nous pouvons désormais détecter les activités suspectes, analyser les journaux d'alerte, et réagir rapidement en cas d'incident. L'intégration de Snort nous offre ainsi une visibilité accrue sur les menaces potentielles et constitue une base solide pour la détection d'intrusions réseau.

Conclusion générale

Dans un environnement numérique où les cybermenaces ne cessent d'évoluer, garantir la sécurité des infrastructures réseau est devenu un enjeu majeur pour toute entreprise. Ce mémoire s'est inscrit dans cette problématique en portant sur la mise en place d'un système de détection et de prévention d'intrusion (IDS/IPS), au sein de l'infrastructure de groupe cevital. Au cours de ce travail, nous avons consolidé nos connaissances dans les domaines des réseaux informatiques et de leur sécurisation, en mettant en évidence le rôle crucial de l'administrateur réseau dans la prévention et la gestion des menaces. La maîtrise des bases du fonctionnement réseau est indispensable pour anticiper et contrer les multiples formes d'attaques auxquelles une infrastructure peut être exposée. L'analyse approfondie de l'architecture réseau de lentreprise Cevital nous a permis d'identifier la problematque, puis de proposer une solution adaptée et concrète. Pour ce faire, nous avons déployé Snort sur une plateforme pfSense, configurée pour inspecter le trafic entrant et sortant sur notre reseau. Plusieurs scénarios d'attaques simulées ont été réalisés, émanant de machines internes et externes, afin de valider l'efficacité de la solution. Les résultats obtenus à l'issue de notre projet ont été satisfaisants et conformes aux objectifs fixés. Cette réalisation a permis d'apporter une réponse concrète et efficace aux besoins de l'entreprise Cevital en matière de sécurité réseau. Elle a démontré la pertinence de notre approche et la capacité des solutions mises en place à renforcer la surveillance et la protection de l'infrastructure informatique dans un environnement réel. Notre stage au sien de Cevital nous a offert une opportunité précieuse de mettre en pratique nos connaissances théoriques en sécurité informatique dans un contexte professionnel. Il nous a également permis de maîtriser des outils clés du domaine, tout en développant une approche méthodique face aux problématiques de cybersécurité rencontrées sur le terrain. À l'avenir, nous envisageons d'enrichir notre solution Snort par l'intégration d'un système de corrélation de logs (SIEM) tel que Splunk ou ELK, afin d'améliorer l'analyse et la réponse aux incidents. L'utilisation de l'intelligence artificielle et de l'apprentissage automatique est également envisagée pour renforcer la détection des menaces émergentes. Ainsi, nous élargirons surveillance à d'autres équipements critiques et la formation continue du personnel resteront des priorités pour consolider la posture globale de sécurité et faire face efficacement aux cybermenaces futures

Bibliographie

Sources principales (ouvrages et documents)

1. **Goshentech**. « Comprendre les réseaux informatiques : concepts de base et terminologie ». https ://goshentech.fr/comprendre-les-reseaux-informatiques-concepts-de-base-et-terminologie/ [Consulté le 9 mars 2025].

2. Andrew S. Tanenbaum, David J. Wetherall, *Computer Networks*, 5e édition, Pearson, 2010.

3. Kurose, J. F., Ross, K. W., *Computer Networking : A Top-Down Approach*, Pearson, 2016.

4. Peterson, L. L., Davie, B. S., *Computer Networks : A Systems Approach*, Morgan Kaufmann, 2011.

5. Zimmermann, H., « OSI Reference Model », *IEEE Transactions on Communications*, vol. 28, n°4, 1980, pp. 425–432.

6. Stallings, W., *Network Security Essentials : Applications and Standards*, 6e édition, Pearson, 2017.

7. Droms, R., Lemon, T., *The DHCP Handbook*, Sams Publishing, 1999.

8. Solange Ghernaouti, *Cybersécurité : sécurité informatique et réseaux*, 5e édition, Dunod, 2016.

9. Lazarevic, A., Kumar, V., Srivastava, J., « Intrusion Detection : A Survey », *Managing Cyber Threats*, Springer, 2005.

10. Bejtlich, R., *The Tao of Network Security Monitoring*, Addison-Wesley, 2004.

11. Sandhu, R. et al., « Role-Based Access Control Models », *IEEE Computer*, vol. 29(2), 1996.

12. Bace, R. G., Mell, P., *Intrusion Detection Systems*, NIST SP 800-31, 2001.

13. Scarfone, K., Mell, P., *Guide to Intrusion Detection and Prevention Systems (IDPS)*, NIST SP 800-94, 2007.

Sources web

14. Wikipedia. Articles divers (Hôte, réseaux, sécurité, pfSense). https ://fr.wikipedia.org/ [Consulté fév.-mars 2025].

15. IBM. « Network Topology », « Cybersecurity Risk Assessment », « What is SIEM ? ». https ://www.ibm.com/ [Consulté en mars 2025].

16. TechSyncer. *Types of Network Topology Explained*. https ://www.techsyncer.com/fr/types-of-network-topology-explained.html [13 fév. 2025].

17. Atera. *Topologie réseau*. https ://www.atera.com/fr/glossary/topologie-reseau/ [7 fév. 2025].

18. OpenClassrooms. *Chiffrez vos connexions réseau*. https ://openclassrooms.com/fr/courses/176187
securisez-vos infrastructures/5515516-chiffrez-vos-connexions-reseau [14 mars 2025].

19. Coursera. *Authentication*. https ://www.coursera.org/fr-FR/articles/authentication
[9 mars 2025].

20. C-Risk. *Fondamentaux de la sécurité de l'information*. https ://www.c-risk.com/fr/blog/fondamen
securite-information [9 mars 2025].

21. RiskInsight-Wavestone. https ://www.riskinsight-wavestone.com/gestion-des-acces
[14 mars 2025].

22. OVHCloud. https ://www.ovhcloud.com/fr/learn/what-is-dns-attack/ [14 mars 2025].

23. Fortinet. *IDS/IPS : Qu'est-ce que c'est ?*. https ://www.fortinet.com/fr/resources/cyberglossary/i
detection-system [10 mars 2025].

24. Juniper Networks. https ://www.juniper.net/fr/fr/research-topics/what-is-ids-ips.html
[10 mars 2025].

25. WPG Consulting. https ://wpgc.io/blog/intrusion-detection-systems-the-complete-
guide/ [10 mars 2025].

26. Hostomize. https ://hostomize.com/blog/implementing-ids-ips-systems/ [10 mars
2025].

27. Blossom2Be. https ://www.blossom2be.com/optimisez-la-surveillance-reseau-avec-
idsips/ [17 mars 2025].

28. Tech Pratique. https ://tech-pratique.fr/guide-ultime-pour-mettre-en-place-un-systeme-
ids-ips-efficace-dans-votre-reseau-dentreprise-securisez-vos-donnees.php [17 mars 2025].

29. Neox Networks. https ://www.neox-networks.com/en/solutions/suricata-performance-
increase/ [15 mars 2025].

30. Microsoft. https ://www.microsoft.com/en-us/security/business/security-101/what-
is-siem [15 mars 2025].

31. Suricata. https ://docs.suricata.io/en/latest/performance/high-performance-config.html
[11 mars 2025].

32. Snort. https ://www.snort.org [ENTRE LE 10 ET 19 mars 2025].

33. Netgate. https ://www.netgate.com/pfsense-features [20 mars 2025].

34. Cybergeneration. https ://cybergeneration.tech/network-monitoring-and-logging-with-
pfsense-snort-and-splunk [20 mars 2025].

35. Jain Tech. https ://jaintech.co.in/best-practices-for-implementing-network-intrusion-
detection-systems-ids [10 mars 2025].

36. YouTube. *Introduction au modèle TCP/IP*. https ://www.youtube.com/watch ?v=kAbWOiyfg44
[Consulté le 20 février 2025].

37. N,BATTAT, "Cours sécurité " 2024/2025. [En ligne].

Résumé

Ce mémoire a été réalisé dans le cadre du projet de fin d'études à l'Université Abderrahmane Mira de Bejaïa, en vue de l'obtention du diplôme de Master en Administration et Sécurité des Réseaux Informatiques.

Dans un contexte où les cybermenaces deviennent de plus en plus sophistiquées, l'intégration d'IDS/IPS avec un focus particulier sur Snort permet de détecter, alerter, voire bloquer les activités malveillantes en temps réel. Dans le cadre de notre projet, nous avons installé et configuré pfSense, renforcé par l'outil Snort, qui permet de détecter en temps réel les tentatives d'intrusion . Cette architecture assure une protection proactive du réseau contre les attaques potentielles.

Ce stage nous a permis de renforcer nos connaissances en sécurité informatique, tout particulièrement dans la mise en place et la gestion de solutions comme pfSense et Snort. Grâce à ce travail, nous avons atteint l'objectif fixé dès le début de notre mémoire : contribuer à la sécurisation du réseau de CEVITAL.

Mots clés : IDS/IPS, Snort, pfSense, Sécurité informatique, Réseauinformatique,Intrusion,Cybermenaces, CEVITAL

Abstract

This work is part of the final project at Abderrahmane Mira University - Bejaia, aimed at obtaining a Master's degree in Administration and Network Security

In a context where cyber threats are becoming increasingly sophisticated, the integration of IDS/IPS systems, particularly with a focus on Snort ; enables the detection, alerting, and even blocking of malicious activities in real time.. With cyber threats becoming more advanced every day, using IDS/IPS solutions—especially Snort—makes it possible to detect, alert, and sometimes even block malicious activity in real time. For our project, we installed and configured pfSense, enhanced with Snort, to help detect intrusion attempts and secure the network. This setup offers strong, proactive protection against possible attacks.

This internship allowed us to strengthen our knowledge of computer security, particularly in the implementation and management of solutions such as pfSense and Snort. Thanks to this work, we have achieved the objective set from the beginning of our thesis : to contribute to securing the CEVITAL network..

keywords : IDS/IPS, Snort, pfSense, Sécurité informatique, Réseauinformatique,Intrusion,Cybermenaces, CEVITAL