REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'enseignement supérieur et de la recherche scientifique
UNIVERSITE LARBI TEBESSI – TEBESSA
Faculté des Sciences Exactes et des Sciences
de la Nature et de la Vie
Département Mathématique et Informatique

MÉMOIRE DE FIN D'ÉTUDE

POUR L'OBTENTION DU DIPLÔME DE MASTER

DOMAINE : MATHÉMATIQUES ET INFORMATIQUE

FILIÈRE : INFORMATIQUE

OPTION : RÉSEAUX ET SÉCURITÉ INFORMATIQUE

- Réalisée Par : **- GASMI Aimen**

Thème

PROPOSITION D'UNE ARCHITECTURE RESEAUX COMPUS SECURISE PAR UN FIREWALL OPENSOURCE PFSENSE

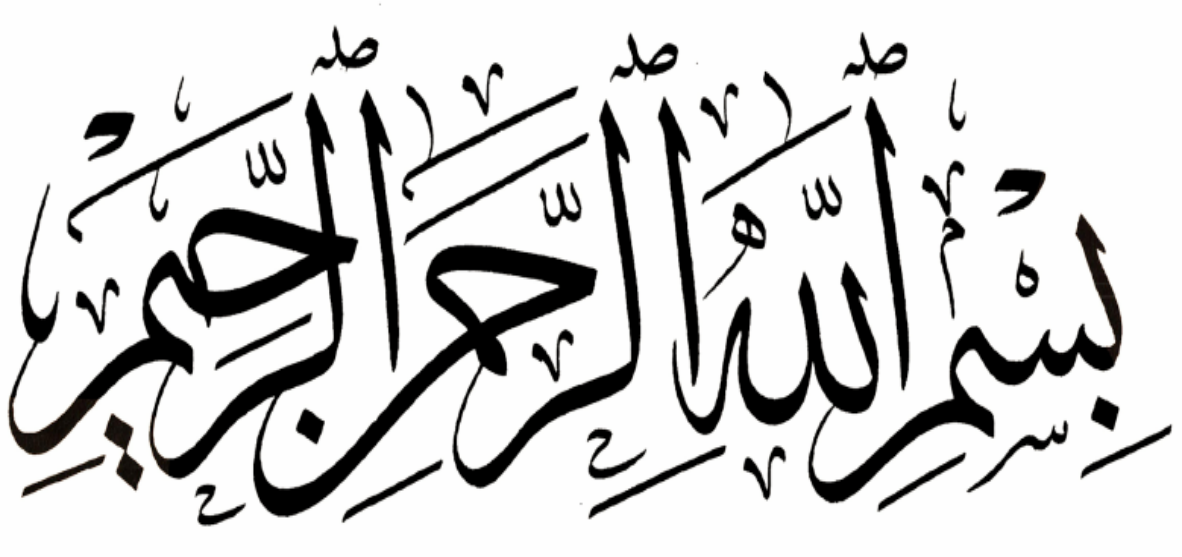
- Devant le jury :

Dr. **MEKHAZNIA Tahar**	MCA	Université de Tébessa	Président
Dr. **SAHRAOUI Abdellatif**	MCA	Université de Tébessa	Examinateur
Dr. **MERZOUG Soltane**	MCA	Université de Tébessa	Encadreur

- Date de soutenance :

06/06/2023

Année Universitaire : 2022/2023


بسم الله الرحمن الرحيم

Dédicaces

Je dédie ce travail à ma chère mère et mon père pour leurs encouragements permanents, et leurs soutien moral, ainsi qu'à mes sœurs en particulier, et toute ma famille pour leur soutien tout au long de mon parcours universitaire.

Merci d'être toujours là pour moi. ...

.....

GASMI Aimen

Remerciement

NOUS tenons dans un premier temps à remercier le bon dieu le tout-puissant qui nous a donné le courage et la volonté pour mener à bien ce modeste travail.

Nous tenons à exprimer notre sincère reconnaissance et nos vifs remerciements à tous ceux qui ont contribué de près ou de loin à l'élaboration de ce travail.

Tout d'abord à Docteur " Merzoug Soltane " l'encadreur de mémoire de master pour son encadrement. Son expérience et ses qualités scientifiques ont toujours été sources d'enrichissement me permettant de mener à bien ce travail.

Docteur " Mekhaznia Tahar " d'avoir accepté de présider le jury de notre soutenance.

Docteur " Sahraoui Abdellatif " d'avoir accepté de juger ce modeste travail.

Madame " CHATOUH Fayrouz " Administrateur du Centre de Calcul (CSRTED), pour son acceptation de faire le stage au niveau du centre et pour son aide et ses remarques pertinentes qui ont apporté une amélioration certaine à notre travail.

Monsieur " Boudraa Walid " l'encadreur de stage pour son aide et sa patience, qu'il trouve en ces lignes l'expression de notre gratitude.

Monsieur " Hamouda Djallel " pour son aide et ses remarques pertinentes qui ont apporté quelques améliorations à notre travail.

Sans oublier les amis « Abdellmalek Fathi , Hafdallah Iheb , Chergui Abdelmoumene Zakaria et Tout les autres amis » et les enseignants de département d'informatique de l'université de Tébessa "LARBI TEBESSI", qui se sont succédé durant notre cursus, sans eux nous n'aurions pas pu atteindre nos objectifs.

A vous tous on dit <Merci>

Résumé

L'Université Larbi Tébessi accueille chaque année des milliers de nouveaux bacheliers (d'Algérie et du monde entier). Elle met à leur disposition son réseau, qui est alors à la merci de toutes sortes d'utilisateurs ! Pour protéger ce réseau, nous avons proposé une architecture réseau sécurisée par le pare-feu open source PfSense, et pour cela nous avons mené une étude de l'architecture existante. Cela nous a permis de le critiquer et de proposer des solutions afin de proposer une nouvelle architecture réseau. Nous avons également proposé un système de détection d'attaque entraîné sur data-set CICDDOS2019, basé sur le modèle de réseau neuronal profond (DNN) et intégré dans PfSense pour détecter et bloquer automatiquement les attaques.

Mots clés : PfSense , GNS3 , Pare-Feu , Intelligence Artificial , Apprentissage profondeur , DNN , CICDDOS2019 .

Abstract

Larbi Tebessi University welcomes thousands of new graduates every year (from Algeria and around the world). It makes its network available to them, which is then at the mercy of all kinds of users! To protect this network, we proposed a network architecture secured by the PfSense open source firewall, and for this we conducted a study of the existing architecture. This allowed us to criticize it and propose solutions in order to propose a new network architecture. We also proposed an attack detection system trained on CICDDOS2019 data-set, based on the deep neural network (DNN) model and integrated in PfSense to automatically detect and block attacks.

Key words : PfSense , GNS3 , Firewall , Intelligence Artificial, Deep Learning , DNN , CICDDOS2019 .

الملخص

ترحب جامعة العربي التبسي بالآلاف من الطلبة الجدد كل عام (من الجزائر ومن جميع أنحاء العالم) .إنها تجعل شبكتها متاحة لهم، والتي تكون بعد ذلك تحت رحمة جميع أنواع المستخدمين !لحماية هذه الشبكة، اقترحنا بنية شبكة مؤمنة بجدار حماية PfSense مفتوح المصدر، ولهذا أجرينا دراسة للبنية الحالية .سمح لنا هذا بانتقادها واقتراح حلول من أجل اقتراح بنية شبكة جديدة .لقد اقترحنا أيضًا نظام لاكتشاف الهجمات تم تدريبه على مجموعة البيانات CICDDOS2019 ، استنادًا إلى نموذج الشبكة العصبية العميقة (DNN) ومتكامل في PfSense لاكتشاف الهجمات ومنعها تلقائيًا.

الكلمات المفتاحية : PfSense ، GNS3 ، جدار الحماية ، الذكاء الاصطناعي ، التعلم العميق ، DNN ، CICDDOS2019 .

Table des Matières

Liste des Figures

Liste des Tableaux

Liste des Acronymes

API Application Programming Interface

CNN Convolutional Neural Networks

DDoS Distributed Denial of Service attack

DL Deep Learning

DNN Deep Neural Networks

DoS Denial of Service

GNS3 Graphical Network Simulator

IA Intelligence Artificial

IDS Instruction Detection System

IP Internet Protocol

IPS Intrusion Prevention System

LAN Local Area Network

ML Machine Learning

NSL-KDD Network Security Laboratory - Knowledge - Discovery and Data Mining

OSI Open System Interconnect

RNN Recurrent Neural Networks

SDN Software Defined Networking

SVM Support Vector Machine

TCP Transmission Control Protocol

UDP User Datagram Protocol

VLAN Virtual Local Area Network

VPN Virtual Private Network

Introduction Générale

Introduction Générale

Dans la plupart des organisations informatisées, la sécurité des réseaux informatiques est un sujet essentiel qui favorise le développement des échanges d'informations dans tous les domaines. Cette évolution correspond à l'augmentation du nombre d'utilisateurs du réseau, qu'ils soient connus ou inconnus, ces utilisateurs ne sont pas forcément pleins de bonne volonté envers ces réseaux. Ils peuvent exploiter les vulnérabilités des réseaux et des systèmes pour tenter d'accéder à des informations sensibles afin de les lire, les modifier ou les détruire, pour affecter le bon fonctionnement du système ou même par curiosité.

Ainsi l'université ne déroge pas à cette règle, notamment auprès de la communauté universitaire (enseignants, responsables, fonctionnaires, étudiants, etc.) qui ne cesse d'augmenter. Cette sécurité assurera la confidentialité, l'intégrité, la disponibilité et la non-répudiation. De nombreux outils et moyens sont disponibles pour cela, tel que des solutions matérielles, des logiciels d'audit, des systèmes de détection d'intrusion (IDS), des pares-feux, des réseaux locaux virtuels (VLAN), des antivirus et des réseaux privés virtuels (VPN).

Une fois ces réseaux apparus, il est devenu nécessaire de renforcer les mesures de sécurité afin de maintenir la confidentialité, l'intégrité et le contrôle des accès au réseau pour réduire les risques d'attaques.

Le stage que nous avons effectué au centre de calcul de l'université Larbi Tebessi - Tebessa, nous a permis de découvrir son réseau et de comprendre son fonctionnement.

Le but de notre travail est de proposer d'une architecture réseau base sur le firewall pfsense avec une nouvelle stratégie basée sur intelligente de Deep Learning pour identifier les attaques et le contrôle d'accès au réseau pour réduire les risques d'attaques.

Afin de réaliser les objectifs visés, nous avons organisé ce travail en quatre chapitres:

- Le premier chapitre est consacré aux généralités sur les Réseaux, la Sécurité Informatique et Deep Learning.

- Le deuxième chapitre est focalisé sur les techniques de l'intelligence artificiel pour détecter les attaques.

- Le troisième chapitre concerne la proposition d'architecture Réseau et Système détection des attaques

- Le quatrième chapitre est consacré pour la présentation de l'environnement de développement, et simulation avec une discussion sur les résultats obtenus.

Chapitre 1

Généralités sur les Réseaux, la Sécurité Informatique et Deep Learning

Chapitre 1 : Généralités sur les Réseaux, la Sécurité Informatique et Deep Learning

Introduction

La sécurité des réseaux informatiques est un sujet fondamental pour améliorer l'échange d'informations dans tous les domaines, et l'expansion des réseaux informatiques et leur importance croissante ont créé le problème de la sécurité des systèmes de communication. Dans la plupart des organisations informatiques, le partage des données entre les appareils est une préoccupation majeure. Il est nécessaire de renforcer les mesures de sécurité afin de maintenir la confidentialité, l'intégrité et le contrôle des accès au réseau pour réduire les risques d'attaques.

Nous avons divisé ce premier chapitre en trois parties. Dans la première partie, nous aborderons les concepts de réseaux informatiques et leurs classifications, tandis que dans la deuxième partie, nous passerons à la sécurité informatique, ses objectifs, et son utilisation dans les réseaux informatiques, avec la connaissance des différentes attaques. Puis, dans la troisième partie, nous parlerons de Deep Learning et de ses divisions, et terminerons ce chapitre par une conclusion.

1. Généralités sur les réseaux

1.1. Définition d'un réseau

Un réseau informatique est un ensemble d'équipements interconnectés pour échanger des données et des ressources. Le but principal d'un réseau informatique est de permettre aux utilisateurs de partager des informations, des logiciels, des périphériques et des ressources de stockage. Les périphériques réseau (tels que les ordinateurs, les routeurs, les commutateurs, etc.) sont connectés à différentes topologies de réseau via des supports de transmission (tels que paire torsadée et fibre optique) [1].

1.2. Classification des réseaux

Les réseaux informatiques peuvent être classés selon différents critères, tels que leur étendue, leur topologie, leur mode de fonctionnement, etc. Voici quelques-unes des classifications les plus courantes :

- **Réseau personnel (PAN - Personnel Area Network) :** est un type de réseau informatique utilisé pour connecter des périphériques dans un environnement personnel, tel qu'un bureau ou une maison. Un PAN peut être utilisé pour connecter des ordinateurs, des tablettes, des smartphones, des imprimantes et d'autres périphériques ensemble.
- **Réseau local (LAN - Local Area Network) :** est un type de réseau informatique qui relie des périphériques dans un environnement géographique limité, comme un bâtiment, un campus universitaire ou un bureau. Les réseaux locaux peuvent être câblés ou sans fil, et ils sont souvent utilisés pour permettre la communication entre des ordinateurs, des imprimantes et d'autres périphériques.
- **Réseau métropolitain (MAN - Métropolitain Area Network) :** est un type de réseau informatique qui couvre une zone géographique étendue, comme une ville ou une région métropolitaine. Les réseaux métropolitains sont souvent utilisés pour connecter plusieurs réseaux locaux (LAN) ensemble, en fournissant une connectivité à haute vitesse pour les utilisateurs sur une zone géographique plus large.
- **Réseau étendu (WAN - Wide Area Network) :** est un type de réseau informatique qui couvre une grande zone géographique, telle qu'un pays, une région ou même le monde entier. Les réseaux étendus sont utilisés pour connecter des réseaux locaux (LAN) distants, des succursales d'entreprises et des centres de données ensemble.

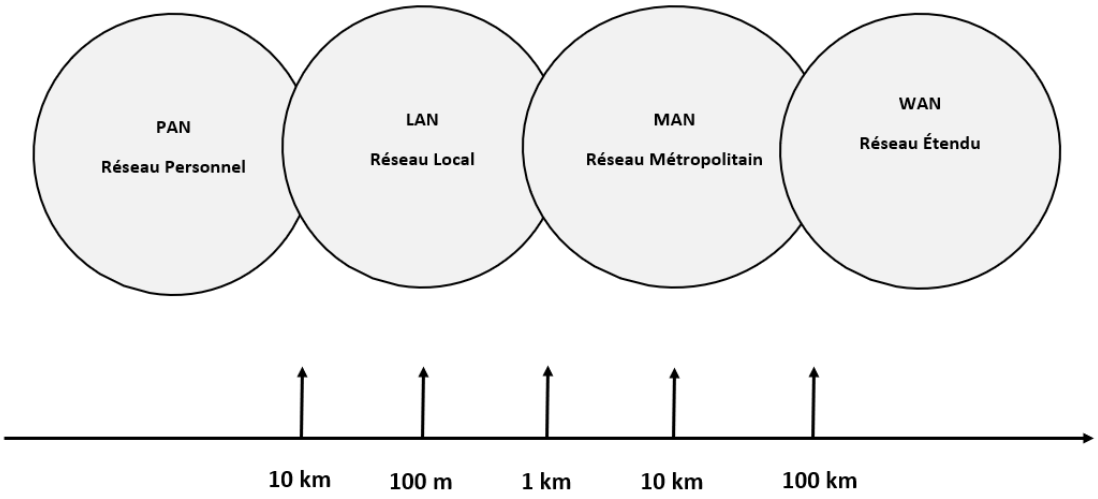


Figure 1 – Catégories des réseaux informatiques *[2]*

1.3. Les types des réseaux

Il existe plusieurs types de réseaux informatiques qui présentent des caractéristiques différentes :

- **Internet :** est un ensemble de réseaux d'ordinateurs interconnectés, utilisant un ensemble de protocoles de communication standard, tels que le protocole TCP/IP, qui permettent à des ordinateurs et des périphériques de communiquer entre eux en utilisant des adresses IP uniques. Les données sont acheminées à travers un réseau de routeurs et de serveurs à travers le monde, ce qui permet de relier les utilisateurs à des sites Web et à d'autres services en ligne à partir de n'importe où dans le monde.
- **Intranet :** est un réseau informatique privé utilisé à l'intérieur d'une organisation pour permettre à ses employés de partager des informations et de travailler ensemble de manière plus efficace. Contrairement à Internet, qui est un réseau public, un intranet est un réseau privé accessible uniquement aux membres de l'organisation. Les informations contenues dans l'intranet sont généralement protégées par un pare-feu et sont accessibles uniquement aux employés de l'organisation. L'intranet peut inclure un certain nombre de services et d'applications, tels que des bases de données d'entreprise, des outils de collaboration, des systèmes de gestion de contenu, des applications de gestion de projets, des forums de discussion, des calendriers partagés et des annuaires d'employés.
- **Extranet :** est un réseau informatique qui relie une organisation à des partenaires, des fournisseurs, des clients et d'autres parties prenantes externes. L'extranet permet aux parties prenantes de l'organisation d'accéder à certaines ressources de l'organisation, telles que des bases de données ou des systèmes de gestion des commandes, mais ces ressources sont protégées par des mesures de sécurité et ne sont accessibles qu'aux utilisateurs autorisés. La sécurité est un aspect crucial de l'extranet, car il est essentiel de protéger les informations de l'organisation contre tout accès non autorisé. Les mesures de sécurité incluent des pares-feux, des protocoles de sécurité avancés tels que SSL ou TLS, des politiques de mots de passe, des contrôles d'accès et des techniques de chiffrement pour protéger les données en transit.

2. La Sécurité Informatique

2.1. Définition de la sécurité informatique

La sécurité informatique est l'ensemble des mesures techniques, organisationnelles et humaines visant à protéger les systèmes informatiques, les réseaux, les données et les utilisateurs contre les menaces internes et externes. Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques.

La sécurité réseau est une branche de l'informatique qui consiste à protéger tous les éléments d'un réseau informatique pour empêcher l'accès non autorisé, le vol de données, l'utilisation abusive d'une connexion réseau, la modification des données, etc. Elle vise donc à fournir des méthodes et des mécanismes de défense proactifs pour protéger un réseau contre les menaces externes et internes. [3].

2.2. Objectifs de la sécurité informatique

Les objectifs de la sécurité informatique sont multiples, mais ils ont tous pour but de protéger les systèmes informatiques, les réseaux, les données et les utilisateurs contre les menaces internes et externes. Voici les principaux objectifs de la sécurité informatique :

- **Confidentialité :** garantir que les informations sensibles et les données confidentielles ne sont accessibles qu'aux personnes autorisées.
- **Intégrité :** garantir que les informations sont précises, complètes et fiables et qu'elles ne sont pas altérées de manière non autorisée.
- **Disponibilité :** garantir que les informations et les services sont disponibles pour les utilisateurs autorisés quand ils en ont besoin.
- **Authenticité :** garantir que les informations proviennent de sources fiables et que les utilisateurs sont qui ils prétendent être.
- **Non-répudiation :** garantir que les utilisateurs ne peuvent pas nier avoir effectué une action ou une transaction.
- **Respect des lois et des règlementations :** se conformer aux lois et aux règlementations en vigueur concernant la sécurité et la protection des données.
- **Continuité d'activité :** garantir que les services informatiques sont disponibles en cas d'incident ou de catastrophe.

- **Responsabilité :** définir clairement les responsabilités de chaque personne impliquée dans la sécurité informatique et assurer la gestion des risques de sécurité informatique.

2.3. Terminologie de la sécurité informatique

La sécurité informatique utilise une terminologie spécifique pour décrire les différentes menaces, vulnérabilités et mesures de protection. Voici quelques termes couramment utilisés en sécurité informatique :

- **Attaque :** une tentative non autorisée de compromettre la sécurité d'un système informatique, d'un réseau ou de données.
- **Vulnérabilité :** une faiblesse ou une lacune dans un système informatique, un réseau ou une application qui peut être exploitée par des attaquants.
- **Malware :** un logiciel malveillant, tel qu'un virus, un cheval de Troie, un ransomware ou un spyware, qui est conçu pour endommager ou compromettre un système informatique.
- **Pare-feu :** un dispositif de sécurité qui contrôle le trafic réseau entrant et sortant et peut bloquer les attaques malveillantes.
- **Cryptographie :** l'utilisation d'algorithmes de chiffrement pour protéger les données sensibles et confidentielles.
- **Authentification :** le processus de vérification de l'identité d'un utilisateur ou d'un système informatique.
- **Autorisation :** le processus qui détermine les actions que l'utilisateur est autorisé à effectuer après avoir été authentifié.
- **Gestion des identités et des accès :** les processus et les outils pour gérer les identités des utilisateurs, les droits d'accès et les autorisations.
- **Audit de sécurité :** l'examen des systèmes informatiques, des réseaux et des données pour identifier les vulnérabilités et les mesures de protection nécessaires.
- **Plan de continuité d'activité :** un plan qui décrit les mesures à prendre pour maintenir les services informatiques en cas d'incident ou de catastrophe.

2.4. Les attaques réseau

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Ces attaques sont pour la plupart lancées automatiquement à partir de

machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques [4].

2.4.1. Les différentes étapes d'une attaque

Les étapes d'une attaque informatique peuvent varier en fonction de l'objectif et de la complexité de l'attaque.

- **Reconnaissance :** l'attaquant collecte des informations sur la cible, telles que son adresse IP, son système d'exploitation, les applications qu'elle utilise et les éventuelles vulnérabilités qui pourraient être exploitées.
- **Scanning :** l'attaquant explore le réseau de la cible pour détecter les ports ouverts, les services actifs et les failles de sécurité potentielles.
- **Exploitation :** l'attaquant utilise les vulnérabilités identifiées pour accéder à la cible, installer des logiciels malveillants ou prendre le contrôle du système.
- **Escalade de privilèges :** si l'attaquant n'a pas déjà les privilèges nécessaires pour atteindre son objectif, il peut chercher à obtenir des privilèges d'administrateur pour accéder à des informations plus sensibles ou effectuer des actions malveillantes.
- **Maintien de l'accès :** une fois que l'attaquant a réussi à accéder au système, il peut chercher à rester discret pour continuer à collecter des informations ou à effectuer des actions malveillantes.
- **Effacement des traces :** l'attaquant peut effacer les traces de son activité pour éviter d'être détecté.

Il est important de noter que ces étapes ne se produisent pas toujours dans cet ordre et que les attaques peuvent être lancées à partir de différents points d'entrée. Les entreprises et les particuliers doivent mettre en place des mesures de sécurité pour réduire les risques d'attaques et détecter rapidement les activités suspectes sur leur réseau.

2.4.2. Les différents types d'attaques Réseaux

Il existe trois types d'attaques :

- **Attaque directe :** Il s'agit d'une attaque dans laquelle le pirate informatique tente de pénétrer directement dans le système ou le réseau ciblé sans passer par une tierce partie. Les attaques de force brute, de dépassement de tampon et de contournement d'authentification sont des exemples d'attaques directes.

- **Attaque indirecte par rebond :** Il s'agit d'une attaque dans laquelle le pirate informatique utilise un système tiers pour lancer l'attaque. Le pirate utilise le système tiers comme "rebond" pour masquer son adresse IP et sa localisation. Les pirates utilisent souvent des botnets (réseaux d'ordinateurs infectés) pour lancer l'attaque.
- **Attaque indirecte par réponse :** Il s'agit d'une attaque dans laquelle le pirate informatique exploite les réponses du système ciblé pour obtenir des informations sensibles ou pour accéder au système.

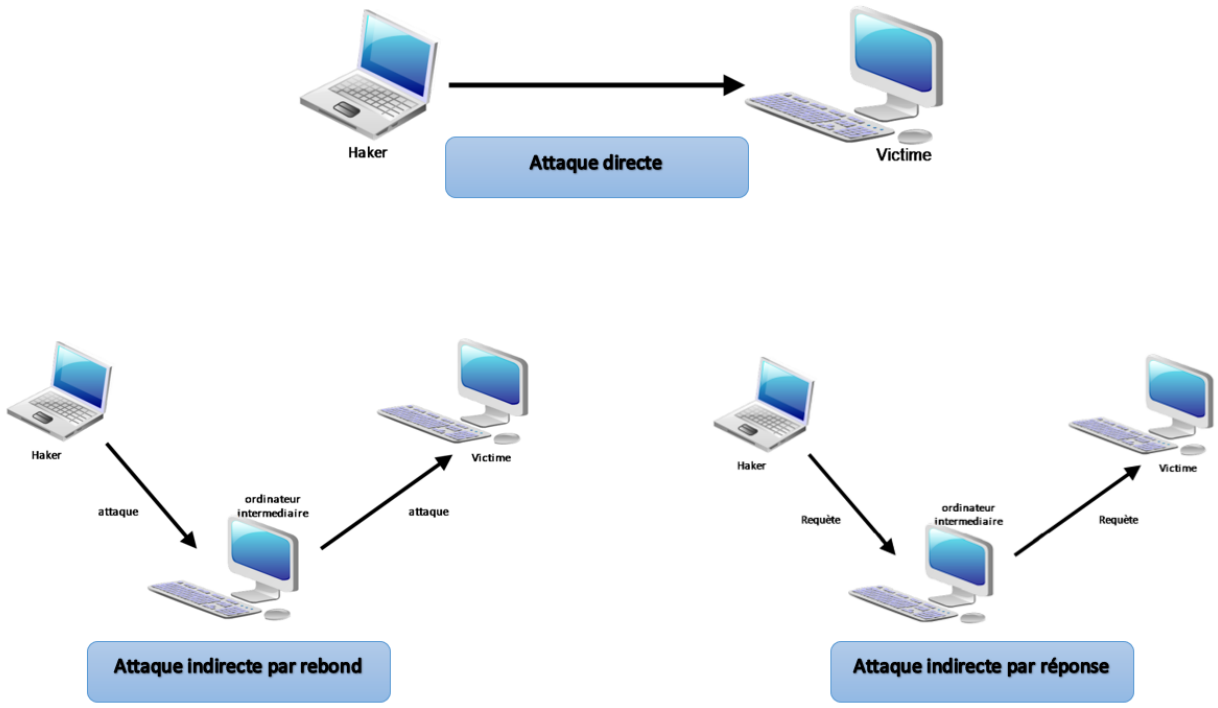


Figure 2 - Différents types d'attaques Réseaux *[2]*

2.4.3. Quelques attaques courantes

- **Attaques de déni de service (DoS) :** Ces attaques visent à submerger un système avec un grand nombre de demandes afin de le rendre indisponible pour les utilisateurs légitimes. Ces types d'attaque sont très faciles à mettre en place et très difficile a empêcher [5].
- **Attaques de déni de service distribué (DDoS) :** Ces attaques utilisent un grand nombre d'ordinateurs zombies pour submerger un système avec un grand nombre de demandes, rendant ainsi son accès impossible.

- **Attaques de phishing :** Les attaques de phishing sont des tentatives d'obtenir des informations personnelles et sensibles (comme les identifiants de connexion et les mots de passe) en se faisant passer pour une source fiable et légitime.
- **Attaques d'ingénierie sociale :** Ces attaques visent à manipuler les utilisateurs pour qu'ils révèlent des informations sensibles, telles que des identifiants de connexion ou des informations de carte de crédit.
- **Attaques de l'homme du milieu :** Ces attaques impliquent l'interception des communications entre deux parties afin de les espionner ou de modifier les données échangées.
- **Attaques par injection SQL :** Ces attaques visent à exploiter des failles de sécurité dans les applications Web pour accéder à des données confidentielles ou modifier le fonctionnement de l'application.
- **Attaques par force brute :** Ces attaques utilisent des programmes automatisés pour tenter de deviner les identifiants de connexion en essayant toutes les combinaisons possibles jusqu'à trouver le bon.
- **Attaques de défiguration :** Ces attaques consistent à modifier le contenu d'un site web pour afficher des messages malveillants ou des contenus offensants.

2.5. Les éléments à sécuriser dans un réseau

Effectivement, la sécurisation d'un réseau informatique implique de protéger trois types d'éléments : le matériel, les programmes et les données.

- **Le matériel :** les équipements réseau tels que les routeurs, les commutateurs, les pare-feux, les serveurs, les ordinateurs, les périphériques de stockage, les appareils mobiles et les points d'accès sans fil doivent être protégés contre les attaques physiques, les vols et les accès non autorisés. Il est donc important de prendre des mesures pour protéger physiquement ces équipements, tels que l'utilisation de systèmes de verrouillage, de contrôle d'accès et de surveillance vidéo.
- **Les programmes :** les programmes, ou logiciels, tels que les systèmes d'exploitation, les applications, les scripts et les codes doivent être protégés contre les vulnérabilités et les attaques de logiciels malveillants. Les mesures de protection comprennent l'installation régulière de correctifs de sécurité, l'utilisation d'antivirus, de pare-feux, de filtrage web et de politique de sécurité pour les logiciels.

- **Les données :** les données stockées sur le réseau, telles que les informations personnelles, les données financières, les données de santé et les secrets d'entreprise, doivent être protégées contre les accès non autorisés, les fuites, les pertes et les vols. Les mesures de protection comprennent l'utilisation de méthodes de cryptage, de politique de sécurité pour les données, de sauvegardes régulières, de contrôle d'accès et de surveillance des activités des utilisateurs.

En résumé, la sécurisation d'un réseau informatique doit prendre en compte tous ces éléments pour protéger efficacement les données et les ressources de l'entreprise. Il est important de mettre en place une stratégie de sécurité complète qui inclut des mesures de sécurité physiques, logicielles et de données pour minimiser les risques d'attaques et de pertes de données.

2.6. Firewall

2.6.1. Définition d'un Firewall

Un pare-feu (en anglais, firewall) est un dispositif de sécurité informatique qui contrôle et filtre les communications entre un réseau privé (comme une entreprise ou une organisation) et un réseau public (comme Internet). Le rôle principal d'un pare-feu est de protéger un réseau informatique des menaces externes, telles que les attaques de pirates informatiques, les virus, les logiciels malveillants et les accès non autorisés. Un routeur doit décider au coup par coup du sort de chaque paquet, avec seulement une faible possibilité d'analyse historique, alors qu'un pare-feu efficace contre les attaques subtiles doit pouvoir faire des choses plus compliquées [6].

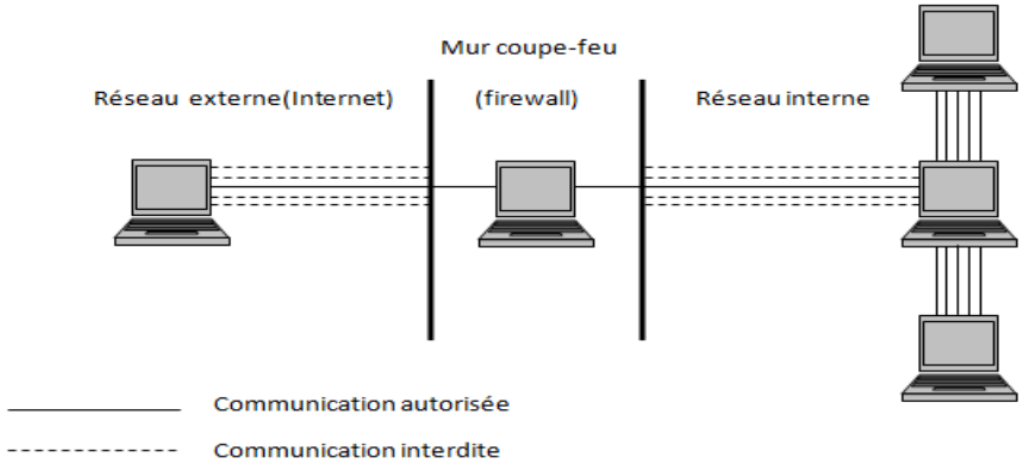


Figure 3 – Firewall *[7]*

2.6.2. Principe de fonctionnement

Lorsqu'on utilise un firewall pour contrôler le trafic réseau, il est possible de définir différentes actions à effectuer sur les paquets qui correspondent aux règles définies. Les trois actions les plus courantes sont :

- **Autoriser la connexion [allow] :** Cette action permet de laisser passer les paquets qui correspondent aux règles définies. Par exemple, si une règle autorise les connexions entrantes sur un certain port, un paquet arrivant sur ce port sera autorisé à passer.
- **Bloquer la connexion [deny] :** Cette action bloque les paquets qui correspondent aux règles définies. Par exemple, si une règle interdit les connexions entrantes sur un certain port, un paquet arrivant sur ce port sera bloqué.
- **Rejeter la demande de connexion sans avertir l'émetteur [drop] :** Cette action est similaire au blocage, mais contrairement à ce dernier, elle ne renvoie pas de réponse au paquet. Le paquet est simplement ignoré et l'émetteur ne reçoit pas de message d'erreur. Cette méthode est souvent utilisée pour les attaques de type "port scanning" ou "ping flooding", où un attaquant envoie un grand nombre de paquets dans le but de repérer des ports ou de saturer la bande passante.

2.6.3. Les différents types de filtrage

Les trois types de filtrage que vous avez mentionnés sont des techniques courantes utilisées dans les firewalls pour contrôler le trafic réseau :

- **Filtrage simple de paquet :** Le filtrage simple de paquets est le type le plus élémentaire de filtrage et il fonctionne en se basant sur les caractéristiques des paquets individuels tels que l'adresse source et de destination, le protocole et les numéros de port. Le firewall compare chaque paquet entrant avec les règles de filtrage et prend une décision en fonction de ces règles. Ce type de filtrage est rapide et efficace, mais il est limité dans sa capacité à identifier les attaques sophistiquées qui utilisent des techniques de contournement.
- **Filtrage dynamique :** Le filtrage dynamique, également appelé filtrage de session, est une technique plus avancée qui consiste à examiner l'ensemble de la session plutôt que chaque paquet individuellement. Le firewall crée une table de session pour chaque connexion et examine l'état de la connexion pour déterminer si elle doit être autorisée ou bloquée. Ce type de filtrage est plus efficace pour détecter les attaques sophistiquées qui

utilisent des techniques de contournement, mais il est également plus complexe et consomme plus de ressources.

- **Filtrage applicatif :** Le filtrage applicatif est le type le plus avancé de filtrage et il analyse les données applicatives contenues dans les paquets plutôt que simplement leurs en-têtes. Il utilise des signatures ou des règles spécifiques à l'application pour identifier les attaques potentielles et bloquer ou autoriser les connexions en conséquence. Ce type de filtrage est particulièrement efficace pour les applications Web et les services cloud, mais il est également plus complexe et nécessite des mises à jour régulières des signatures et des règles pour rester efficace.

En général, les firewalls utilisent une combinaison de ces différents types de filtrage pour offrir une protection complète contre les attaques réseau. Les choix de types de filtrage dépendent des politiques de sécurité de l'organisation et des besoins spécifiques de protection.

3. Deep Learning

3.1. Définition de l'apprentissage en profondeur « Deep Learning »

L'apprentissage en profondeur (ou Deep Learning en anglais) est une branche de l'intelligence artificielle qui se concentre sur la création de modèles d'apprentissage automatique complexes et hiérarchiques en utilisant des réseaux de neurones artificiels. Contrairement à l'apprentissage machine traditionnel, qui peut nécessiter la sélection et l'ingénierie manuelle de caractéristiques à utiliser pour classer les données, l'apprentissage en profondeur permet à un système de reconnaître des structures dans les données en utilisant des couches de neurones interconnectés pour apprendre des représentations de plus en plus abstraites des données.

Deep Learning est un type de méthodes d'apprentissage automatique basées sur l'apprentissage de représentations de données [8].

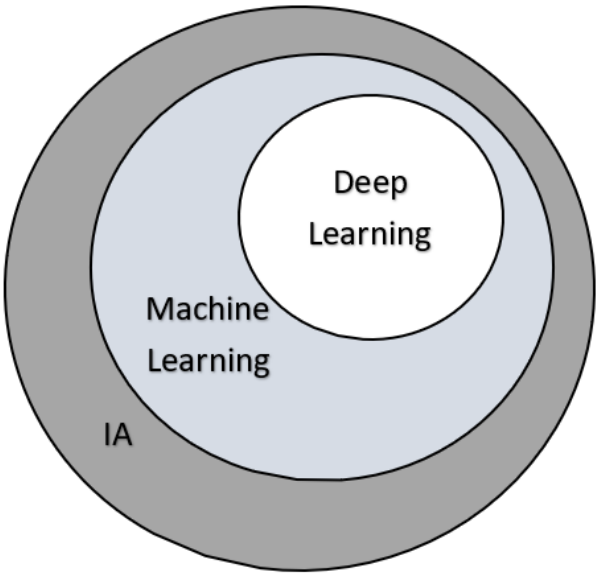


Figure 4 – Deep Learning est lié à Machine Learning et à l'intelligence artificielle *[9]*

3.2. Les architectures d'apprentissage en profondeur

Généralement, l'architecture des réseaux profondes est organisée en couches de neurones pour n'importe quel type de ces réseaux ; une Couche d'entrée (Input Layer), une ou plusieurs Couches cachées (Hidden Layers) et une Couche de sortie (Output Layer). Chaque paire de couches voisines est connectée. Les connexions entre eux appelées poids (Weights). Les "neurones" d'une même couche généralement appelés "nœuds" n'ont aucune association, la Figure 5 illustré une architecture standard d'un modèle de réseau de neurones profond [10].

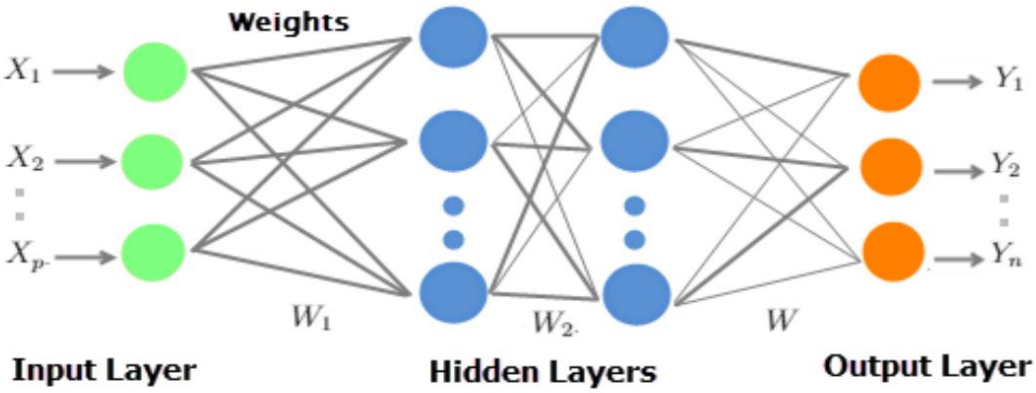


Figure 5 - L'architecture d'un modèle Deep Learning [11].

3.3. Types d'apprentissage profondeur

Il existe principalement trois types d'apprentissage en profondeur (Deep Learning) :

- **L'apprentissage supervisé :** dans ce type d'apprentissage, les données d'entrée sont étiquetées avec des sorties souhaitées, et le modèle est entraîné à prédire ces sorties en minimisant l'erreur entre les prédictions et les sorties souhaitées. C'est le type d'apprentissage le plus couramment utilisé en Deep Learning, et il est utilisé pour des tâches telles que la classification d'images, la prédiction de prix, ou la reconnaissance vocale.
- **L'apprentissage non supervisé :** dans ce type d'apprentissage, les données d'entrée ne sont pas étiquetées, et le modèle est entraîné à découvrir des structures dans les données. L'objectif est de trouver des motifs ou des groupes de données similaires, sans avoir besoin de connaître à l'avance les sorties souhaitées. Les auto encodeurs et les réseaux génératifs adversaires sont des exemples d'apprentissage non supervisé.
- **L'apprentissage par renforcement :** dans ce type d'apprentissage, un agent doit apprendre à prendre des décisions pour maximiser une récompense donnée. L'agent interagit avec un environnement et reçoit une récompense positive ou négative en fonction de ses actions. L'objectif est d'apprendre une politique qui permet à l'agent de prendre les meilleures décisions possibles pour maximiser la récompense. Cet apprentissage est couramment utilisé dans les jeux vidéo ou la robotique.

3.4. Quelques méthodes d'apprentissage profond

3.4.1. Réseau de neurones profonds (DNN)

Les réseaux de neurones profonds (DNN) sont une classe de réseaux de neurones artificiels (ANN) qui ont plus d'une couche cachée. Ils sont utilisés pour une variété de tâches, notamment la reconnaissance d'images et de la parole, le traitement du langage naturel et les systèmes de recommandation. Les DNN sont généralement composés de plusieurs couches de neurones qui traitent les données de manière hiérarchique, chaque couche apprenant des caractéristiques plus complexes des données d'entrée.

3.4.2. Réseaux de neurones convolutionnels (CNN)

Les réseaux de neurones convolutionnels (CNN) sont un type de réseau de neurones profonds particulièrement bien adapté aux tâches de reconnaissance d'images et de vidéos. Ils sont conçus pour apprendre automatiquement et de manière adaptative des hiérarchies

spatiales de caractéristiques à partir des images d'entrée. Les CNN sont composés de plusieurs couches de neurones qui effectuent des convolutions sur les données d'entrée, ce qui consiste à appliquer un ensemble de filtres à l'entrée pour extraire des caractéristiques utiles à la classification.

3.4.3. Réseaux de neurones récurrents (RNN)

Les réseaux de neurones récurrents (RNN) sont un type de réseau de neurones qui peuvent traiter des données séquentielles, telles que des séries temporelles ou du texte en langage naturel. Ils sont capables d'utiliser des informations des étapes de temps précédentes dans leurs calculs, ce qui les rend bien adaptés aux tâches qui impliquent des dépendances séquentielles. Les RNN sont composés d'unités répétitives qui traitent une entrée à la fois et maintiennent un état caché, qui est mis à jour à chaque étape de temps et sert de mémoire des entrées précédentes du réseau.

Conclusion

Dans ce chapitre, nous avons défini les concepts de base des réseaux informatiques et exploré leur classification et les différents types de réseaux existants. Et la sécurité à adopter pour traiter les attaques auxquelles les systèmes informatiques sont confrontés et avons mis en évidence l'importance des pare-feu pour renforcer la sécurité des réseaux. Ainsi que les concepts de base de Deep Learning et les différentes architectures de réseaux de neurones profonds. Le chapitre suivant sera consacré aux techniques de l'intelligence artificiel pour détecter les attaques.

Chapitre 2

Les techniques de L'IA pour détecter les attaques

Chapitre 2 : Les techniques de L'IA pour détecter les attaques

Introduction

L'intelligence artificielle est une technologie émergente qui offre un potentiel immense pour améliorer la sécurité informatique. Au cours des dernières décennies, l'IA a été l'un des sujets de recherche scientifique les plus actifs, ce qui a permis de développer des algorithmes sophistiqués pour améliorer la détection des attaques informatiques. Les cybermenaces sont devenues de plus en plus sophistiquées et les organisations sont confrontées à des risques de plus en plus complexes. Par conséquent, l'utilisation de l'IA peut aider les entreprises à renforcer leur sécurité informatique et à se protéger contre les cyberattaques.

L'IA peut être utilisée pour détecter les activités suspectes et les comportements malveillants en temps réel, ce qui peut aider les organisations à prendre des mesures préventives avant que les attaques ne se produisent. Les algorithmes d'IA peuvent également aider à améliorer la vitesse et l'efficacité de la réponse aux incidents de sécurité, ce qui permet de minimiser les pertes financières pour les entreprises et de réduire les temps d'arrêt.

Cependant, il est important de noter que la qualité des résultats dépendra de la qualité des données utilisées pour entraîner les algorithmes d'IA. Si les données sont incomplètes, biaisées ou mal étiquetées, cela peut entraîner des résultats incohérents et des faux positifs ou négatifs, ce qui peut avoir des conséquences graves pour les organisations. En outre, l'utilisation de l'IA dans la sécurité informatique peut être sujette à des attaques adverses, où les cybercriminels utilisent des techniques d'IA pour contourner les systèmes de sécurité.

Dans ce chapitre, nous allons explorer les techniques d'IA pour détecter les attaques, ainsi que l'utilisation du Deep Learning pour la cybersécurité. Enfin, nous étudions et analysons les bases de données utilisées et plusieurs travaux antérieurs de détection d'attaques basés sur le Deep Learning.

1. L’apprentissage profond pour la cybersécurité

Avec la disponibilité de grandes quantités de données de la cyber infrastructure, des réseaux, des systèmes d'exploitation ou des systèmes d'informations et pour relever les défis de la cybersécurité, ses méthodes et techniques comme l'apprentissage automatique (machine learning), data mining, statistique et capacitance interdisciplinaire elle n'est pas exploitée [12].

Le Deep Learning qui fait partie de l’apprentissage automatique peut être utilisé pour détecter les attaques et les comportements malveillants en analysant les données du réseau ou des systèmes.

Ces méthodes de classification et de prévention sont utilisées pour détecter motifs et comportements propres à divers types de cyberattaques qui perpétuent une réponse cyber en temps réel. Il a la capacité de détecter les attaques lorsqu'elle s'est produit et aussi de la capacité de prédire les futures attaques potentielles [13].

Les méthodes basées sur l'apprentissage approfondi peuvent contribuer à améliorer l'efficacité des systèmes de détection d'intrusion en surmontant certains des défis auxquels sont confrontés les IDS traditionnels, tels que la complexité croissante des attaques et la nécessité de traiter de grandes quantités de données en temps réel.

Dans un autre côté, la collecte de données et de ressources de trafic sur un conduit pour un problème de big-data d'experts en sécurité souhaitant toujours de meilleures performances IDS qui ont un taux de détection la plus élevée et un taux de fausses alarmes le plus bas. Par Consécutives, les approches de Deep Learning qui s'adaptent à une très grande quantité de données. Ces derniers ont été livrés pour la détection d'anomalies du réseau dans le but de différencier les comportements normaux et des comportements anormaux afin de détecter des activités malveillantes ou suspectes d'être malveillantes [14].

2. Les Data-sets

L'ensemble de données utilisé dans les travaux publiés de l'étude approfondie de la cybersécurité joue un rôle important dans la validation de toutes les approches DL proposées. Certains de ces ensembles de données ne sont pas facilement accessibles en

raison de problèmes de confidentialité. Un ensemble de données conçu pour détecter une cyberattaque [15].

- **KDD99** (Knowledge Discovery and Data Mining Cup 1999) est un ensemble de données largement utilisé pour la recherche en détection d'intrusion. Il a été créé par le National Institute of Standards and Technology (NIST) et est composé de données de trafic réseau d'un environnement simulé avec différents types d'attaques. L'ensemble de données KDD99 a été largement utilisé comme ensemble de données de référence pour évaluer les performances de différents systèmes de détection d'intrusion et algorithmes d'apprentissage automatique. Cependant, il a été critiqué pour plusieurs raisons, notamment son manque de représentativité du trafic réseau et des attaques du monde réel, sa distribution déséquilibrée des types d'attaque et la présence de fonctionnalités redondantes et non pertinentes [16].
- **NSL-KDD** (Network Security Lab-KDD) est un ensemble de données utilisé pour la recherche en détection d'intrusion. Il a été créé par le laboratoire de sécurité réseau de l'université de Tehran en Iran en réponse aux critiques concernant l'ensemble de données KDD99. L'ensemble de données NSL-KDD est basé sur l'ensemble de données KDD99, mais il a été prétraité pour résoudre certains des problèmes de KDD99, tels que la redondance et la pertinence des fonctionnalités, la distribution déséquilibrée des types d'attaque et l'utilisation d'attaques obsolètes. Il contient environ 2,5 millions de connexions réseau simulées et est divisé en trois ensembles : l'ensemble d'apprentissage, l'ensemble de test et l'ensemble de validation. NSL-KDD a été largement utilisé pour évaluer les performances de divers systèmes de détection d'intrusion et algorithmes d'apprentissage automatique. Cependant, il a également été critiqué pour ne pas représenter avec précision le trafic réseau réel et les attaques, tout en ayant des problèmes de surapprentissage et de généralisation limitée [17].
- **MAWI** (Monitoring and Analysis of Internet Traffic) est un ensemble de données de trafic réseau collecté par l'Université de Vienne en Autriche depuis 2004. Il s'agit d'un des plus anciens et des plus vastes ensembles de données de trafic réseau disponibles pour la recherche. L'ensemble de données MAWI contient des données de trafic réseau de différents types, tels que le trafic de backbone, le trafic de site web, le trafic de serveur de messagerie, le trafic de transfert de fichiers, etc. Les données ont été collectées dans un environnement de production et contiennent à la fois du trafic normal et des attaques.

L'ensemble de données MAWI est utilisé pour la recherche en analyse de trafic, en sécurité informatique, en apprentissage automatique, en réseaux de communication et en télécommunications. Les données sont disponibles gratuitement pour la recherche et l'analyse, mais leur manipulation et leur analyse peuvent être difficiles en raison de leur taille et de leur complexité. Les chercheurs peuvent utiliser les données pour développer et tester des outils de détection d'anomalies, de prévention des attaques, de surveillance de la qualité de service, de la planification de capacité et d'autres applications liées aux réseaux de communication [18].

- **ISCX** (Information Security Center of Excellence) est un ensemble de données de trafic réseau collecté par l'Université de New Brunswick au Canada. Il s'agit d'un ensemble de données très complet pour la recherche en sécurité informatique. L'ensemble de données ISCX contient des données de trafic réseau de différents types, tels que le trafic de courrier électronique, le trafic de serveur web, le trafic de serveur de base de données, le trafic de VoIP, le trafic de VPN, etc. Les données ont été collectées dans un environnement de laboratoire et contiennent à la fois du trafic normal et des attaques. L'ensemble de données ISCX est utilisé pour la recherche en sécurité informatique, en détection d'anomalies, en apprentissage automatique, en réseaux de communication et en télécommunications. Les données sont disponibles gratuitement pour la recherche et l'analyse. Les chercheurs peuvent utiliser les données pour développer et tester des outils de détection d'anomalies, de prévention des attaques, de surveillance de la qualité de service, de la planification de capacité et d'autres applications liées aux réseaux de communication [19].
- **CIC DoS** (Canadian Institute for Cybersecurity Denial-of-Service) est un ensemble de données de trafic réseau spécialement conçu pour la détection d'attaques de déni de service (DoS) et de déni de service distribué (DDoS). Il a été créé par le Canadian Institute for Cybersecurity de l'Université du Nouveau-Brunswick. L'ensemble de données contient environ 15 types d'attaques de DoS/DDoS, y compris des attaques par amplification, par fragmentation et par épuisement de ressources. Il contient également des données de trafic réseau normales pour servir de référence pour la détection d'anomalies. L'ensemble de données est divisé en deux parties : l'ensemble d'apprentissage et l'ensemble de test. L'ensemble de données CIC DoS est utilisé pour évaluer les performances des outils de détection d'anomalies et de sécurité réseau dans la

détection d'attaques de DoS/DDoS. Il est également utilisé pour la recherche en apprentissage automatique et en sécurité informatique. L'ensemble de données est disponible gratuitement pour la recherche et l'analyse [19].

- **CIC DDoS** (Canadian Institute for Cybersecurity Distributed Denial of Service) est un ensemble de données de trafic réseau spécialement conçu pour la détection d'attaques de déni de service distribué (DDoS). Il a été créé par le Canadian Institute for Cybersecurity de l'Université du Nouveau-Brunswick. L'ensemble de données contient plusieurs types d'attaques DDoS, y compris des attaques par réflexion, par amplification et par fragmentation. Il contient également des données de trafic réseau normales pour servir de référence pour la détection d'anomalies. L'ensemble de données est divisé en deux parties : l'ensemble d'apprentissage et l'ensemble de test. L'ensemble de données CIC DDoS est utilisé pour évaluer les performances des outils de détection d'anomalies et de sécurité réseau dans la détection d'attaques DDoS. Il est également utilisé pour la recherche en apprentissage automatique et en sécurité informatique. L'ensemble de données est disponible gratuitement pour la recherche et l'analyse [19].

Data-set public	**Type**	**Étiqueté**	**Année**	**[Réf]**
KDD99	Trafic du réseau	Oui	1999	[16]
NSL-KDD	Trafic du réseau	Oui	2009	[17]
MAWI dataset	Trafic internet	Oui	2011	[18]
ISCX dataset	Trafic du réseau	Oui	2012	[19]
CIC DoS dataset	Trafic du réseau	Oui	2017	[19]
CIC DDoS dataset	Trafic du réseau	Oui	2019	[19]

Tableau 1 - Ensembles de données publies sur la cybersécurité

3. Travaux connexes pour la détection des attaques basé sur le DL

Les travaux relatifs à la détection d'intrusions basés sur le Deep Learning ont connu une forte croissance ces dernières années. Différentes approches ont été développées pour détecter les attaques sur les réseaux informatiques et les systèmes, notamment en utilisant des réseaux de neurones convolutifs, des réseaux de neurones récurrents, des réseaux de neurones profonds et l'apprentissage par renforcement.

- **Salama et al** [20]**.** Présente une approche hybride combinant le réseau de croyances profondes (DBN) et la machine à vecteurs de support (SVM) pour la détection d'intrusion dans les réseaux. Le réseau DBN est utilisé comme méthode de réduction de dimension pour obtenir de meilleures caractéristiques d'apprentissage, suivies d'un classifieur SVM. Les performances de l'approche DBN-SVM sont testées sur le data-set NSL-KDD. Le nombre de caractéristiques est réduit de 41 à 5 grâce au réseau DBN, qui sont ensuite transmises à un classifieur SVM pour effectuer une classification binaire (normale/attaque). Les résultats montrent une exactitude supérieure à 90% pour cette méthode proposée. De plus, le réseau DBN est comparé à d'autres méthodes d'analyse de données comme l'ACP, le Gain Ratio et le Chi-Square, montrant qu'il est plus performant en tant que méthode de réduction des caractéristiques.
- **Alom et al** [21]**.** Présente un système de détection d'intrusion basé sur les réseaux de croyances profondes (DBN) pour améliorer la sécurité des réseaux. Le DBN est utilisé pour extraire automatiquement les caractéristiques importantes des données de trafic réseau, puis un classifieur est utilisé pour détecter les intrusions. Les performances de la méthode sont évaluées sur un data-set réel et les résultats montrent une précision élevée dans la détection d'intrusions. Les résultats ont montré que la précision de détection du système a atteint 97,5% avec seulement 50 itérations.
- **Vinayakumar et al** [22]**.** A analysé l'efficacité du réseau neuronal convolutionnels (Convolutional Neural Network, CNN) pour la détection d'intrusions en modélisant les événements de trafic du réseau en tant que séries temporelles de paquets TCP/IP sur des périodes de temps prédéfinies. Les auteurs ont utilisé une approche inspirée du traitement du langage naturel avec une couche de convolution 1D pour traiter les données de série temporelle. Différentes architectures de CNN ont été proposées, comprenant une couche d'entrée, une couche cachée et une couche de sortie, ou une couche cachée composée d'une ou plusieurs couches CNN suivies de FFN ou de RNN/LSTM/GRU pour déterminer l'architecture optimale. Toutes les expériences ont été réalisées sur 1000 époques et les performances de chaque modèle ont été évaluées sur l'ensemble de test du data-set KDDCup 99. Les résultats ont montré que le modèle CNN-LSTM a obtenu de bons résultats par rapport aux autres structures de réseau CNN, avec une précision de détection d'intrusions de 99%. Les auteurs ont conclu que les

algorithmes de CNN ont surpassé les résultats du défi KDDCup 99 et d'autres résultats publiés pour la détection d'intrusions.

- **Al-Yaseen et al** [23]**.** Ont proposé un système de détection d'intrusions basé sur un modèle multi-niveau combinant une machine à vecteurs de support (Support Vector Machine, SVM) hybride et une machine d'apprentissage extrême (Extreme Learning Machine, ELM), avec une modification de l'algorithme K-means pour la classification des données. L'approche proposée combine les avantages de la SVM et de l'ELM pour améliorer la précision de la détection d'intrusions. Les auteurs ont utilisé un algorithme de clustering K-means modifié pour réduire le bruit dans les données d'entrée et améliorer la qualité des caractéristiques extraites. Ensuite, les données prétraitées ont été utilisées pour entraîner un modèle hybride SVM-ELM à plusieurs niveaux, composé de plusieurs SVM et ELM en cascade pour améliorer la performance de détection. Les expériences ont été menées sur un ensemble de données de détection d'intrusions et les résultats ont montré que l'approche proposée a atteint une précision de détection d'intrusions de 67%. Les auteurs ont conclu que leur modèle hybride SVM-ELM basé sur la modification de K-means peut améliorer la performance de détection d'intrusions par rapport aux méthodes traditionnelles de SVM et d'ELM utilisées individuellement.
- **Sharafaldin et al** [24]**.** Ont présenté une étude sur le développement d'un ensemble de données réaliste pour les attaques par déni de service distribué (DDoS) ainsi qu'une taxonomie pour classer ces attaques. Les auteurs ont utilisé un ensemble de données de captures de trafic réseau pour générer un ensemble d'attaques DDoS synthétiques, en reproduisant les caractéristiques de différents types d'attaques réelles dans un environnement de laboratoire contrôlé. L'ensemble de données CICDDoS2019, qui comprend 11 types d'attaques DDoS, permet d'évaluer efficacement les algorithmes et les systèmes IDS/IPS pour la détection des attaques DDoS.ce qui en fait l'un des ensembles de données les plus complets pour la détection d'attaques DDoS. Les résultats obtenus ont montré une précision globale (F1-score) de 69% pour la détection des attaques DDoS. Les auteurs ont également réalisé une analyse complète basée sur les 12 diagrammes RadViz des facteurs les plus pertinents pour chaque type de trafic réseau, ce qui permet de mieux comprendre les caractéristiques et les schémas de chaque type d'attaque DDoS.

- **Hamouda et al** [10]**.** Ont utilisé le dataset CICDDoS2019 pour entraîner trois modèles d'apprentissage en profondeur discriminants afin de détecter les attaques DDoS. Ils ont utilisé la technique de sous-échantillonnage aléatoire pour créer trois sous-ensembles de données distincts pour trois types de classifications. Pour la classification, ils ont utilisé trois modèles d'apprentissage en profondeur supervisés : un réseau de neurones profond (DNN), un réseau de neurones convolutif (CNN) et un réseau de neurones récurrent (RNN). Les classifications multi-classes (normal/attaque) et binaire (normal/attaque) couvrent différents types d'attaques, avec des taux de précision de 80 % pour 7 classes, 99 % pour 2 classes et 60 % pour 13 classes. Les performances des modèles ont été évaluées en utilisant les mesures de précision, de rappel et de score F1.
- **Farage et al** [25]**.** Ont proposé trois modèles IDS (systèmes de détection d'intrusion) basés sur l'apprentissage profond, à savoir un modèle basé sur un réseau neuronal convolutif (CNN), un modèle basé sur un réseau neuronal profond et un modèle basé sur un réseau neuronal récurrent. Les performances de ces modèles sont évaluées en utilisant deux nouveaux ensembles de données réelles, à savoir l'ensemble de données CIC-DDoS2019 et l'ensemble de données TON_IoT, pour deux types de classification (binaire et multi-classe). Les résultats montrent que les approches d'apprentissage profond surpassent les tactiques d'apprentissage automatique conventionnelles en termes de performances. En particulier, le modèle IDS basé sur CNN obtient des performances supérieures aux approches d'apprentissage profond de pointe, évaluées à l'aide des ensembles de données CIC-DDoS2019 et TON_IoT, avec une précision de détection du trafic binaire de 99,95% et une précision de détection du trafic multi-classe de 95%. Cela suggère que le modèle IDS basé sur CNN est efficace pour détecter les attaques DDoS dans le contexte de l'agriculture 4.0.
- **Mittal M et al** [26]**.** Ont utilisé les performances de deux modèles IDS (Intrusion Detection System) basés sur l'apprentissage profond, à savoir le modèle DNN (Deep Neural Network) et le modèle LSTM (Long Short-Term Memory), en utilisant l'ensemble de données CICIDS2017. Ils ont effectué une classification binaire et ont obtenu un taux d'exactitude (accuracy) de 98,72% pour la détection des intrusions. Cela indique que les modèles IDS basés sur l'apprentissage profond, tels que le DNN et le LSTM, sont efficaces pour détecter les intrusions dans l'ensemble de données CICIDS2017.

Article	Année	Domaine	Méthode	Dataset	Mesures de performances
Salama et al [20].	2011	IDS	DBN - SVM	NSL-KDD	Accuracy = 90%
Alom et al [21].	2015	IDS	DBN	NSL-KDD	Accuracy = 97.5%
Vinayakumar et al [22].	2017	IDS	CNN - RNN	KDD99	Accuracy = 99.99% Precision = 99.99% Recall = 99.99% F1-Score = 99.99%
Al-Yaseen et al [23].	2017	IDS	SVM - ELM	KDD99	2 classes : Accuracy = 95.75%
Sharafaldin et al [24].	2019	IDS	Id3 - RF - Naive Bayes - Logistic regression	CICDDoS2019	F1-Score : 69 %
Hamouda et al [10].	2020	IDS	CNN – DNN - RNN	CICDDoS2019	13 classes : Precision = 71% Recall = 62% F1-Score = 56%
Farage et al [25].	2021	IDS	CNN - DNN - RNN	TON_IoT CICDDoS2019	CNN : Accuracy = 95 % RNN : Accuracy = 94 % DNN : Accuracy = 94 %
Mittal M et al [26].	2022	IDS	DNN - LSTM	CICIDS2017	Classification binaire : Accuracy = 98.72%

Tableau 2 - Travaux antérieurs connexes pour la détection d'attaques

Conclusion

Des différentes approches et architectures d'apprentissage profond ont été appliquées à la détection d'intrusions. Ces algorithmes de Deep Learning ont montré des performances variables en fonction des ensembles de données sélectionnés et des caractéristiques d'entrée utilisées. Il est important de noter que l'utilisation des mêmes approches et techniques d'apprentissage ne garantit pas toujours des résultats similaires pour différentes classes d'attaques potentielles. Il est donc essentiel de bien comprendre les caractéristiques des données et les types d'attaques ciblées pour sélectionner les approches de Deep Learning les plus appropriées pour la détection des intrusions. De plus, il existe toujours des défis à relever, notamment la disponibilité et la qualité des données, la complexité et la sophistication des attaques, ainsi que l'interprétabilité des modèles de Deep Learning. Ainsi, il est essentiel de continuer à explorer et à développer de nouvelles approches et techniques d'apprentissage profond pour améliorer la détection des intrusions.

Chapitre 3

Proposition d'architecture Réseau et Système détection des attaques

Chapitre 3 : Proposition d'architecture Réseau et Système détection des attaques

Introduction

Dans ce chapitre, nous allons explorer en détail le réseau de l'université de Tébessa et nous suggérons un système pour la détection des attaques. Dans la première partie, nous commençons par une présentation globale du réseau existant et de ses zones, ainsi que des critiques et suggestions sur l'infrastructure. Nous proposons ensuite une architecture réseau et système améliorée qui prend en compte les vulnérabilités et les risques potentiels. Dans la deuxième partie, nous examinons en détail les attaques DDoS et proposons un système de détection basé sur un modèle de Deep Neural network (DNN) pour détecter ces attaques. Nous présentons également les résultats et les comparons avec les travaux connexes.

Partie I : Présentation de l'architecture existante et proposition des solutions

1. Présentation globale du réseau

Le réseau informatique de l'université de Tebessa est constitué de trois zones, sa topologie physique est en étoile étendue (Figure 6), chaque zone à l'architecture d'un arbre, et qui est connectée au backbone (zone 1).

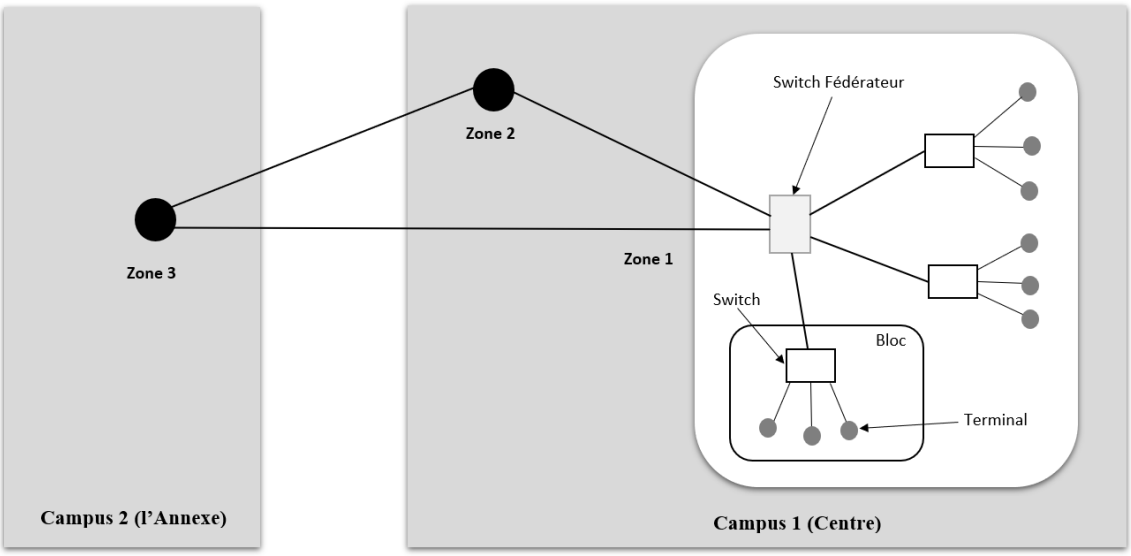


Figure 6 - La topologie physique du réseau local de L'université de Tebessa.

Choisir le Campus 1 (Centre) comme le plus important, car il comporte deux zones, en particulier la zone 1 car il contient le centre de calcul qui héberge la salle des administrateurs ainsi que tous les serveurs du réseau local. Le Campus 2 (l'Annexe) étant directement connecté au Campus 1 (Centre) via la fibre optique.

Chaque zone regroupe des blocs proches les uns des autres en termes physique, en d'autres termes, constitués de blocs avoisinants et ce de la manière suivante :

Zone 1 :

- Centre de calcul (CSRTED) Partie 1
- Laboratoire de l'informatique Partie 1
- Laboratoire de télécommunication.

Zone 2 :

- Centre de calcul (CSRTED) Partie 2
- Laboratoire de l'informatique Partie 2
- Laboratoire de Chimie et Electronique.
- Bureaux des Enseignants.
- Bloc 1.
- Bloc2.
- Bloc3.
- Bloc4.
- Bloc5.
- Bloc6.
- Rectorat
- Vice Rectorat
- Auditorium
- Institut Des Mines
- Faculté Science Et Technologie.
- Département Génie Civil
- Bibliothèque Centrale
- Bibliothèque Des Mines

Tout cela est illustré par le schéma de la Figure 7 :

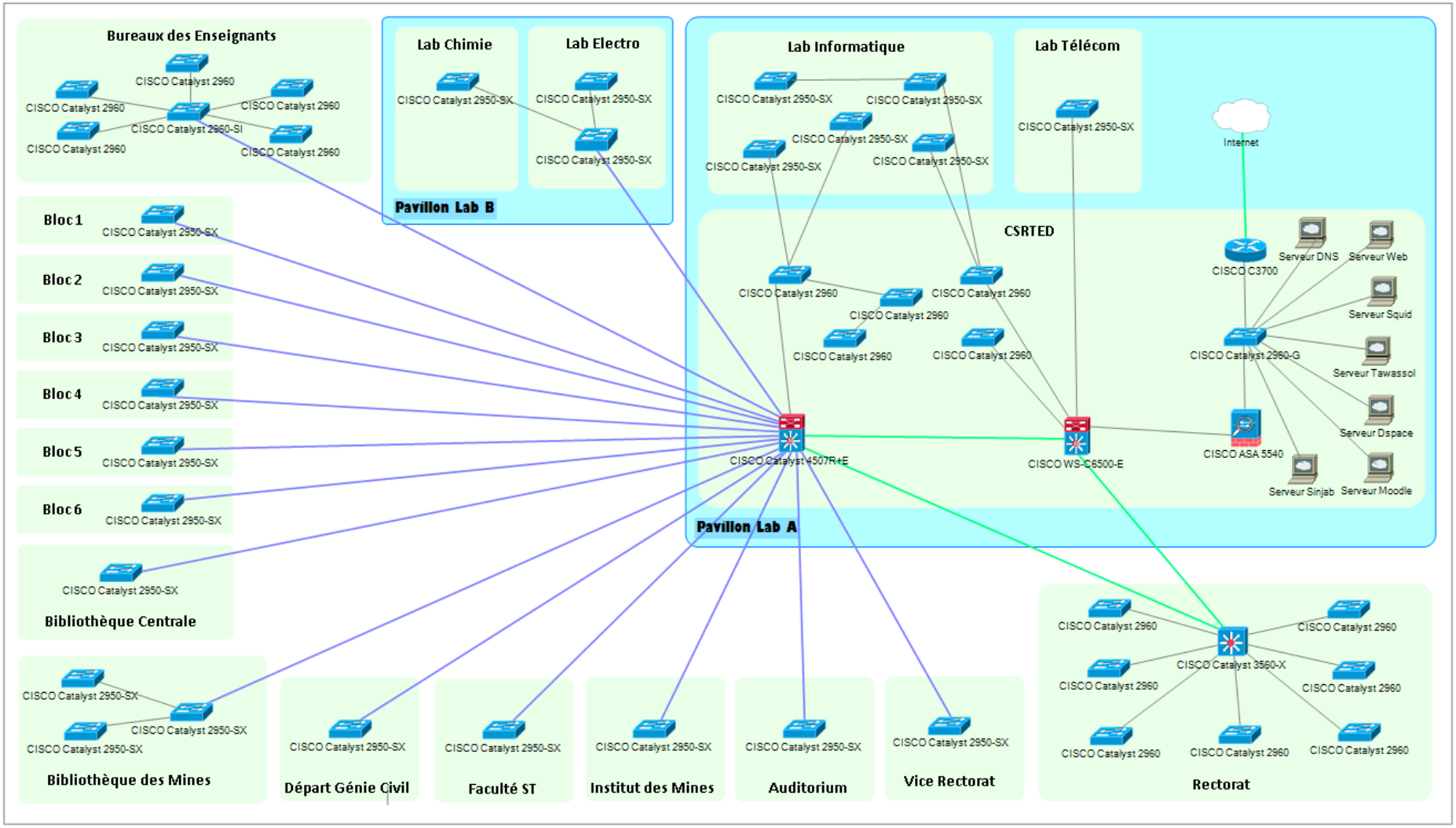


Figure 7 - Architecture Réseau Existante de Campus 1

2. Description détaillée des Zones

Le choix de la zone 1 comme étant le backbone (épine dorsale en anglais) est justifié par le fait de la présence du centre de calcul qui héberge la salle des administrateurs ainsi que tous les serveurs du réseau local.

Dans cette partie nous allons décrire les zones :

2.1. Description du Zone 1 (Backbone)

Description du backbone (Zone 1) La zone 1 est le backbone du réseau, elle permet la connexion en amont vers l'extérieur car c'est à ce niveau que se trouve le routeur, on trouve aussi le pare-feu qui se charge de filtrer les paquets entrants. Ce système de pare-feu permet aussi le routage inter-LAN car l'une de ces interfaces est reliée directement à un switch fédérateur et que ce dernier offre une liaison vers la zone 3, un autre vers la zone 2, comme l'illustre la Figure 8.

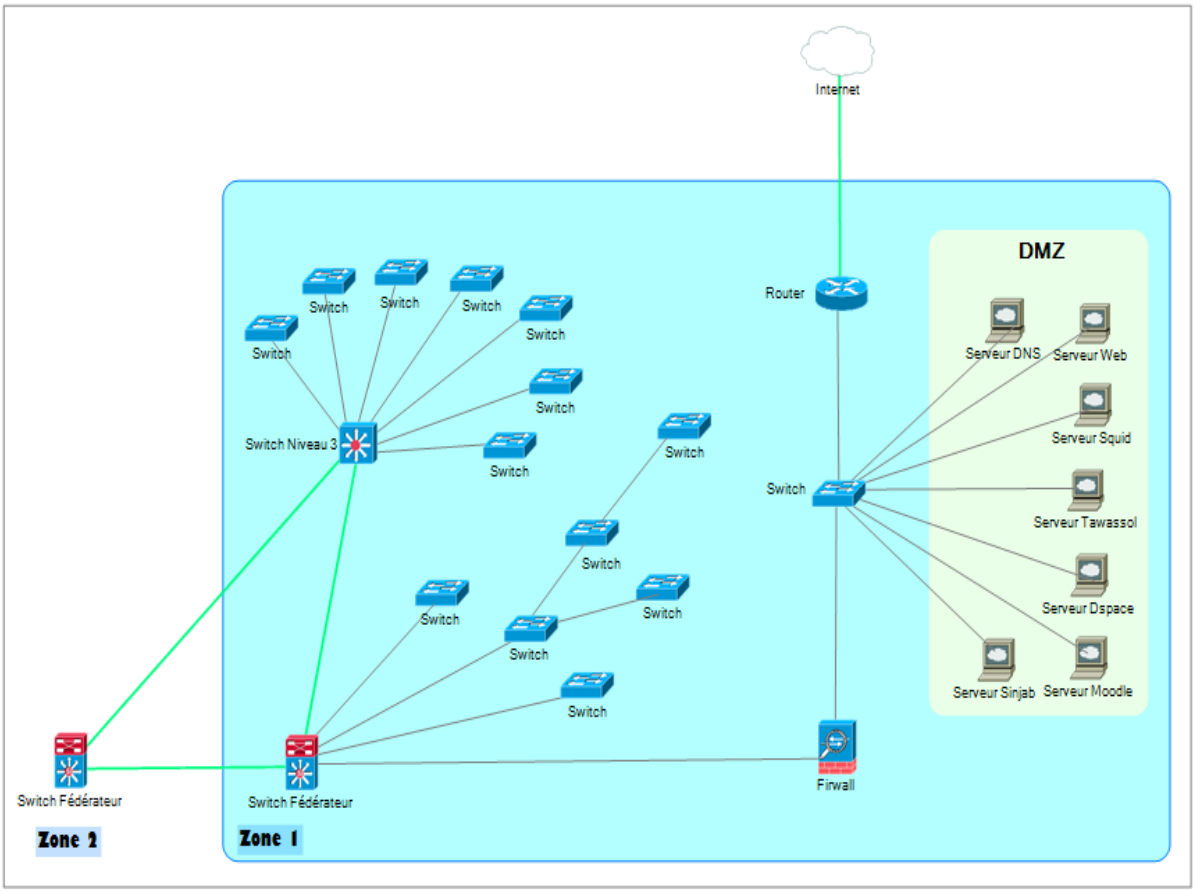


Figure 8 - Description de la Zone 1 (backbone)

2.2. Description du Zone 2

La Zone 2 contient un Switch fédérateur qui relie les switchs a distants avec fibre optique multimode et les switchs à proximité avec câble cuivre. Ce switch fédérateur est lié à l'autre Switch fédérateur de la Zone 1 et switch niveau 3 par fibre optique monomode. Comme l'illustre la Figure 9.

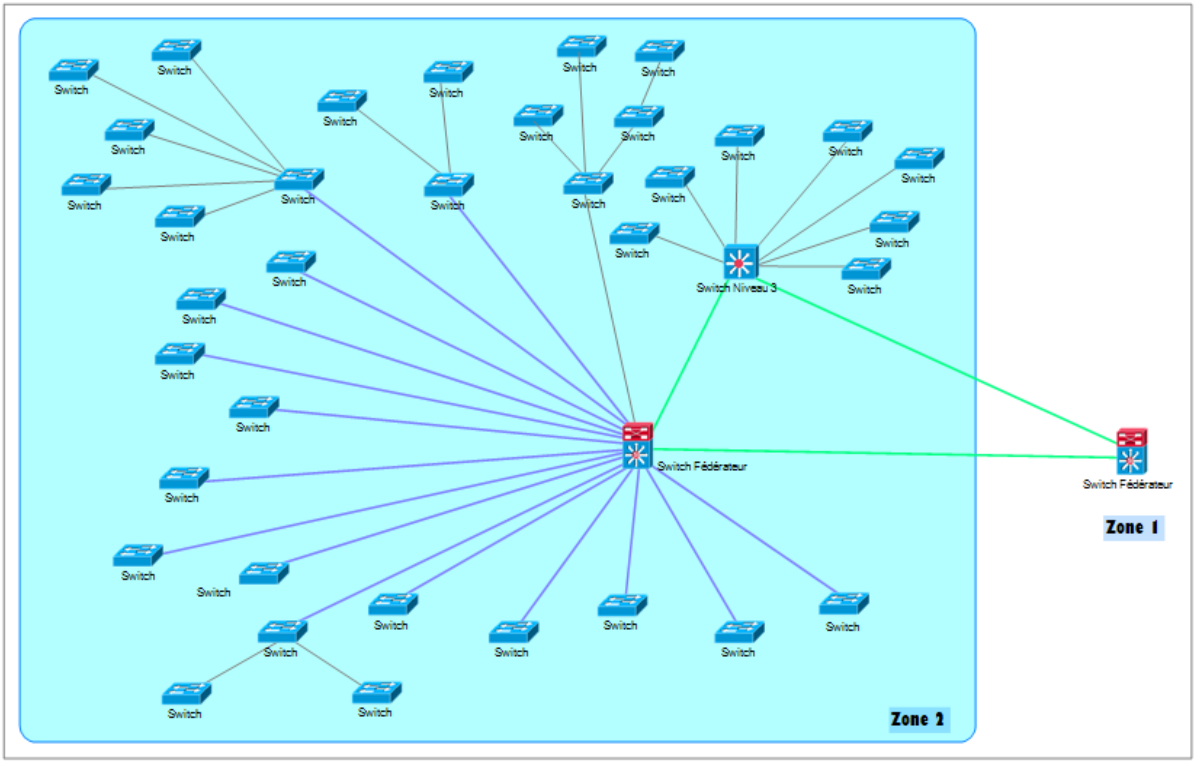


Figure 9 - Description de la Zone 2

3. Critique et suggestion sur le réseau

Il existe de nombreuses critiques de ce réseau actuel, et pour cela nous citerons les plus importantes et mentionnerons les suggestions.

3.1. DMZ

La création d'une zone démilitarisée (DMZ) est une étape cruciale pour améliorer la sécurité du réseau. La DMZ est une zone intermédiaire entre le réseau local (LAN) et l'Internet, où les serveurs publics sont placés. Elle agit comme une barrière de protection pour empêcher les accès directs depuis l'Internet vers le LAN, minimisant ainsi les risques de compromission du réseau interne.

3.2. IDS/IPS

La présence d'un système de Détection et Prévention d'Intrusions (N-IDS/IPS) est essentielle pour détecter et prévenir les actes malveillants ou les comportements anormaux sur les principaux liens du réseau, notamment du LAN vers la DMZ ou vers l'extérieur, ainsi que de l'extérieur vers la DMZ. Cependant, intégrer le N-IDS/IPS en tant que module dans le pare-feu actuel pourrait surcharger davantage ce dernier. Il serait donc préférable de le mettre en place en tant que module distinct afin de soulager la charge sur le pare-feu.

3.3. VLANs

La configuration de VLANs (Virtual Local Area Networks) peut être bénéfique pour améliorer la sécurité et la gestion du réseau. Les VLANs permettent de segmenter le réseau en sous-réseaux virtuels, isolant ainsi les différents types de trafic et limitant la visibilité et l'accès aux autres parties du réseau.

3.4. Serveur d'Antivirus

Il faut noter que le firewall ne protège pas très bien des virus. Beaucoup de manières permettent de coder des fichiers pour les transférer. En d'autres termes, un firewall ne peut pas remplacer l'attention et la conscience des utilisateurs qui doivent respecter un certain nombre de règles pour éviter les problèmes., notamment par le biais de fichiers attachés à des e-mails ou par des supports de stockage. Il est donc important de mettre en place des mesures globales et efficaces pour lutter contre les virus dans un réseau, notamment en s'assurant que chaque poste de travail dispose d'un antivirus à jour.

La mise en place d'un serveur d'antivirus centralisé peut être une étape importante dans cette lutte, car il permet de bloquer les messages infectés par des virus ou indésirables sur le serveur avant qu'ils n'atteignent les machines des utilisateurs finaux. Cela peut également permettre d'envoyer des notifications à l'administrateur du réseau et au destinataire lorsqu'un message a été bloqué, ce qui facilite la gestion de la sécurité antivirus.

Dans un réseau universitaire avec un effectif croissant et varié, il peut être difficile de faire respecter des règles strictes de sécurité, telles que ne jamais ouvrir un fichier attaché à un e-mail sans en vérifier la provenance. Par conséquent, il est essentiel de mettre en place des

mesures techniques telles qu'un serveur d'antivirus centralisé pour renforcer la sécurité du réseau et minimiser les risques liés aux virus et autres malwares.

Cependant, il est également important de sensibiliser les utilisateurs aux bonnes pratiques de sécurité, notamment en matière d'ouverture de fichiers ou de gestion des supports de stockage. La vigilance et la conscientisation des utilisateurs restent des éléments clés dans la prévention des infections par des virus. En combinant des mesures techniques et des bonnes pratiques de sécurité des utilisateurs, il est possible de mieux protéger le réseau contre les virus et autres menaces.

3.5. VPN pour les accès distants

La mise en place d'un réseau privé virtuel (VPN) pour les accès distants à l'université est une mesure de sécurité importante. Elle permet aux membres de centre d'accéder aux ressources internes du réseau depuis des emplacements extérieurs de manière sécurisée. Le VPN utilise des protocoles de sécurité pour crypter les données qui sont échangées entre le client distant et le réseau interne de l'université, ce qui assure une protection contre l'interception ou la modification non autorisée des données. De plus, l'authentification des utilisateurs est généralement requise avant d'accéder au réseau via le VPN, ce qui renforce la sécurité en empêchant l'accès non autorisé.

4. Architecture proposée

Après ces quelques critiques et suggestions sur le réseau actuel, nous proposons la nouvelle architecture qui est représentée dans la Figure 10 Et Proposition de partitionner et nommer les VLANs dans le Tableau 3.

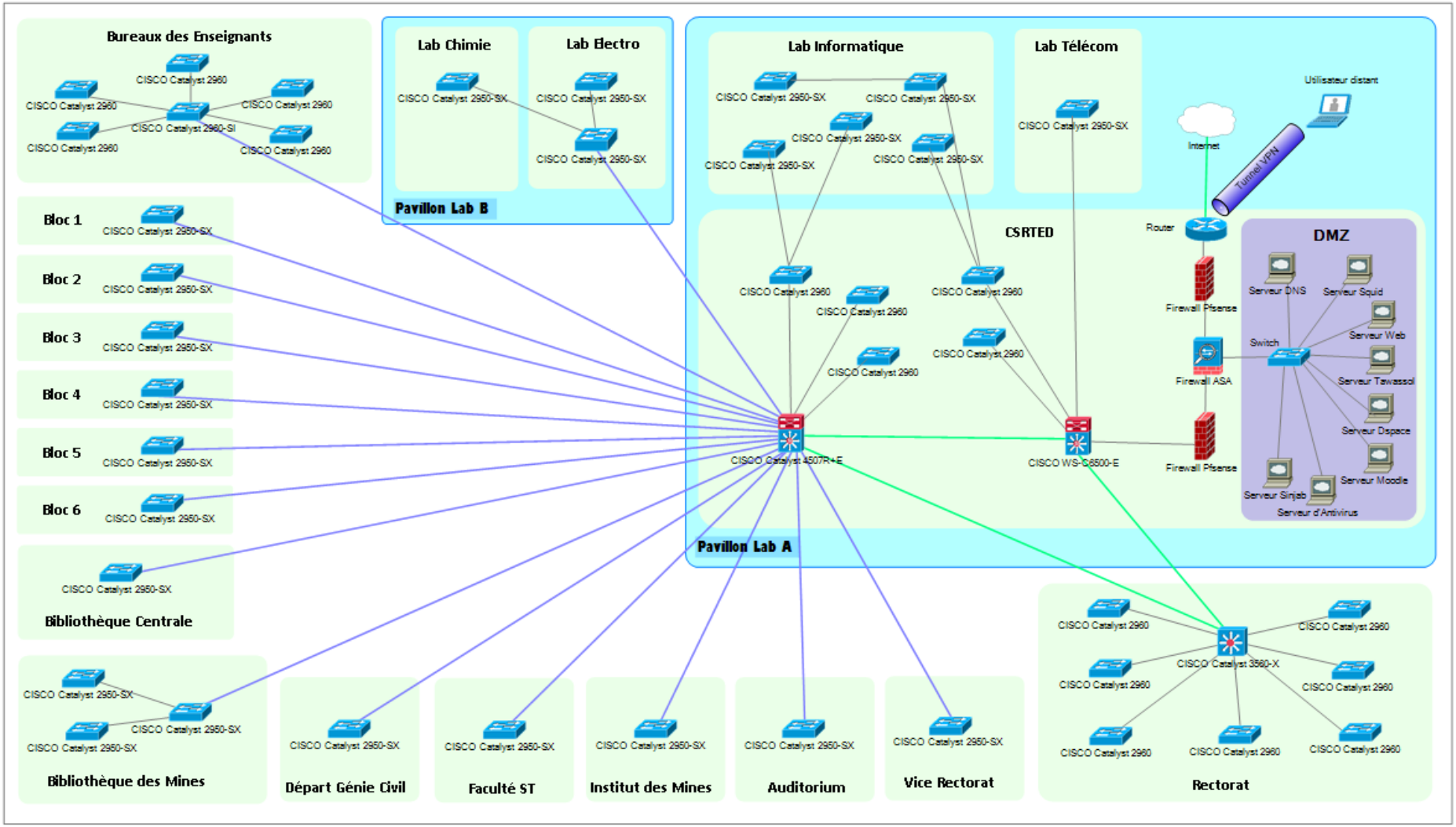


Figure 10 - Schéma de la Nouvelle Architecture Possible.

N° VLAN	Service(s)	Nombre de Switch
10	CSRTED	5
20	Laboratoire de l'informatique	5
30	Laboratoire de Chimie	1
40	Laboratoire Electronique.	2
50	Les Blocs	6
60	Bureaux des Enseignants.	6
70	Rectorat	7
80	Vice Rectorat	1
90	Institut Des Mines	1
100	Département Génie Civil	1
110	Bibliothèque Centrale	1
120	Bibliothèque Des Mines	3
130	Faculté Science Et Technologie.	1
140	Auditorium	1
150	Les caméras de surveillance IP	….

Tableau 3 - Proposition de partitionner et nommer les VLANs

Cette étude du réseau de notre université nous a permis de mieux comprendre son architecture et de concrétiser nos connaissances accumulées jusqu'à présent. En effet, grâce à cette étude, nous avons pu émettre des critiques sur l'architecture existante, suggérer quelques solutions et proposer une nouvelle architecture pour le réseau. Il est vrai qu'une bonne proposition pourrait nécessiter le renouvellement du matériel existant et représenter un investissement financier important. Cependant, cette nouvelle proposition d'architecture offre sans aucun doute une meilleure sécurité et une plus grande flexibilité du réseau en utilisant les capacités disponibles dans le centre.

Partie II : Un système de détection des attaques dans le Réseau

1. Dataset

L'ensemble de données choisi pour cette étude c'est CIC-DDoS-2019 data-set, fourni par l'Institut canadien de cybersécurité (CIC) [19]. Il rassemble des informations sur les flux réseau réels tout en utilisant certaines des attaques DDoS les plus récentes et les plus connues. Chaque point de données (ou flux réseau) dans ces formats plus condensés, qui transportent principalement des métadonnées sur les connexions réseau et excluent la charge utile, rassemble tous les paquets qui partagent un ensemble particulier de fonctionnalités dans un intervalle de temps donné. L'ensemble de données comporte deux versions de données, des données PCAP bruts et des données CSVs Les auteurs sont utilisées l'analyseur du trafic CICFlowMeter-V3 pour extraire plus 80 caractéristiques depuis les fichiers PCAPs et les résultats ont été sauvegardé dans des fichiers CSVs structurés et étiquetés par l'Université de New Brunswick [24].

L'ensemble de données comprend deux sous-ensembles, le premier ensemble de données de 7 attaques (03-11-2019) et le deuxième ensemble de données de 12 attaques (01-12-2019).

1.1. Dataset 7 Attaques (03- 11-2019)

L'ensemble de données contenait 7 attaques DDOS différentes et à jour (LDAP , MSSQL , NetBIOS , Portmap , UDPLag , UDP , Syn). L'ensemble complet contient 19,750,116 enregistrements, dont 19,694,438 correspondent à des attaques DDoS, tandis que les 55,678 autres correspondent à un trafic réseau bénin (légitime/normale).

Les Attaques	Nombre des Instances
Syn	4,284,751
UDPLag	721,097
LDAP	2,108,110
MSSQL	5,159,870
NETBIOS	3,454,578
Portmap	186,960
UDP	3,779,072
Total	**19,694,438**

Tableau 4 - Le nombre des instances pour chaque attaque dans Dataset 7 Attaques

1.2. Dataset 12 Attaques (01- 12-2019)

L'ensemble de données en question contient 12 attaques DDoS différentes, et constitue la version la plus récente disponible. L'ensemble complet contient 50,063,112 enregistrements, dont 50,006,249 correspondent à des attaques DDoS, tandis que les 56,863 autres correspondent à un trafic réseau bénin (légitime/normale). Ce dataset comporte également 86 caractéristiques (Features), dont 6 sont étiquetées et caractérisent le flux lui-même en fonction de **Source IP**, **Source Port**, **Destination IP**, **Destination Port**, **Protocole** et **Timestamp** (temps d'attaques), ainsi que plus de 80 autres caractéristiques relatives au trafic réseau.

Les Attaques	Nombre des Instances
DNS	5,071,011
LDAP	2,179,930
MSSQL	4,522,492
NetBIOS	4,093,279
NTP	1,202,642
SNMP	5,159,870
SSDP	2,610,611
SYN	1,582,289
TFTP	20,082,580
UDP	3,134,645
UDP-Lag	366,461
WebDDoS	439
Total	**50,006,249**

Tableau 5 - Le nombre des instances pour chaque attaque dans Dataset 12 Attaques

2. Taxonomie des attaques DDoSs

Le déni de service distribué (DDoS) est une attaque intrusive qui consiste en l'envoi d'une grande quantité de paquets vers une ressource cible dans le but de perturber temporairement ou définitivement les services fournis par cette ressource. Les auteurs ont proposé une taxonomie de ces attaques, divisée en deux grandes catégories : les attaques par réflexion et les attaques par exploitation [24].

- **Les attaques DDoS par réflexion :** consistent à dissimuler l'identité de l'attaquant en utilisant des botnets pour envoyer des requêtes (par exemple des requêtes HTTP) à la victime via des serveurs réflecteurs. L'adresse IP source de l'attaquant est définie comme

l'adresse IP cible afin de submerger la victime avec des paquets de réponse. Ces attaques sont réalisées en utilisant les protocoles de la couche transport, tels que le protocole de contrôle de transmission (TCP), le protocole de datagramme utilisateur (UDP) ou une combinaison de ces protocoles [24].

- **Les attaques DDoS par exploitation :** consistent à tenter d'exploiter directement le service distant. Ces attaques peuvent être menées en utilisant les protocoles de la couche transport TCP ou UDP.

Une classification de ces attaques DDoS est basée sur ces catégories, ainsi que sur les protocoles réseau utilisés, comme illustré dans la Figure 11.

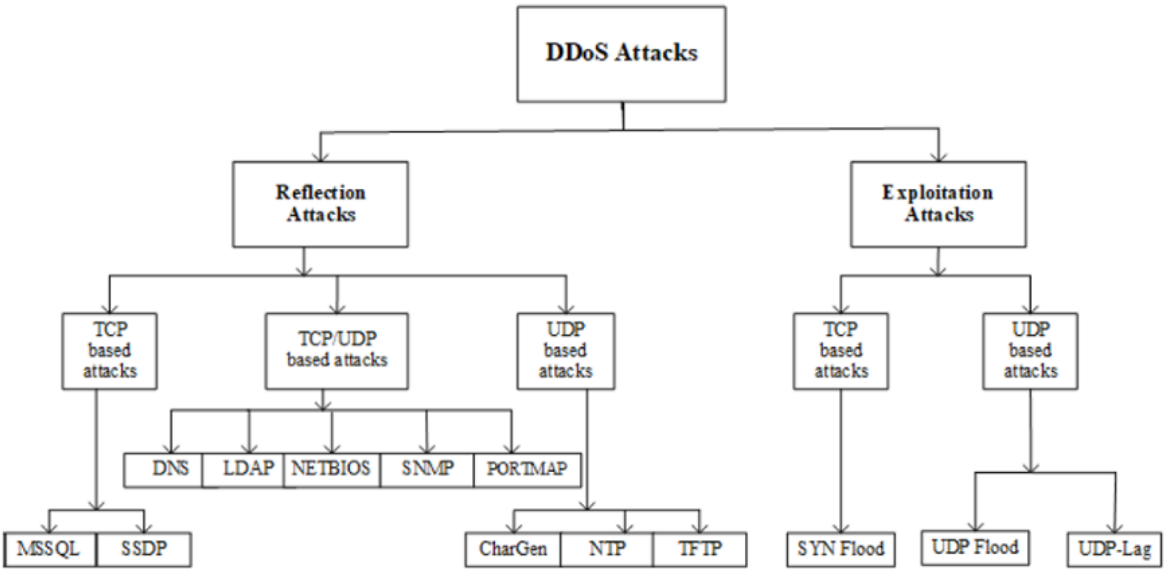


Figure 11 - Les attaques par réflexion et les attaques par l'exploitation *[24]*.

3. La préparation des données

Les performances des méthodes de Deep Learning dépendent fortement de la quantité et de la qualité des données d'apprentissage. Plus il y a de données de qualité, plus les résultats sont précis et bons. Dans notre cas, nous disposons d'une quantité de données suffisante.

Cependant, en raison du déséquilibre des classes de données, il est nécessaire de réduire ces données.

La préparation des données implique une opération essentielle est la réduction des données avant de les traiter.

3.1. La réduction des données

La masse de Dataset constitue de tailles plus de 22 Go dans le Dataset 12 Attaques et de taille plus de 8 Go dans le Dataset 7 Attaques. La lecture et la préparation des données n'étaient pas des taches faciles avec cette énorme quantité de données même lorsque on a travaillé sur un pc gamer qui offre 16 Go de RAM.

Le volume de l'ensemble de données nous oblige à faire réduire un nombre important des échantillons.

- **Dataset_7Attaques :** Se compose de 7 fichiers CSVs comportent que 8 classes dont 7 classes sont des attaques DDos et le 8 éme classe désigne le trafic normale (La classe BENIGN).

  Un échantillon d'apprentissage de 19,31 % a été prélevé sur le total dataset, et cet échantillon a été divisée (20 % pour le Test et 80 % pour le Validation) .

	N° Classes	**Les Classes concernés**	**Nombre d'instances pour l'apprentissage**	**Nombre d'instances pour le Test**
Dataset_7Attaques (8-Classes)	0	BENIGN	45,049	9,010
	1	LDAP	494,496	98,899
	2	MSSQL	489,558	97,912
	3	NETBIOS	854,581	170,916
	4	Portmap	90,148	18,030
	5	Syn	1,062,313	212,463
	6	UDP	776,078	155,216
	7	UDPLag	1,873	374
		Total	**3,814,096**	**762,820**

Tableau 6 - Sous ensembles_1 (Dataset_7attaques)

- **Dataset_12Attaques :** Se compose de 11 fichiers CSVs comportent que 13 classes dont 11 classes et le 12éme classe (WebDDoS qui n'existent pas dans les données de test ont été modifié aussi en Other classe) sont des attaques DDos et le 13éme classe désigne le trafic normale (La classe BENIGN).

Un échantillon d'apprentissage de 12,72 % a été prélevé sur le total dataset, et cet échantillon a été divisée (20 % pour le Test et 80 % pour le Validation) .

	N° Classes	Les Classes concernés	Nombre d'instances pour l'apprentissage	Nombre d'instances pour le Test
Dataset_12Attaques (13-Classes)	0	BENIGN	24,224	4,845
	1	DNS	188,975	37,795
	2	LDAP	780,828	156,166
	3	MSSQL	964,358	192,872
	4	NetBIOS	885,233	176,330
	5	NTP	881,648	177,047
	6	SNMP	495,288	99,058
	7	SSDP	196,148	39,229
	8	UDP	196,851	39,370
	9	Syn	790,597	158,119
	10	TFTP	782,322	156,464
	11	UDPLag	182,896	36,579
	12	WebDDoS	421	84
		Total	**6,369,789**	**1,273,958**

Tableau 7 - Sous ensembles_2 (Dataset_12attaques)

3.2. Les pré-traitements des données

Afin de construire un modèle très précis, il est important d'effectuer des analyses exploratoires sur l'ensemble de données et ses caractéristiques. Le pré-traitement de l'ensemble de données est effectué avant d'être appliqué au réseau neuronal profond. Les étapes de pré-traitement sont comme les suivantes :

- Tout d'abord, l'ensemble de données a été filtré pour supprimer toutes les lignes redondantes représentant les instances de classe. Ensuite, une analyse a été effectuée pour détecter toutes les valeurs "**NAN**" (Not A Number) ou "**INF**" (Infinite Value). Ces valeurs peuvent être considérées comme des valeurs manquantes et affectent négativement les performances des modèles finaux, car les algorithmes de Deep Learning ou de machine learning en général ont du mal à les traiter.
- Les statistiques descriptives résumant la dispersion et la distribution de l'ensemble de données ont révélé la présence de colonnes vides dont les valeurs sont toujours 0. Ces caractéristiques ne contiennent aucune information discriminatoire permettant de

différencier les classes d'attaque. Au contraire, elles peuvent conduire à de mauvais résultats. Les colonnes suivantes ont été identifiées comme vides et ont été supprimées : **"Bwd PSH Flags"**, **"Fwd URG Flags"**, **"Bwd URG Flags"**, **"FIN Flag Count"**, **"PSH Flag Count"**, **"ECE Flag Count"**, **"Fwd Avg Bytes/Bulk"**, **"Fwd Avg Packets/Bulk"**, **"Fwd Avg Bulk Rate"**, **"Bwd Avg Bytes/Bulk"**, **"Bwd Avg Packets/Bulk"** et **"Bwd Avg Bulk Rate"**.

- La colonne **Label**, qui indique la classe de chaque instance, a été encodée en utilisant une technique courante appelée **"One-Hot-Encoding"**. Cette technique convertit chaque catégorie en une colonne distincte avec une valeur de 1 si l'instance appartient à cette classe et 0 sinon.
- Avant de passer à l'apprentissage, la normalisation est une étape importante pour les données de qualité où chaque instance des classes fournit des informations pertinentes pour décrire sa classe. Cette étape a pour effet de réduire le taux d'apprentissage et de faciliter la convergence du modèle, tout en pouvant également avoir un effet de régularisation pour réduire l'erreur de généralisation.
- La **bibliothèque Scikit-learn** dispose également d'un algorithme pour traiter les ensembles de données déséquilibrés en définissant le paramètre **"class_weight"**.

4. Architecture de modèle

Dans ce travail, nous avons utilisé la méthode de réseau profond DNN et avons apporté plusieurs modifications pour améliorer les résultats.

- Tout d'abord, nous avons dimensionné les couches d'entrée en fonction du nombre d'entités (ou de "features") dans le vecteur d'entrée. Ensuite, nous avons choisi la fonction d'activation ReLU, qui a donné de meilleurs résultats que d'autres fonctions comme tanh et sigmoid.
- Les couches de sortie ont été dimensionnées en fonction du nombre de classes et nous avons utilisé la fonction d'activation **Softmax** pour la classification multicouche. Cette fonction attribue une probabilité à chaque sortie (dont la somme est égale à 1), ce qui nous a permis de sélectionner la catégorie ayant la plus grande probabilité et de faire correspondre cette catégorie à l'affinité attendue.

- Nous avons également utilisé la technique dropout pour éviter le sur-apprentissage. Cette technique consiste à désactiver un certain pourcentage de neurones dans le réseau afin de produire un modèle plus généralisable.
- En somme, ces différentes techniques ont permis d'améliorer les résultats de notre modèle de réseau profond DNN.

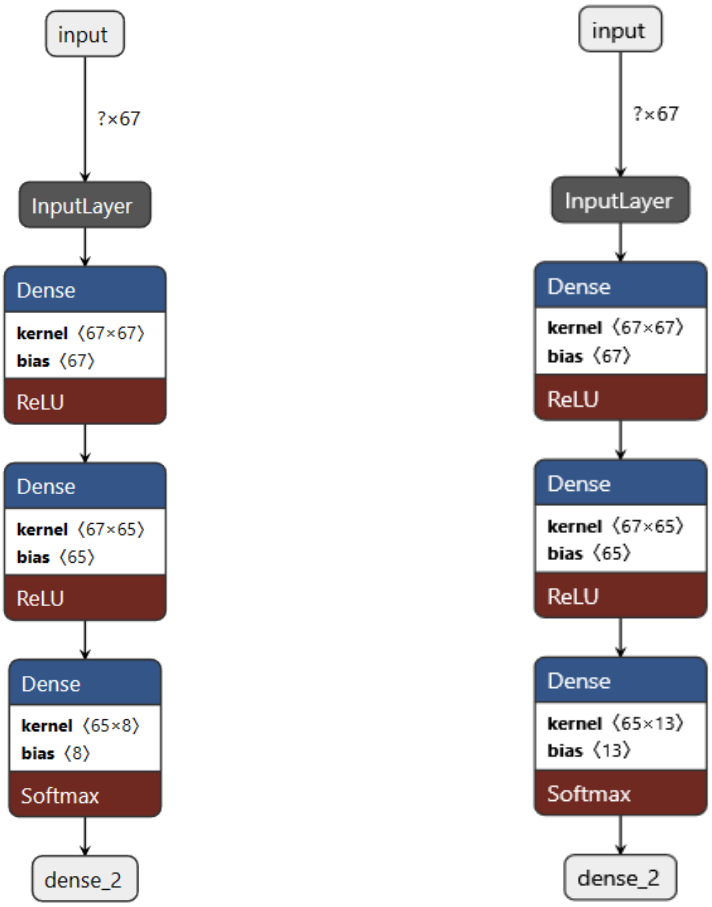


Figure 12 - L'architecture de modèle proposée pour les deux classifications

5. Un modèle de d'attaques basée sur Deep Neural network (DNN)

Le modèle DNN proposé à une architecture comprenant une seule couche, avec une couche d'entrée et une couche de sortie (Figure 12). Grâce à des couches cachées contenant un grand nombre de paramètres, le réseau DNN est capable d'extraire automatiquement des caractéristiques complexes à partir de données brutes, dans le but de déterminer les propriétés statistiques sous-jacentes des paquets normaux et des paquets correspondant à différentes attaques. L'ajout de couches cachées rend le modèle plus complexe, ce qui peut améliorer les résultats, mais peut également entraîner un sur-apprentissage. Après avoir ajusté les fonctions d'activation, le nombre d'échantillons par lot et la fonction d'optimisation, ce modèle a été entraîné sur 50 époques pour les deux classifications (8 classes et 13 classes).

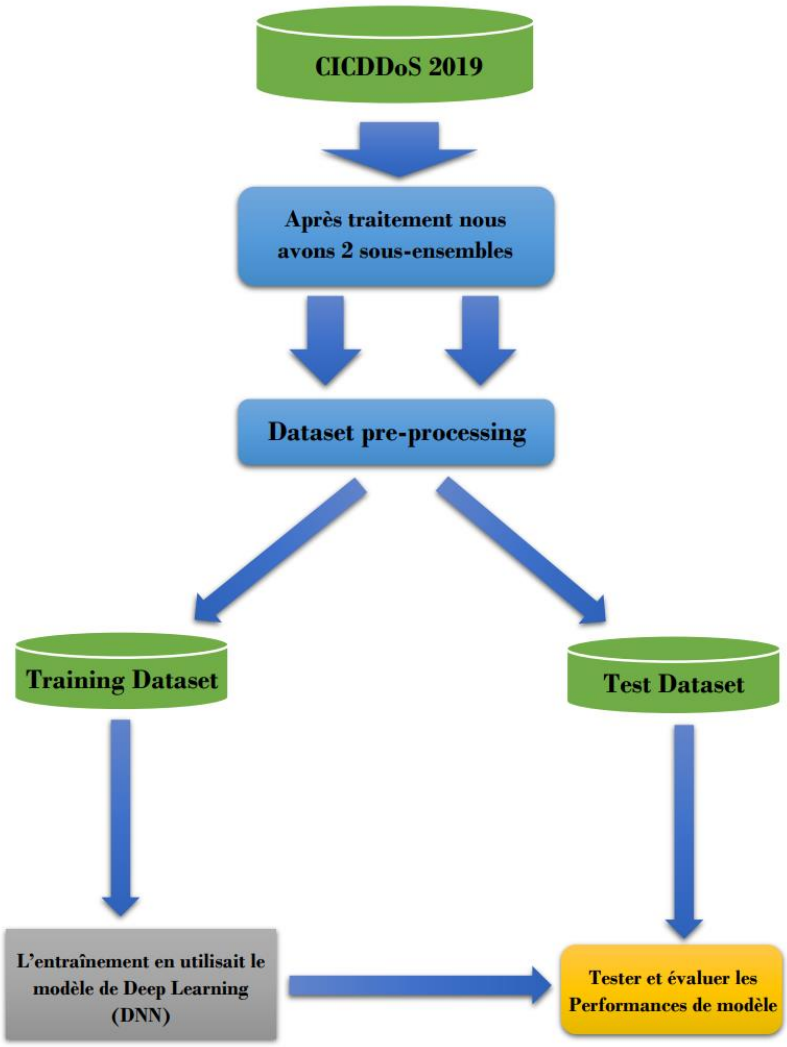


Figure 13 - Schéma conceptuel de notre méthode d'implémentation DL

6. Résultat et Discussion

Nous avons implémenté un modèle de Deep Learning DNN. Ce modèle a été formés et testés sur 2 sous-ensembles de données différentes du CICDDoS2019 Dataset.

6.1. Les mesures d'évaluation des modèles

Les mesures de performance de la classification courantes incluent :

- **Accuracy (précision) :** mesure la proportion de prédictions correctes par rapport à l'ensemble des prédictions. Elle est calculée en divisant le nombre de prédictions correctes par le nombre total de prédictions.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

- **Recall (rappel) :** mesure la capacité du modèle à identifier tous les exemples positifs. Elle est calculée en divisant le nombre de vrais positifs par la somme des vrais positifs et des faux négatifs.

$$Recall = \frac{TP}{TP + FN}$$

- **Precision (précision) :** mesure la proportion de prédictions positives correctes par rapport à l'ensemble des prédictions positives. Elle est calculée en divisant le nombre de vrais positifs par la somme des vrais positifs et des faux positifs.

$$Precision = \frac{TP}{TP + FP}$$

- **F1 score :** mesure la précision et le rappel d'un modèle en combinant ces deux mesures en une seule valeur. Elle est calculée en prenant la moyenne harmonique de la précision et du rappel.

$$F1\ Score = 2\ \times \frac{Recall \times Precision}{Recall +\ Precision}$$

- **La matrice de confusion :** mesure de performance de la classification qui permet de visualiser les prédictions correctes et incorrectes d'un modèle. Elle est représentée sous la forme d'une matrice où les lignes représentent les classes réelles et les colonnes représentent les classes prédites. La matrice de confusion est divisée en quatre parties :

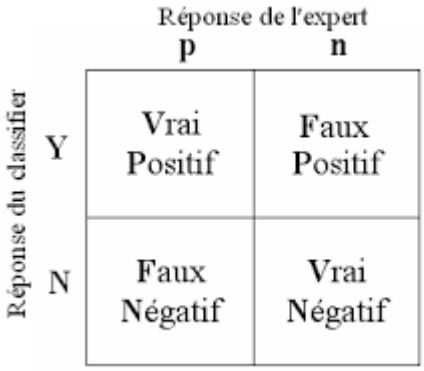


Figure 14 - Matrice de confusion

- **Vrais positifs (True positives) :** les exemples qui ont été correctement identifiés comme appartenant à la classe positive.
- **Faux positifs (False positives) :** les exemples qui ont été incorrectement identifiés comme appartenant à la classe positive.
- **Vrais négatifs (True negatives) :** les exemples qui ont été correctement identifiés comme n'appartenant pas à la classe positive.
- **Faux négatifs (False negatives) :** les exemples qui ont été incorrectement identifiés comme n'appartenant pas à la classe positive.

Ces mesures sont souvent utilisées pour évaluer les performances des modèles de classification.

6.2. Résultat

- **La première expérimentation (8-classes classifications) :** a été réalisée sur le sous-ensemble de données 1 (Tableau 6). Les modèles sont évalués directement sur l'ensemble de test. Le modèle est formé sur 50 époques. Cela signifie que ces modèles apprennent mieux et font de meilleures prédictions après chaque période d'amélioration (Figure 15). Les meilleurs résultats avec une précision 97%, le Tableau 8 montre le rapport de classification des attaques.

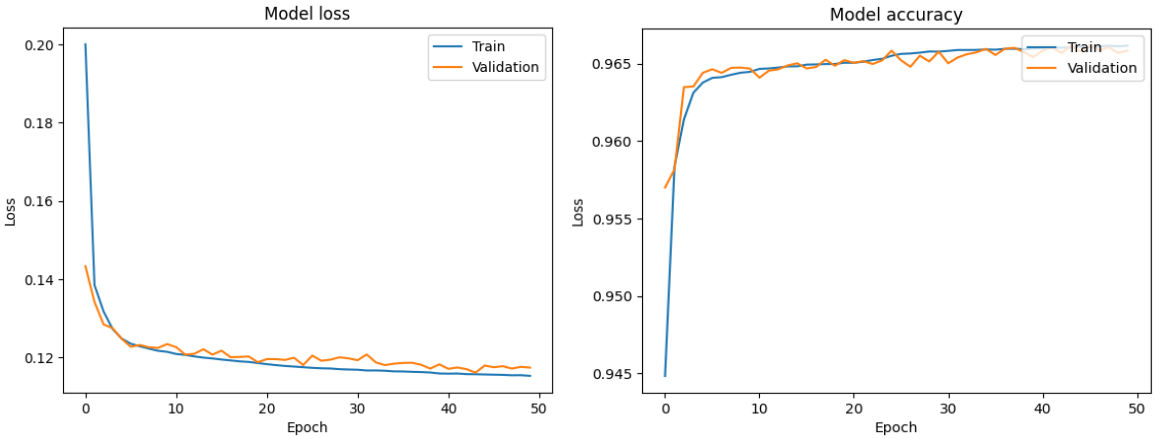


Figure 15 - L'exactitude et le perte de modèle proposés (8-classes)

	precision	recall	f1-score	support
0	1.00	0.99	0.99	9010
1	0.98	0.99	0.98	98899
2	0.96	0.97	0.96	97912
3	0.91	1.00	0.95	170916
4	0.96	0.00	0.00	18030
5	1.00	1.00	1.00	212463
6	0.99	0.98	0.99	155216
7	0.59	0.26	0.36	374
accuracy			0.97	762820
macro avg	0.92	0.77	0.78	762820
weighted avg	0.97	0.97	0.95	762820

Tableau 8 - Le rapport de classification (8-classes)

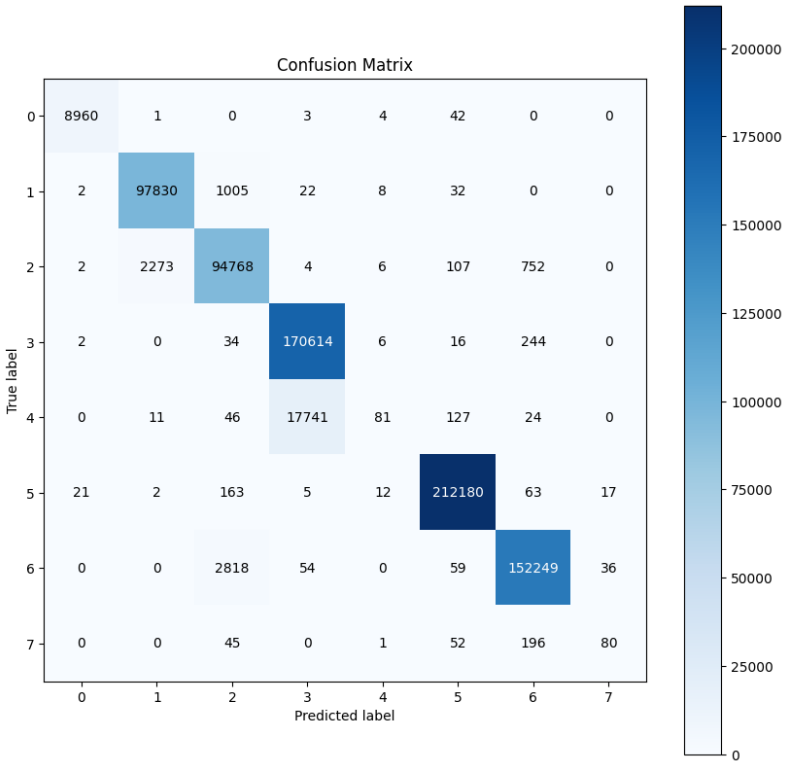


Figure 16 - Matrice de confusion (8-classes)

- **La deuxième expérimentation (13-classes classifications) :** a été réalisée sur le sous-ensemble de données 2 (Tableau 7). Les modèles sont évalués directement sur l'ensemble de test. Le modèle est formé sur 50 époques. Cela signifie que ces modèles apprennent mieux et font de meilleures prédictions après chaque période d'amélioration (Figure 17). Les meilleurs résultats avec une précision 81%, le Tableau 9 montre le rapport de classification des attaques.

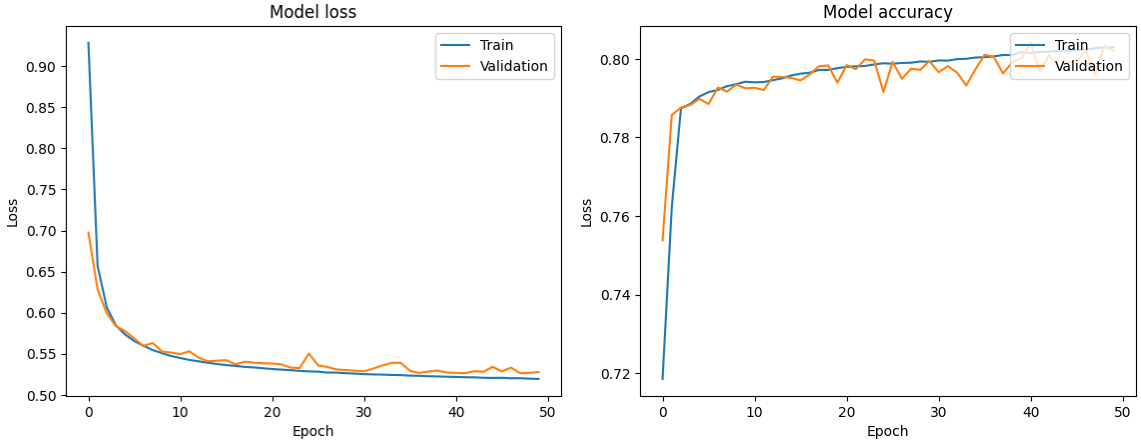


Figure 17 - L'exactitude et le perte de modèle proposés (13-classes)

	precision	recall	f1-score	support
0	0.98	0.99	0.99	4845
1	0.67	0.09	0.16	37795
2	0.65	0.96	0.77	156166
3	0.89	0.92	0.91	192872
4	0.97	0.96	0.97	176330
5	0.78	0.94	0.86	177047
6	0.58	0.15	0.24	99058
7	0.53	0.23	0.32	39229
8	0.50	0.78	0.61	39370
9	0.79	1.00	0.88	158119
10	0.99	0.83	0.90	156464
11	0.95	0.31	0.46	36579
12	0.00	0.00	0.00	84
accuracy			0.81	1273958
macro avg	0.71	0.63	0.62	1273958
weighted avg	0.81	0.81	0.77	1273958

Tableau 9 - Le rapport de classification (13-classes)

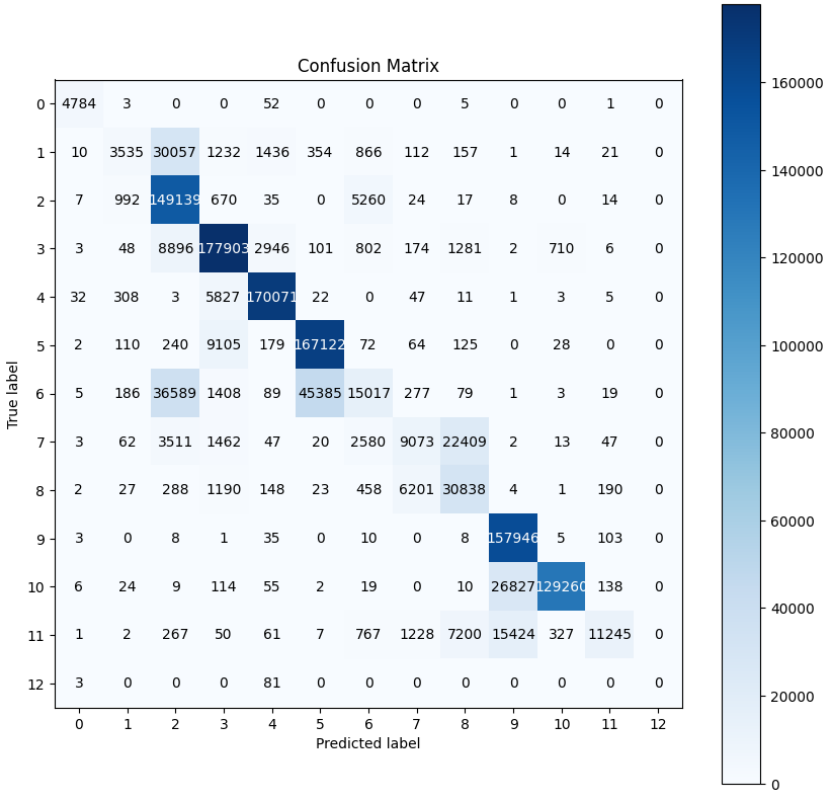


Figure 18 - Matrice de confusion (13-classes)

Les résultats pourraient être améliorés si l'environnement de travail était optimal. En effet, nous avons rencontré des difficultés pour distinguer certains types d'attaques qui présentent des caractéristiques similaires, comme l'attaque SSDP et l'attaque SNMP, ainsi que Portmap et UDP. Même les administrateurs réseau ont des difficultés à les différencier. De plus, il est impossible de modifier les propriétés d'attaque, ce qui peut annuler les bons résultats obtenus en manipulant les propriétés du modèle.

6.3. Comparaison entre nos résultats et les travaux connexe

Nous avons comparé nos résultats finals avec les résultats de l'article < *Un système de détection d'intrusion pour la* cybersécurité. > [10].

- D'après les premières observations, on a des bons résultats en comparaison avec l'article de comparaison.
- Notre modèle de 8 classes a un très bon résultat avec un accuracy 97 % et F1-score de 95%, et un recall de 97% et précision de 97%.
- Notre modèle de 13 classes a un très bon résultat avec un accuracy 81 % et F1-score de 77%, et un recall de 81% et précision de 81%.

Le tableau suivant montre les différents résultats obtenus :

		Nos Rrésultats	**Article**
8-Classes	Accuracy	97 %	Indisponible
	Precision	**97 %**	85 %
	Recall	**97 %**	83 %
	F1-Score	**95 %**	82 %
13-Classes	Accuracy	81 %	Indisponible
	Precision	**81 %**	71 %
	Recall	**81 %**	62 %
	F1-Score	**77 %**	56 %

Tableau 10 - Comparaison entre nos résultats et les résultats d'autre article *[10]*

Conclusion

Dans ce chapitre, nous avons proposé une architecture améliorée pour la détection des attaques dans le réseau. Nous avons commencé par une présentation détaillée du réseau existant, de ses zones et des critiques et suggestions sur l'infrastructure. Nous avons ensuite proposé une architecture réseau et système améliorée qui prend en compte les vulnérabilités et les risques potentiels. Dans la deuxième partie, nous avons examiné en détail les attaques DDoS et proposé un système de détection basé sur un modèle de Deep Neural network (DNN) pour détecter ces attaques. Les résultats ont montré que notre système de détection a une précision élevée pour détecter les attaques DDoS. Dans le chapitre suivant, nous allons intégrer le système proposé et évaluer ses performances en temps réel.

Chapitre 4

Présentation de l'environnement de développement et simulation

Chapitre 4 : Présentation de l'environnement de développement et simulation

Introduction

Le présent chapitre vise à présenter en détail l'environnement de développement et de simulation utilisé dans le cadre de cette étude. Nous allons vous expliquer les différents logiciels utilisés tels que VMware Workstation, GNS3 et PFSENSE, et expliquerons comment ils ont été intégrés pour créer un environnement propice à nos expérimentations. Ensuite, nous aborderons l'installation et la configuration basique de PfSense sous VMware. Nous détaillerons les étapes nécessaires pour installer PfSense, ainsi que les configurations de base requises pour son bon fonctionnement. De plus, nous discuterons de l'installation du package API dans PfSense, qui nous permettra d'intégrer un modèle de détection dans un script. Enfin, nous explorerons en détail le modèle de détection dans un script et son intégration dans PfSense. Nous présenterons les résultats de nos expérimentations et entamerons une discussion approfondie sur ces résultats.

1. Description de l'environnement de travail

Dans ce travail les logiciels utilisés Sont :

- VMware Workstation 15.5 Pro
- GNS3 2.2.21
- PfSense 2.6.0

1.1. VMware Workstation 15.5 Pro

Figure 19 - Logo de VMWARE WORKSTATION 15.5 PRO *[27]*

VMware Workstation 15.5 Pro est un logiciel de virtualisation populaire développé par VMware Inc. Il permet aux utilisateurs d'exécuter plusieurs systèmes d'exploitation sur un seul ordinateur en créant des machines virtuelles (VM). Ces VM peuvent être utilisées pour exécuter différents systèmes d'exploitation tels que Windows, Linux, MacOs, et bien d'autres, simultanément sur une seule machine physique.

Fonctionnalités clés de VMware Workstation 15.5 Pro :

- **Support de plusieurs systèmes d'exploitation :** Il prend en charge un large éventail de systèmes d'exploitation, y compris Windows, Linux, MacOs, et plus encore. Les utilisateurs peuvent créer et exécuter des VM avec différents systèmes d'exploitation sur la même machine hôte.
- **Plateforme de virtualisation puissante :** VMware Workstation fournit une plateforme de virtualisation robuste et stable, permettant aux utilisateurs d'exécuter des applications et des services gourmands en ressources au sein des machines virtuelles.
- **Instantanés et clonage :** Vous pouvez prendre des instantanés de vos machines virtuelles à différents moments, ce qui peut être utile pour les tests, le dépannage ou pour revenir à un état connu. De plus, vous pouvez cloner des VM existantes pour créer des duplicatas ou des modèles à utiliser ultérieurement.
- **Partage de VM :** VMware Workstation 15.5 Pro permet de partager facilement des machines virtuelles. Vous pouvez partager des VM avec des collègues ou les transférer vers d'autres ordinateurs exécutant VMware Workstation ou VMware Fusion.
- **Mode Unity :** Cette fonctionnalité vous permet d'intégrer les applications du système d'exploitation invité dans le bureau du système d'exploitation hôte, offrant ainsi une expérience fluide et facilitant le travail sur plusieurs systèmes d'exploitation.
- **Prise en charge de DirectX 10.1 et OpenGL 3.3 :** VMware Workstation 15.5 Pro offre une meilleure prise en charge des graphiques, permettant aux utilisateurs d'exécuter des applications et des jeux gourmands en graphismes au sein des machines virtuelles.
- **VM sécurisées :** Il propose diverses fonctionnalités de sécurité, notamment la prise en charge d'un module de plateforme sécurisée virtuel (TPM), d'un moteur de chiffrement virtuel et de technologies de sécurité basées sur la virtualisation (VBS) de Microsoft.

1.2. GNS3 2.2.21

Figure 20 - Logo GNS3 *[28]*

GNS3 2.2.21 est une version spécifique du logiciel de réseau virtuel GNS3, qui est une plateforme de simulation et de virtualisation utilisée par les professionnels des réseaux informatiques. GNS3 permet de créer des topologies de réseaux complexes en utilisant des machines virtuelles, des routeurs, des commutateurs et d'autres périphériques réseau virtuels.

Caractéristiques de GNS3 :

- **Simulation de réseaux :** GNS3 permet de simuler des réseaux complexes en utilisant des machines virtuelles, des routeurs, des commutateurs et d'autres équipements réseau virtuels. Cela permet aux professionnels des réseaux de tester et de déployer des configurations de réseau avant de les mettre en œuvre dans des environnements réels.
- **Intégration de périphériques réels :** GNS3 offre la possibilité d'intégrer des périphériques réels dans les topologies de réseau virtuel. Cela permet aux utilisateurs de connecter leurs propres routeurs ou commutateurs physiques à GNS3 et de les utiliser dans leurs simulations.
- **Large compatibilité :** GNS3 est compatible avec plusieurs systèmes d'exploitation, y compris Windows, Linux et macOS. Il prend également en charge diverses plateformes matérielles, ce qui permet aux utilisateurs de choisir la configuration matérielle la mieux adaptée à leurs besoins.
- **Bibliothèque d'appareils virtuels :** GNS3 propose une bibliothèque d'appareils virtuels préconfigurés, notamment des routeurs Cisco, des commutateurs Juniper, des pares-feux, etc. Ces appareils peuvent être facilement intégrés dans les topologies de réseau.

- **Interface graphique conviviale :** GNS3 offre une interface graphique intuitive qui facilite la création et la gestion des topologies de réseau virtuel. Les utilisateurs peuvent faire glisser et déposer des appareils virtuels sur une toile et les connecter ensemble pour former des réseaux virtuels complexes.
- **Prise en charge des images d'IOS :** GNS3 permet d'utiliser les images d'IOS (Internetwork Operating System) de Cisco pour émuler des routeurs Cisco dans les simulations. Cela offre aux utilisateurs une expérience plus réaliste et une compatibilité avec les configurations existantes.

1.3. PFSENSE 2.6.0

Figure 21 - Logo PfSense *[29]*

PfSense 2.6.0 est une version spécifique du système d'exploitation open source PfSense, qui est utilisé pour créer des pares-feux et des routeurs à source ouverte. PfSense offre une plateforme robuste et personnalisable pour sécuriser et gérer les réseaux informatiques.

Caractéristiques de PfSense :

- **Pare-feu avancé :** PfSense offre des fonctionnalités de pare-feu puissantes pour protéger les réseaux contre les menaces en ligne. Il prend en charge les règles de pare-feu, le filtrage d'adresse IP, le filtrage d'URL, la détection d'intrusion et bien plus encore.
- **Routage avancé :** PfSense permet de configurer des fonctionnalités de routage avancées, y compris la gestion de plusieurs interfaces réseau, le routage statique, le routage dynamique (RIP, OSPF, BGP), les tunnels VPN et la redirection de port.
- **VPN :** PfSense offre la possibilité de créer des connexions VPN sécurisées, notamment des VPN IPsec, OpenVPN et L2TP/IPsec. Cela permet aux utilisateurs de sécuriser les communications réseau et de se connecter de manière sécurisée à des réseaux distants.

- **Agrégation de liens et équilibrage de charge :** PfSense prend en charge l'agrégation de liens (bonding) pour combiner plusieurs connexions réseau physiques en une seule connexion logique. Il offre également des fonctionnalités d'équilibrage de charge pour optimiser l'utilisation de la bande passante.
- **Portail captif :** PfSense permet de créer des portails captifs pour fournir un accès Internet contrôlé aux utilisateurs. Cela peut être utile dans les environnements publics, tels que les hôtels, les cafés ou les entreprises offrant un accès Wi-Fi invité.
- **Reporting et surveillance :** PfSense offre des outils de surveillance et de génération de rapports pour visualiser et analyser le trafic réseau, les connexions VPN, les journaux de pare-feu et d'autres statistiques réseau.
- **Extensions et intégrations :** PfSense est extensible grâce à un système de packages qui permet d'ajouter des fonctionnalités supplémentaires, telles que des proxies web, des systèmes de détection d'intrusion (IDS/IPS), des serveurs de messagerie et bien d'autres.

2. Installation et Configuration basique de PfSense sous VMware

Pour mettre en place PfSense, il est recommandé de suivre l'architecture suivante :

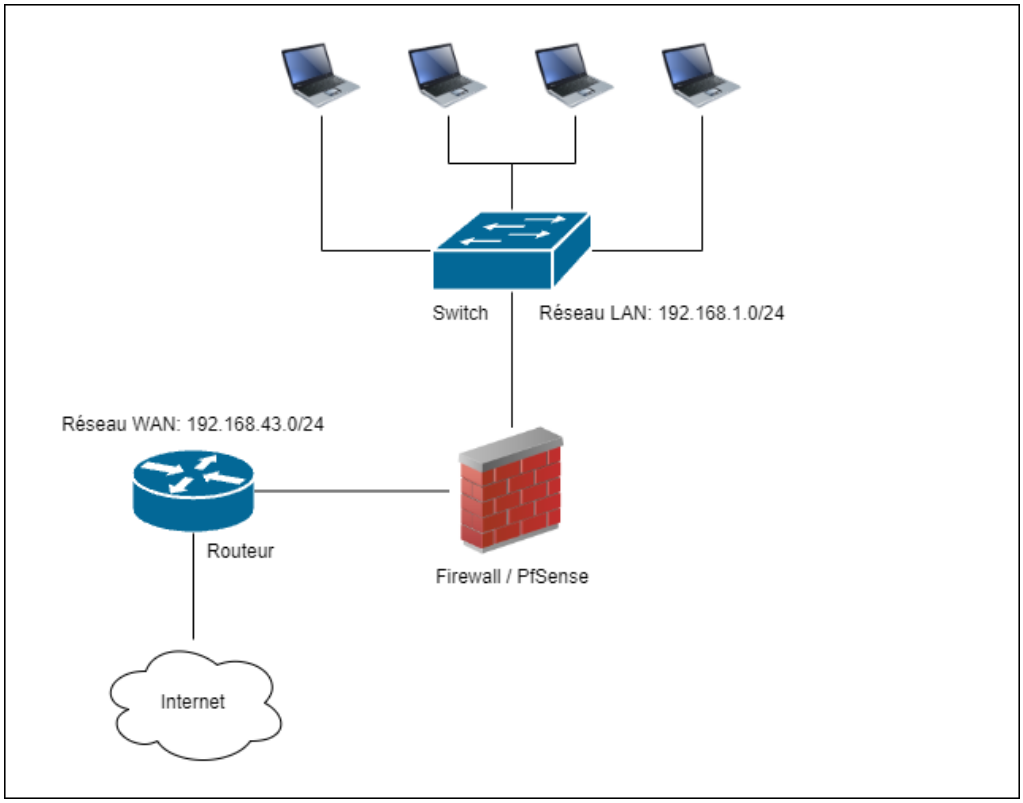


Figure 22 - Architecture réseau avec Firewall PfSense

2.1. Installation de PfSense

- Création d'une machine virtuelle :

  On crée une Machine Virtuelle sous VMware avec les spécifications suivantes :

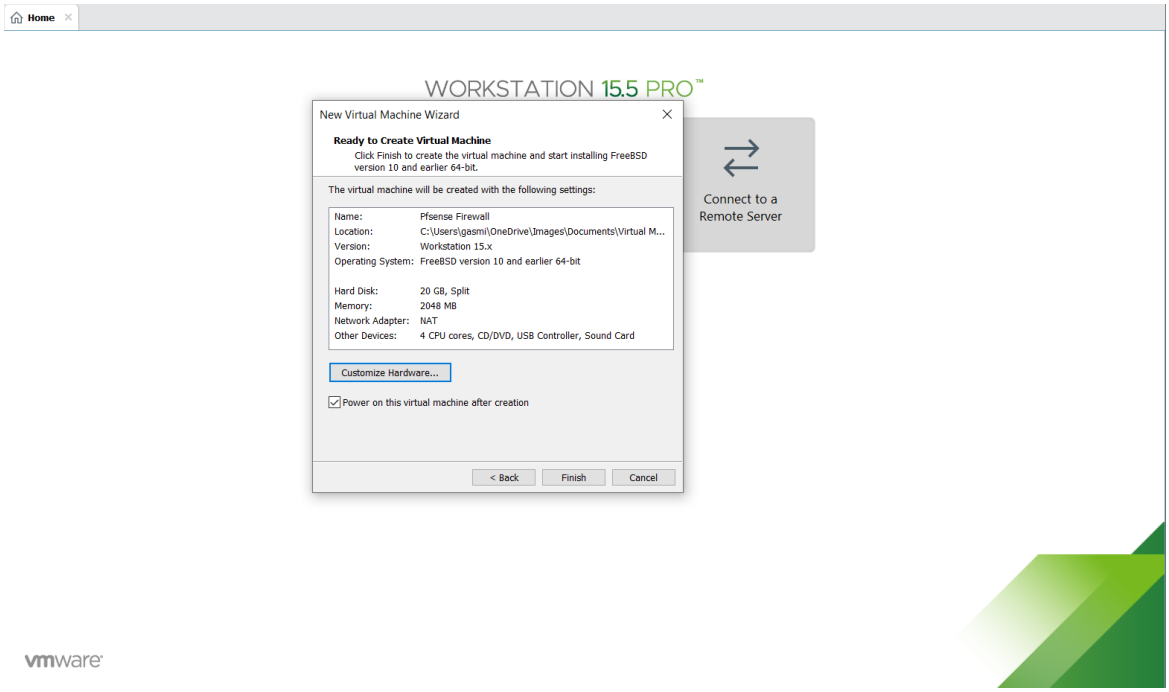


Figure 23 - Machine virtuelle

- On clique sur **Finish**, la fenêtre s'affiche :

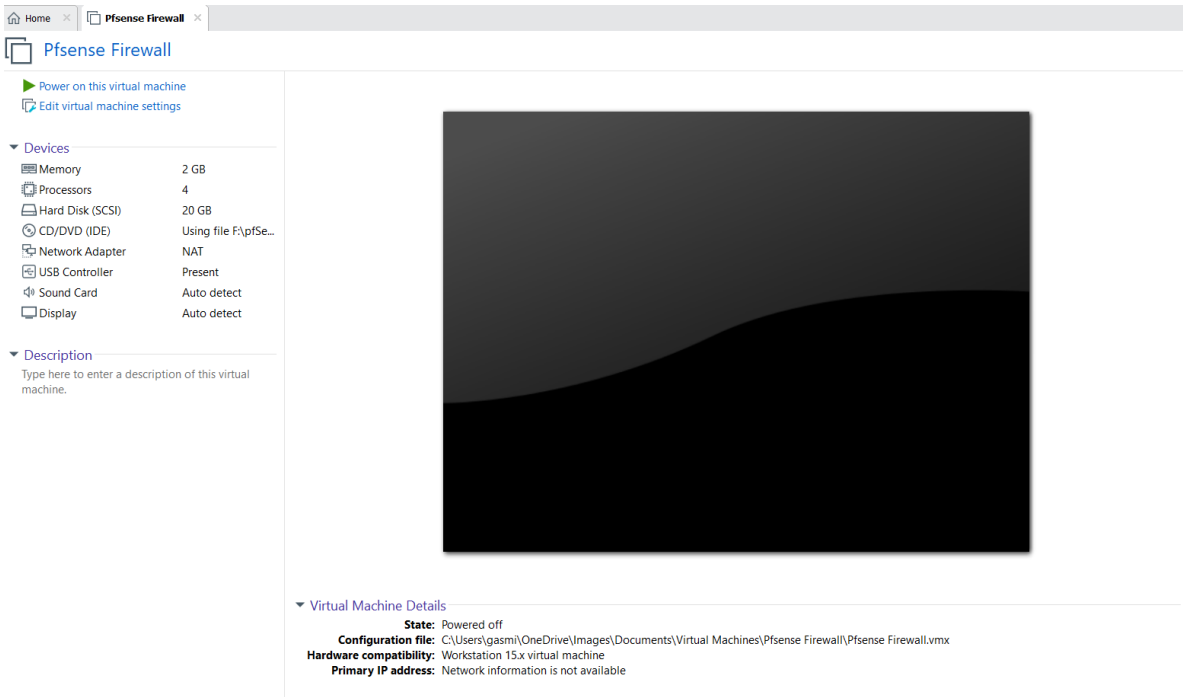


Figure 24 - Machine virtuelle : compatibilité du matériel virtuel

- Avant de commencer l'installation, notre machine doit être équipée en minimum de deux cartes réseaux et configurer ces cartes sous Virtual Network. Pour ce projet on va utiliser deux interfaces :
  - LAN (VMnet0) : 192.168.1.0 /24.
  - WAN (VMnet2) : Pont (connecté direct a réseau physique 192.168.43.0 /24).

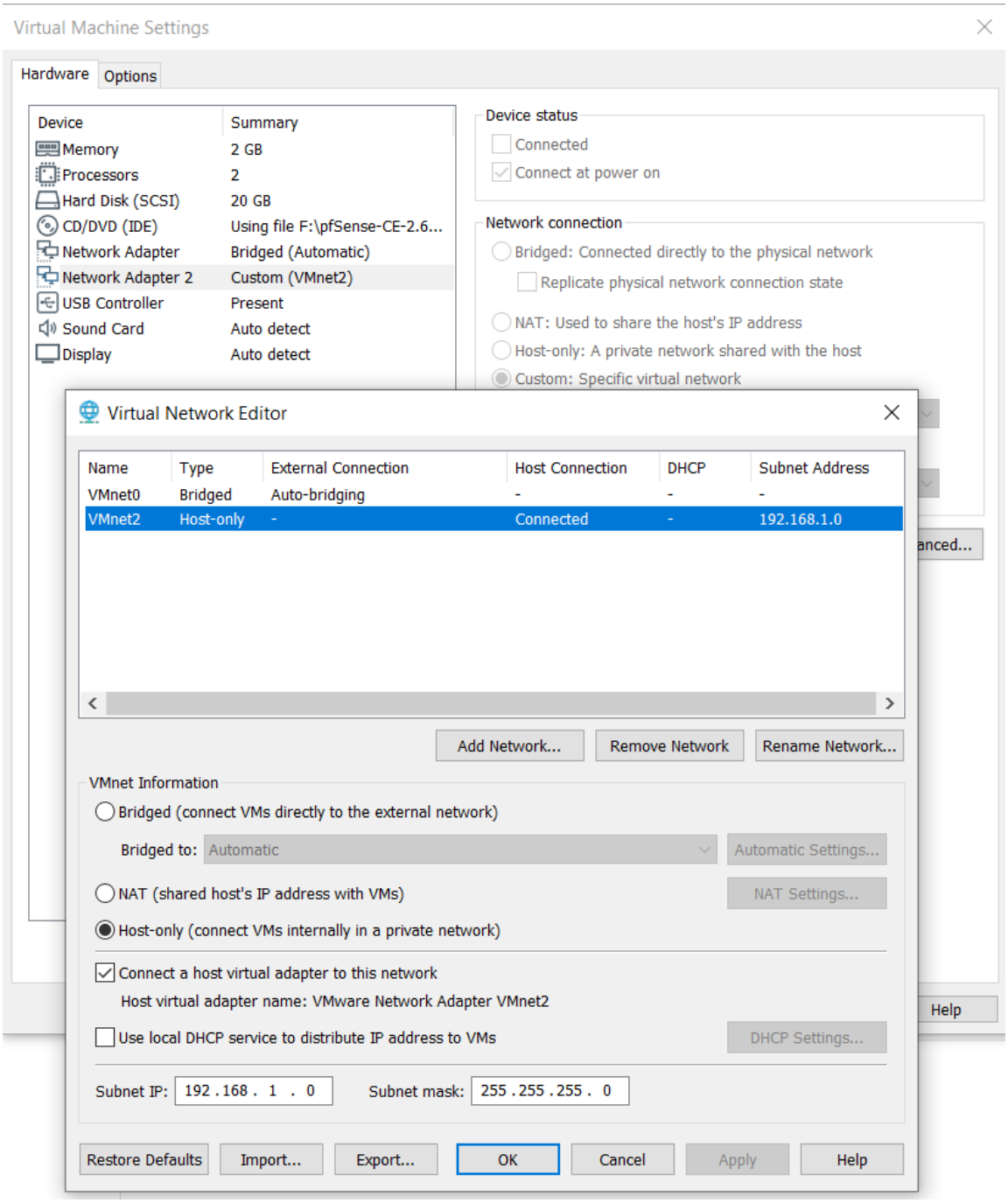


Figure 25 - Configuration les cartes réseaux sous Virtual Network

- On clique sur **power on this vertual machine** pour commencer l'installation de PfSense. La fenêtre suivante s'affiche. Clique sur Enter pour choisit le 1er choix.

Figure 26 - PfSense-installation : mode de démarrage

- L'installation se termine ici

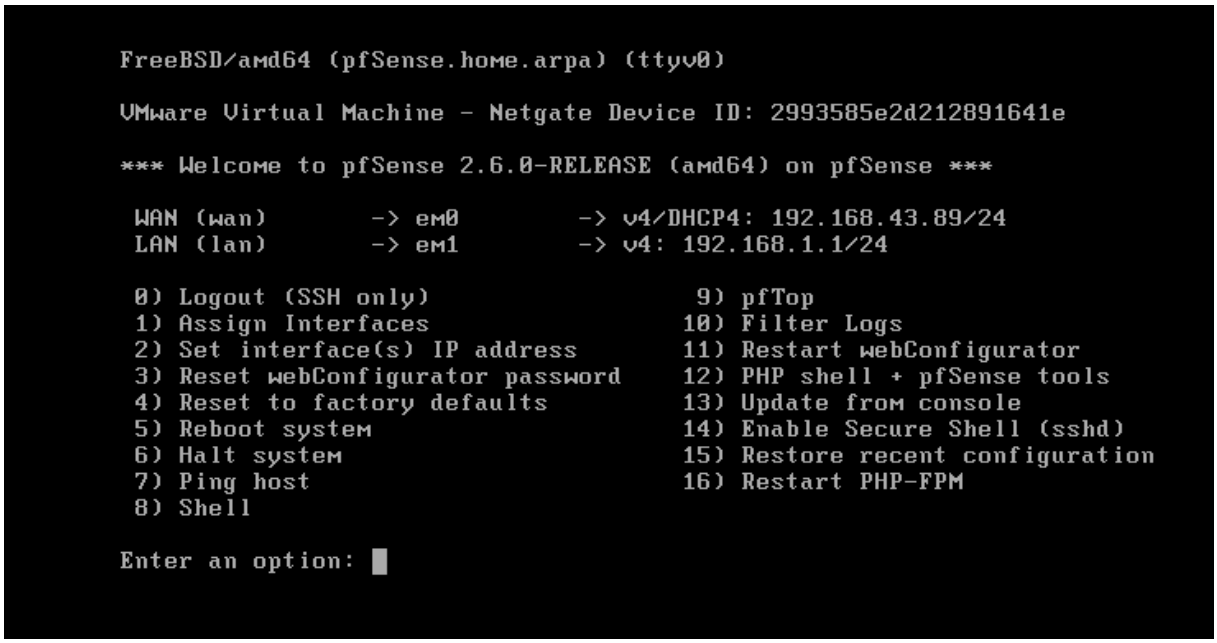


Figure 27 - PfSense : installation terminée

- Pour se connecter à l'interface web de configuration de PfSense on utilise l'adresse IP de l'interface LAN : **192.168.1.1** , Cette page s'affiche :

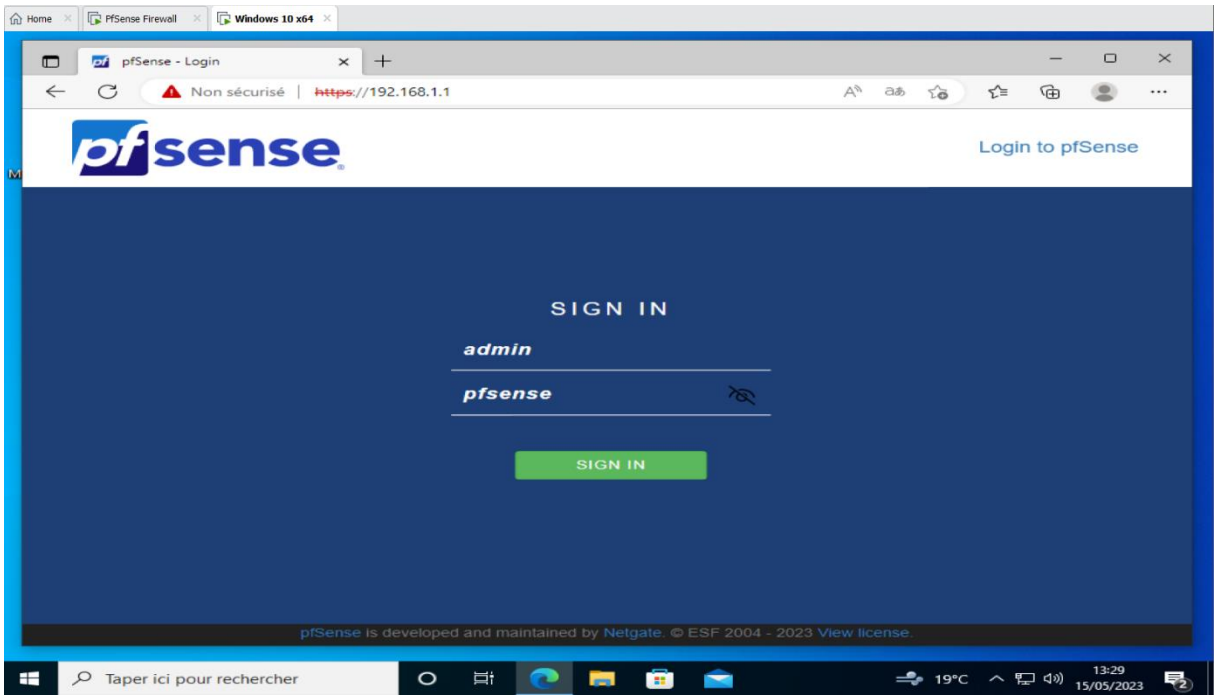


Figure 28 - Page d'identification de PfSense

- «Username/Password» par défaut est « admin/pfsense ».

2.2. Configuration Basique de PfSense

- **Autoriser l'accès au serveur PfSense depuis le WAN :**
  - Accéder au **Firewall / Rules / WAN** et on clique **Add**

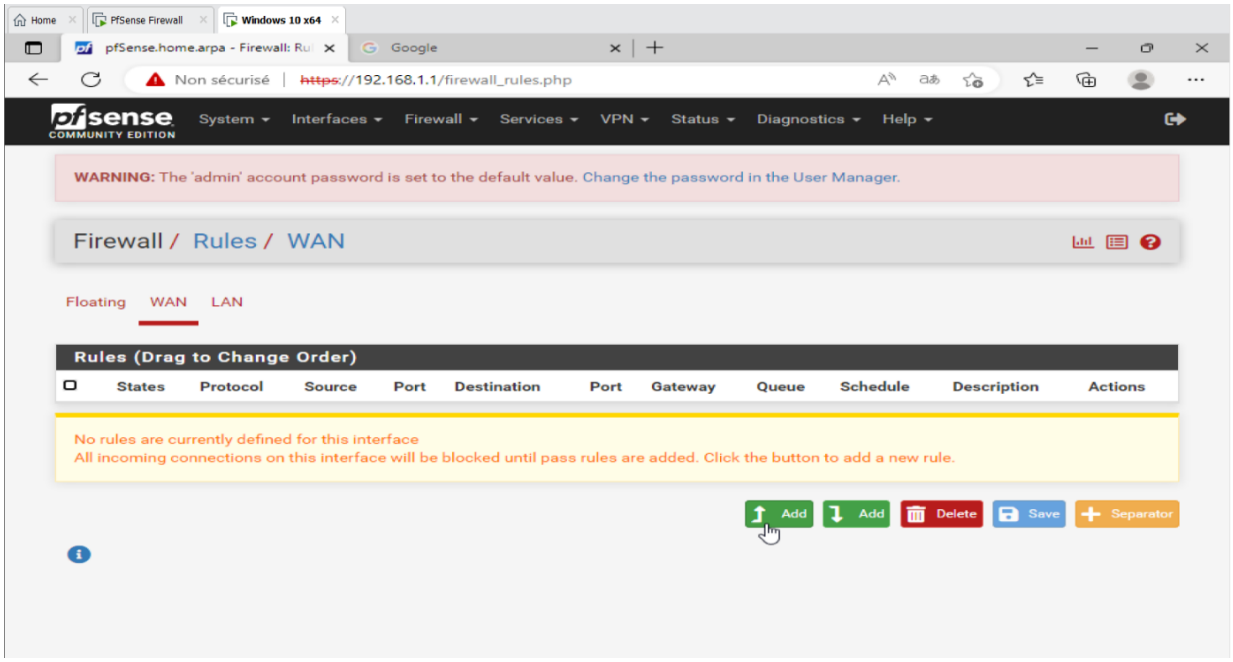


Figure 29 - Ajouter les règles dans PfSense

- Entrez les données comme indiqué, puis cliquez sur **Save**

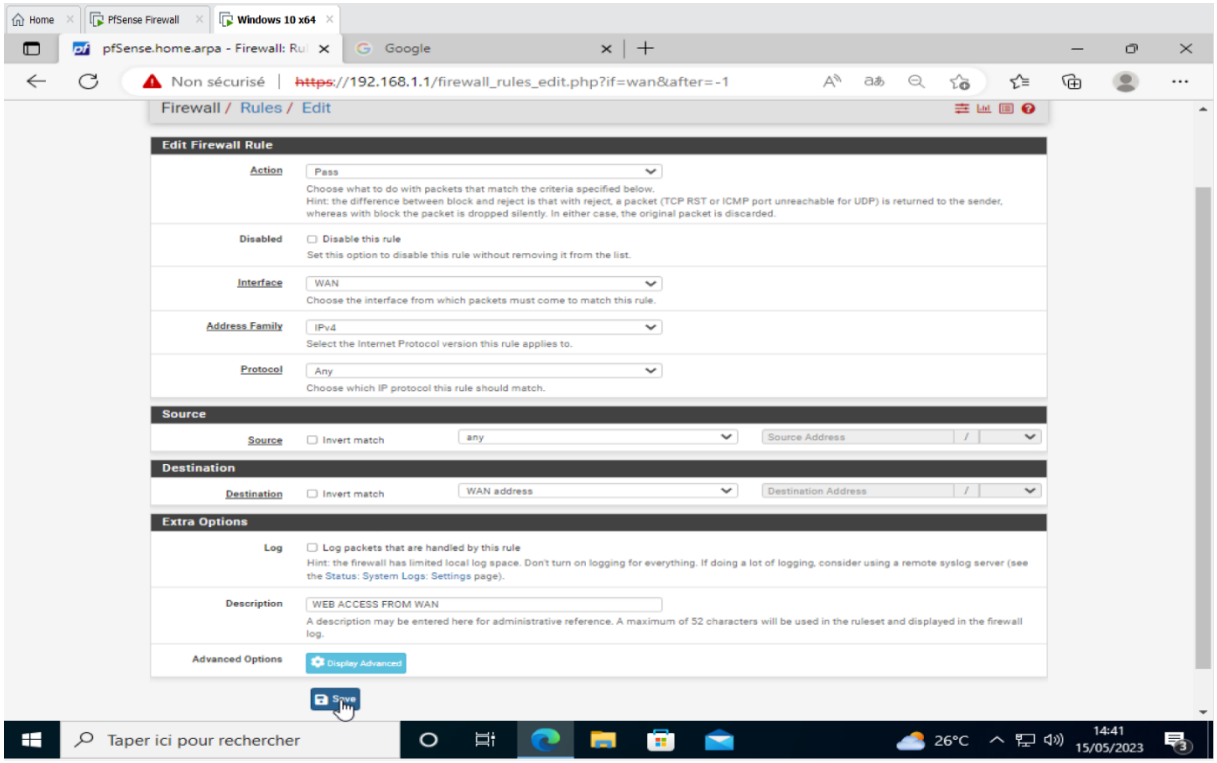


Figure 30 - Modifier la règle

- Enfin on clique sur **Apply Changes**

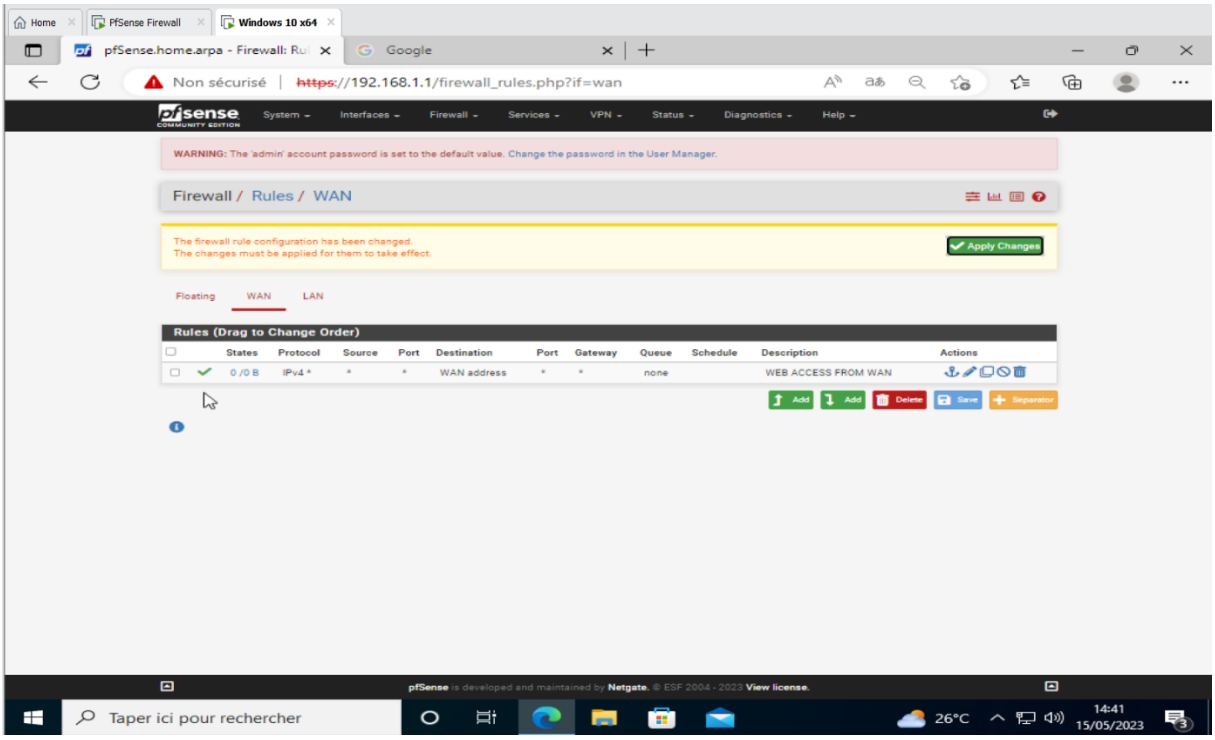


Figure 31 - Appliquer les modifications de règles

- **Créer un compte pour accéder depuis le WAN :**

- Accéder au **System / User Manager / Users** et on clique **Add** pour créer le compte.

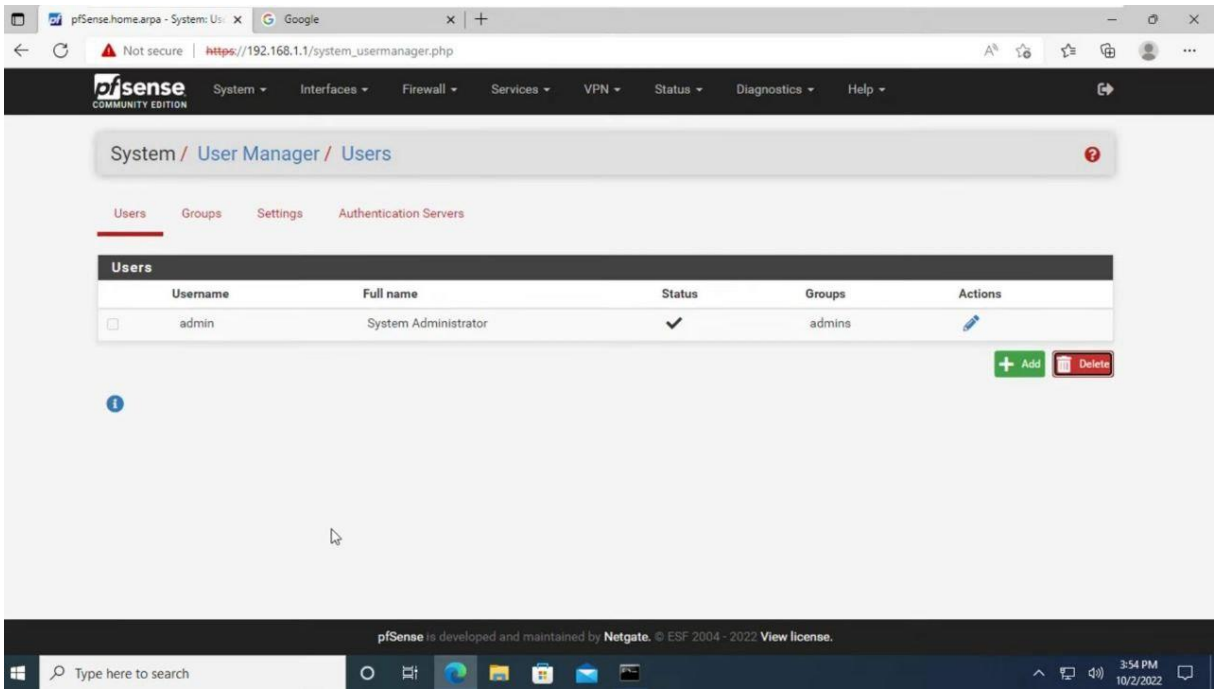


Figure 32 - Ajouter nom d'utilisateur et mot de passe

2.3. Installation de Package API dans PfSense

Afin d'intégrer notre modèle au PfSense, nous devons installer le package API PfSense et l'étudier pour connaître l'API nécessaire pour extraire les principales informations d'intégration.

- Tout d'abord, installez le package api sur le serveur Pfsense

```
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 8

[2.6.0-RELEASE][root@pfSense.home.arpa]/root: pkg add https://github.com/jaredhe
ndrickson13/pfsense-api/releases/latest/download/pfSense-2.6-pkg-API.txz && /etc
/rc.restart_webgui
```

Figure 33 - L'installation d'un package API sur le serveur PfSense

- Après avoir terminé l'installation, j'ai remarqué que l'**API** a été ajoutée dans le menu **System**
- Ensuit accéder au **System / API / Settings** et Entrez les données comme indiqué, puis cliquez sur **Save**
- Enfin cliquez sur **Generate** pour obtenir un **API Token** .

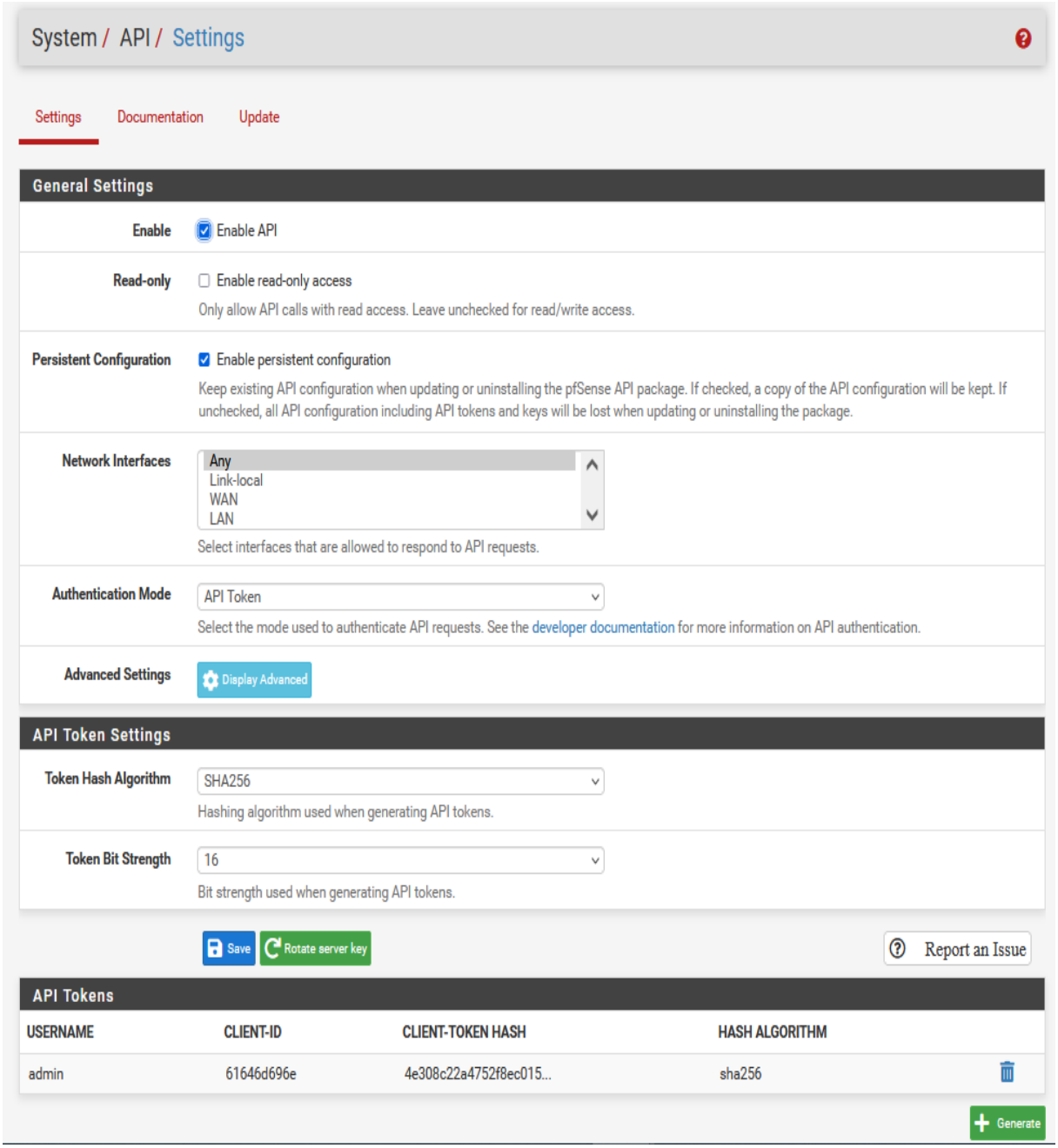


Figure 34 - Obtenir un API Token

3. Le modèle de détection dans un script et l'intégrer dans PfSense

Tout d'abord utiliser le programme d'Insomnia pour étudier et obtenir l'api de trafic réseau.

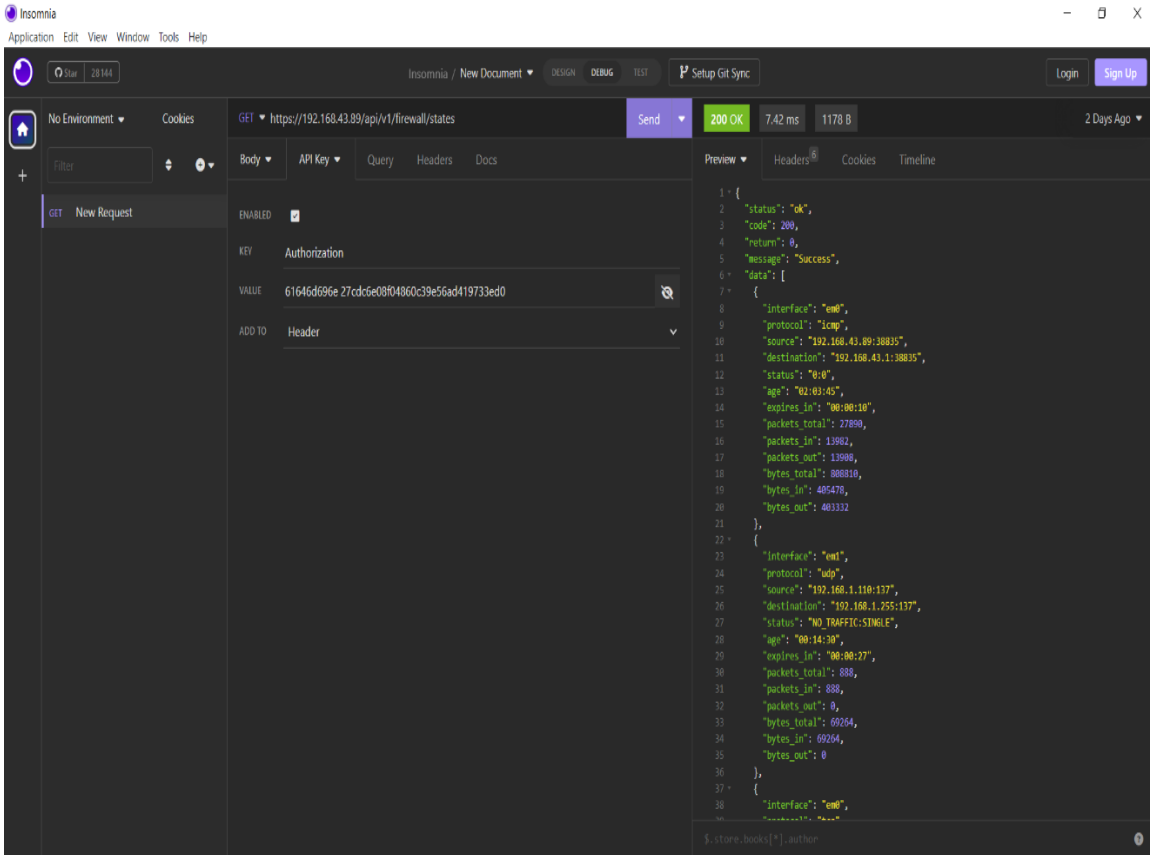


Figure 35 - Obtenir l'API de trafic réseau en utilise programme Insomnia

Je n'ai pas obtenu l'API de trafic total qui a suffisamment des caractéristiques requis par notre modèle, nous avons donc utilisé une autre API (**api/v1/firewall/status**) pour tester notre modèle où nous n'avons obtenu que 6 caractéristiques sur 67.

Dans ce script nous avons extrait les données de l'api (**api/v1/firewall/status**) et les avons passées dans notre modèle, où en cas d'attaque, le script bloque l'attaque par l'api (**api/v1/firewall/rule**) avec l'avertissement de l'attaque et en mentionnant son type.

```python
import requests
import json
import numpy as np

from keras.models import load_model

def block(source_ip, index):
    url = api_url + "v1/firewall/rule"
    payload = {
        "apply": True,
        "dst": str(source_ip),
        "interface": ["wan"],
        "ipprotocol": "inet",
        "protocol": "any",
        "src": "192.168.43.89",
        "type": "block",
        "descr": f"Block IP address, possibility of {attacks[index]} attack"
    }
    response = requests.post(url, headers=headers, data=json.dumps(payload), verify=False)
    if response.status_code == 200:
        print("IP address blocked successfully.")
    else:
        print("Failed to block IP address. Status code:", response.status_code)
        print("Response:", response.text)

def detect(packet):
    source_ip, source_port = packet['source'].split(":")
    if packet['protocol'] == 'tcp':
        protocol = '6'
    elif packet['protocol'] == 'udp':
        protocol = '17'
    else:
        protocol = '0'
    hours, minutes, seconds = map(int, packet['age'].split(":"))
    duration = hours * 3600 + minutes * 60 + seconds

    flow = {
        'Protocol': protocol,
        'Flow Duration': duration,
        'Total Fwd Packets': packet['packets_out'],
        'Total Backward Packets': packet['packets_in'],
        'Total Length of Fwd Packets': packet['bytes_out'],
        'Total Length of Bwd Packets': packet['bytes_in'],
    }
    converted_flow = {}
    for key, value in flow.items():
        converted_flow[key] = float(value)
    input_data = np.array(list(converted_flow.values())).reshape(1, -1)
    prediction_result = model.predict(input_data)[0]
    index_of_prediction = np.where(prediction_result == 1)[0]
    if prediction_result[0] == 1:
        print("It's not an attack")
        return
    block(source_ip, index_of_prediction[0])

def fetch_data(api_url):
    response = requests.get(api_url, headers=headers, verify=False)
    if response.status_code == 200:
        return response.json()
    else:
        print("API request failed with status code:", response.status_code)
        return None

def compare_data(current_data, previous_data):
    return len(current_data) != len(previous_data)

def handle_changes(data):
    print("API data has changed!")
    flow = data['data'][-1]
    if flow['status'] != "NO_TRAFFIC:NO_TRAFFIC":
        detect(flow)

def process_flow(data):
    for packet in data:
        if packet['status'] != "NO_TRAFFIC:NO_TRAFFIC":
            detect(packet)

attacks = ['BENIGN', 'DNS', 'LDAP', 'MSSQL', 'NetBIOS', 'NTP', 'SNMP', 'SSDP', 'UDP', 'Syn', 'TFTP', 'UDP-lag',
'WebDDos']

api_url = "https://192.168.43.89/api/"
headers = {
    "Content-Type": "application/json",
    "Authorization": f"61646d696e 27cdc6e08f04860c39e56ad419733ed0"
}

model = load_model('models/aimen13.h5')

url = api_url + "v1/firewall/states"

previous_data = None
while True:
    current_data = fetch_data(url)
    if current_data:
        if previous_data is None:
            previous_data = current_data
            process_flow(previous_data['data'])
        elif compare_data(current_data, previous_data):
            handle_changes(current_data)
            previous_data = current_data
```

Figure 36 - Script de détection d'attaque dans PfSense

4. Résultat et Discussion

Enfin, après avoir terminé et exécuté le script, nous avons remarqué que des attaques Syn et DNS étaient détectées et que la source de l'attaque était automatiquement bloquée dans PfSense.

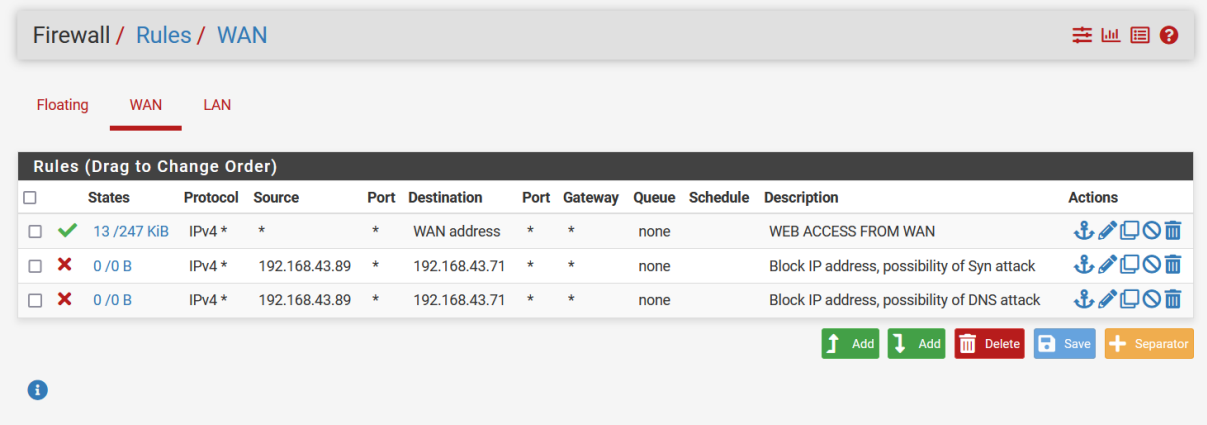


Figure 37 - Le script a automatiquement bloqué l'attaque dans PfSense.

Notre étude est la première dans ce domaine, et je n'ai trouvé aucune étude antérieure d'intégration d'un modèle de détection d'attaques testé sur le dataset CICDDOS2019 et PfSense.

Conclusion

Ce chapitre a fourni une présentation détaillée de l'environnement de développement et de simulation utilisé dans cette étude. Nous avons décrit les différents logiciels utilisé, tels que VMware Workstation, GNS3 et PFSENSE, qui ont été intégrés pour créer un environnement propice à nos expérimentations. Nous avons discuté de l'installation et de la configuration basique de PfSense sous VMware, mettant l'accent sur l'importance de ces étapes pour assurer le bon fonctionnement de notre environnement. De plus, nous avons souligné l'installation du package API dans PfSense, qui nous a permis d'intégrer un modèle de détection dans un script. Ainsi que les étapes nécessaires pour sa mise en œuvre. Enfin, nous avons présenté les résultats de nos expérimentations et initié une discussion approfondie. Nous avons évalué les performances et l'efficacité du modèle de détection dans un script intégré à PfSense.

Conclusion Générale

Conclusion Générale

Le travail que nous avons accompli a pour principal objectif la proposition d'une architecture réseau sécurisée par firewall PfSense pour l'université de Larbi Tébessi - Tébessa. Le PfSense contient notre modèle d'apprentissage en profondeur DNN qui détecte et bloque automatiquement les attaques disponibles dans data-set CICDDOS2019. Ce projet nous a permis d'appliquer les connaissances acquises au cours de notre formation, de nous familiariser avec l'environnement dynamique et d'avoir une idée plus approfondie de la sécurité des réseaux.

Dans cette thèse, nous avons fourni quelques informations générales sur les réseaux et la sécurité informatique ainsi que l'intelligence artificielle et ses applications dans la détection des attaques. Nous avons ensuite étudié l'architecture existante du réseau et ces différentes zones, ce qui nous a permis de critiquer cette architecture et de suggérer quelques solutions afin de proposer une nouvelle avec une meilleur fluidité et sécurité du réseau. Dans cette nouvelle architecture, nous avons proposé une zone démilitarisée (DMZ) pour améliorer la sécurité des serveurs, et également proposé un serveur antivirus et un tunnel VPN pour l'accès à distance. Enfin, nous avons suggéré la présence de deux pare-feu PfSense contenant notre modèle afin de protéger la zone contre les attaques provenant du réseau interne (LAN) et externe (Internet). Ensuite, nous avons proposé un système de détection d'attaques de data-set CICDDOS2019 basé sur le modèle de réseau neuronal profond (DNN). Enfin, nous avons installé PfSense et installé le package API dans PfSense, ce qui nous a permis d'inclure le modèle de détection dans un script. Ainsi que les étapes nécessaires à sa mise en œuvre. Nous avons présenté les résultats de nos expériences et entamé une discussion approfondie. Nous avons évalué les performances et l'efficacité du modèle de détection dans un script intégré à PfSense.

La réalisation de ce projet a été bénéfique et fructueux pour nous dans le sens où il nous a permis d'apporter une contribution à l'université de Larbi Tébessi - Tébessa. En plus de notre étude est la première dans ce domaine d'intégration d'un modèle de détection d'attaques entraîné sur le data-set CICDDOS2019 et PfSense, mais aussi d'approfondir et d'acquérir de nouvelles connaissances qui seront utiles et déterministes pour nous à l'avenir.

Bibliographie

Bibliographie

[1] *Ltd Huawei Technologies Co. (2023). Data Communications and Network Technologies. Springer Nature Singapore.*

[2] *Belhocine, M., & Abid, Y. (2015). Proposition d'une architecture réseaux sécurisée pour l'université A. Mira de Bejaïa (Doctoral dissertation, Université A/Mira de Bejaia).*

[3] *Sadiqui, A. (2019). Sécurité des réseaux informatiques. ISTE Group.*

[4] *Llorens, C., Levier, L., & Valois, D. (2006). Tableaux de bord de la sécurité réseau, 2 ème édition. Eyrolles, 560p.*

[5] G. Jean-Olivier, P. d. A. Marcio et . A. Marcelo, «Attaques Informatique,» *Centro Brasileiro de Pesquisas F´ısicas – CBPF,* n° %1CBPF-NT-007/00 , p. 6.

[6] *Bloch, L., Queinnec, C., Wolfhugel, C., Makarévitch, N., & Schauer, H. (2009). Sécurité informatique: principes et méthode.*

[7] J.-F. PILLOU et J.-P. BAY, Tout sur la Sécurité informatique 4 éme édition, Paris: Dunod, 2016.

[8] *Learning, D. (2020). Deep learning. High-dimensional fuzzy clustering.*

[9] *Schmidt-Erfurth, U., Sadeghipour, A., Gerendas, B. S., Waldstein, S. M., & Bogunović, H. (2018). Artificial intelligence in retina. Progress in retinal and eye research, 67, 1-29..*

[10] *HAMOUDA, D. (2020). Un système de détection d'intrusion pour la cybersécurité.*

[11] *Liu, W., Wang, Z., Liu, X., Zeng, N., Liu, Y., & Alsaadi, F. E. (2017). A survey of deep neural network architectures and their applications. Neurocomputing, 234, 11-26.*

[12] *Dua, S., & Du, X. (2016). Data mining and machine learning in cybersecurity. CRC press.*

[13] *Masud, M., Khan, L., & Thuraisingham, B. (2011). Data mining tools for malware detection. CRC Press.*

[14] *Sommer, R., & Paxson, V. (2010, May). Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE symposium on security and privacy (pp. 305-316). IEEE.*

[15] *Alazab, M., KP, S., Srinivasan, S., Venkatraman, S., & Pham, Q. V. (2021). Deep learning for cyber security applications: A comprehensive survey.*

[16] «kddcup99 dataset,» Irvine Univ of California, [En ligne]. Available: http://kdd.ics.uci.edu/databases/. [Accès le 10 04 2023].

[17] *Choudhary, S., & Kesswani, N. (2020). Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT. Procedia Computer Science, 167, 1561-1573..*

[18] «MAWILab - Documentation,» [En ligne]. Available: http://www.fukuda-lab.org/mawilab/documentation.html. [Accès le 11 04 2023].

[19] «Cic datasets,» Univ of new Brunswick , [En ligne]. Available: https://www.unb.ca/cic/datasets/index.html. [Accès le 11 04 2023].

[20] *Salama, M. A., Eid, H. F., Ramadan, R. A., Darwish, A., & Hassanien, A. E. (2011). Hybrid intelligent intrusion detection scheme. In Soft computing in industrial applications (pp. 293-303). Springer Berlin Heidelberg.*

[21] *Alom, M. Z., Bontupalli, V., & Taha, T. M. (2015, June). Intrusion detection using deep belief networks. In 2015 National Aerospace and Electronics Conference (NAECON) (pp. 339-344). IEEE.*

[22] *Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017, September). Applying convolutional neural network for network intrusion detection. In 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1222-1228.*

[23] *Al-Yaseen, W. L., Othman, Z. A., & Nazri, M. Z. A. (2017). Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system. Expert Systems with Applications, 67, 296-303.*

[24] *Sharafaldin, I., Lashkari, A. H., Hakak, S., & Ghorbani, A. A. (2019, October). Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-8). IEEE.*

[25] *Ferrag, M. A., Shu, L., Djallel, H., & Choo, K. K. R. (2021). Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0. Electronics, 10(11), 1257.*

[26] *Mittal, M., Kumar, K., & Behal, S. (2022). Deep learning approaches for detecting DDoS attacks: A systematic review. Soft Computing, 1-37.*

[27] [En ligne]. Available: https://www.virtualizationhowto.com/2018/09/vmware-workstation-pro-15-released-with-new-features/. [Accès le 22 05 2023].

[28] [En ligne]. Available: https://fr.m.wikipedia.org/wiki/Fichier:GNS3_logo.png. [Accès le 22 05 2023].

[29] [En ligne]. Available: https://en.wikipedia.org/wiki/File:PfSense_logo.png. [Accès le 22 05 2023].