REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTRE DE L'ENSEINGEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE ABDARAHMANE MIRA - BEJAIA

FACULTE DES SCIENCES EXACTES

DEPARTEMENT D'INFORMATIQUE

Mémoire Fin D'études

En vue d'obtention du diplôme Master en informatique

Option : Administration Et Sécurité Des Réseaux

Etude et mise en place d'un système de gestion des informations et des évènements de sécurité (SIEM) et détection prévention d'intrusion (IDS/IPS)

Réalisé par :

- **Mlle KACED Amina**
- **Mme ZIDOUNI Tassadit**

Soutenu le 02 juillet 2024 devant le jury compose de :

Président	**Mr. SALHI Nadir**	**Université A MIRA-BÉJAIA**
Examinatrice	**Mlle. HOUHA Amel**	**Université A MIRA-BÉJAIA**
Encadrant	**Mr. TOUAZI Djoudi**	**Université A MIRA-BÉJAIA**

Promotion 2023 – 2024

﴿ بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ﴾

Remerciments

En premier lieu, au nom du Dieu tout-puissant, nous exprimons notre gratitude pour nous avoir accordé le courage, la santé et la détermination nécessaires pour mener à bien ce travail.

Nous tenons à remercier Mr. **Touazi**, pour son encadrement de qualité, et priseurs conseils . Nous apprécions profondément la confiance qu'il nous a témoignée et l'opportunité qu'il nous a offerte de travailler sous sa direction.

Nos sincères remerciements vont également aux membres du jury pour leur acceptation d'évaluer notre travail.

Président Mr **SALHI université A Mira Bejaia**

Examinatrice Mlle **HOUHA université A Mira Bejaia**

Dédicace

Je temoingne une profonde gratitude au bon **Dieu** tout puissant, d'abord de m'avoir donné la volonte et la patience pour accomplir ce modeste travail. Alors je dédie ce mémoire

À mes chers parents, ma mére **Farida** et mon père **Lyes :**

Maman, ma figure emblématique aucune dédicace ne pourrait exprimer mon respect, mon amour éternel et ma gratitude pour vos sacrifices pour mon éducation et mon bien-être. Merci pour votre soutien et votre amour depuis mon enfance. J'espère que votre bénédiction m'accompagnera toujours.

Papa, vos encouragements et votre motivation constante ont été essentiels dans mes études. Que ce modeste travail soit l'accomplissement de vos souhaits tant formulés, le fruit de vos innombrables sacrifices. Tu es mon héros, je t'aime plus que les mots ne puissent t'exprimer. Puisse Dieu, le Très Haut, vous accorder santé, bonheur et longue vie.

À mon cher frère **Younes** et à ma chère sœur **Sarah** : Merci pour votre soutien et votre affection. Vous avez toujours été là pour moi, et je suis fière et reconnaissante de vous avoir dans ma vie. **À** Ma chère belle-sœur **Amel.**

À mes grands-parents, mon grand-père **Makhlouf LALAM** dit **Rabah**, et ma grand-mère setti **Fatiha**, je vous adresse toute ma gratitude pour vos prières et votre amour constants. Vos bénédictions sont précieuses et je les porte avec moi chaque jour. Que Dieu vous accorde une longue vie remplie de santé, bonheur et sérénité.

À tous mes enseignants de mon cursus scolaire, du primaire, du moyen, du secondaire et de l'enseignements supérieur. Également à mon instituteur, mon cher deuxième papa, qui m'a appris à lire et à écrire Mr **LEBTANI Mohammed Yahia** que dieu l'accueil dans son vaste paradis. Et aussi a mon professeur **Bachir Yahia Cherif**, je vous adresse formellement mes remerciements.

À toute ma famille, mes oncles **Brahim**, **Yahia**, **Hafid, Mourad, Abdelkader** et mon très cher oncle **Djamel** paix a son âme. Mes chères tantes **Kahina**, **Fadila** et **Laldja**.

Je tiens à remercier chaleureusement ma chère binôme **Tassadit** et sa famille pour leur soutien et leur encouragement tout au long de ce projet.

À tous mes amis sans exception, et a tous qui m'ont aidé de près ou de loin

« *Amina* »

Dédicace

Toutes les lettres ne sauraient trouver les mots qu'il faut… Tous les mots ne sauraient exprimer la gratitude, L'amour, le respect, la reconnaissance…

Aussi, c'est tout simplement que

Je dédie ce mémoire

À ma famille :

Symbole de reconnaissance pour tout le soutien et l'amour quelle m'a porté depuis toujours

Mes parents, mes enfants **Abdelkader** et **Idir.**

À ma binôme **Amina** et à toute sa famille :

Je vous suis reconnaissant pour votre soutien et votre collaboration précieuse tout au long de ce projet.

À tous mes amis :

Je souhaite exprimer ma gratitude à tous mes amis qui ont toujours été présents pour moi, m'encourageant et me motivant à donner le meilleur de moi-même, sourtout **M.M**

« *Tassadit* »

Table de matières

Sommaire

Liste de figures

Table de figures

Liste de tableaux

Acronymes

Technologie et Réseaux

- **CCNA** : Cisco Certified Network Associate
- **CCNP S&R** : Cisco Certified Network Professional - Security and Routing
- **C#** : C sharp
- **CSS** : Cascading Style Sheets
- **DDR4** : Double Data Rate 4
- **ESXI** : Elastic Sky X Integrated
- **FTTH/FTTX** : Fiber-To-The-Home/ Fiber-To-The-X
- **Gbit/s** : gigabits par seconde
- **HTML5** : HyperText Markup Language 5
- **HPE 1820-24G Managed L2** : Hewlett Packard Enterprise
- **IP** : Internet Protocol
- **ISR 4331** : Integrated Services Router
- **L.S** : Ligne Spécialisée
- **NTS** : New Technology & Solutions
- **PDG** : Président Directeur Général
- **PHP** : Hypertext Preprocessor (initialement Personal Home Page)
- **RAM** : Random Access Memory
- **SAV** : Service Après-Vente
- **SQL** : Structured Query Language
- **UHD** : Ultra High Definition

Réseaux et Communications

- 2**FA** : Two-Factor Authentication
- **3DES** : Triple DES
- **ACL** : Access Control List
- **AES** : Advanced Encryption Standard
- **CD-ROM** : Compact Disc Read-Only Memory
- **DDOS** : Distributed Denial of Service
- **DES** : Data Encryption Standard
- **DHCP** : Dynamic Host Configuration Protocol
- **DMZ** : Demilitarized Zone
- **DNS** : Domain Name System
- **DOS** : Denial of Service
- **DSA** : Digital Signature Algorithm
- **ECC** : Elliptic Curve Cryptography
- **FTP** : File Transfer Protocol
- **HTTP** : Hypertext Transfer Protocol
- **HTTPS** : Hypertext Transfer Protocol Secure
- **IETF** : Internet Engineering Task Force
- **IEEE** : Institute of Electrical and Electronics Engineers
- **ISO** : International Organization for Standardization
- **LAN** : Local Area Network

- **MAN** : Metropolitan Area Network
- **NIST** : National Institute of Standards and Technology
- **NOS** : Network Operating System
- **OSI** : Open Systems Interconnection
- **PAN** : Personal Area Network
- **POP3** : Post Office Protocol version 3
- **RADIUS** : Remote Authentication Dial-In User Service
- **RSA** : Rivest, Shamir, Adleman
- **SAN** : Storage Area Network
- **SMS** : Short Message Service
- **SNMP** : Simple Network Management Protocol
- **SNTP** : Simple Network Time Protocol
- **SSH** : Secure Shell
- **TCP/IP** : Transmission Control Protocol/Internet Protocol
- **UDP** : User Datagram Protocol
- **USB** : Universal Serial Bus
- **VLAN** : Virtual Local Area Network
- **VPN** : Virtual Private Network
- **WAN** : Wide Area Network
- **XSS** : Cross-Site Scripting

Sécurité et Gestion

- **AST** : Application Security Testing
- **CI/CD** : Continuous Integration/Continuous Deployment
- **DAST** : Dynamic Application Security Testing
- **DLP** : Data Loss Prevention
- **EDR** : Endpoint Detection and Response
- **FreeBSD** : Free Berkeley Software Distribution
- **GDPR** : General Data Protection Regulation
- **HIPAA** : Health Insurance Portability and Accountability Act
- **IA** : Intelligence Artificielle (ou Internal Audit selon le contexte)
- **IAM** : Identity and Access Management
- **IAST** : Interactive Application Security Testing
- **ICMP** : Internet Control Message Protocol
- **IDS/IPS** : Intrusion Detection System/Intrusion Prevention System
- **PCI DSS** : Payment Card Industry Data Security Standard
- **SAST** : Static Application Security Testing
- **SCADA** : Supervisory Control and Data Acquisition
- **SEM** : Security Event Management
- **SIEM** : Security Information and Event Management
- **SIEMaaS** : Security Information and Event Management as a Service
- **SIM** : Security Incident Management/ Security Information Management
- **SOAR** : Security Orchestration, Automation, and Response
- **UEBA** : User and Entity Behavior Analytics
- **URL** : Uniform Resource Locator
- **USM** : Unified Security Management
- **WAF** : Web Application Firewall

Autres Concepts et Outils

- **API** : Application Programming Interface
- **DevOps** : Development and Operations
- **DS** : Deployment Server
- **GNS3** : Graphical Network Simulator 3
- **HEC** : HTTP Event Collector
- **HF** : Heavy Forwarder
- **IoT** : Internet of Things
- **ISP** : Internet Service Provider (Fournisseurs de Services Internet)
- **MAC** : Media Access Control
- **Nmap** : Network Mapper
- **OSPF** : Open Shortest Path First
- **SCTP** : Stream Control Transmission Protocol
- **SHC** : Search Head Clustering
- **SH** : Search Head
- **SPL** : Search Processing Language
- **UF** : Universal Forwarder

Introduction générale

Dans le contexte actuel des entreprises, la sécurité informatique est devenue un enjeu incontournable en raison de la numérisation croissante des données et des systèmes d'information. Les cyberattaques, de plus en plus fréquentes et sophistiquées, représentent une menace sérieuse pour la confidentialité, l'intégrité et la disponibilité des informations critiques. Les solutions de sécurité classiques, souvent fragmentées et ponctuelles, n'offrent pas une protection globale suffisante, laissant les systèmes exposés à des risques importants. Une approche plus intégrée et proactive de la sécurité est donc essentielle pour protéger efficacement les actifs numériques des entreprises contre les attaques complexes.

Face à cette réalité, il est crucial pour les entreprises d'adapter leurs systèmes et leurs politiques de sécurité, ainsi que de mettre en place des outils de surveillance continue en temps réel. C'est ici que le SIEM (Security Information and Event Management) joue un rôle crucial en offrant une visibilité claire et détaillée sur les activités suspectes au sein des systèmes d'information. En complément, les solutions IDS/IPS (Intrusion Detection System/Intrusion Prevention System) détectent et préviennent les intrusions en temps réel. Ensemble, ces outils permettent une analyse approfondie des événements de sécurité, la reconstitution des séquences d'attaques, et la mise en œuvre de mesures appropriées pour une réponse rapide et efficace aux incidents de sécurité.

Dans cette optique, notre travail vise à étudier et mettre en œuvre deux solutions de gestion de sécurité (IDS/IPS et SIEM) renforcer la posture de sécurité de l'entreprise VMS Bejaia, assurant ainsi la protection des données sensibles et la continuité des opérations. Pour atteindre cet objectif, nous avons structuré cette étude de la manière suivante :

- Le premier chapitre est consacré à la présentation de l'organisme d'accueil, VMS Bejaia, client fourni par Campus NTS. Nous y avons également étudié la problématique particulière à laquelle cette entreprise fait face, en examinant ses causes et ses conséquences, avant de suggérer une solution appropriée.
- Le deuxième chapitre explore l'état actuel des connaissances sur la sécurité des réseaux informatiques, en discutant des concepts fondamentaux des réseaux et de l'importance cruciale de la sécurité informatique. Il examine aussi les divers types d'attaques et les moyens de défense disponibles.
- Dans le troisième chapitre, nous examinerons les outils de sécurité, en mettant en avant deux solutions : l'IDS/IPS avec l'utilisation de Snort, ainsi que l'intégration de la solution SIEM avec un accent particulier sur le choix de Splunk. Nous fournirons une analyse approfondie de leurs caractéristiques, architectures et fonctionnements.
- Le quatrième et dernier chapitre de notre réalisation se concentre sur le déploiement des deux solutions Snort et SPLUNK Enterprise dans l'environnement de simulation proposé.

Chapitre 1 :
Présentation de l'organisme d'accueil et étude de l'existant

1.1 Introduction

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

1.2 Section 1 : Présentions de l'entreprise « Campus NTS »

1.2.1 Création et évolution

NTS est une jeune entreprise axée sur la recherche, la conception et la mise en œuvre de solutions, d'intégration de systèmes de sécurité, d'importation et de la distribution d'équipements et de matériels de sécurité des réseaux et des télécommunications, de la formation et le conseil. Elle a été créé en 2020 à Bejaia par Yassine DJEBBARI, qui a de nombreuses d'années d'expérience et a réalisé d'importants projets dans différents secteurs et régions du pays, comme référence :

- Air Algérie.
- Retelem Alger.
- Poste d'Algérie.
- Adèle.
- RATP ALJAZAIR.
- La technologie.
- Géant de l'électronique BBR.
- Morsi.
- Université de Bejaïa.
- Cité universitaire à Bejaïa (Targa Ouzamour, 17 octobre...etc).
- SARL Alphas Bejaïa.
- Providentia Béjaïa.

1.2.2 La localisation de l'entreprise

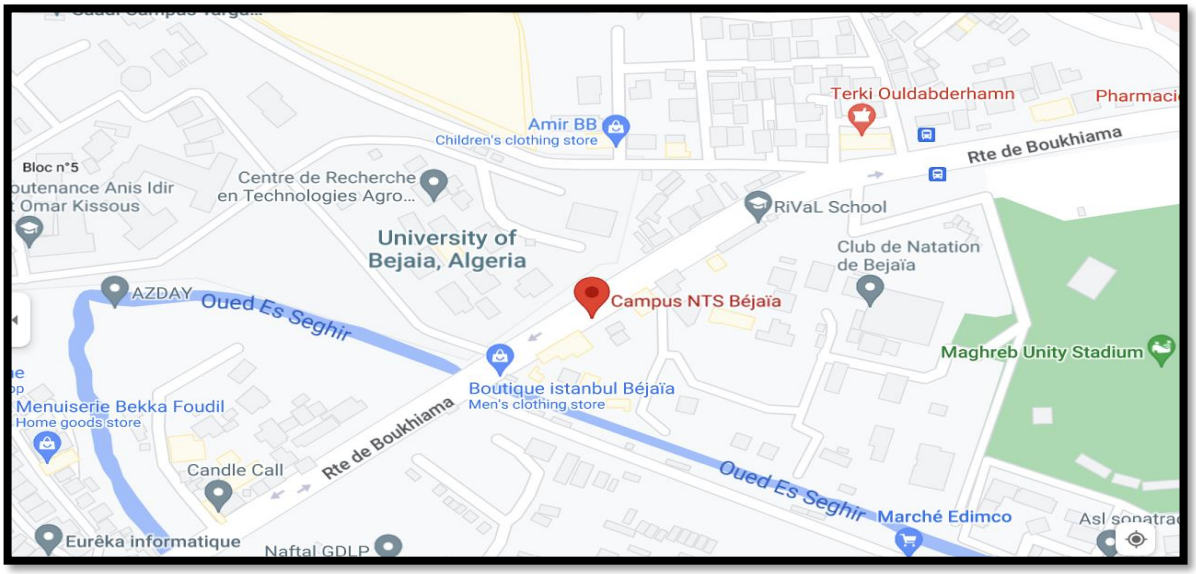

Figure 1 Localisation de l'entreprise NTS

1.2.3 Fiche technique

Le tableau 1 ci-dessous représente quelques informations relatives à l'entreprise dans laquelle nous avons effectué notre stage de projet de fin d'étude.

DENOMINATION	CAMPUS NTS
LOGO	
Siege	Bâtiment a les beaux quartiers Targa Ouzemour, BEJAÏA 06000
Secteurs d'activités	Informatique et télécommunication
Numéro de fax	044 204 400
Numéro de téléphone	0770446101
Email	CONTACT@CAMPUS-NTS.COM
Site internet	HTTP://WWW.CAMPUS-NTS.COM/

Tableau 1 Identification sur campus NTS

1.2.4 Objectifs, Missions et activités de l'Entreprise « N.T.S »

Les objectifs, les missions et les activités sont représentées dans la figure 2 :

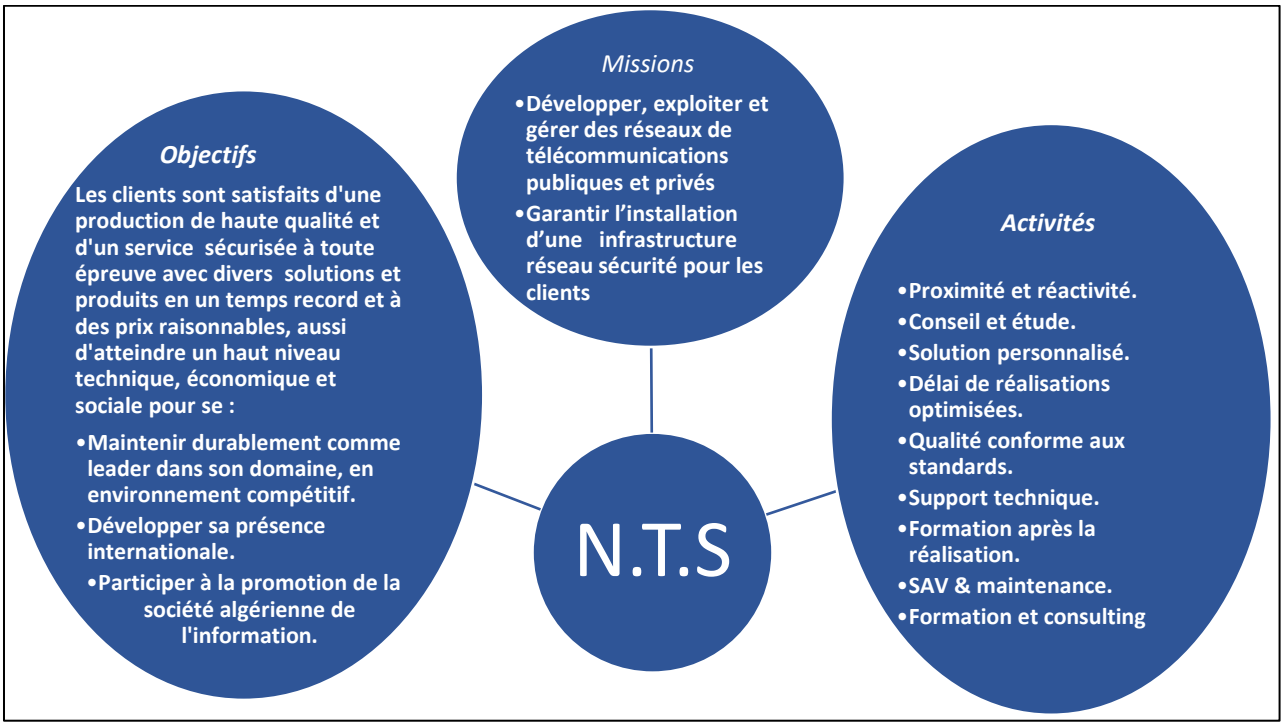

Figure 2 Objectifs, Missions et Activités de l'NTS.

1.2.5 Organigramme général de l'organisme d'accueil

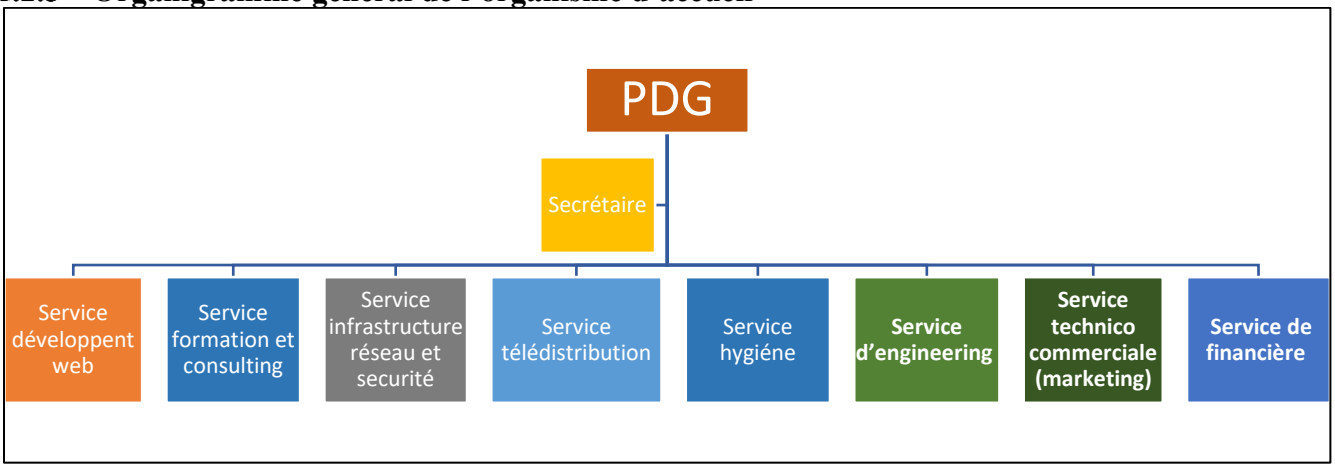

Figure 3 L'organigramme de campus NTS.

Nous allons nous contenter de présenter ci- dessous la description de l'organigramme du campus NTS (voir la figure 3) dans lequel cet apprentissage termine le stage :

A. Service développement web

Il est responsable de la création des sites web, des applications pour internet, applications mobiles ou des solutions logicielles adaptées aux besoins des clients utilisant des langages de programmation informatique tels que : HTML5, CSS, JavaScript ou PHP. En général, il représente les tâches liées au développement du site Web en améliorant son positionnement sur les moteurs de recherche qui seront hébergés sur Internet.

B. Service formation et consulting

Ce secteur a été créé par le campus NTS pour offrir des stages et des formations professionnelles dans les domaines suivants :

- Installation et configuration des réseaux informatiques.
- Administration et sécurité des réseaux et système.
- Installation et configuration des firewalls (pfsense, Sophos, fortigate, palo alto…).
- Installation et configuration des réseaux sans fil professionnel.
- Installation et configuration des caméras de surveillance analogique et numérique.
- Fibre optique les réseaux d'accès FTTH/FTTX.
- Création des sites web.
- Programmation (C, C++, C#, Java, Python…etc.).
- Electricités Bâtiments et industriels.
- Formation Cisco CCNA, CCNP S&R.
- Virtualisation.
- Microsoft server, SQL.
- Cyber sécurité.

Ces stages s'adressent aux étudiants, ouvriers, entreprises en fin de projet et à tous ceux qui apprécient le terrain pour développer leurs compétences en sécurité, acquérir des qualifications supérieures et leur expérience en entreprise. NTS repose sur la capacité des ressources et des structures à délivrer à ses clients et à ses partenaires (Alhua, Hikvision, Cisco, Legend, Mikrotik, Zkteco, Commax, D-link, Alcatel-Lucent, Synology, Microsoft, Apollo, Panasonic, Huawei).

C. Service d'accueil

- **Présentation de service infrastructure réseau et sécurité**

L'infrastructure réseau est au cœur des opérations commerciales dans la plupart des industries. Il peut être considéré comme le centre sensible de toute l'organisation informatique car il centralise les données, simplifie les échanges de données et facilite la communication entre les employés. A ce titre, il est un outil important pour le fonctionnement normal de l'entreprise et nécessite une attention constante en matière de sécurité. Ceci afin d'empêcher le nombre croissant et l'affectation des attaques externes et internes.

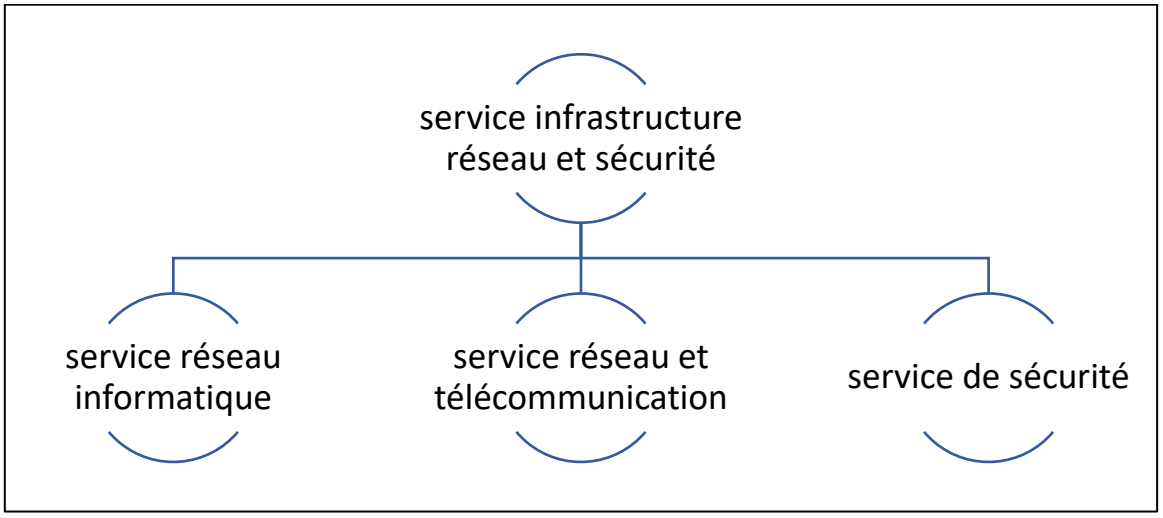

Figure 4 Organigramme de service d'accueil

➢ **Service réseau informatique :**

Ce service représente tous les appareils et périphériques au sein d'une entreprise qui sont physiquement ou virtuellement connectés les uns aux autres à partir d'un wifi professionnel ou d'autre méthodes afin de partager des ressources ou des informations. En fait, l'infrastructure réseau offre un large éventail de fonctionnalités pour les clients de services et les producteurs de services, telles que :

Limitation de débit, analyse, vérification, surveillance et enregistrement et sécurisation du réseau de cette entreprise.

➢ **Service réseau et Télécommunication :**

Les services de télécommunications sont conçus pour transmettre des informations en un temps réel (synchronisation des informations) sous forme analogique ou numérique à l'exception de la radio et de la télévision. La plupart de ces services peuvent aider les clients à identifier leurs besoins en matière d'infrastructure de télécommunications. Voici des exemples de services d'infrastructure de télécommunications :

- Pose de fibre optique.
- Emplacement du site de la tour cellulaire.
- Test d'antenne radio.
- Installation d'équipements téléphoniques standards et réseau de données.
- Téléphonie standard

➢ **Service de sécurité**

Cette entreprise NTS accomplit à la fois le gardiennage et l'installation des systèmes de sécurité électroniques. Aussi elle fournit aux clients des solutions complètes et fiables pour protéger leurs ressources.

Les services qu'elle réalise sont les suivants :

- Caméras de surveillance
- Alarme anti- intrusion
- Détection incendie
- Pointeuse et Contrôles d'accès
- Vidéophonie

D. Service télédistribution

Ce service est spécialisé dans la transmission de données par câble (fibre optique, paire torsadée et onde horizontale) ou autres systèmes de distribution (paraboles collectif, télévision numériques terrestre et audiovisuelle). Son objectif principal est de garantir l'installation de ces supports de transmission à haut débit. Enfin, les services de télédistribution ont été appelés à jouer un rôle majeur dans l'émergence des nouveaux médias tel que :

- Rediffusion de programmation par satellite.
- Transmission de chaînes de télévision par abonnement.
- Services interactifs.
- Programmation locale.

E. Service d'engineering

Il est constitué d'une équipe multidisciplinaire d'experts dont la mission est de rechercher et d'analyser les besoins des clients pour trouver la meilleure solution spécifique à leur projet.

L'équipe de campus NTS n'hésite pas à se circuler sur le terrain pour consulter l'état d'avancement du projet afin de faire face à d'éventuelles difficultés qui auraient pu survenir auparavant. Cette équipe est composée :

- D'ingénieurs en télécommunications.
- D'informaticiens en gestion et sécurité des réseaux.
- D'administrateurs de systèmes d'information.
- D'informaticiens en programmation.
- De techniciens fibre.
- De techniciens supérieurs en informatique.

Leurs propositions sont en recherche informatique et sécurité et leurs cotations est dans la recherche sur les réseaux et les systèmes de télécommunication.

F. Service technico commerciale (marketing)

Leurs offres ne se limitent pas à de simples fournitures standards. Ils disposent d'une équipe qui s'assure de répondre aux besoins et au confort de ses précieux clients dans le but de développer les services de cette entreprise. Par ailleurs, ce service commercialise aussi les services proposés par campus NTS.

G. Service de financière

Le service financier situé au cœur de l'entreprise, représente l'ensemble des personnes chargées de la fonction comptable. Il intervient pour faire de bons investissements en prévenant d'éventuels risques de perte. Ce service contient un ensemble de tâches et rôles au sein de la société NTS :

- Les tâches principales du Service des finances :
  - Assurer une saine gestion des ressources financières de l'entreprise par la planification.
  - La coordination et le contrôle de toutes les politiques et procédures requises pour la protection des actifs.
  - La production des informations financières exactes et pertinentes afin que le gestionnaire puisse prendre la décision éclairée.

- Le rôle du service financier :

  - La préparation et du suivi des budgets de fonctionnement et d'investissement.
  - La préparation des états financiers.
  - La gestion de la trésorerie et de des encaissements.
  - La rémunération des employés, des comptes à payer.
  - De l'acquisition des biens et services pour l'ensemble de l'entreprise, des projets de recherche.
  - La réception des marchandises et du courrier.

H. Service hygiène

La sécurité et la santé occupent une place prépondérante dans les conditions de travail. L'employeur est en effet responsable de la santé et de la sécurité de ses salariés. Il coordonne ses différentes équipes et attribue les moyens nécessaires tel que :

- Des actions de prévention des risques professionnels et de la pénibilité au travail.
- La mise en place d'une organisation et de moyens adaptés.

1.3 Section 2 : Etat des lieux

1.3.1 Présentation du réseau VMS Bejaia :

L'entreprise a une architecture en couches et, pour assurer la communication entre ses différents services, elle connecte ces vlans à une connexion L.S (Ligne Spécialisée publique symétrique) en fibre optique fournie par Algérie télécom, Le schéma ci-dessous nous montre l'infrastructure du réseau VMS Bejaia :

A. Présentation de l'architecture réseau existant dans l'entreprise

VMS Bejaia construit un réseau en choisissant une topologie arborescente pour connecter ses différents appareils, comme illustré dans la figure suivante :

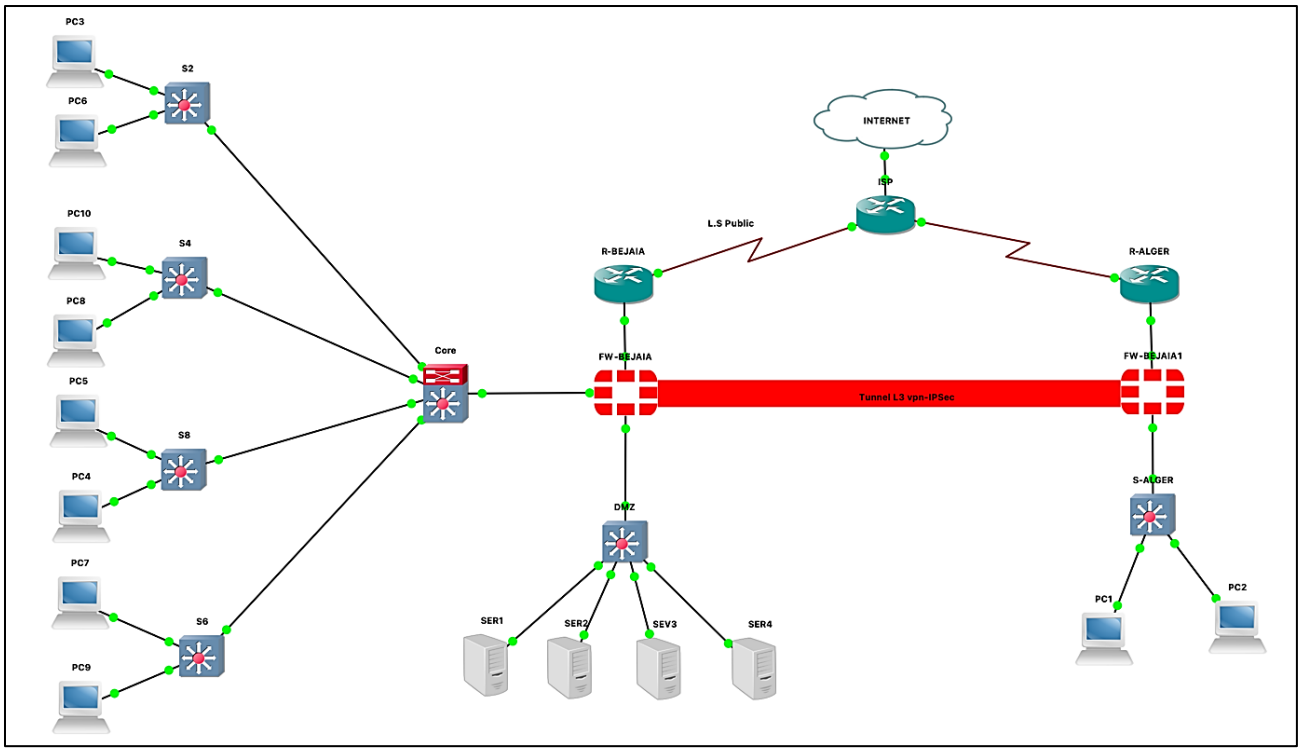

Figure 5 Architecture de réseau VMS Bejaia

B. Analyse du parc informatique

➢ **Présentation d'environnement hard et soft :**

Nom de l'équipement	Le hardware (hard)	Software (soft)
Routeur	ISR 4331	IOS (International Organisation for Standardisation)
Pare-feu	PFSENSE	FREEBSD
SWITCH	HPE 1820-24G MANAGED L2 HPE 1920-24G MANAGED L3	LINUX
SERVER	ESHP PROLIANT DL380P GENERATION 10	• ESXI • GOAUTODIAL • SERVER WINDOWS 2022
PC PORTABLE	DELL IAER 35 R	WINDOWS 10

Tableau 2 L'environnement hardware et le software

➢ **Les caractéristiques des équipements par niveaux :**

Nom de l'équipement	Modèle	Caractéristiques
Router 	ISR 4331	• **Ram:** 4 g0 (installer) /16 go (maximum) • **Mémoire flash :**4000 mo • **Débit :**100 mb/s • **Protocole de liaison de données :** Ethernet, Fast Ethernet et gigabit-ethernet
Pare-feu 	PFSENSE	• **Débit :** 4000 Mbit/s • **Débit ips :** 2700mbit/s • **Debit vpn Ip sec:** 560 mbit/s • **@ IP/numéro de port**
Switch 	**HPE 1920**	• **Ports :** 24 ports • **Mémoire flash :** 16mo • **Mémoire ram :** 128mo • **Capacite de commutation :** 32 Gbit/s
Switch 	**HPE 1820**	• **Ports :** 24 ports • **Mémoire flash :** 128mo • **Mémoire ram :** 512mo • **Capacite de commutation :** 56 Gbit/s
Server 	HP PROLIANT DL380P GENERATION 10	• Processor intel Xeon • Silver 4110 (octo-core 2.1 Ghz / 3.0 Ghz turbo-16 threads-cache 11mo) • 16 g0 ddr4 rdimm (1x 16 go -12 slots)
PC portable 	DELL IAER 35 R	• **AMD core :** i5 8th génération • **Ram :** 8go • **Disque :** 256go • **Ecran :** UHD graphies 620 ($1920 \times 1080 \times 32b$)

Tableau 3 Détails des ressources disponibles de l'entreprise

1.4 Section 3 : Problématiques et Solutions proposées

1.4.1 Problématiques

Le processus d'évaluation et d'analyse de l'infrastructure existante de l'entreprise VMS Bejaia a révèle plusieurs facteurs de faiblesse contribuant à l'échec de la détection des attaques. Nous allons en présenter quelques-unes :

- La gestion de la sécurité au sein de l'infrastructure de VMS Bejaia est rendue complexe par la diversité des appareils et des logiciels, entraînant des vulnérabilités et des configurations variées.
- L'absence de vue d'ensemble complète et en temps réel de tous les systèmes et réseaux entraîne une détection tardive des incidents de sécurité.
- Risque d'attaques sophistiquées qui ciblent spécifiquement l'entreprise.

Ces faiblesses compromettent la capacité de l'entreprise à détecter, répondre et anticiper efficacement les menaces de sécurité. Il devient crucial de déployer des solutions adaptées afin de renforcer de manière proactive la sécurité globale du système.

1.4.2 Objectifs à atteindre

Les objectifs visés incluent :

- Améliorer la détection précoce des incidents de sécurité.
- Renforcer la capacité de réponse rapide aux menaces sophistiquées.
- Assurer une vue d'ensemble complète et en temps réel de l'infrastructure de sécurité.
- Réduire les vulnérabilités dues à la diversité des appareils et des logiciels.

1.4.3 Propositions

Dans le but de résoudre ses défis, nous avons proposé deux solutions :

1) **Implémentation d'un SIEM (Système de Gestion des Informations et des Événements de Sécurité) :**

- Collecte et corrélation des données de sécurité à partir de diverses sources.
- Analyse avancée des événements pour détecter les menaces et les comportements anormaux.
- Génération d'alertes en temps réel pour une réponse proactive aux incidents.

2) **Déploiement d'IDS/IPS (Système de Détection et de Prévention d'Intrusion) :**

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

1.5 Conclusion

Dans ce chapitre, nous avons donné un aperçu de l'infrastructure de client de VMS Bejaia fournie par Campus NTS, identifiant un problème crucial qui a nécessité la recherche et la mise en œuvre d'une nouvelle architecture de réseau sécurisée. Le prochain chapitre se concentrera sur les aspects de sécurité des réseaux informatiques.

Chapitre 2 La sécurité des réseaux informatiques

2.1 Introduction

Dans l'ère numérique moderne, les réseaux informatiques sont essentiels pour faciliter la communication, le partage de ressources et l'accès à l'information globalement. Toutefois, cette connectivité accrue nécessite une protection renforcée contre les menaces omniprésentes. Ce chapitre explore les bases de la sécurité des réseaux informatiques, avec un aperçu des principes, concepts et technologies clés.

Tout d'abord, nous décrirons les réseaux informatiques. Ensuite, nous aborderons la sécurité des réseaux, les menaces potentielles (comme les virus, logiciels malveillants, attaques…etc.). Et enfin les mécanismes de protection (Authentifications, chiffrement, IDS/IPS…).

2.2 Le réseau informatique

Un réseau informatique est un système interconnecte de dispositifs, tels que des ordinateurs et des périphériques, relies par des moyens de transmission comme le câble coaxial, la fibre optique ou la paire torsadée. Ces réseaux facilitent la communication et le partage de ressources à différentes échelles, allant des réseaux personnels (PAN) couvrant de courtes distances, aux réseaux locaux (LAN) dans des bâtiments ou campus, aux réseaux métropolitains (MAN) couvrant des zones urbaines, jusqu'aux réseaux étendus (WAN) s'étendant sur de vastes distances géographiques. Les réseaux peuvent adopter diverses topologies physiques comme en bus, en étoile, en anneau ou en maillage, influençant la manière dont les données sont transmises. Les éléments constitutifs incluent des équipements comme les commutateurs, routeurs, modems, vlans, serveurs et passerelles, ainsi que des logiciels réseau comprenant des protocoles de communication et des systèmes d'exploitation réseau comme TCP/IP et divers services réseau comme DNS, DHCP, HTTP, et autres. Les modèles de référence OSI et TCP/IP fournissent un cadre standard pour la gestion et la communication efficace au sein des réseaux informatiques, facilitant ainsi l'accès à l'information et soutenant le développement économique à l'échelle mondiale.

2.3 Sécurité des réseaux informatique

Figure 6 Sécurité des réseaux informatiques

2.3.1 Définition de la sécurité informatique

La sécurité informatique recouvre l'ensemble des techniques et technologies permettant de réduire les risques de fuites d'informations, de modifications de données ou de détériorations des services. Elle utilise diverses méthodes et architectures pour atteindre un certain niveau de protection, réduisant ainsi la vulnérabilité des systèmes contre les menaces accidentelles ou intentionnelles. Elle assure que les ressources du système d'information d'une organisation (matérielles ou logicielles) sont utilisées exclusivement dans le cadre prévu. [1] [2] [3].

2.3.2 Définition de système informatique

Ensemble de matériels tels que des ordinateurs, des serveurs, des périphériques, ainsi que de logiciels comme les systèmes d'exploitation et les applications, qui interagissent pour traiter, stocker et transmettre des données et des informations.

2.3.3 Importance de la sécurité informatique dans le monde numérique moderne

La sécurité informatique a pour but de garantir la confidentialité, la protection des informations sensibles, la continuité des services et la prévention contre toutes divulgation, altération ou destruction et également à les minimiser. [4]

2.3.4 Objectifs de la sécurité informatique

La sécurité Informatique consiste principalement à protéger les informations d'un système contre toutes divulgation, altération ou destruction.

• La disponibilité : Garantir que les systèmes ou services sont accessibles et fonctionnels sans interruptions majeures.
• L'intégrité : Garantir que les informations n'ont pas été modifiées par des entités non autorisées ou inconnues.
• La confidentialité : Empêcher la divulgation d'informations a des entités non autorisées à les connaitre.
• L'authentification : Prouver qu'une information ou une entité provient de la source annoncée.
• La non répudiation : Prévenir les entités de réfuter (nier) leurs actions antérieures ou leurs engagements.

2.3.5 Menaces en sécurité informatique

Les menaces (malware) en sécurité informatique peuvent toucher les composants matériels, logiciels ou données, et peuvent être classées en deux grandes catégories : [1]

- Les menaces non intentionnelles (accidentelles) :
  - Bugs logiciels : Erreurs de programmation qui peuvent entraîner des failles de sécurité.
  - Les pannes matérielles : Défaillances des composants physiques qui peuvent perturber les systèmes informatiques.
- Les menaces intentionnelles :
  - Passives : Interceptions où des attaquants écoutent ou surveillent les communications sans altérer les données, compromettant la confidentialité.
  - Actives : Incluent des interceptions, des interruptions (perturbation des services), des modifications (altération des données) et des fabrications (insertion de fausses informations).

A. Virus, vers et logiciels malveillants

Les logiciels malveillants, également connus sous le nom de malwares, sont des programmes informatiques conçus dans le but de causer des dommages, de perturber le fonctionnement normal d'un système informatique ou de perturber la sécurité des données. Ils peuvent inclure différents types telles que :

1) **Virus :** Les virus informatiques, nommés pour leur capacité à infecter plusieurs fichiers, se propagent via e-mails et supports physiques comme les clés USB (disquettes). Le premier virus selon le NIST, "Brain", créé en 1986 par deux frères pour lutter contre le piratage de leurs logiciels, infectait le secteur d'amorçage des disquettes, facilitant ainsi sa diffusion.

2) **Vers (Worms) :** Les vers se diffusent sans intervention humaine via les réseaux, exploitant les failles des systèmes pour infecter d'autres machines. Ils se multiplient rapidement et peuvent contenir des charges malveillantes visant à voler ou supprimer des fichiers, tout en notamment parfois les performances des systèmes infectés.
3) **Adware :** Logiciel publicitaire qui affiche des publicités indésirables sur un ordinateur, généralement intégré à des logiciels gratuits.
4) **Spyware :** Logiciel conçu pour espionner les activités d'un utilisateur sans son consentement, collectant souvent des informations personnelles.
5) **Chevaux de Troie (Trojans) :** Programme malveillant déguisé en application légitime pour tromper l'utilisateur, souvent utilisé pour prendre le contrôle d'un système.
6) **Ransomwares :** Logiciels malveillants qui chiffrent les fichiers d'un utilisateur ou bloquent l'accès à un système jusqu'à ce qu'une rançon soit payée pour obtenir la clé de déchiffrement ou la restauration de l'accès.

B. Piratage et attaques informatiques

– **Piratage (hacking) :** est l'accès non autorisé aux systèmes, réseaux ou données pour voler, corrompre ou altérer des informations. Les pirates exploitent les failles de sécurité pour contourner les mesures de protection et accéder à des données sensibles, avec des motivations variées telles que le vol d'informations ou le sabotage.
– **Les attaques :** est une action malveillante qui exploite les failles d'un système informatique. Les attaques informatiques peuvent être menées par des individus malveillants, des groupes de hackers, des organisations criminelles, des États-nations, ou d'autres acteurs malveillants.
  • Attaque interne : utilisateur malveillant, erreur involontaire, ...
  • Attaque externe : Piratage, virus, intrusion, …

Quelques exemples d'attaques : attaques XSS (Cross-Site Scripting), attaque d'anniversaire, attaque par écoute clandestine, attaque par déni de service (DOS ou DDOS), attaque par injection SQL, attaque par mot de passe.

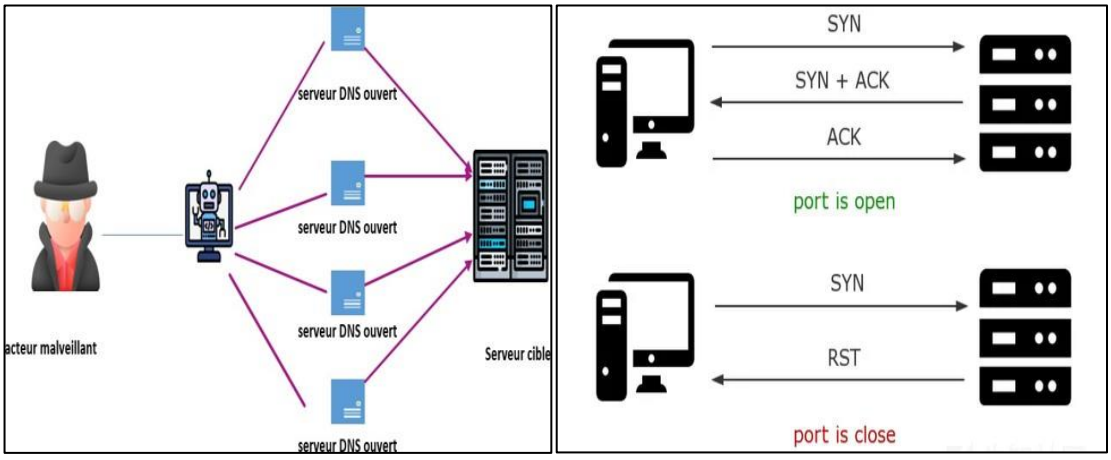

Figure 7 Attaque DOS, par analyse de port

C. Ingénierie sociale

L'ingénierie sociale est une méthode d'attaque qui exploite les faiblesses humaines. Cette technique utilisée par les cybercriminels pour manipuler les individus et les inciter à divulguer des informations confidentielles ou à effectuer des actions indésirables

‘‘L'ingénierie sociale consiste à entrer en relation avec un individu dans le but de lui soutirer des informations confidentielles à des fins frauduleuses. Pour les cybercriminels, l’ingénierie sociale est une pratique de manipulation. Cette stratégie « sociale » et non technique est fréquemment utilisée par les cybercriminels pour mener des attaques ciblées et de grande envergure, afin de dérober des données, de l'argent, et bien plus encore’’. [5]

On peut citer: Phishing (hameçonnage), Spear-Phishing (harponnage), baiting…

D. Espionnage et surveillance

- L'espionnage informatique désigne la pratique de collecter secrètement des informations sensibles ou confidentielles à des fins d'analyse, de surveillance ou d'exploitation, souvent réalisée par des entités étatiques, des organisations criminelles ou des acteurs malveillants.
- La surveillance numérique fait référence à la surveillance et à la collecte d'informations à travers des moyens électroniques et numériques, souvent réalisée pour des raisons de sécurité, de renseignement ou de contrôle, que ce soit par des gouvernements, des entreprises ou d'autres entités.

2.3.6 Principes de base de la sécurité informatique

Les principes incluent la protection des réseaux, des données et des utilisateurs, la gestion des vulnérabilités et la réponse aux incidents pour assurer une sécurité globale. [6]

2.3.7 Mécanisme de sécurité informatique

A. Authentification

1. **Mots de passe :** Les mots de passe sont essentiels pour sécuriser l'accès aux comptes en ligne. Pour assurer une protection efficace, il est recommandé d'utiliser des mots de passe complexes incluant des lettres, des chiffres et des caractères spéciaux, de les changer régulièrement, et d'utiliser des gestionnaires de mots de passe pour une gestion sécurisée et efficace.
2. **Authentification a deux facteurs :** L'authentification à deux facteurs (2FA) renforce la sécurité en ajoutant une vérification supplémentaire au-delà du mot de passe, comme un code SMS, une application de génération de code ou un dispositif matériel. Cela diminue significativement le risque d'accès non autorisé même en cas de compromission du mot de passe initial.

B. Contrôle d’accès

1. **Listes de contrôle d’accès (ACL) :** Une liste de contrôle d'accès (ACL) est un ensemble de règles ordonnées utilisées pour filtrer le trafic réseau entrant ou sortant, permettant de définir les types de trafic autorisés ou bloqués aux interfaces des appareils, jouant un rôle clé dans la gestion de la bande passante et la sécurité réseau, en spécifiant quels utilisateurs ou systèmes peuvent accéder à quelles ressources et quelles actions ils peuvent effectuer. Il existe plusieurs types dont on peut citer [7] [8]:

- **ACL standard :**

- Filtrent les paquets en se basant uniquement sur l’adresse IP source.
- Offrent un filtrage basique et simple du trafic.

- **ACL étendues :**

- Permettent un contrôle plus précis que les ACL standard.
- Peuvent filtrer le trafic selon le protocole, le port, l’adresse IP source et l’adresse IP de destination.

- **ACL dynamiques :**

- Aussi connues sous le nom d'ACL « lock-and-key ».
- Permettent aux administrateurs d'accorder un accès temporaire aux utilisateurs pour certaines zones du réseau.

- **ACL réflexives :**

- Utilisées pour permettre aux paquets IP de retourner à l'expéditeur.
- Créées et supprimées de manière dynamique, elles renforcent la sécurité du réseau.

- **ACL à caractère temporel :**

- Permettent de limiter l'accès à un réseau ou à un appareil en fonction de l'heure et du jour de la semaine.

2. Rôles et privilèges

Les rôles et privilèges sont des mécanismes de gestion des accès qui permettent d'assigner des permissions spécifiques à des utilisateurs ou groupes d'utilisateurs en fonction de leur rôle au sein de l'organisation. Cette méthode simplifie la gestion des accès et assure que les utilisateurs disposent uniquement des permissions nécessaires pour accomplir leurs tâches.

a) Définition des rôles :

- **Rôle Administrateur :** Accès complet à toutes les ressources et capacités de gestion du système.
- **Rôle Utilisateur :** Accès limité aux ressources nécessaires pour réaliser des tâches spécifiques.
- **Rôle Invité :** Accès restreint, souvent limité à des ressources en lecture seule.

Privilèges :

- **Lecture :** Permet de consulter les informations.
- **Écriture :** Permet de modifier ou de supprimer des informations.
- **Exécution :** Permet d'exécuter des programmes ou des scripts.

C. Chiffrement

Le chiffrement symétrique et le chiffrement asymétrique sont les deux principales catégories de chiffrement [9] [1] [10].

1. **Chiffrement symétrique :** Le chiffrement symétrique utilise la même clé pour chiffrer et déchiffrer les données. Cette méthode est rapide et efficace pour le traitement de grandes quantités de données, mais la sécurité repose sur la protection de la clé partagée.

Exemples :

— AES (Advanced Encryption Standard)
— DES (Data Encryption Standard)
— 3DES (Triple DES)

2. **Chiffrement asymétrique :** Le chiffrement asymétrique utilise une paire de clés, une clé publique pour chiffrer les données et une clé privée pour les déchiffrer. Cette méthode est plus sécurisée pour le partage de clés et les communications sécurisées, mais elle est plus lente et consomme plus de ressources.

Exemples :

— RSA (Rivest-Shamir-Adleman)
— ECC (Elliptic Curve Cryptography)
— DSA (Digital Signature Algorithm)

D. Outils de sécurité des réseaux

1. **Pares-feux (Firewalls) :** Les pares-feux sont des dispositifs de sécurité réseau qui contrôlent et filtrent le trafic entrant et sortant selon des règles définies. Ils servent à

protéger les réseaux contre les accès non autorisés et les attaques en bloquant ou autorisant le trafic en fonction de critères tels que les adresses IP, les ports et les protocoles. Les types de pares-feux :

- **Pare-feu à état :**
  - Examine l'état des connexions pour autoriser ou bloquer le trafic.
  - Maintient une table d'état des connexions pour gérer le flux de données.
- **Pare-feu de paquet :**
  - Filtrage basé sur les adresses source et destination des paquets.
  - Il s'agit d'une méthode de filtrage basique utilisée pour contrôler le flux de paquets.
- **Pare-feu de niveau application :**
  - Inspecte le trafic jusqu'au niveau de l'application pour des règles plus fines.
  - Permet de contrôler et de filtrer spécifiquement le trafic en fonction des applications et des protocoles utilisés.

2. **DMZ :** La DMZ (Zone démilitarisée) est une zone du réseau située entre un réseau interne sécurisé et un réseau non sécurisé, comme Internet. Elle contient des ressources accessibles au public tout en isolant les systèmes internes critiques. Les serveurs Web, les serveurs de messagerie et les serveurs FTP sont souvent placés dans la DMZ pour limiter l'accès direct aux systèmes internes sensibles.
3. **IDS/IPS (Intrusion Detection System/Intrusion Prevention System) :** Les IDS et IPS sont des systèmes de détection et de prévention des intrusions qui surveillent et analysent le trafic réseau pour détecter les activités suspectes ou malveillantes.

- **IDS (Système de détection d'intrusion) :** Analyse le trafic en temps réel pour identifier les anomalies ou les signatures d'attaques.
- **IPS (Système de prévention d'intrusion) :** Agit activement pour bloquer ou atténuer les attaques détectées en temps réel.

E. Outils de sécurité des applications

1. Tests de sécurité des applications (AST)

Les tests de sécurité des applications (AST) sont essentiels pour identifier et prévenir les vulnérabilités dans les applications logicielles tout au long de leur cycle de développement. Voici les principales techniques utilisées :

- Analyse Statique de Sécurité des Applications (SAST) : Examine le code source, binaire ou intermédiaire pour détecter les failles de sécurité potentielles avant l'exécution de l'application.
- Tests Dynamiques de Sécurité des Applications (DAST) : Simulent des attaques externes en inspectant l'application en cours d'exécution pour identifier les vulnérabilités exploitées par un attaquant.
- Tests Interactifs de Sécurité des Applications (IAST) : Intègrent les tests SAST et DAST en examinant les applications pendant leur exécution, permettant de détecter les failles lorsque l'application interagit avec d'autres systèmes.
- Intégration et Automatisation : L'intégration de ces outils dans les processus de développement CI/CD permet de détecter rapidement les problèmes de sécurité et de les corriger avant le déploiement.

2. Pare-feu d'application web (WAF)

Les pares-feux d'application web (WAF) sont des dispositifs de sécurité spécifiquement conçus pour protéger les applications web contre divers types d'attaques :

- Protègent en inspectant et filtrant le trafic HTTP/HTTPS entrant et sortant pour détecter et bloquer les attaques comme les injections SQL, les attaques XSS (Cross-Site Scripting), etc.
- Offrent une défense proactive contre les attaques zero-day et les menaces ciblées qui visent spécifiquement les applications web.
- Facilitent l'intégration avec les environnements de développement et de production pour assurer une protection continue et ajustable selon les besoins spécifiques de sécurité de chaque application.

2.4 Conclusion

Dans ce chapitre, nous avons exploré les bases des réseaux informatiques et de la sécurité, en définissant les réseaux et en examinant leurs types, topologies, menaces et stratégies de protection. Ces connaissances sont cruciales pour comprendre le fonctionnement des infrastructures numériques et pour assurer leur intégrité et leur sécurité.

Un administrateur réseau et système doit maîtriser ces fondements pour anticiper les différentes formes d'attaques potentielles et sécuriser les données de l'organisation.

Dans le chapitre suivant, nous aborderons divers concepts liés aux deux solutions proposées SIEM et IDS/IPS, poursuivant ainsi notre exploration de la sécurité informatique et de ses applications pratiques dans la protection des réseaux et des systèmes.

Chapitre 3
La gestion de la sécurité

3.1 Introduction

Dans le domaine de la sécurité informatique, la protection contre les menaces et les attaques constitue une priorité cruciale pour toute organisation moderne. Ce chapitre explore deux aspects essentiels de la sécurité : la détection et la prévention des intrusions, ainsi que les systèmes de gestion des informations et des événements de sécurité (SIEM).

Le chapitre 3 explore en profondeur les aspects cruciaux de la détection et de la prévention des intrusions, ainsi que le système de gestion des informations et des événements de sécurité (SIEM). Nous commencerons par définir ces concepts essentiels, en mettant l'accent sur leur importance dans le domaine de la sécurité informatique, leurs principes de base et leurs objectifs.

Premièrement, nous examinerons en détail les systèmes de détection (IDS) et de prévention (IPS), en expliquant comment ces outils surveillent le trafic réseau et les journaux système pour détecter les signes d'intrusions. Nous discuterons également des stratégies de prévention, telles que la configuration de pare-feu, l'utilisation de politiques de sécurité robustes, ainsi que le rôle crucial des IDS/IPS dans le blocage des attaques connues et le renforcement de la sécurité des systèmes.

Nous aborderons également le système Snort, un outil populaire dans le domaine de la sécurité informatique. Nous explorerons son histoire, son évolution et son mode de fonctionnement, en détaillant ses mécanismes avancés de détection des intrusions, qui le rendent particulièrement efficace dans la protection contre les cybermenaces.

Deuxièmement, nous nous pencherons sur les SIEM, qui intègrent la gestion des informations de sécurité (SIM) et la gestion des événements de sécurité (SEM). Nous analyserons leur architecture typique, incluant la collecte, la normalisation, la corrélation, l'analyse et le reporting des événements de sécurité. En mettant l'accent sur des plateformes comme Splunk, nous montrerons comment les SIEM améliorent la posture de sécurité en permettant une surveillance centralisée, une corrélation avancée des événements et une réponse rapide aux incidents de sécurité.

3.2 Section 1: IDS (Intrusion Detection Systems) et IPS (Intrusion Prevention Systems)

3.2.1 Introduction à la détection et la prévention

La détection et la prévention sont deux concepts fondamentaux de la sécurité informatique visant à protéger les systèmes et les réseaux contre les menaces et les attaques potentielles.

La détection en sécurité informatique consiste à repérer les activités suspectes ou malveillantes sur un réseau ou un système en surveillant le trafic réseau, les journaux système et d'autres sources de données. Son objectif principal est d'alerter les administrateurs sur les incidents de sécurité potentiels pour qu'ils puissent réagir rapidement et efficacement.

La prévention en sécurité informatique implique l'adoption de mesures proactives pour empêcher les attaques et les intrusions. Cela comprend la configuration de pare-feu, l'établissement de politiques de sécurité, l'utilisation d'antivirus, de systèmes IDS/IPS, ainsi que la formation des utilisateurs. Son objectif est de diminuer les risques d'incidents de sécurité en bloquant les attaques connues et en renforçant la sécurité des systèmes et réseaux.

La détection et la prévention en sécurité informatique sont essentielles pour protéger efficacement les systèmes contre les menaces et attaques potentielles, renforçant ainsi la sécurité globale des organisations. [11]

3.2.2 Fondements de la détection et la prévention

A. Principes de base :

- **Proactivité :** anticiper et conter les menaces potentielles avant qu'elles ne deviennent des incidents de sécurité.
- **Compréhension des menaces :** connaitre les différentes menaces et vulnérabilités pour contrer les attaques.
- **Surveillance continue :** observer en permanence le réseau et les activités pour détecter les intrusions.
- **Réactivité rapide :** répondre rapidement aux menaces détectées pour limiter les dommages.
- **Méthodologie basée sur les risques :** évaluer les risques spécifiques et les prioriser les mesures de sécurité.

B. Objectifs de la détection et de la prévention en sécurité informatique :

- **Identification des menaces :** reconnaitre les activités suspectes, les tentatives d'intrusion et les comportements anormaux qui pourraient indiquer une attaque imminente.
- **Réponse rapide aux incidents :** signaliser rapidement les menaces détectées aux équipes de sécurité pour limiter les dommages potentiels et restaurer l'intégrité du système.
- **Traçabilité :** suivre et enregistrer les activités des utilisateurs et des systèmes pour faciliter la reconstruction des événements en cas d'incident ou d'enquête.
- **Confidentialité :** protéger les informations sensibles contre l'accès non autorisé pour garantir leur confidentialité.
- **Intégrité :** garantir que les données restent exactes et complètes en évitant toute altération non autorisée.
- **Disponibilité :** s'assurer que les systèmes et les données sont disponibles et utilisables lorsque nécessaire pour éviter les interruptions de service.
- **Non-répudiation :** fournir des preuves indéniables qu'une action a été effectuée par une entité spécifique pour empêcher toute négation de responsabilité.
- **Authentification :** vérifier l'identité des utilisateurs et des systèmes pour garantir leur légitimité et leur autorisation d'accès.
- **Prévention des pertes financières :** réduire les risques de pertes financières causées par des incidents de sécurité tels que le vol de données ou les fraudes.
- **Protection de la réputation :** éviter les atteintes à la réputation de l'organisation en protégeant ses actifs numériques.
- **Conformité réglementaire :** respecter les lois, les réglementations et les normes en matière de sécurité informatique pour éviter les sanctions et les amendes.
- **Sécurité physique :** protéger les infrastructures physiques hébergeant les systèmes informatiques contre les menaces physiques telles que le vol ou les catastrophes naturelles**.**

3.2.3 Technologies de détection

A. Systèmes de détection d'intrusion (IDS) :

Un IDS est un système de surveillance automatisé qui analyse le trafic réseau ou les journaux système à la recherche de signes d'activité non autorisée ou anormale. Il alerte les administrateurs lorsqu'il détecte une intrusion potentielle.

B. Analyse comportementale

L'analyse comportementale dans un IDS est le processus par lequel l'IDS surveille, analyse et identifie les comportements normaux et anormaux sur un réseau ou un système informatique, dans le but de détecter et de prévenir les intrusions et les activités malveillantes.

- **Surveillance continue :** L'IDS surveille en permanence les activités sur le réseau ou sur les systèmes informatiques pour détecter les comportements inhabituels ou suspects.
- **Création de profils de comportement :** À partir des données collectées, l'IDS établit des profils de comportement normal pour les utilisateurs, les applications et les systèmes. Ces profils servent de référence pour identifier les écarts par rapport aux comportements attendus.
- **Détection des anomalies :** Lorsque l'IDS détecte des activités qui ne correspondent pas aux modèles de comportement normal, il les identifie comme des anomalies potentielles. Cela peut inclure des tentatives d'accès non autorisées, des changements inattendus dans les schémas de trafic réseau, etc.
- **Analyse des corrélations :** Pour améliorer la précision de la détection, l'IDS peut corréler plusieurs événements ou anomalies pour identifier des schémas d'activité suspects. Par exemple, une série d'événements apparemment inoffensifs peut être identifiée comme une attaque coordonnée lorsqu'ils sont examinés dans leur ensemble.
- **Alertes et notifications :** Lorsqu'une activité anormale est détectée, l'IDS déclenche des alertes ou des notifications pour informer les administrateurs de sécurité. Ces alertes peuvent être envoyées par e-mail, SMS ou d'autres moyens pour permettre une réponse rapide.
- **Adaptabilité et apprentissage continu :** L'IDS doit être capable de s'adapter aux nouveaux comportements malveillants et aux évolutions du paysage des menaces. Cela peut nécessiter des mises à jour régulières des modèles de comportement et des algorithmes de détection.

C. Les logs d'un système de détection d'intrusion (IDS) :

Sont des enregistrements détaillés des activités observées par l'IDS. Ces logs sont essentiels pour identifier, analyser et répondre aux incidents de sécurité. Chaque log IDS contient :

-Date et Heure : Chaque entrée de log inclut un horodatage précis, indiquant quand l'activité suspecte a été détectée.

-Source et Destination : Les logs précisent les adresses IP sources et destinations, permettant d'identifier d'où provient le trafic et où il est dirigé.

- Type d'Intrusion : Les logs indiquent le type d'attaque détectée (par exemple, tentative d'accès non autorisé, attaque par déni de service, etc.).

- natures et Règles : Pour les systèmes basés sur des signatures, les logs incluent les signatures ou les règles spécifiques qui ont été déclenchées.

- Détails du Trafic : Informations sur les protocoles utilisés, les ports impliqués et la quantité de données échangées.

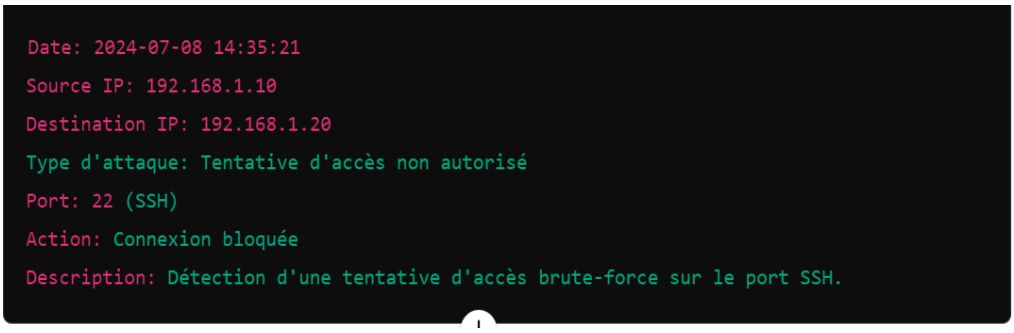

Figure 8 Exemple de log IDS

D. Surveillance des journaux (logs) :

La surveillance des journaux (logs) de l'IDS est une pratique essentielle consistant à collecter, analyser et surveiller en continu les événements liés à la sécurité. Cette surveillance permet de détecter les activités suspectes ou anormales, de déclencher des alertes en cas de menace potentielle, et de corréler les événements pour identifier des schémas d'attaque.

3.2.4 Technologies de prévention

A. Systèmes de prévention d'intrusion (IPS) :

Un IPS est un système de sécurité qui surveille activement le trafic réseau ou les activités système à la recherche de comportements anormaux ou de signatures d'attaques connues. Contrairement à un IDS qui se contente de détecter les intrusions, un IPS est capable de prendre des mesures actives pour bloquer ou empêcher ces intrusions.

B. Filtrages des paquets :

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

C. Contrôles d'accès :

Le contrôle d'accès se réfère à la capacité de l'IPS à réguler le flux de trafic réseau en fonction de règles prédéfinies.

- Détection des intrusions
- Analyse et décision
- Application de politiques de sécurité
- Contrôle du trafic
- Réponse en temps réel

3.2.5 Outils de détection et de prévention

A. Exemples d'outils IDS/IPS :

- Snort
- Suricata
- Bro (maintenant appelé Zeek)
- Cisco Firepower

B. Logiciels de surveillance des journaux :

- Snort_inline
- Suricata_inline

- Splunk Enterprise Security
- SolarWinds Security Event Manager (formerly Log & Event Manager)

C. Solutions de filtrage des paquets :

- **Firewalls réseau :** Contrôlent le trafic en fonction de règles de sécurité prédéfinies.
- **Systèmes de prévention des intrusions (IPS) :** Détectent et neutralisent les activités malveillantes en temps réel.
- **Filtrage de contenu :** Bloque les fichiers, URL ou applications malveillants.
- **Filtrage de niveau applicatif :** Identifie et bloque les attaques spécifiques au niveau des applications.
- **Systèmes de prévention de la perte de données (DLP) :** Empêchent la fuite de données sensibles.
- **Proxy :** Contrôle et filtre le trafic internet selon des règles de sécurité définies.

3.2.6 Méthodologies de détection et de prévention

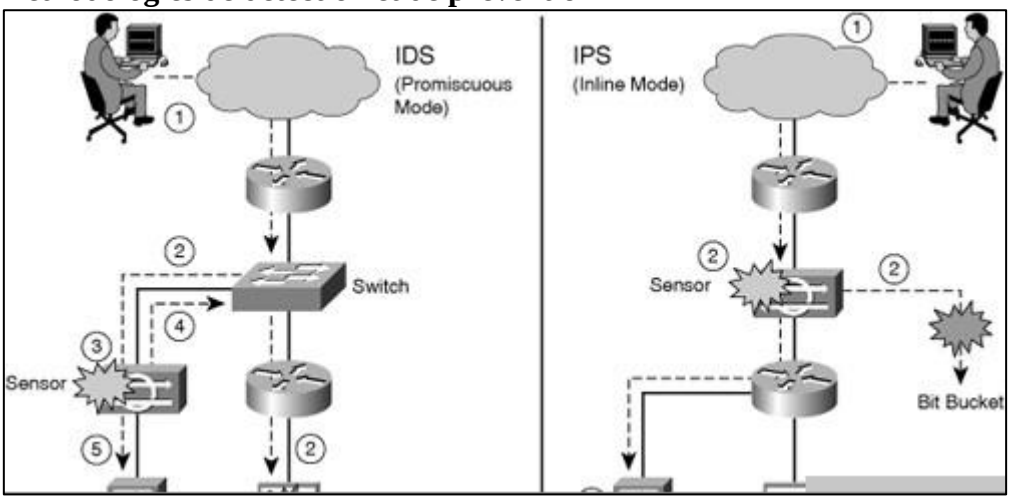

Figure 9 Fonctionnement d'IDS et IPS

A. Méthodes de détection des menaces :

- Analyse de signatures : Comparaison des données avec des signatures connues de menaces.
- Analyse comportementale : Surveillance des comportements anormaux des utilisateurs, des applications et des systèmes.
- Détection d'anomalies : Surveillance continue des modèles de trafic et d'activité pour identifier des déviations significatives.
- Analyse de vulnérabilités : Identification des failles connues dans les systèmes et les logiciels.
- Intelligence sur les menaces : Utilisation d'informations externes pour identifier de nouvelles techniques d'attaques et les tendances en matière de cybermenaces.
- Analyse de la réputation : Évaluation de la réputation des adresses IP, des domaines, des fichiers ou des applications pour identifier les sources potentielles de menaces.

B. Méthodes de prévention des menaces :

- Mise en place de pare-feu : Contrôle du trafic réseau et application de règles de sécurité.
- Déploiement de systèmes de prévention des intrusions (IPS) : Surveillance en temps réel du trafic réseau pour neutraliser les activités malveillantes.
- Utilisation de solutions de sécurité Endpoint : Installation de logiciels de sécurité sur les dispositifs Endpoint pour détecter et prévenir les attaques.

- Sécurisation des applications et des services : Mise en œuvre de bonnes pratiques de sécurité, de correctifs réguliers et de contrôles d'accès.
- Sensibilisation à la sécurité et formation des utilisateurs : Éducation des utilisateurs sur les bonnes pratiques de sécurité informatique et la reconnaissance des menaces.
- Utilisation de technologies de chiffrement : Protection des données sensibles en transit et au repos par chiffrement.

3.2.7 Gestion des incidents

Un processus crucial pour détecter, répondre et atténuer les menaces. Elle commence par une détection proactive des risques, suivie d'une évaluation minutieuse et de mesures immédiates pour contenir et neutraliser l'incident. Une analyse post-incident est ensuite effectuée pour identifier les améliorations nécessaires. Enfin, un suivi continu garantit l'efficacité des mesures correctives et prévient les futures occurrences.

A. Processus de détection des incidents :

- Surveillance continue : Systèmes de surveillance pour repérer les activités suspectes.
- Analyse des alertes : Étude des alertes générées par les outils de sécurité.
- Investigation approfondie : Analyse approfondie pour déterminer la nature et les causes des incidents.
- Notification et escalade : Communication des incidents aux équipes de sécurité et parties prenantes, avec une éventuelle escalade en fonction de leur gravité.

B. Processus de prévention des incidents :

- Évaluation des risques : Identification des vulnérabilités et des menaces pour évaluer les risques potentiels.
- Mise en œuvre de contrôles de sécurité : Déploiement de mesures telles que les mises à jour, la configuration correcte des systèmes et la mise en place de dispositifs de sécurité.
- Formation et sensibilisation : Sensibilisation des employés à la sécurité et formation sur la reconnaissance des menaces et les bonnes pratiques.
- Gestion des accès et des identités : Contrôle de l'accès aux ressources sensibles et gestion des identités pour réduire les risques de compromission.

3.2.8 Intégration avec d'autres technologies de sécurité

A. Intégration avec les pares-feux :

- Blocage automatique : L'IDS/IPS surveille le trafic réseau à la recherche d'activités suspectes ou de menaces potentielles. Lorsqu'une menace est détectée, l'IDS/IPS peut envoyer une alerte au pare-feu pour bloquer automatiquement le trafic malveillant, empêchant ainsi les attaques de réussir.
- Enrichissement des règles de pare-feu : Les informations sur les menaces détectées par l'IDS/IPS peuvent être utilisées pour enrichir les règles de pare-feu. Par exemple, si un IDS/IPS identifie une adresse IP malveillante, cette adresse peut être ajoutée à la liste de blocage du pare-feu pour empêcher tout accès ultérieur de cette adresse.
- Corrélation des événements : L'IDS/IPS peut corréler les événements détectés avec les activités observées par le pare-feu. Cette corrélation permet une meilleure compréhension de la nature des attaques et de leur impact potentiel sur le réseau.
- Coordination de la réponse aux incidents : En cas d'incident de sécurité, l'IDS/IPS et le pare-feu peuvent coordonner leur réponse pour contenir rapidement la menace et minimiser les dommages. Par exemple, l'IDS/IPS peut signaler une attaque au pare-feu, qui peut alors bloquer le trafic malveillant et alerter les administrateurs.

B. Intégration avec les systèmes de gestion des identités et des accès (IAM) :

L'intégration d'IDS/IPS avec IAM permet une approche holistique de la sécurité en combinant la détection des menaces avec la gestion des identités et des accès. Cette intégration offre plusieurs avantages :

- Automatisation et Conformité : Les systèmes IDS/IPS automatisés s'intègrent harmonieusement à la pile de sécurité existante, assurant une protection efficace contre les menaces connues avec un minimum de ressources. Cette automatisation joue également un rôle crucial dans la satisfaction des exigences de conformité aux normes réglementaires telles que GDPR, PCI DSS ou HIPAA, démontrant ainsi l'engagement envers la sécurité des données et des systèmes.
- Application de Politiques de Sécurité : La configuration des IDS/IPS permet une application agile des politiques de sécurité au niveau du réseau. Par exemple, en intégrant IAM avec IDS/IPS, il devient possible de bloquer sélectivement le trafic en provenance de sources spécifiques ou d'appliquer des politiques contextuelles pour des utilisateurs ou des appareils particuliers, renforçant ainsi la posture de sécurité globale de l'organisation.
- Visibilité étendue : L'intégration des IDS/IPS avec IAM offre une vue d'ensemble plus complète des activités réseau en combinant les données de détection des menaces avec les informations d'identification des utilisateurs et des appareils. Cette visibilité accrue permet aux équipes de sécurité d'identifier rapidement les comportements anormaux ou les tentatives d'accès non autorisées, renforçant ainsi la capacité à réagir efficacement aux menaces émergentes.
- Réponse plus rapide aux incidents : Grâce à une meilleure visibilité et à des politiques de sécurité plus granulaires, les équipes de sécurité peuvent réagir plus rapidement aux incidents. En combinant la détection en temps réel des IDS/IPS avec les capacités de gestion des accès des systèmes IAM, les actions correctives peuvent être déclenchées automatiquement dès qu'une menace est détectée, minimisant ainsi le temps de réaction et réduisant les dommages potentiels.
- Sécurité renforcée des applications : L'intégration des systèmes IAM avec les IDS/IPS permet d'appliquer des politiques de sécurité basées sur les identités et les rôles aux applications et aux services réseau. Cela permet de limiter l'accès aux ressources sensibles uniquement aux utilisateurs autorisés, renforçant ainsi la sécurité des applications et réduisant les risques d'exploitation des vulnérabilités.

3.2.9 Snort

A. Présentation générale de Snort :

Snort est un système de détection d'intrusions réseau (IDS) open source, créé en 1998 par Martin Roesch. Il fonctionne en analysant le trafic réseau en temps réel pour détecter les comportements malveillants ou les signatures d'attaques connues, y compris les tentatives d'intrusion, les scans de port, les attaques par déni de service (DDoS) et d'autres activités suspectes. Grâce à son architecture modulaire, il peut être utilisé dans une variété d'environnements, des réseaux domestiques aux infrastructures d'entreprise. Son utilisation est répandue dans les environnements informatiques pour renforcer la sécurité et protéger les réseaux contre les menaces en ligne. [12]

B. Historique et évolution de Snort :

Snort a débuté comme un projet open source visant à fournir une solution de détection d'intrusions réseau accessible à tous. Au fil du temps, il est devenu l'un des outils IDS les plus largement utilisés au monde, offrant une protection essentielle contre les menaces informatiques pour les organisations de toutes tailles.

- Création SNORT (1998) : À l'époque, les solutions commerciales étaient coûteuses.
- Versions initiales (version 1.0 en 1999) : Elles se concentraient sur la détection des signatures d'attaques connues en analysant le trafic réseau en temps réel.
- Adoption et popularité : il a gagné en popularité dans la communauté de la sécurité informatique en raison de sa gratuité, de sa flexibilité et de sa capacité à détecter un large éventail de menaces.
- Développement continu : ajouter des capacités avancées telles que la détection d'anomalies et l'analyse comportementale.
- Intégration avec d'autres technologies : il peut être utilisé en conjonction avec des systèmes de prévention d'intrusions (IPS), des pares-feux et des systèmes de gestion des événements et des informations de sécurité (SIEM).
- Versions majeures : les mises à jour ont permis à Snort de rester pertinent et compétitif sur le marché de la sécurité informatique.

C. Fonctionnement de Snort

Snort commence à capturer puis à analyser le trafic réseau en temps réel, détecter les comportements malveillants ou les signatures d'attaques connues, déclencher des alertes en cas de détection d'une menace, et permet aux administrateurs de prendre des mesures pour protéger le réseau contre les intrusions. (Voir Figure 10)

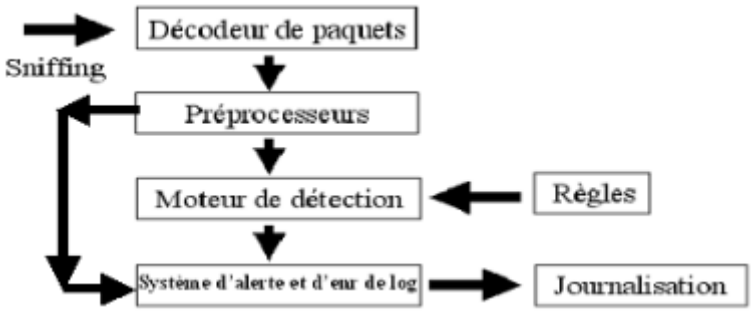

Figure 10 Fonctionnement de Snort

D. Mode de fonctionnement

Snort peut fonctionner selon trois modes principaux :

- **En mode Sniffer** : Snort capture et analyse le trafic réseau sur une interface spécifique en mode promiscuité, ce qui signifie qu'il écoute et collecte tous les paquets qui transitent sur le réseau, indépendamment de leur destination. Cela permet à Snort de surveiller tout le trafic réseau passant par cette interface.
- **Mode Packet Logger :** Dans ce mode, Snort capture et enregistre les paquets qui correspondent à des règles prédéfinies dans un fichier de logs. Contrairement au mode Sniffer, il n'analyse pas les paquets en temps réel, mais les stocke pour une analyse ultérieure. Ce mode est utile pour examiner le trafic passé après un événement particulier ou pour une analyse rétrospective.
- **Le mode Réseau :** est une combinaison des modes Sniffer et Packet Logger. Snort capture le trafic réseau en temps réel et l'analyse en fonction des règles définies. Les paquets qui correspondent à des règles prédéfinies sont enregistrés dans un fichier de logs pour une référence ultérieure. Ce mode offre à la fois la capacité d'analyse en temps réel et la possibilité de stocker les données pour une analyse postérieure.

E. Mécanismes de détection des intrusions :

- **Détection de signatures :** Snort identifie les modèles de trafic correspondant à des attaques connues à l'aide de règles de détection basées sur des signatures. Ces règles définissent des caractéristiques spécifiques des paquets réseau associées à des attaques connues.
- **Détection d'anomalies :** En plus de la détection de signatures, Snort peut détecter des comportements anormaux sur le réseau. Il surveille les schémas de trafic habituels et identifie les variations significatives qui pourraient indiquer une activité suspecte, comme un volume de trafic anormalement élevé ou des tentatives de connexion inhabituelles.
- **Analyse de protocole :** Snort comprend des préprocesseurs pour l'analyse approfondie de différents protocoles réseau. Ces préprocesseurs lui permettent de comprendre les spécificités de chaque protocole (TCP, UDP, ICMP, HTTP, etc.) et d'identifier les anomalies ou les comportements suspects associés à ces protocoles.
- **Détection de flux :** Snort effectue une analyse de flux pour suivre le flux de données entre différentes entités réseau. Il peut détecter les tentatives de communication suspectes ou les schémas de trafic qui pourraient indiquer une tentative d'intrusion en surveillant les relations entre les paquets réseau.
- **Intégration avec d'autres outils :** Snort peut être intégré avec d'autres outils de sécurité et de gestion des événements pour une détection plus avancée des intrusions. Par exemple, il peut être associé à des systèmes de gestion des informations et des événements de sécurité (SIEM) pour une analyse centralisée des alertes de sécurité et une réponse coordonnée aux incidents.

3.2.10 Les avantages et inconvénients d'IDS et IPS

Aspect	IDS (Systèmes de Détection d'Intrusion)	IPS (Systèmes de prévention d'intrusion)
Avantages	**Surveillance en temps réel** : détecte les activités suspectes immédiatement.	**Protection proactive** : bloque les attaques en temps réel, empêchant les intrusions.
	Detection des attaques connues : utilise des signatures pour identifier des modèles de comportement.	**Reduction des dommages** : minimise les impacts des incidents de sécurité en bloquant les attaques.
	Analyse post-incident : Fournit des journaux détaillés pour l'analyse des incidents après leur occurrence.	**Automatisation** : automatise la réponse aux menaces, réduisant le besoin d'intervention humaine immédiate.
	Réactions limitées : ne bloque pas les attaques, se contente de détecter et d'alerter.	**Impact sur les performances du réseau** : peut introduire de la latence en analysant le trafic en temps réel.

Inconvénients	**Faux positifs** : génère de nombreux faux positifs, surchargeant les alertes et rendant difficile la gestion des véritables incidents.	**Risque de faux positifs** : peut bloquer des trafics légitimes, perturbant les opérations normales.
	Maintenance continue : Nécessite des mises à jour régulières des signatures et des règles pour rester efficace contre les nouvelles menaces.	**Complexité de la gestion** : nécessite une expertise spécialisée pour une configuration optimale et éviter le blocage de trafics légitimes.

Tableau 4 Avantages et inconvénients d'IDS/IPS

3.3 Section 2 : Les systèmes de gestion des informations et des événements de sécurité (SIEM)

3.3.1 Présentation de SIEM :

Un SIEM (Security Information and Event Management) est une solution de cybersécurité qui collecte, analyse et corrèle les données de divers systèmes de sécurité pour détecter les incidents et faciliter la gestion des alertes. Il permet de centraliser les logs et les événements de sécurité afin de fournir une vue d'ensemble et des rapports en temps réel sur l'état de la sécurité d'une organisation. Les SIEM sont utilisés dans les différents domaines tels que : la sante, les finances, industriels, services publics, et les services en ligne…etc. [13] [14] [15] [16] [17]

3.3.2 Fonctionnalités et Composantes des SIEM :

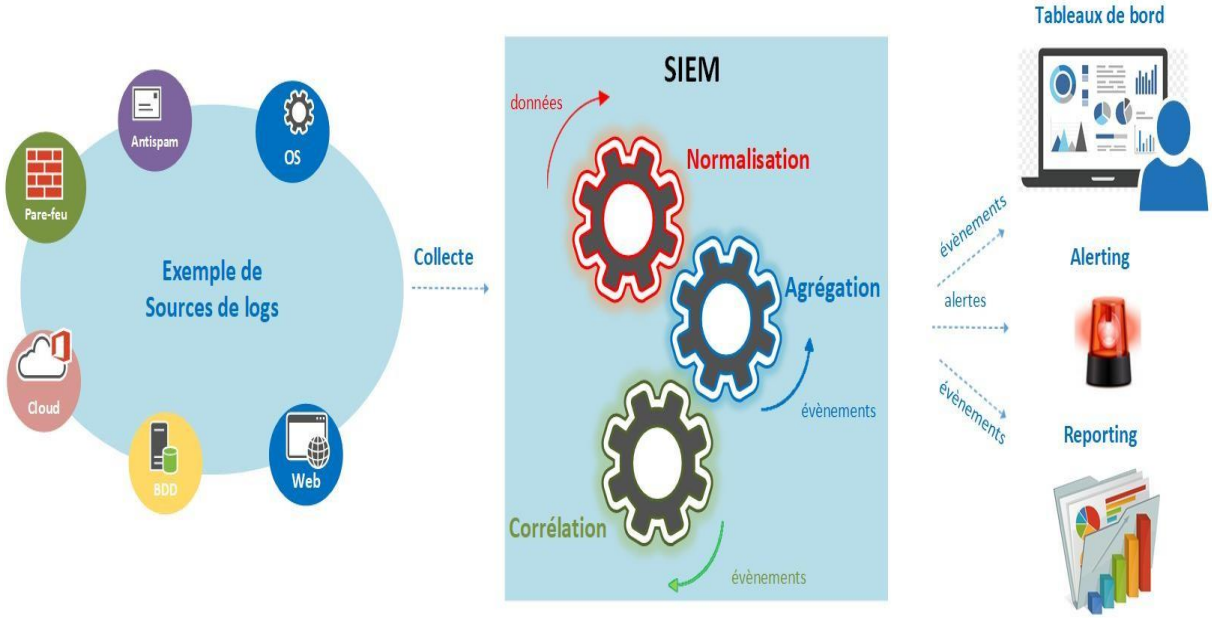

Figure 11 Fonctionnement de SIEM

A. Collecte des Logs (Log Collection) :

- **Agents (collecteurs)** : Logiciels installés sur les systèmes sources (serveurs, routeurs, pare-feu, etc.) qui collectent les logs et les envoient au SIEM.

```
Timestamp: 2024-07-08T14:35:21Z
Event ID: 10567
Source: Firewall
Source IP: 192.168.1.100
Destination IP: 10.0.0.50
Event Type: Intrusion Attempt
Severity: High
Description: Detected a potential intrusion attempt from IP 192.168.1.100 targeting the in
User: N/A
Action Taken: Connection Blocked
Correlation ID: c9f0e3a2-4e87-4b89-8f2a-b6824d62d4c1
Additional Info: Multiple failed login attempts detected prior to this event.
```

Figure 12 Exemple de log généré par un système SIEM

- **Connecteurs** : Interfaces ou modules qui permettent de collecter les logs de différentes sources et formats.

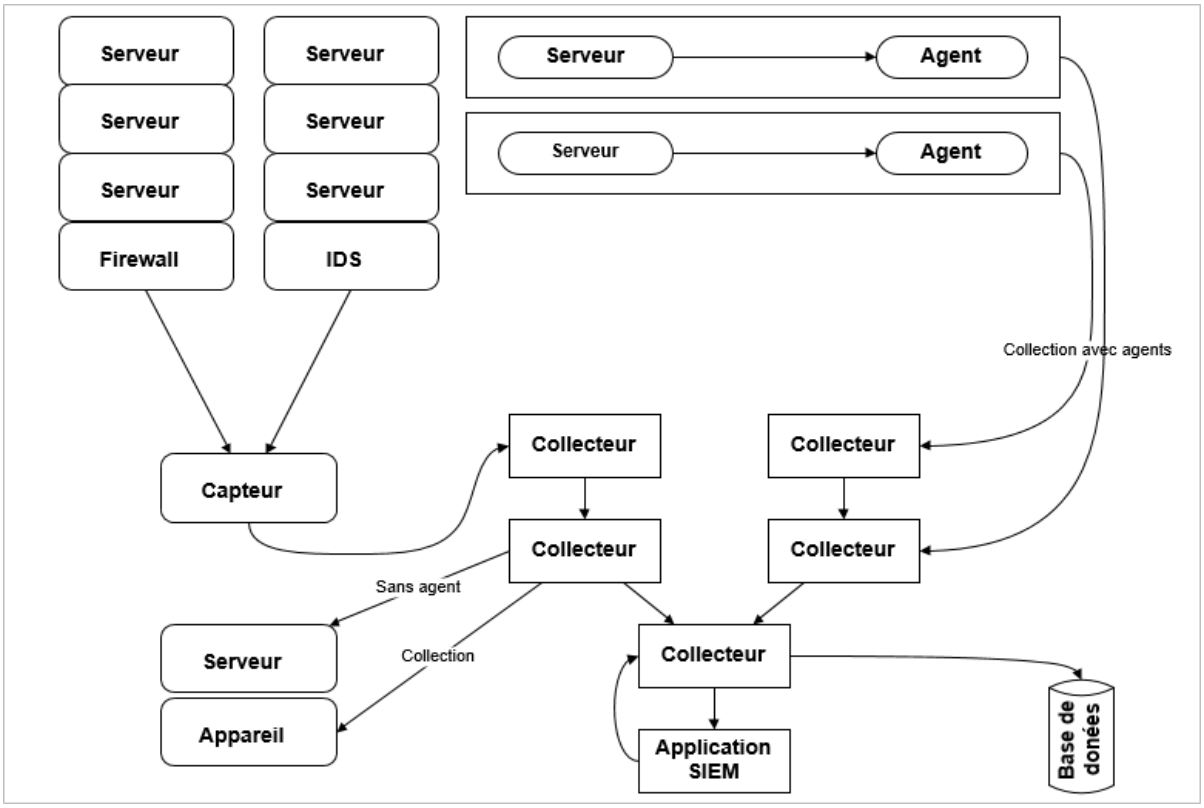

Figure 13 Processus de collecte de données

B. Normalisation des Données (Data Normalisation) :

- **Moteurs d'analyse (Parsing Engines)** : Convertissent les logs provenant de différentes sources en un format standardisé pour une analyse uniforme.
- **Types de données traitées par SIEM :** Elles incluent les logs de systèmes (événements des systèmes d'exploitation comme Windows et Linux, et des serveurs d'applications), les logs réseau (journaux des firewalls, routeurs, switches, et systèmes IDS/IPS), les logs d'applications (journaux des applications métiers et de sécurité), les logs d'authentification et de gestion des accès (journaux des systèmes IAM et contrôleurs de domaine), les logs de services cloud (journaux des activités sur AWS, Azure, Google Cloud, et applications SaaS), les logs de systèmes de sécurité physique (contrôle d'accès et surveillance vidéo), les informations de configuration (détails des configurations système et changements appliqués), les données des flux de réseau (NetFlow, IPFIX, sFlow), les informations sur les vulnérabilités (résultats des scans de vulnérabilité), et les données de threat intelligence

C. Analyse des Événements (Event Analysis) :

- **Moteurs de Corrélation (Correlation Engines)** : Analysent les événements pour détecter les modèles et les anomalies en utilisant des règles prédéfinies ou des algorithmes d'apprentissage automatique.
- **Moteurs de Règles (Rule Engines)** : Déclenchent des alertes basées sur des conditions spécifiques définies dans les règles de sécurité.

D. Stockage des Données (Data Storage) :

- **Bases de Données (Databases)** : Stockent les logs et les événements pour une analyse historique et une conformité réglementaire.
- **Data Warehouses** : Stockent des volumes importants de données pour des analyses à long terme et des rapports.

E. Tableaux de Bord et Rapports (Dashboards and Reporting) :

- **Interfaces Utilisateur (User Interfaces)** : Fournissent une vue centralisée des événements de sécurité et des alertes en temps réel.
- **Outils de Reporting** : Génèrent des rapports personnalisables pour différentes parties prenantes, comme les équipes de sécurité et les auditeurs.

F. Gestion des Alertes (Alert Management) :

- **Systèmes de Notification** : Envoient des notifications aux administrateurs en cas d'incidents critiques via divers canaux (emails, SMS, etc.).
- **Workflows d'Incident :** Gèrent les processus de réponse aux incidents, de l'identification à la résolution.

3.3.3 Défis et limitations

- **Faux positifs et négatifs** : Un des principaux défis des SIEM est la gestion des faux positifs et des faux négatifs. Une mauvaise configuration ou des algorithmes inefficaces peuvent conduire à des alertes inappropriées ou à la non-détection de véritables menaces.

- **Scalabilité** : Avec l'augmentation des volumes de données, la scalabilité des systèmes SIEM devient critique pour maintenir des performances et une efficacité adéquate.
- **Complexité et coûts** : La mise en place et la gestion d'un SIEM peuvent être complexes et coûteuses, nécessitant des ressources spécialisées et une maintenance continue.

3.3.4 Besoins principaux pour l'utilisation d'un SIEM :

A. Détection et Réponse aux Incidents de Sécurité

- **Surveillance en Temps Réel** : Les SIEM offrent une surveillance continue des événements de sécurité, permettant la détection immédiate des incidents et une réponse rapide.
- **Réduction des Temps de Réaction** : En fournissant des alertes en temps réel et des analyses instantanées, les SIEM réduisent le temps nécessaire pour réagir aux incidents de sécurité.

B. Visibilité et Centralisation

- **Vue Globale de la Sécurité** : Les SIEM centralisent les logs et les événements de multiples sources (pare-feu, IDS/IPS, systèmes d'exploitation, etc.) dans une seule interface, offrant une vue d'ensemble de la sécurité du réseau.
- **Corrélation des Événements** : Ils permettent de corréler des événements disparates pour identifier des modèles d'attaque complexes et détecter des menaces sophistiquées.

C. Conformité Réglementaire

- **Maintien de Journaux d'Audit :** Les SIEM aident à maintenir des journaux détaillés des événements de sécurité pour prouver la conformité aux réglementations telles que GDPR, HIPAA, PCI DSS, etc.
- **Génération de Rapports** : Ils offrent des capacités de reporting automatisé pour des audits de conformité réguliers et des inspections.

D. Gestion des Risques et Réduction des Faux Positifs

- **Priorisation des Menaces** : Les SIEM aident à prioriser les menaces en fonction de leur gravité et de leur impact potentiel, permettant aux équipes de sécurité de se concentrer sur les incidents les plus critiques.
- **Réduction des Faux Positifs** : En utilisant des analyses avancées et des règles de corrélation, les SIEM réduisent les faux positifs, ce qui permet aux analystes de sécurité de se concentrer sur les véritables menaces.

E. Automatisation et Réponse Orchestrée

- **Automatisation des Réponses** : Les SIEM peuvent automatiser certaines réponses aux incidents, comme le blocage de l'IP malveillante, réduisant ainsi la charge de travail des équipes de sécurité.

- **Orchestration de la Sécurité** : Ils s'intègrent avec d'autres outils de sécurité pour orchestrer une réponse coordonnée aux incidents (par exemple, intégration avec SOAR).

F. Analyse Comportementale

- **Détection des Anomalies** : Les SIEM utilisent des techniques d'apprentissage automatique pour détecter les anomalies par rapport aux comportements normaux, identifiant ainsi des menaces nouvelles ou inconnues.

G. Évolution et Adaptation

- **Mise à Jour Continue** : Les SIEM évoluent avec les nouvelles menaces et vulnérabilités en mettant à jour régulièrement leurs règles et modèles de détection.

3.3.5 Technologies et méthodologies :

- **Machine Learning et Intelligence Artificielle** : le SIEM utilisent la machine learning et l'intelligence artificielle pour améliorer la détection des menaces pour identifier des comportements anormaux a partir des données historiques
- **Big Data** : permet aux SIEM de gérer et d'analyser de grandes quantités de données en temps réel.
- **Automatisation et orchestration** : sont des tendances croissantes, permettant une réaction plus rapide et plus efficace aux menaces.

3.3.6 Présentation de Splunk :

A. Composants Clés de Splunk :

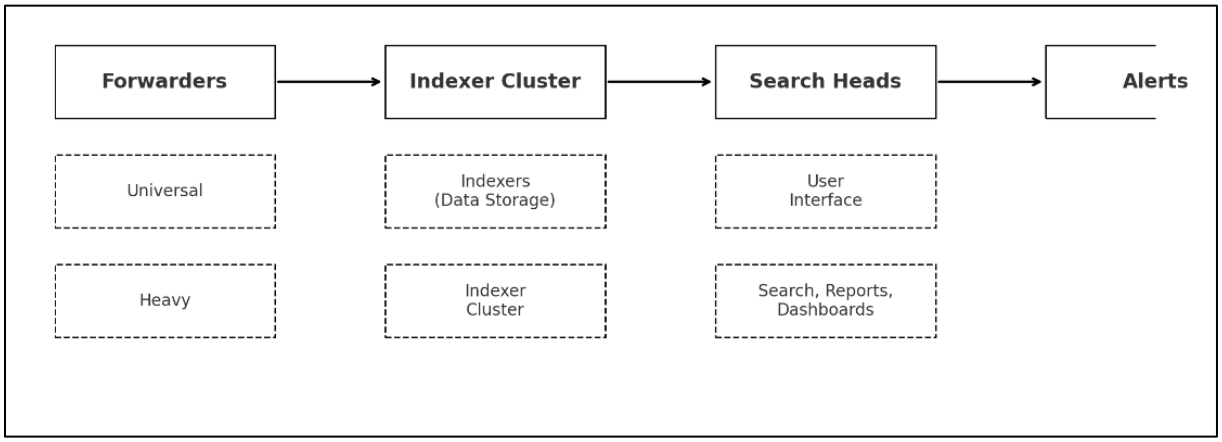

Figure 14 Les composants de Splunk

1) **Forwarders**

- **Universal Forwarder** : Agent léger déployé sur les sources de données pour collecter et transmettre les logs à Splunk Indexers.
- **Heavy Forwarder** : Forwarder avec des capacités supplémentaires de filtrage et de prétraitement des données avant leur envoi aux indexeurs.

2) **Indexers**

- **Indexation des Données** : Les indexeurs reçoivent les données des forwarders, les stockent, et les indexent pour permettre des recherches rapides.
- **Clustering d'Indexeurs :** Permet la redondance et la haute disponibilité en distribuant les données sur plusieurs indexeurs.

3) **Search Heads**

- **Interface de Recherche** : Les Search Heads permettent aux utilisateurs d'exécuter des requêtes sur les données indexées et d'analyser les résultats.
- **Clustering de Search Heads** : Facilite la répartition de la charge de travail de recherche et permet une gestion centralisée des requêtes.

4) **User Interface**

- **Dashboards et Visualisations** : Les utilisateurs peuvent créer des tableaux de bord interactifs et des visualisations pour surveiller les données en temps réel.
- **Reporting** : Génération de rapports automatisés et programmés basés sur les résultats des requêtes.

5) **Alerts**

- **Détection en Temps Réel** : Configuration d'alertes pour notifier les administrateurs en cas de détection d'anomalies ou d'incidents de sécurité.
- **Actions Automatisées** : Les alertes peuvent déclencher des scripts ou des réponses automatisées pour atténuer les menaces.

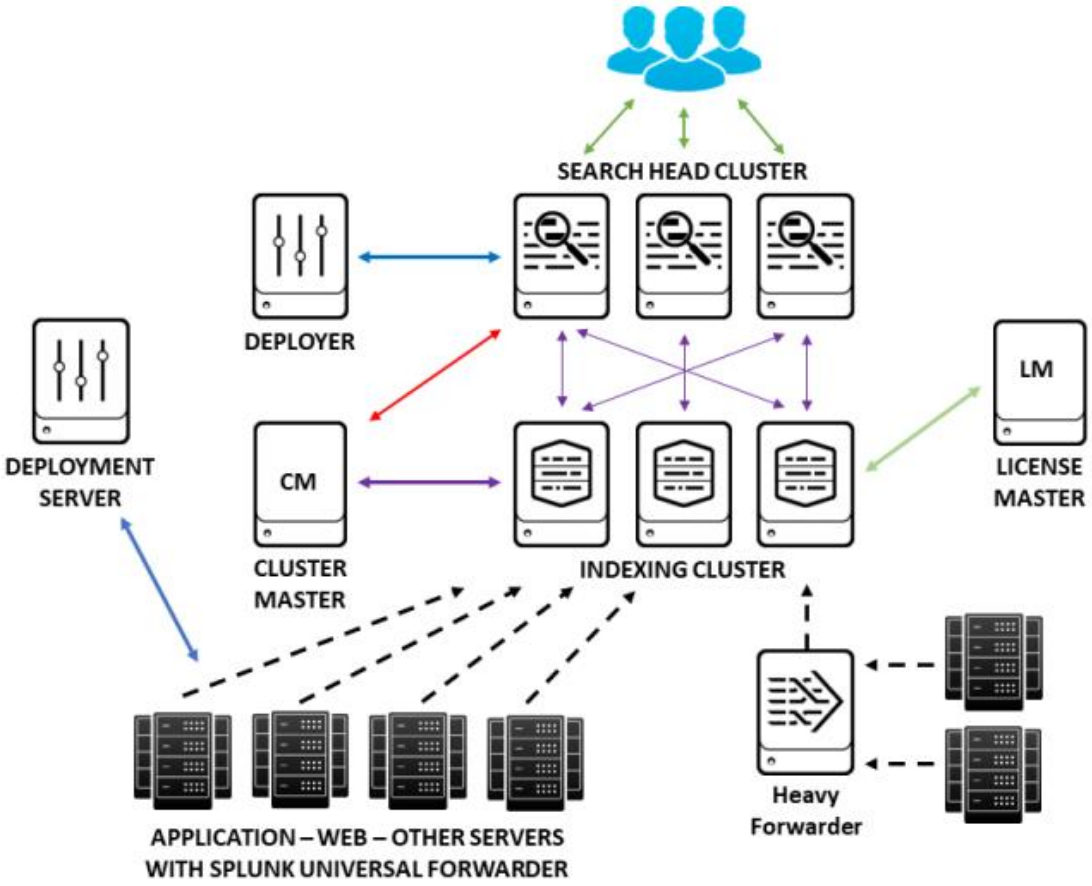

Figure 15 Architecture de Splunk

A. Fonctionnement de SPLUNK [18] [19] [20]

1. **Collecte des Données**
   - Les forwarders collectent des données à partir de diverses sources telles que les serveurs, les applications, les équipements réseau, et les services cloud.
   - Les données sont envoyées aux indexeurs pour stockage et indexation.
2. **Indexation et Stockage**
   - Les indexeurs reçoivent les données brutes, les traitent, et les indexent.
   - Les données indexées sont stockées de manière à permettre des recherches rapides et efficaces.
3. **Recherche et Analyse**
   - Les utilisateurs accèdent aux Search Heads pour exécuter des requêtes sur les données indexées.
   - Les résultats des requêtes peuvent être visualisés à travers des tableaux de bord et des rapports.
4. **Surveillance et Alertes**
   - Splunk surveille en continu les données en temps réel et peut générer des alertes basées sur des conditions prédéfinies.
   - Les alertes peuvent déclencher des actions automatisées pour une réponse rapide aux incidents.
5. **Flexibilité et évolutivité**

Splunk est conçu pour être hautement flexible et évolutif, permettant aux organisations de commencer petit et de croître en fonction de leurs besoins. Il offre des options de déploiement sur site, dans le cloud ou en mode hybride, offrant ainsi une flexibilité maximale pour répondre aux exigences opérationnelles et de conformité spécifique.

B. Historique de Splunk et son évolution :

Splunk, lancé en 2003 comme moteur de recherche de logs, a évolué pour devenir une plateforme avancée de gestion et d'analyse des données. Entre 2007 et 2011, il s'est positionné comme une solution SIEM, ajoutant la visualisation et la détection d'intrusions. De 2012 à 2016, Splunk a introduit des capacités de Big Data et d'apprentissage automatique. Entre 2017 et 2020, l'accent a été mis sur le cloud, l'IoT et DevOps. Depuis 2021, Splunk continue d'intégrer l'IA et d'améliorer l'expérience utilisateur, se concentrant sur l'analyse en temps réel et l'automatisation.

C. Importance de Splunk

Dans le contexte de la gestion et d'analyses des donnes et de la sécurité informatique (voir le tableau suivant) :

Gestion des données	Sécurité informatique
1) Collecte et indexation des données 2) Analyse et visualisation 3) Big data	1) Detection et réponse aux incidents 2) Gestion des informations et évènements de sécurité (SIEM) 3) Conformité et audit 4) Orchestration et automatisation

Tableau 5 Importance de Splunk dans la gestion et l'analyse de données

D. Déploiement : Deployment Server (DS)

Description : Serveur de gestion centralisée utilisé pour déployer des configurations et des applications sur des instances de Splunk, notamment les Universal Forwarders.

Fonction : Gérer et distribuer les configurations et les applications aux différents composants de Splunk.

- Déploiement sur site : Cela signifie que le logiciel ou le système est installé et exécuté localement sur les serveurs ou les machines de l'organisation cliente, par opposition à une solution basée sur le cloud où tout est hébergé sur des serveurs distants accessibles via Internet.
- Déploiement dans le cloud (hybride) : C'est une combinaison de déploiement sur site et de solutions cloud. Certaines parties du système peuvent être hébergées localement (sur site) tandis que d'autres peuvent être déployées sur des serveurs cloud externes. Cela permet souvent une flexibilité accrue et peut répondre à des exigences spécifiques en termes de performance, de sécurité ou de conformité.

E. Sources de données et intégrations :

Splunk peut ingérer différents types de données, notamment :

- **Logs de fichiers texte :** Logs générés par des applications, des serveurs web, des systèmes d'exploitation, etc.

- **Données de machines :** Données provenant de capteurs IoT, de systèmes embarqués, etc.
- **Données structurées** : Données provenant de bases de données relationnelles, de services web, etc.
- **Données de sécurité :** Logs et événements de sécurité, comme des journaux d'authentification, des alertes de sécurité, etc.
- **Données de transaction** : Informations transactionnelles telles que des transactions financières, des données de vente, etc.
- **Données métriques :** Informations spécifiques à une industrie ou à une organisation, comme des données de vente au détail, des données de santé, etc.

F. Intégrations avec d'autres outils et technologies :

Intégration de Splunk avec le pare-feu et des solutions de gestion des informations et des événements de sécurité (SIEM) est essentielle pour renforcer la sécurité réseau et améliorer la visibilité sur les activités suspectes. Voici une approche pour cette intégration :

1) Prérequis :

- **Splunk installé et configuré** : Vous devez avoir une instance Splunk opérationnelle.
- **Accès administrateur** : Accès administrateur à Splunk et aux dispositifs pare-feu.
- **Plugins ou applications** : Certains pare-feu et SIEM peuvent nécessiter des applications ou des plugins spécifiques pour l'intégration avec Splunk.

2) Collecte des données

Pare-feu :

- **Configurer les logs** : Assurez-vous que le pare-feu est configuré pour envoyer des logs. Cela inclut les logs de connexion, les logs de trafic, les logs de détection d'intrusion, etc.
- **Envoi des logs vers Splunk** : Configurez le pare-feu pour envoyer les logs vers Splunk via Syslog (envoyer les logs à l'adresse IP de Splunk sur le port désigné, généralement UDP 514 ou TCP 514), ou bien via HTTP Event Collector (HEC) (envoyer les événements via HTTP ou HTTPS à Splunk, ou d'autres méthodes supportées.

SIEM :

- **Exporter les logs SIEM** : Configurez votre solution SIEM pour exporter les logs et événements pertinents. Cela peut inclure les alertes de sécurité, les logs d'audit, etc.
- **Intégration avec Splunk** : Utilisez les applications Splunk spécifiques pour les intégrations SIEM.

3) Configuration Splunk

- **Recevoir les données**

- Configurer les inputs : Dans Splunk, configurez les inputs pour recevoir les données du pare-feu et du SIEM.
- Pour les données Syslog, configurez un data input pour le port Syslog.
- Pour HEC, configurez un HTTP Event Collector et assurez-vous qu'il est activé et correctement sécurisé.

- **Configurer les source-types :** Définissez des source-types appropriés pour les données reçues afin de les classifier correctement dans Splunk.
- **Configurer des tableaux de bord et des alertes** :

- **Tableaux de bord** : Créez des tableaux de bord personnalisés pour surveiller les activités de pare-feu et les alertes SIEM. Utilisez des visualisations pour afficher des statistiques clés comme le nombre de connexions bloquées, les alertes de sécurité, etc.
- **Alertes** : Configurez des alertes basées sur les données reçues pour notifier les administrateurs en cas d'activités suspectes ou de menaces détectées.

4) Maintenance et optimisation

- **Vérification régulière** : Assurez-vous que les flux de données entre le pare-feu, le SIEM et Splunk sont constants et exempts d'erreurs.
- **Mises à jour** : Gardez vos applications et plugins Splunk à jour pour bénéficier des dernières fonctionnalités et corrections de bugs.
- **Optimisation des recherches** : Optimisez les recherches Splunk pour améliorer les performances et réduire le temps de réponse des requêtes.

3.3.7 Avantages et inconvénients de SIEM

	Avantages	Inconvénients
SIEM	Detection et réponse en temps réel	Complexité de mise en œuvre
	Centralisation des données	Cout élevé
	Visibilité améliorée	Faux positifs
	Automatisation des alertes	Besoin en ressources humaines
	Conformité règlementaire	Maintenance continue
	Analyse post-incident	Complexité des données

Tableau 6 Avantages et inconvénients de SIEM

3.4 Conclusion

Dans ce chapitre, nous avons exploré en profondeur les fondements essentiels pour établir une gestion de sécurité efficace et proactive, capable de détecter et de prévenir les menaces. Nous avons souligné l'importance cruciale des IDS (Systèmes de Détection d'Intrusion) et des IPS (Systèmes de Prévention d'Intrusion) dans la sécurité informatique. L'IDS surveille le trafic et les journaux pour détecter les activités suspectes, alertant ainsi les administrateurs. Complémentairement, l'IPS bloque les intrusions détectées, assurant une réponse proactive pour préserver la sécurité des données. Nous avons examiné en détail les technologies de détection d'intrusions (IDS) et leurs méthodes d'analyse réseau et comportementale, ainsi que les technologies de prévention des intrusions (IPS) telles que le filtrage des paquets et les contrôles d'accès. En outre, nous avons présenté Snort comme exemple spécifique, détaillant son fonctionnement à travers l'utilisation de règles personnalisées pour l'analyse en temps réel du trafic réseau.

Dans la seconde section, nous avons approfondi notre compréhension de l'architecture typique, des composants clés, des rôles et des fonctionnalités avancées des SIEM. Nous avons également étudié en détail les capacités fondamentales de Splunk, son architecture, ses types de données et son intégration avec d'autres outils et technologies.

Dans le prochain chapitre, nous détaillerons les étapes de déploiement et de simulation des deux solutions, Snort IPS et SIEM Splunk, au sein de l'architecture réseau proposée pour l'entreprise VMS Bejaia. Cette étape permettra de mettre en pratique les concepts abordés et d'évaluer leur efficacité dans un environnement simulé, contribuant ainsi à renforcer la posture de sécurité de l'entreprise.

Chapitre 4
Mise en place des solutions proposées

4.1 Introduction

Dans ce chapitre, nous nous concentrons sur la mise en œuvre de la solution SIEM et IDS/IPS proposées pour notre projet. Nous présenterons les différentes configurations nécessaires pour établir l'infrastructure réseau fonctionnelle de l'organisme d'accueil, sur laquelle nos deux solutions seront déployée (détails dans l'annexe). Ensuite, nous décrirons les étapes clés de l'installation du serveur Splunk dans la DMZ et celle de SNORT dans le pare-feu dans cet environnement, y compris la configuration des sources de données, la création de tableaux de bord, et l'utilisation des fonctionnalités avancées de Splunk et SNORT pour la détection des menaces. Enfin, nous évaluerons les performances des deux solutions à l'aide de prototypes d'attaque.

4.2 Environnement de travail :

4.2.1 Composants matériels :

Puisque les ressources matérielles importantes nécessaires pour la simulation et le déploiement de notre projet, il était crucial d'utiliser un PC performant. Ainsi, nous avons utilisé un ordinateur portable aux caractéristiques suivantes :

Nom ordinateur	LenovoX1
Processeur	Intel(R) core (TM) I7-8550U CPU @ 1.80GHZ 1.99 GHZ
Mémoire ram	8 GO
Type de système	Système d'exploitation 64 bits
Système d'exploitation	Windows 11 professionnel
Type du disque dur	256 SSD

Tableau 7 Caractéristiques de l'ordinateur

4.2.2 Composants de simulation : GNS3 et VMware Workstation 17

Nous avons choisi d'utiliser GNS3, un programme de simulation réseau libre. Il offre une interface graphique intuitive qui permet de connecter et de configurer les équipements virtuels ainsi que de tester leur connectivité et aussi nous avons choisi d'utiliser la VMware Workstation 17 car elle nous permet de créer plusieurs machines virtuelles avec différents systèmes d'exploitation sur notre ordinateur physique où on peut créer des applications, faire des tests de sécurité et configurer des réseaux.

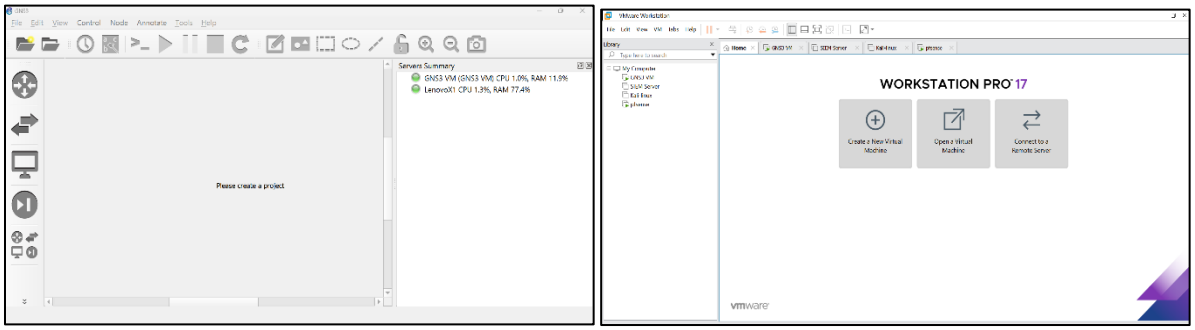

Figure 17 GNS3 et VMware Workstation 17

4.2.3 Logiciels et Systèmes d'exploitation

Composant	Version	Service installer	Prérequis
Windows server	2022	Splunk	RAM: 2GO
Kali Linux	2024	Poste-hacker	RAM: 2GO

Tableau 8 Logiciels et systèmes d'exploitation

4.2.4 Plan d'adressage des différents VLANs

Le tableau recapitule la liste des Vlans disponibles sur l'architecture réseau de la VMS Bejaia

VLAN ID	DESCRIPTION	PLAGE D'ADRESSAGE
1	NATIVE	172.16.1.0/24
2	INFORMATIQUE	172.16.2.0/24
3	GESTION	172.16.3.0/24
4	SERVERS	172.16.4.0/24
5	VOICE	172.16.5.0/24
6	RH	172.16.6.0/24

Tableau 9 Adressage VLANs

4.2.5 Mise en place d'une infrastructure réseau proposée pour le déploiement d'une solution SIEM et IDS/IPS

Comme il est impossible d'implémenter toute l'infrastructure réseau de VMS Bejaia, nous avons simplifié l'architecture pour permettre la mise en place de notre solution capturée sur GNS3 comme suit (voir Annexe 2):

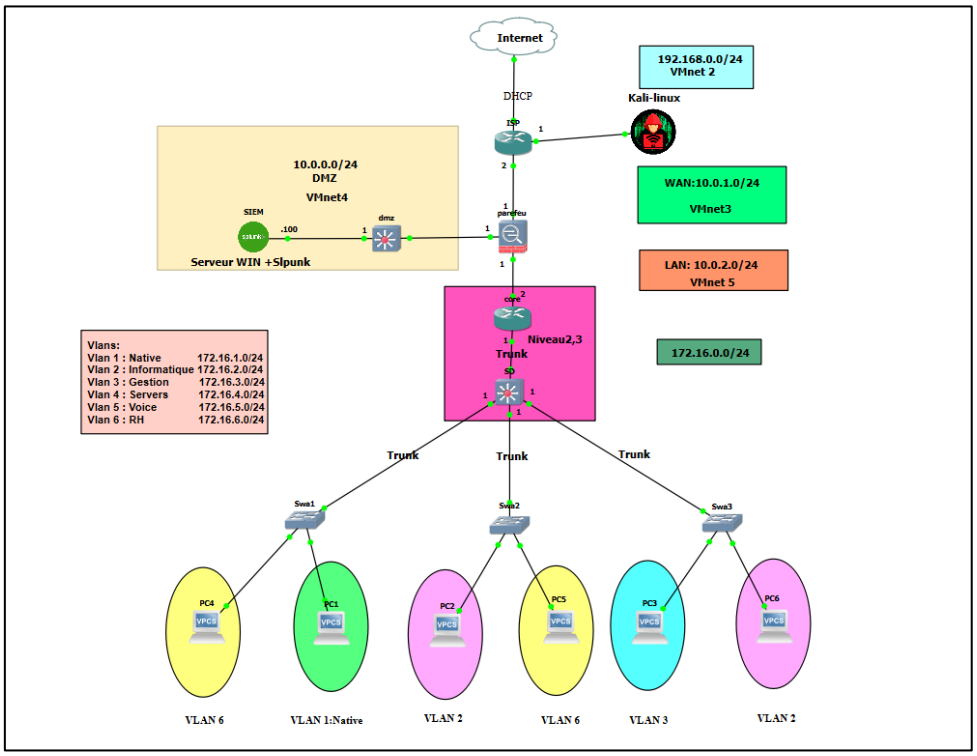

Figure 18 Infrastructure réseau implémenté

4.2.6 Configuration fonctionnelle de l'infrastructure réseau :

Voici un organigramme qui présente les étapes de l'ensemble des configurations nécessaires afin de créer l'infra-structure réseau fonctionnelle de l'organisme d'accueil (VMS de Bejaia) (voir les étapes d'installation et de configuration du LAB sur l'annexe 1) :

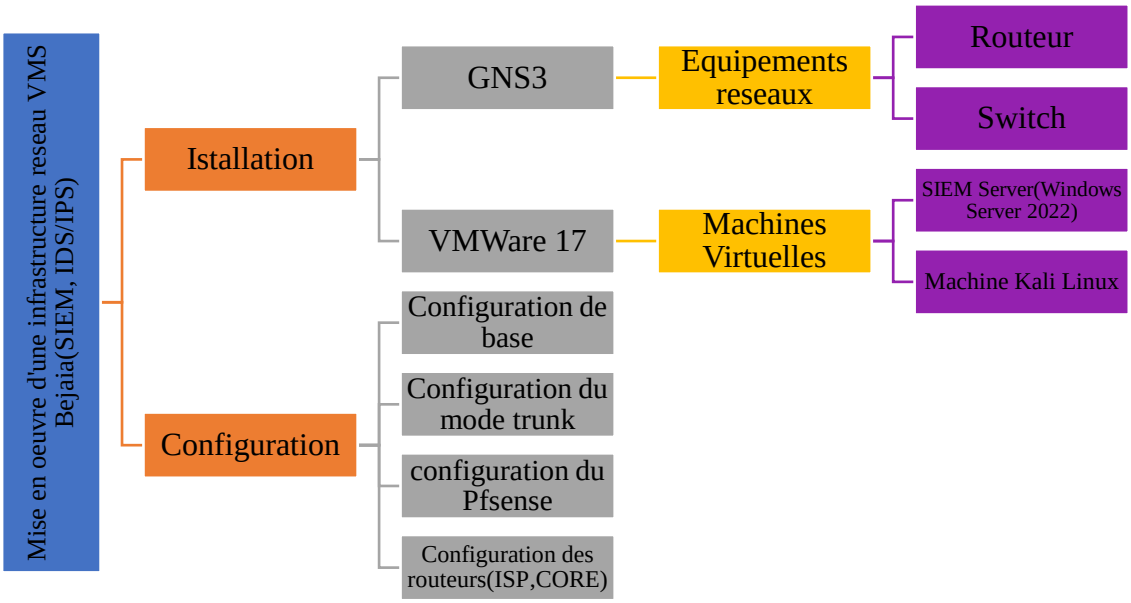

Figure 19 Diagramme de déploiement et de configuration de notre infrastructure réseau

4.2.7 Installation et configuration des outils :

A. Splunk :

Splunk est un outil de sécurité utilise par le SIEM, installer dans le serveur Windows pour renforcer la sécurité du réseau. Voici les étapes à suivre pour cette réalisation :

1) Téléchargement du package du Splunk

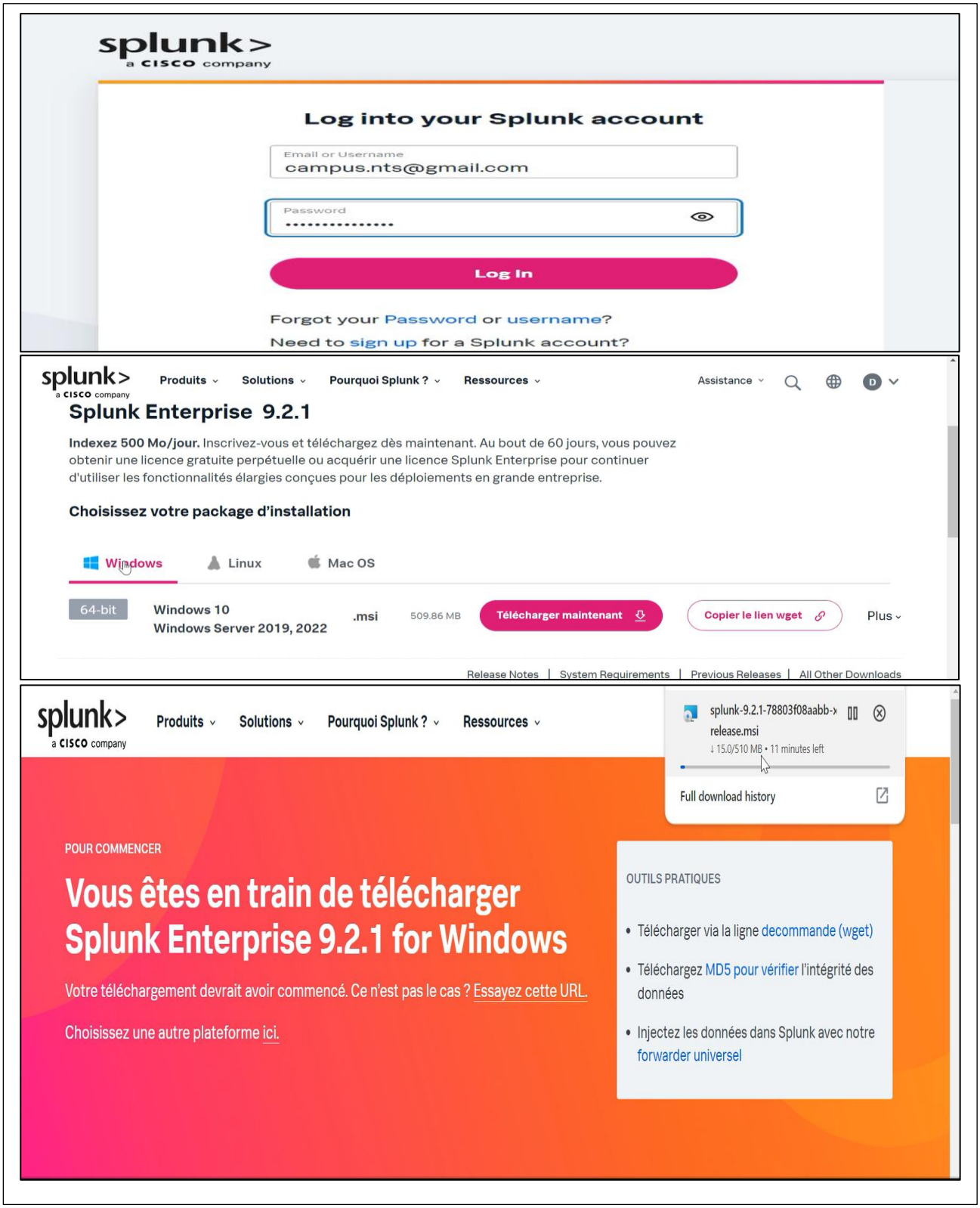

Figure 20 Téléchargement du package de Splunk

2) Ouvrir les ports du Splunk

Ports d'entreprise Splunk	Composant Splunk	Type	Description
514	Journal système	Convention - non recommande	Syslog, TCP ou UDP. Il est recommandé d'envoyer Syslog a un outil de collecte Syslog (Syslog-NG, rsyslog, etc.) Plutôt qu'a Splunk
8000	Interface web	Défaut	Splunk web (http par défaut)
8080, 9887	Indexeurs	Défaut	Réplication de l'indexeur
8081, 8181, 9887	Recherche de têtes	Défaut	Réplication SHC
8088	Collecteur d'évènements HTTP (HEC)	Défaut	Collecte les données envoyées à Splunk via HTTP
8089	Splunk	Défaut	Port de gestion
8089	Indexeurs	Défaut	Accès à l'API REST
8089	Serveur de déploiement	Défaut	Port de gestion pour le serveur de déploiement Splunk.

Tableau 10 Splunk Enterprise – Ports par défaut

3) Installation du Splunk sous Server Windows

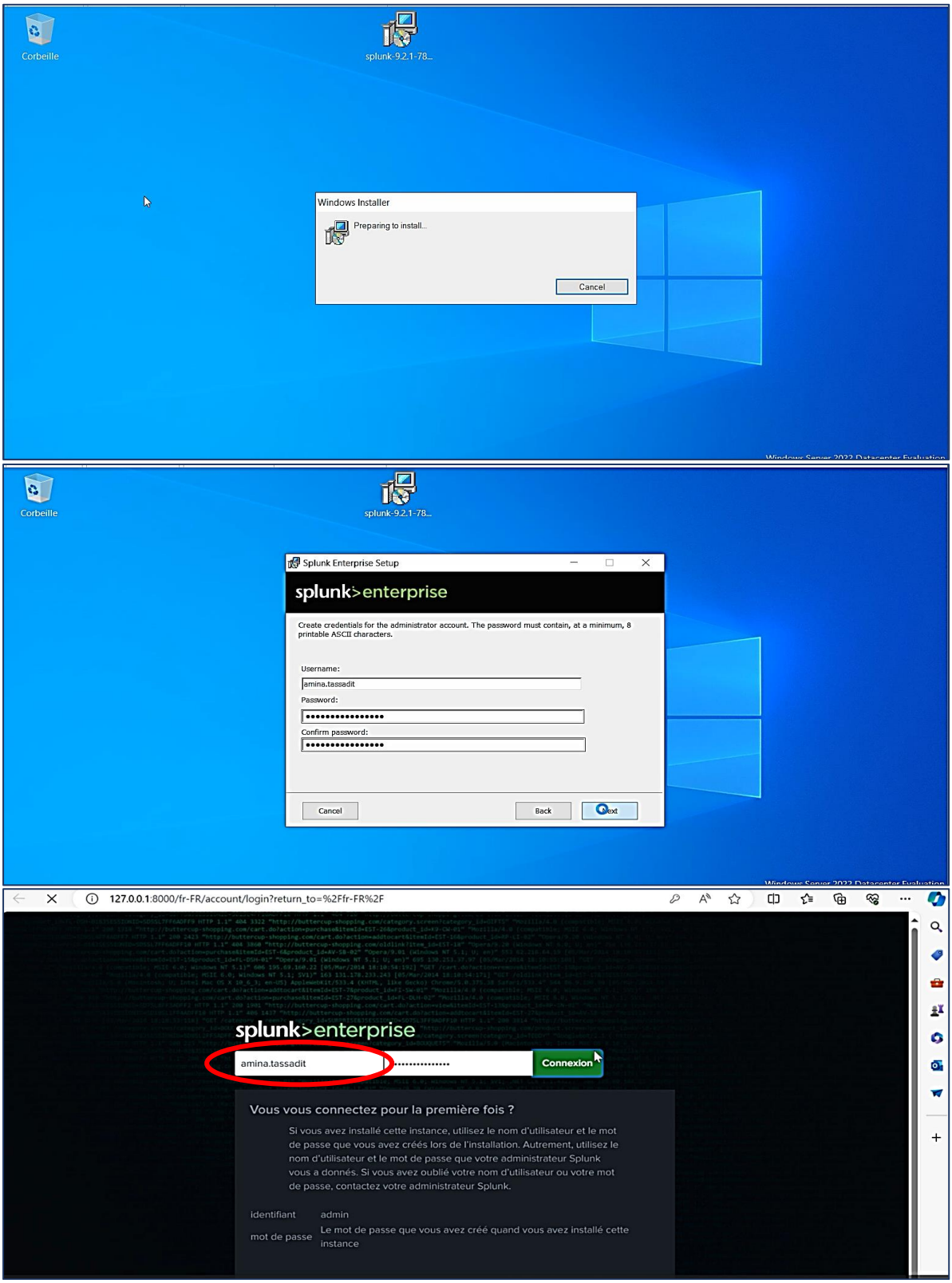

Figure 21 Installation du Splunk sous serveur Windows

4) La solution Splunk

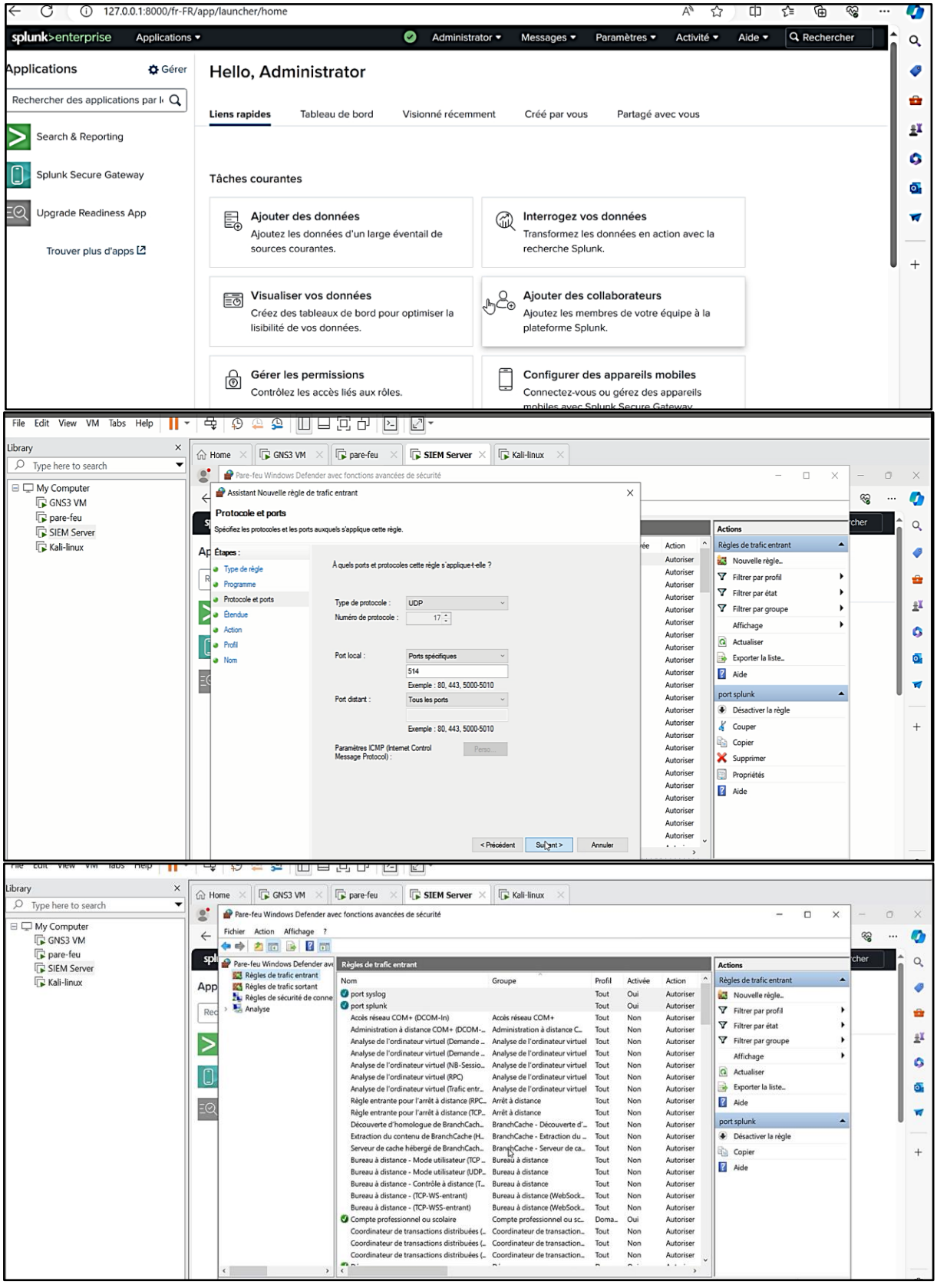

Figure 22 La solution Splunk (1)

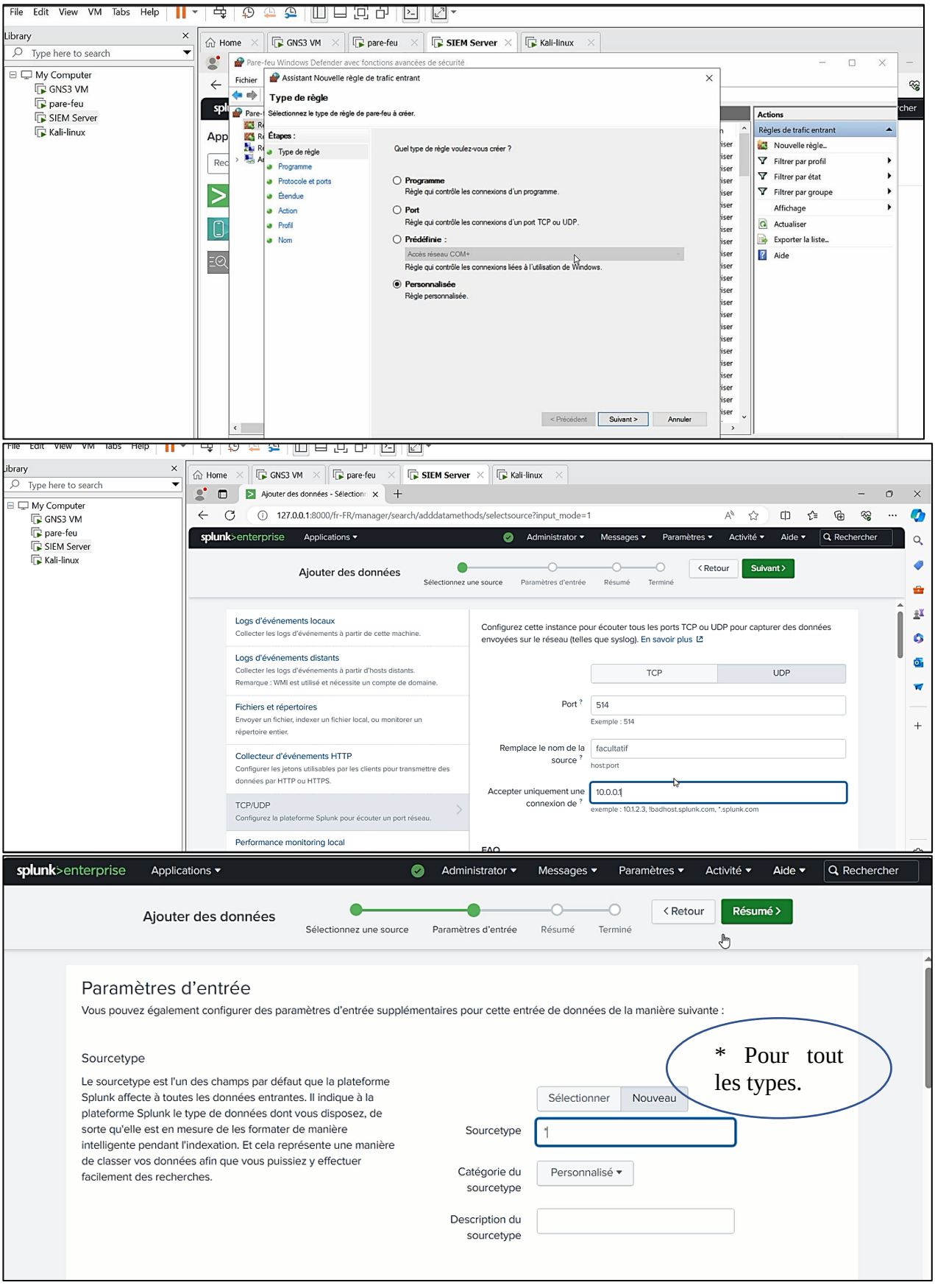

Figure 23 La solution Splunk (2)

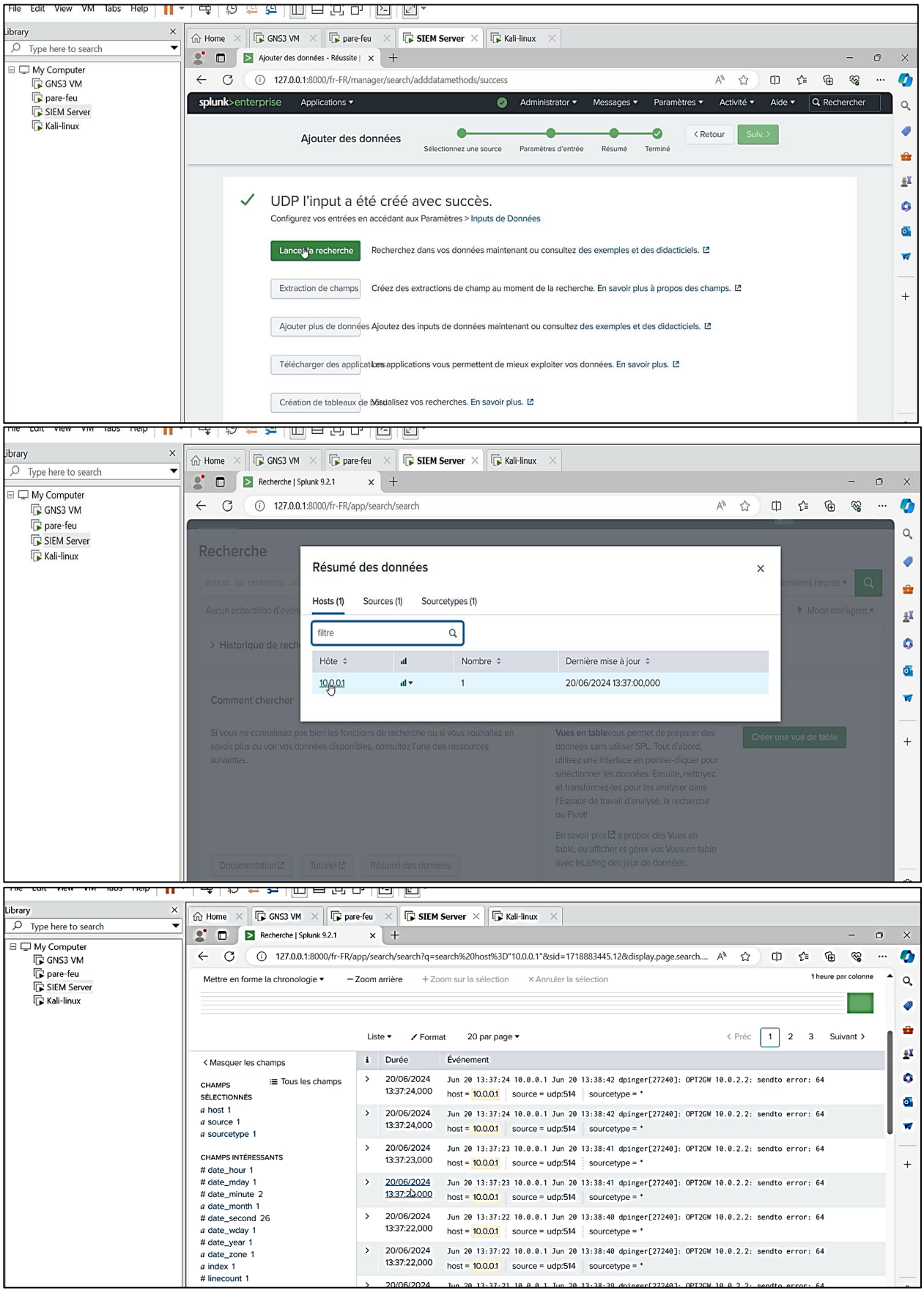

Figure 24 La solution Splunk (3)

B. Snort :

Est un outil des systèmes IDS/IPS, installer dans le Pfsense dans le but d'augmenter le niveau de la sécurité de réseau. Voici les étapes à accomplir pour cette mise en place :

1) Installation du package de Snort sous Pfsense

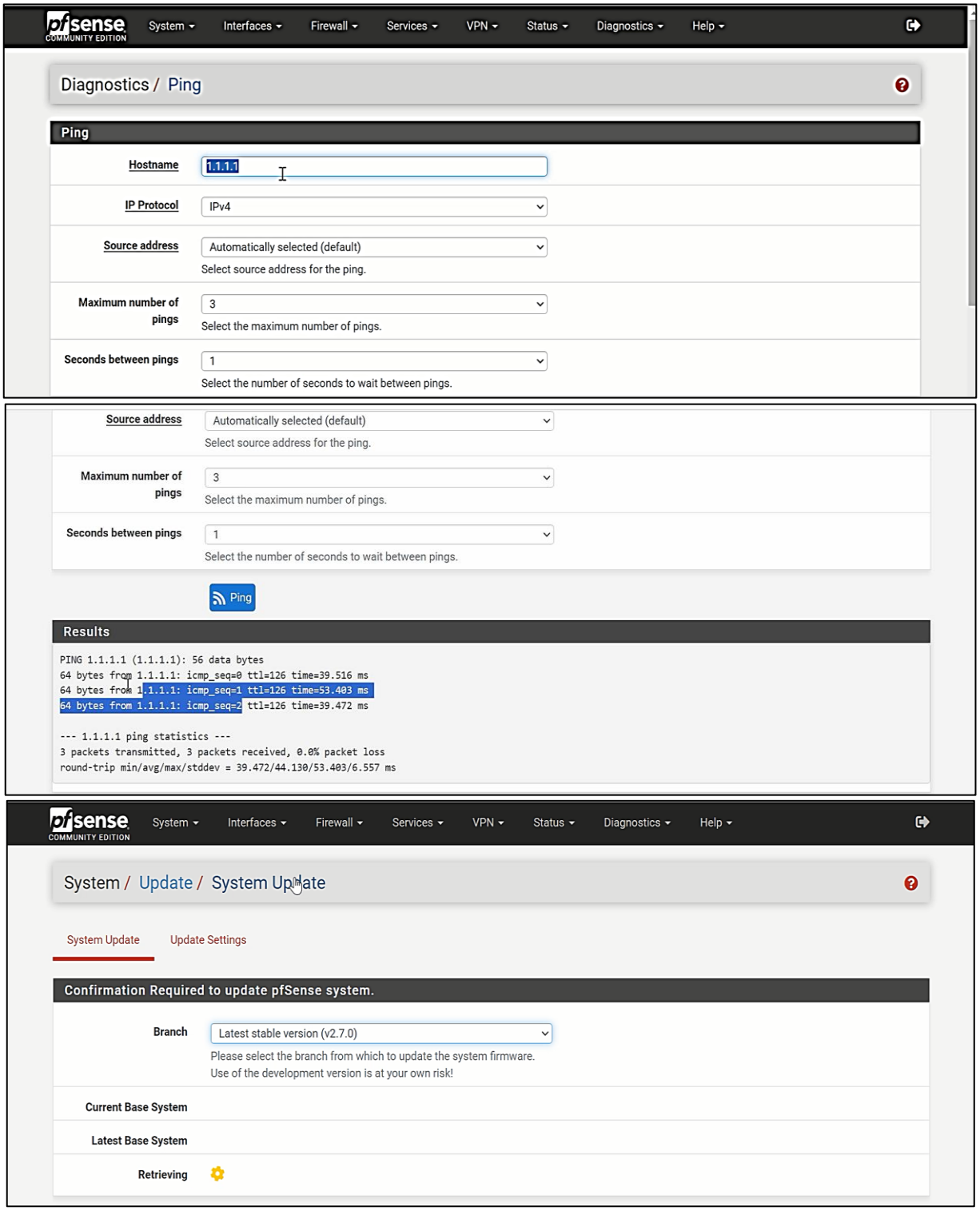

Figure 25 Installation du package de Snort sous Pfsense (1)

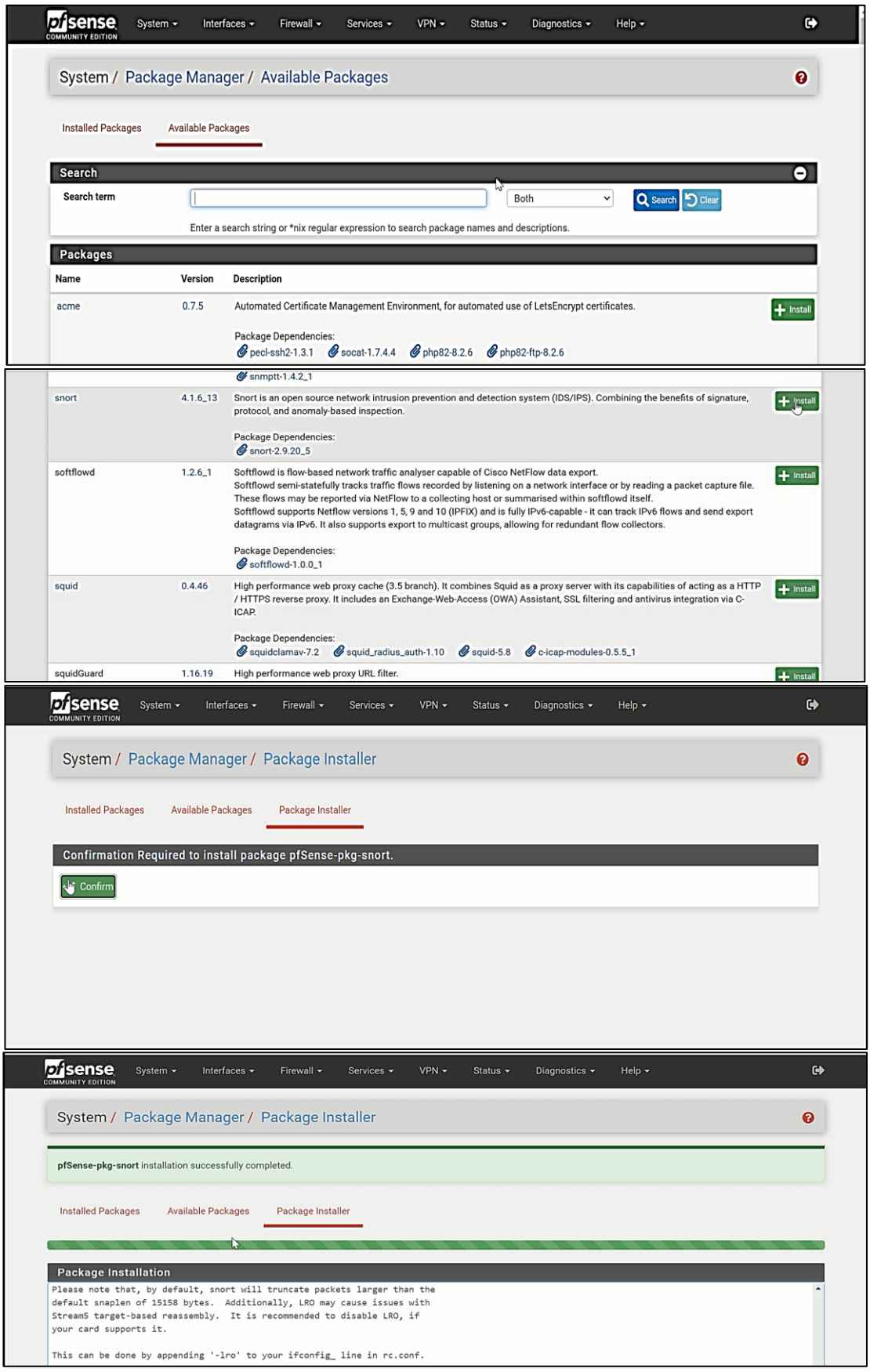

Figure 26 Installation du package de Snort sous Pfsense (2)

2) Installation et paramétrage du Snort

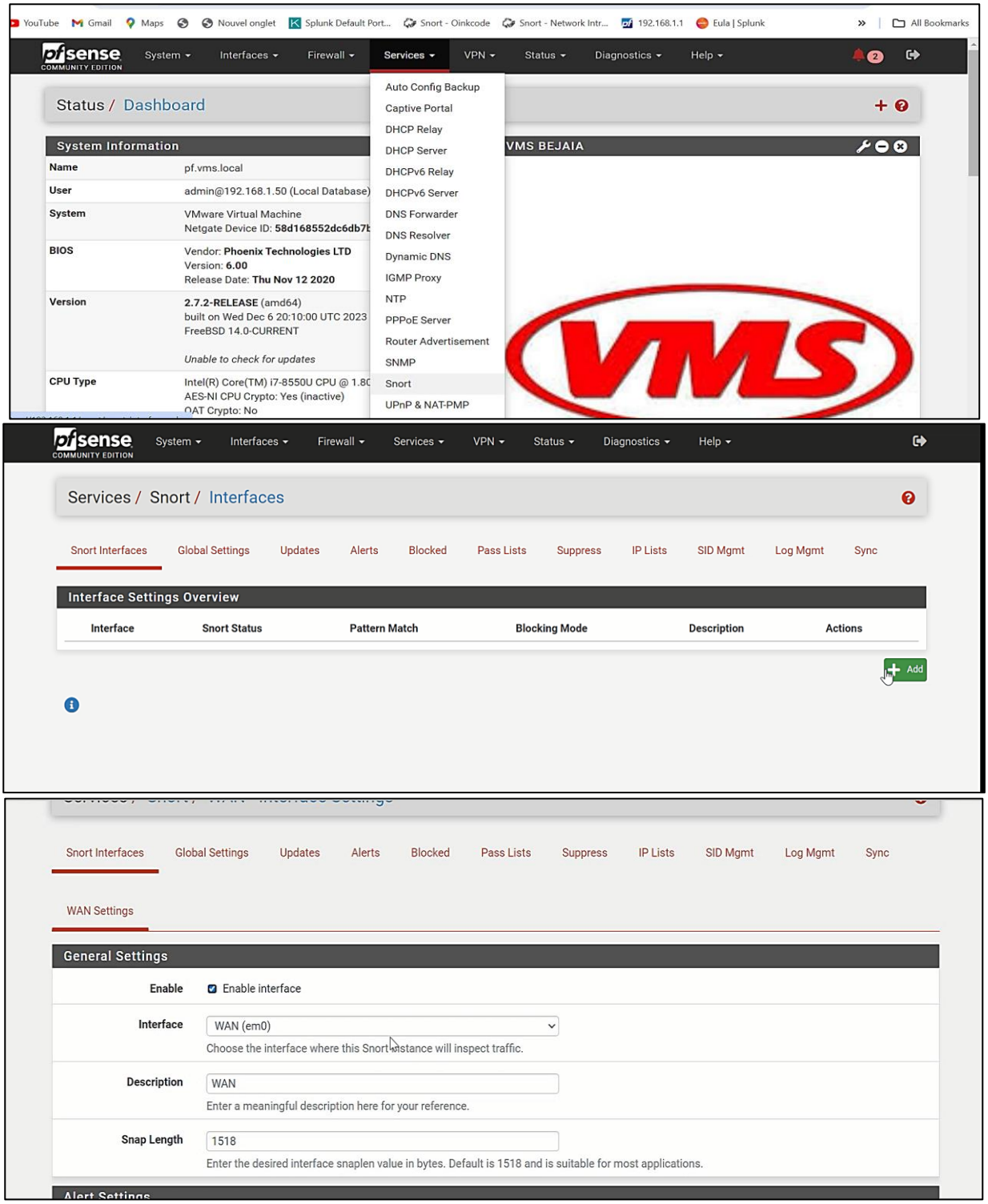

Figure 27 Installation de Snort sous Pfsense (1)

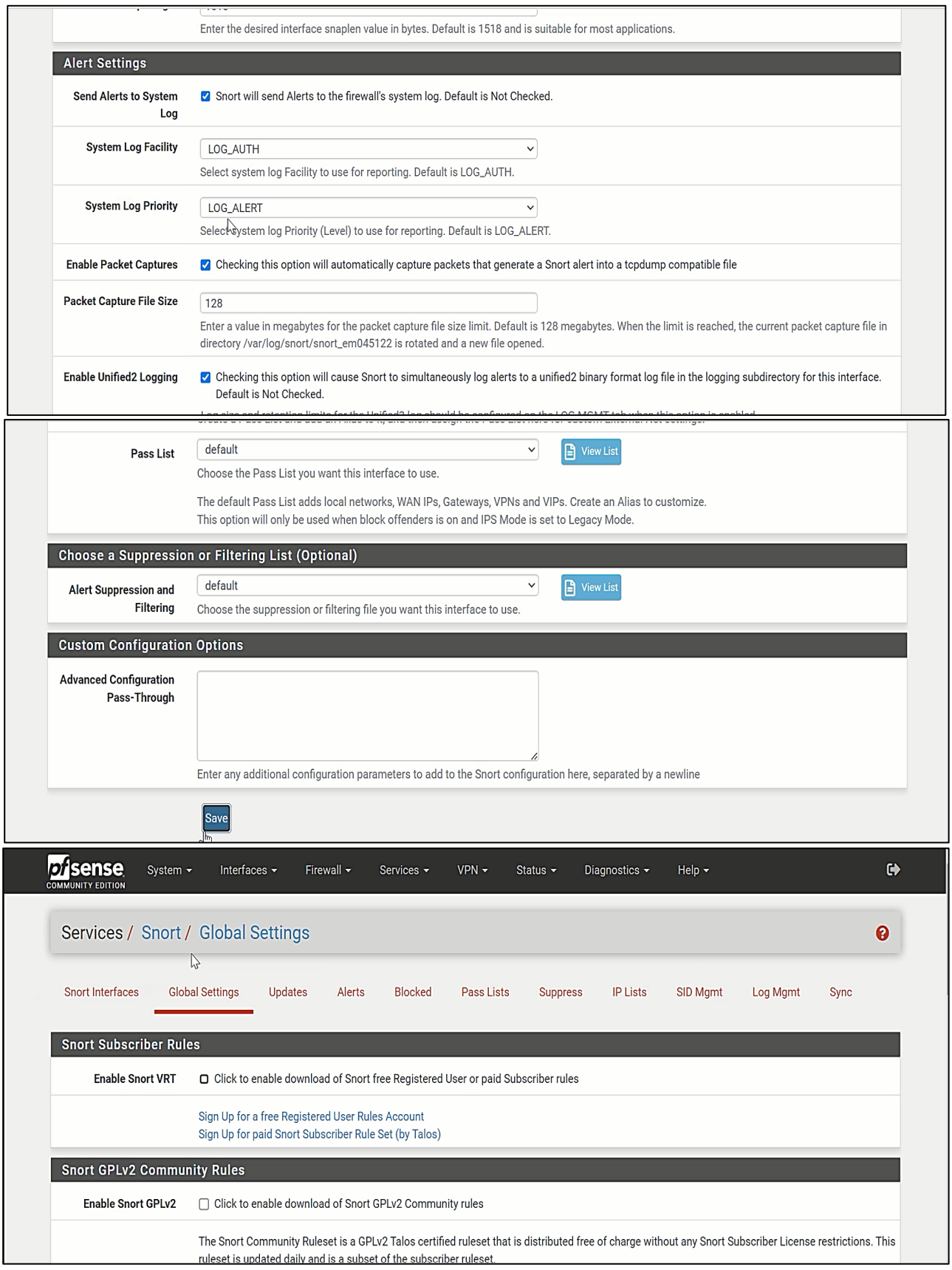

Figure 28 Installation de Snort sous Pfsense (2)

3) La solution Snort :

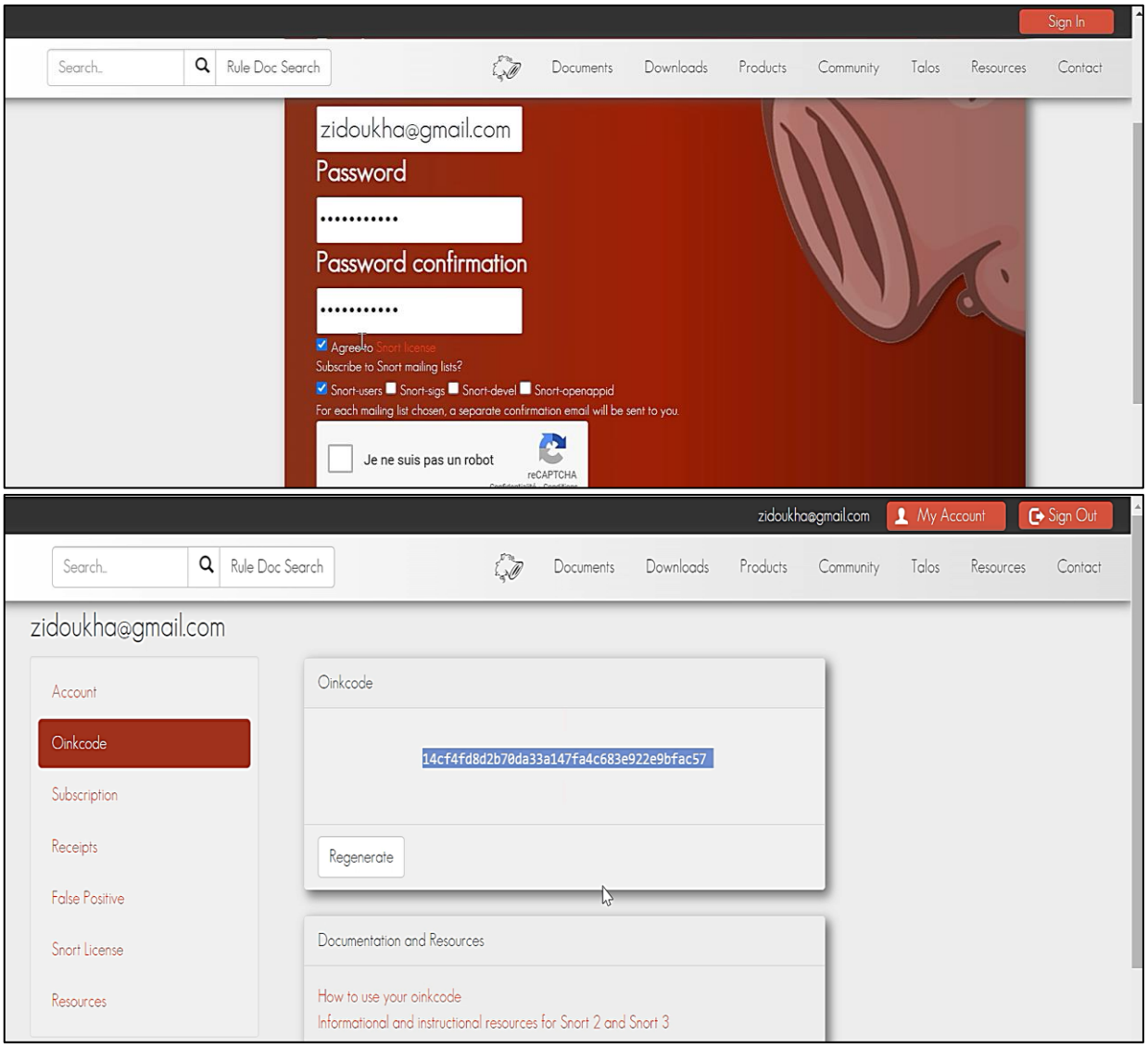

Figure 29 Création du compte Snort

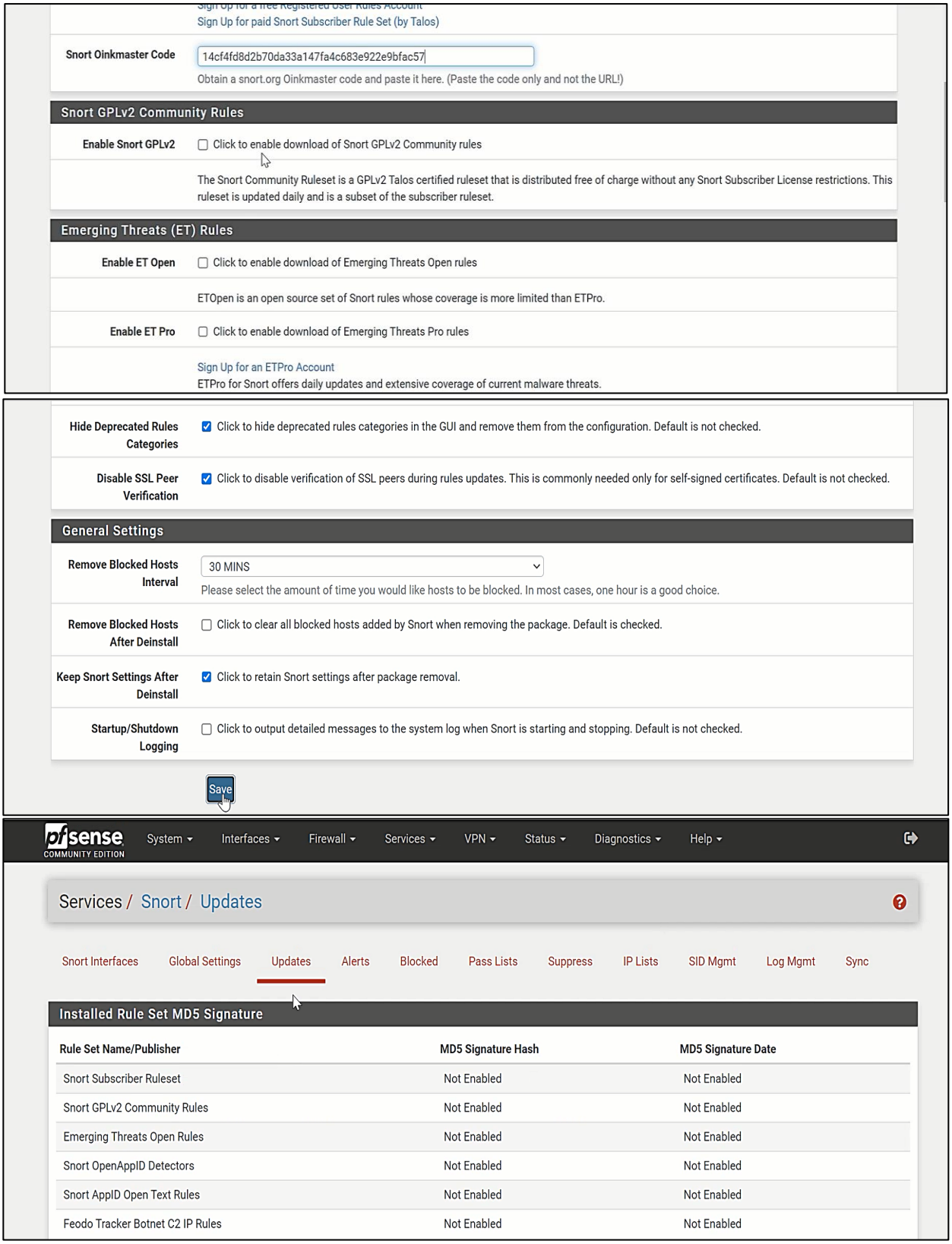

Figure 30 Paramétrage de la solution Snort (1)

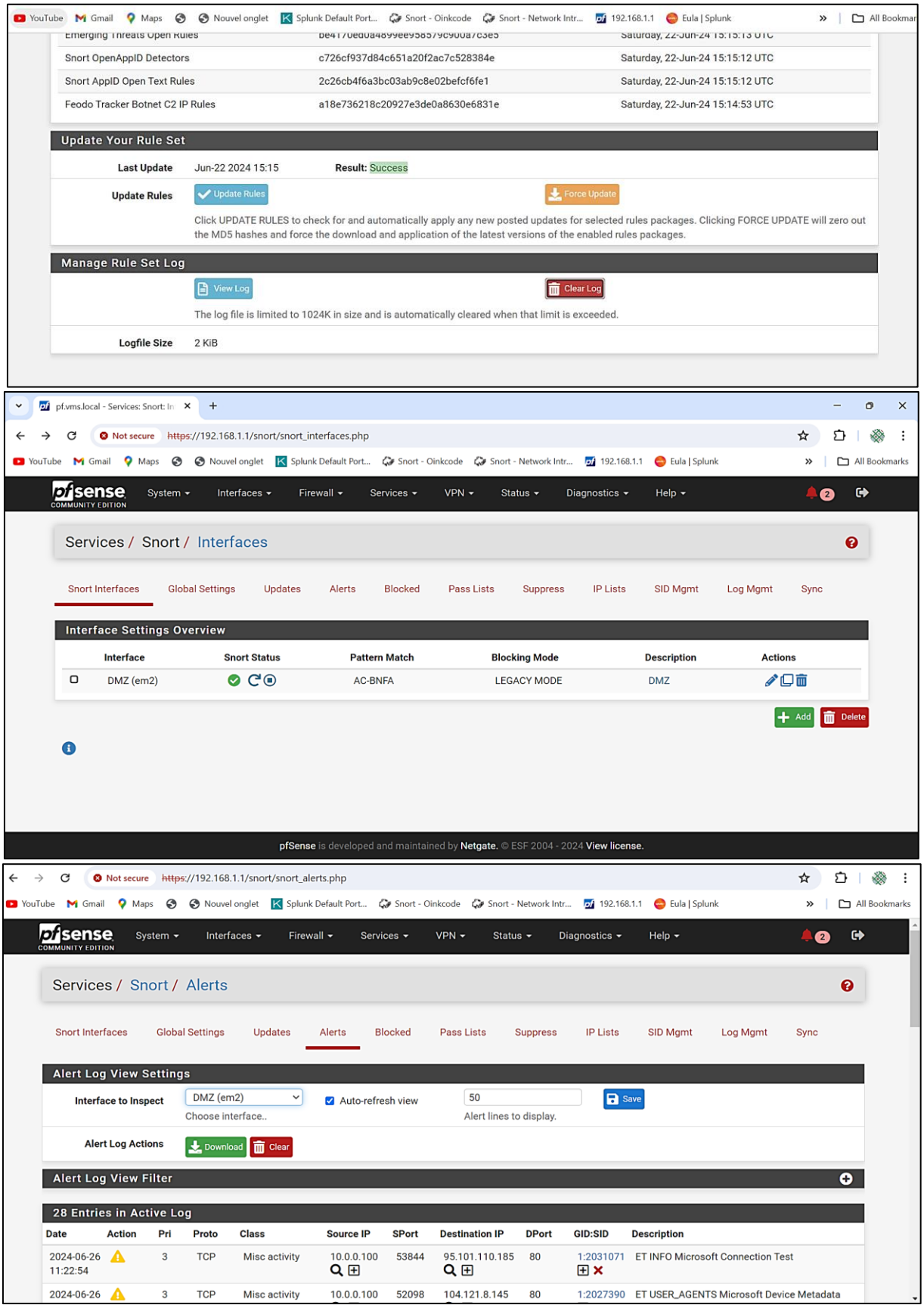

Figure 31 Paramétrage de la solution Snort (2)

4.2.8 Exemple d'attaque

Nous avons utilisé l'attaque Nmap. Nmap sous Kali Linux est un outil polyvalent et puissant pour la découverte, l'audit et la sécurisation des réseaux, essentiel pour les professionnels de la sécurité informatique et les équipes de tests de pénétration. La commande 'nmap -sL' est utilisée pour effectuer "scan de liste". Elle se contente de lister les hôtes d'un réseau sans réellement les scanner. Ce type de scan est souvent appelé "no scan" (sans scan) car il n'envoie aucun paquet aux hôtes cibles, à part éventuellement effectuer des résolutions DNS pour obtenir les noms d'hôte.

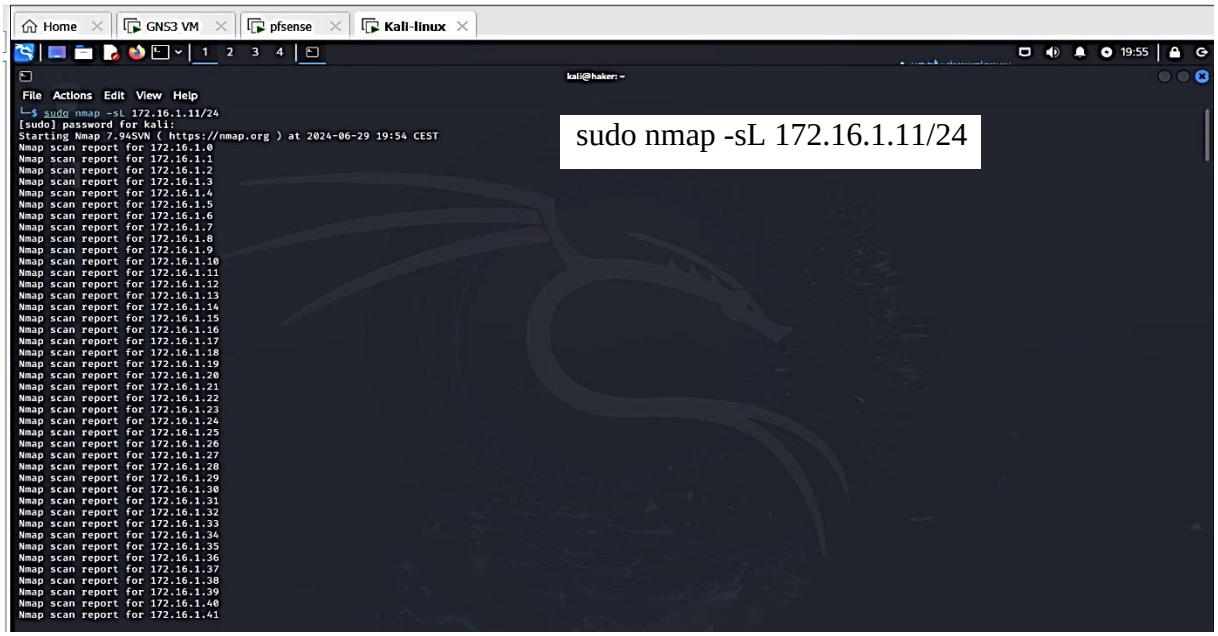

Figure 32 Exemple d'attaque lancée par Kali Linux (nmap -sL)

Cette commande est particulièrement utile lorsque vous souhaitez préparer une liste d'adresses IP à scanner ultérieurement ou simplement voir quelles cibles potentielles existent dans une plage réseau sans alerter les systèmes de sécurité qui pourraient détecter des activités de scan. Voici le résultat de l'exécution de cette commande est capturer par Splunk et Snort :

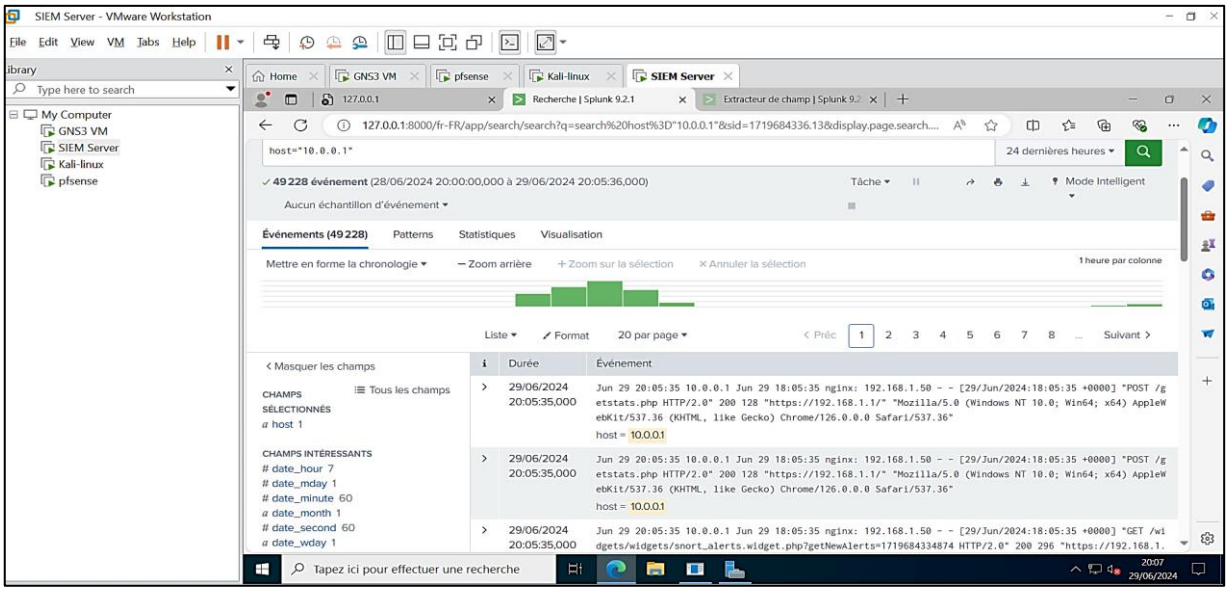

Figure 33 Alerte capture par l'outil Splunk

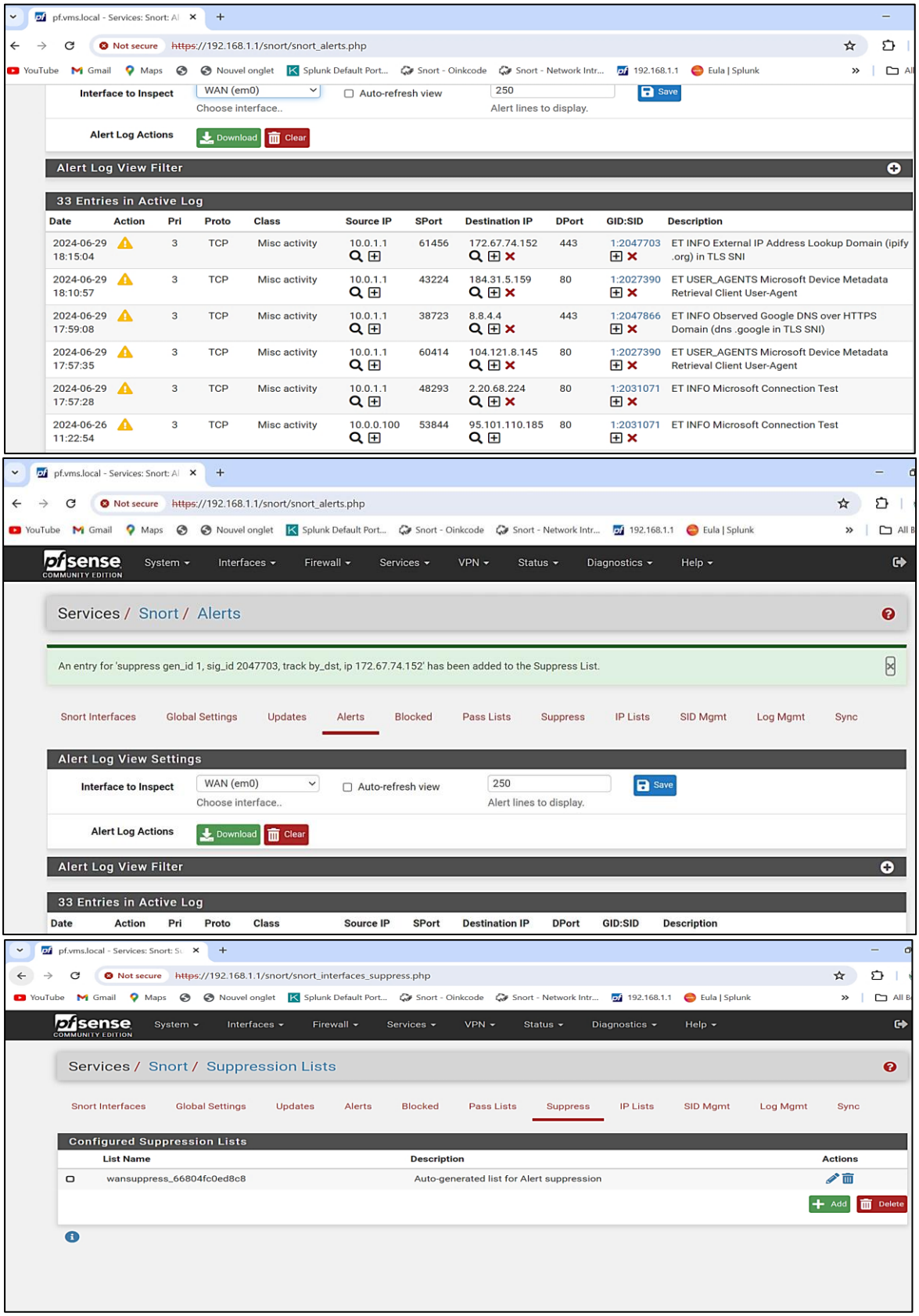

Figure 34 Alerte capturé par l'outil Snort et sa suppression par l'admin

4.3 Conclusion

En conclusion, ce chapitre présente une conception de projet pour l'installation et la configuration d'une plateforme Splunk et Snort au sein de notre infrastructure réseau. Nous avons abordé les procédures d'installation et de déploiement des outils afin de collecter des données à partir de différents systèmes des différents équipements. Grâce à ces installations, nous disposons des capacités nécessaires pour surveiller en temps réel les incidents critiques à l'aide de tableaux de bord personnalisés et d'alertes. De plus, nous sommes en mesure d'analyser les journaux et les événements, de détecter les activités suspectes et de prendre des mesures appropriées en cas de menace ou d'incident.

Conclusion et perspectives

Ce mémoire a exploré en profondeur les défis et les solutions en matière de sécurité des réseaux informatiques au sein de l'infrastructure cliente de VMS Bejaia, fournie par Campus NTS. L'objectif principal était de rechercher et de mettre en œuvre une nouvelle architecture réseau sécurisée pour répondre aux besoins critiques identifiés.

Nous avons approfondi nos connaissances dans les réseaux informatiques et leur sécurité, soulignant l'importance pour un administrateur réseau de maîtriser les fondements afin d'anticiper et de contrer les diverses formes d'attaques potentielles. En étudiant en détail l'architecture réseau de VMS Bejaia, nous avons pu identifier la problématique principale et la solution appropriée. En intégrant les solutions IDS/IPS et SIEM, nous avons démontré comment Snort et Splunk peuvent renforcer la détection, la prévention et la réponse aux menaces, assurant ainsi une protection robuste contre les cyberattaques.

La conception et la mise en œuvre concrètes de la plateforme Splunk et Snort au sein de l'infrastructure de VMS Bejaia ont été réalisées avec succès. Nous avons détaillé les étapes d'installation, de configuration et de déploiement, mettant en lumière notre capacité à surveiller en temps réel, analyser les incidents critiques et répondre efficacement aux menaces émergentes.

Notre stage au sein de VMS Bejaia nous a apporté une expérience pratique précieuse, nous permettant d'appliquer nos connaissances théoriques en administration et sécurité des réseaux. Il nous a également offert une occasion unique de découvrir de manière pratique le domaine de la gestion de la sécurité informatique, renforçant ainsi notre expertise et notre confiance dans ce domaine.

Pour nos futures perspectives, notre déploiement de Splunk et Snort nous guide vers plusieurs axes de développement clés. Nous prévoyons d'améliorer constamment notre sécurité en explorant les avancées technologiques telles que l'intelligence artificielle et l'apprentissage machine pour une détection plus rapide des menaces. L'expansion de la surveillance pour inclure plus de périphériques critiques et le renforcement de nos capacités d'analyse pour des décisions proactives restent prioritaires. Parallèlement, nous mettrons l'accent sur la formation continue du personnel pour renforcer la culture de la sécurité. Enfin, nous resterons vigilants contre les nouvelles menaces en adaptant nos stratégies pour garantir une protection robuste contre les cyberattaques à venir.

Annexe 1

I. Installation Outils de simulation (développements)

Cette partie détaille les phases d'installation des environnements de travail utilisés pour mettre en place notre architecture et nos solutions :

A. GNS3 :

Pour mettre en place une architecture réseau réelle, nous avons choisir d'utiliser GNS3 (Graphical Network Simulator), un programme de simulation réseau libre.

Pour installer GNS3, il est tout d'abord nécessaire de télécharger le fichier exécutable depuis le site 'https://www.gns3.com/'. Ensuite, il suffit de lancer le fichier et de suivre les étapes illustrées dans les figures 35 et 36.

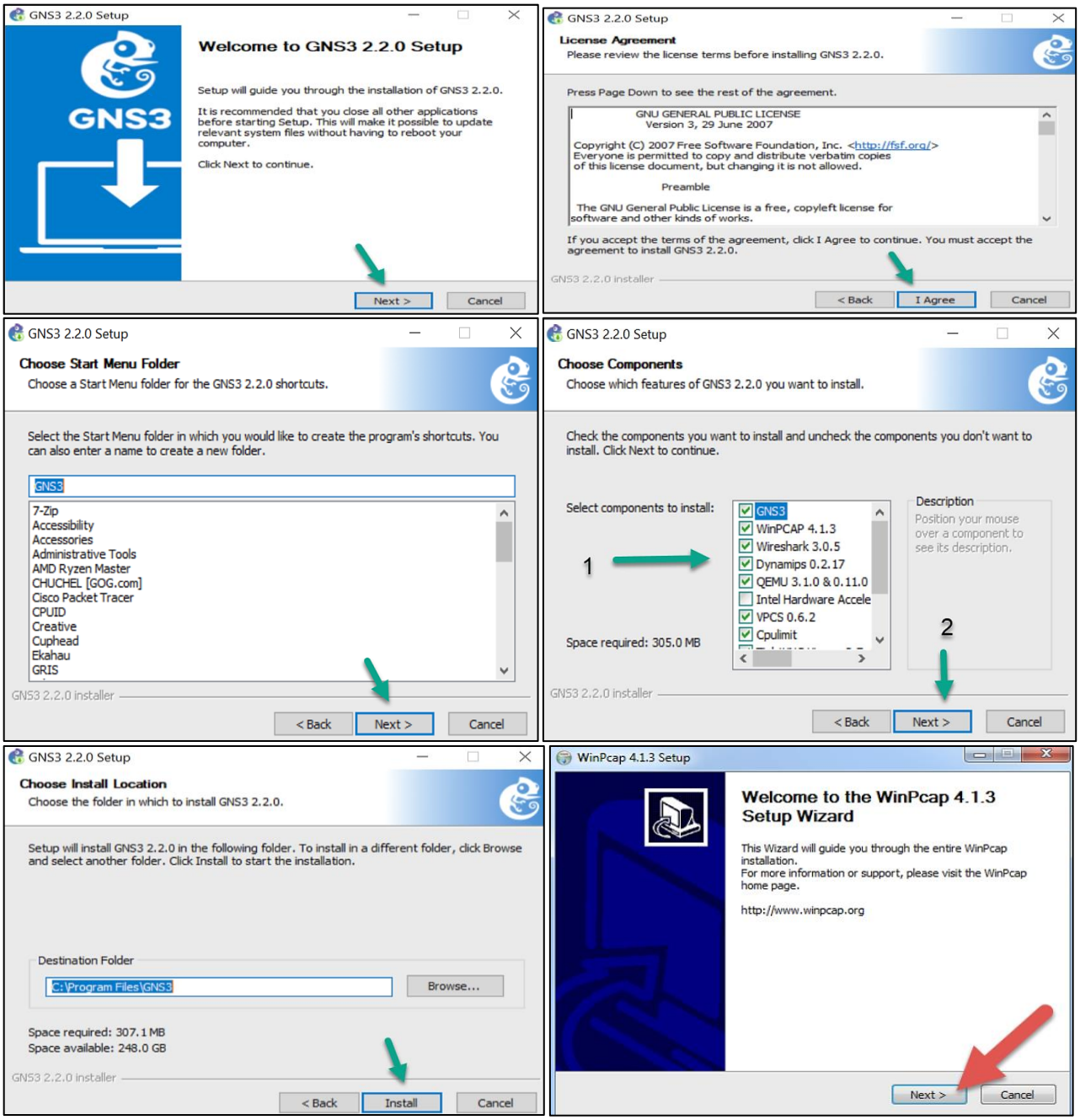

Figure 35 Etapes d'installation de GNS3 (1)

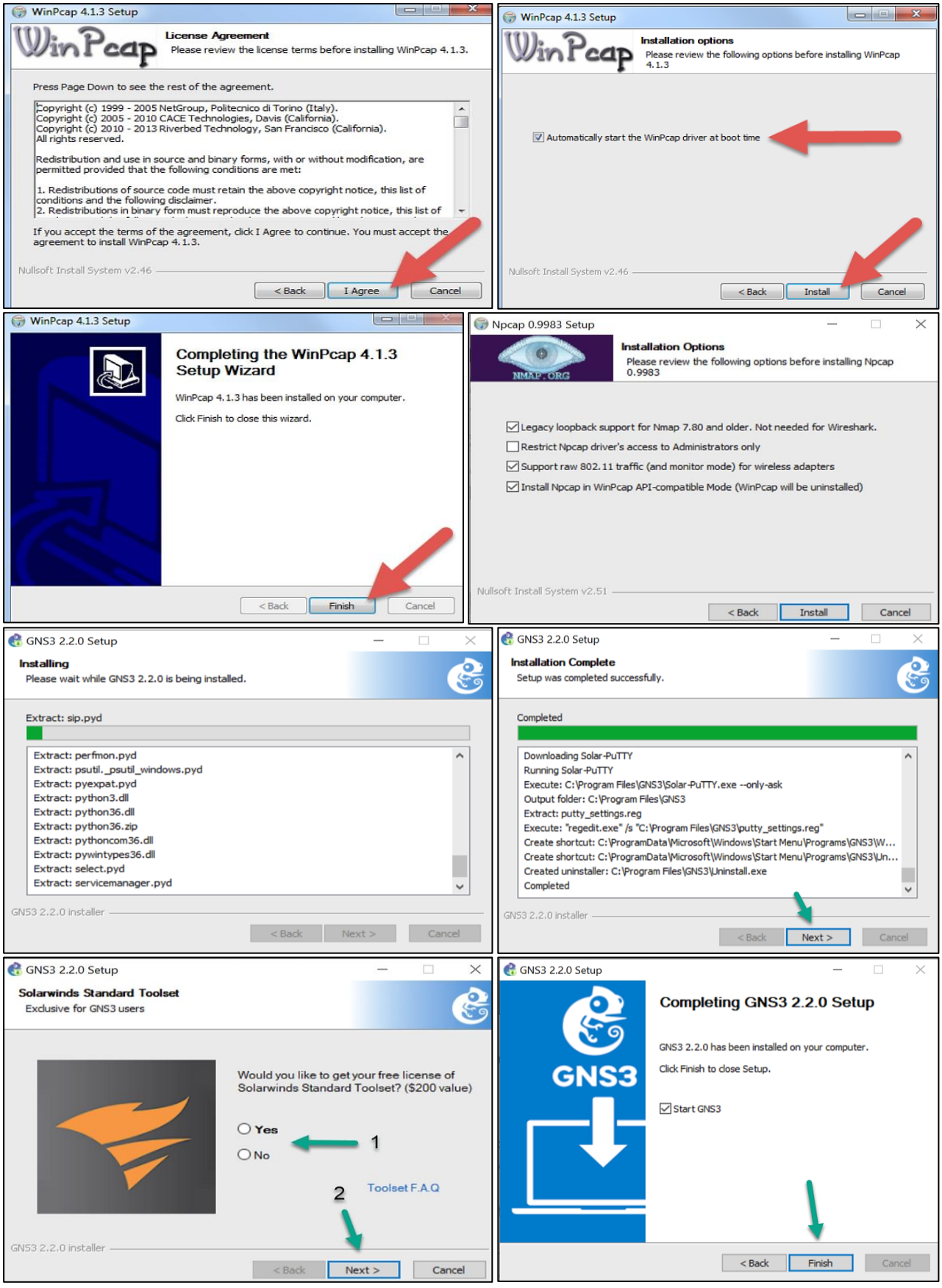

Figure 36 Etapes d'installation de GNS3 (2)

B. VMware Workstation 17 :

Pour l'émulation de notre réseau, nous avons choisi d'utiliser le logiciel de virtualisation 'VMware Workstation 17' pour la création d'une ou plusieurs machines virtuelles de même ou de différents systèmes d'exploitation sur notre ordinateur physique.

Cette version est disponible sur le site suivant : 'https://www.vmware.com/products/worskstation-pro/workstation-pro-evaluation.html/'. Nous téléchargeons alors la version appropriée, puis nous suivons l'installation en suivant les étapes déterminées ci-dessous (figure 37) :

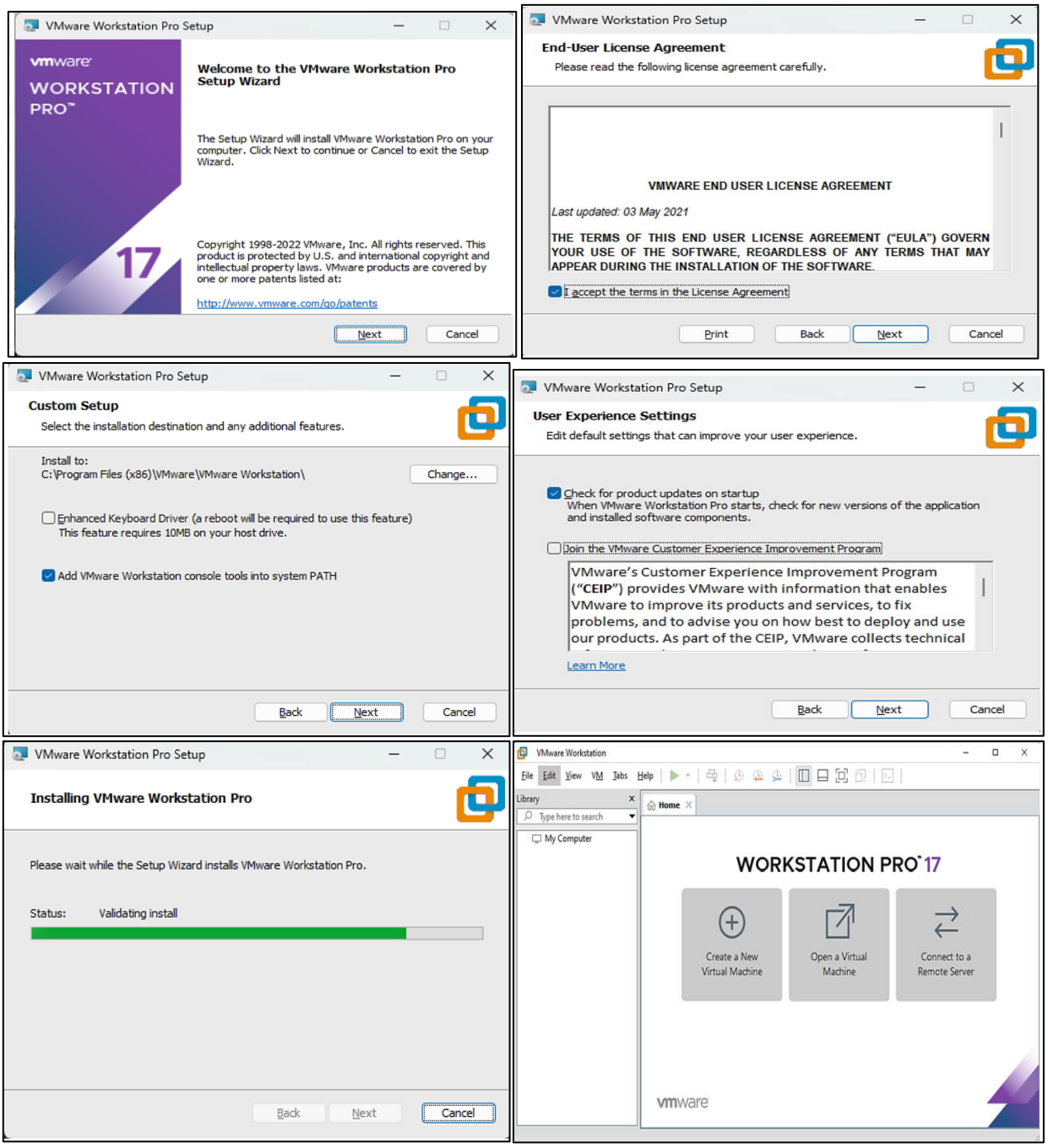

Figure 37 Etapes d'installation de VMware Workstation 17

C. Déploiement des machines virtuelles et serveurs :

En ce qui concerne les postes utilisateurs de notre infrastructure, nous avons utilisé les systèmes d'exploitation adaptes à l'entreprise d'accueil (Server 2022, Kali Linux).
Voici les étapes d'installation des machines virtuelles illustrées dans les figures ci-dessous :

1. Server Windows 2022

En ce qui concerne les postes utilisateurs de notre infrastructure, nous avons utilisé les systèmes d'exploitation adaptes à l'entreprise d'accueil (Server 2022, Kali Linux). Voici les étapes d'installation des machines virtuelles illustrées dans les figures ci-dessous (figures 38,39) :

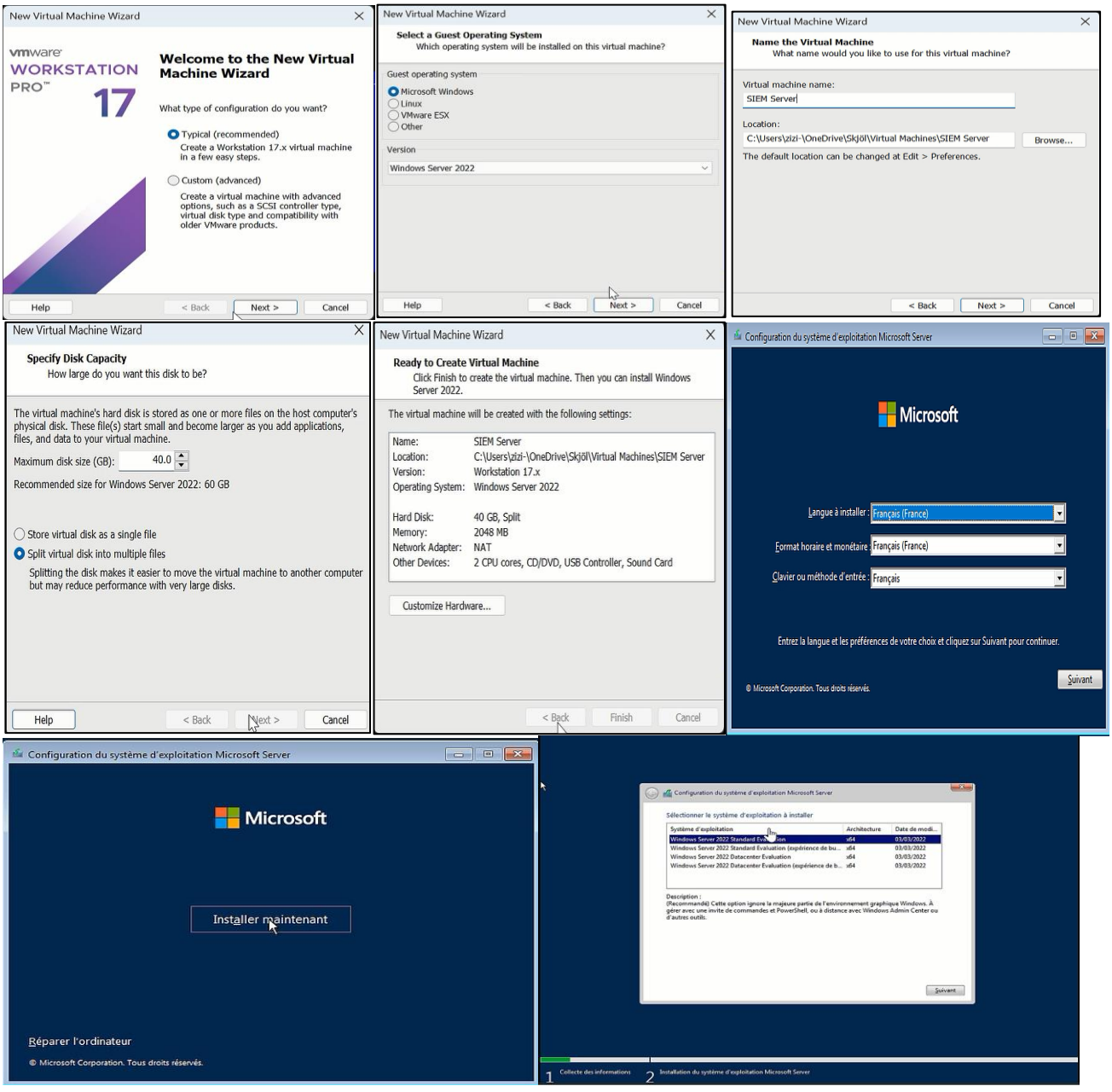

Figure 38 Etapes d'installation de Serveur 2022 (1)

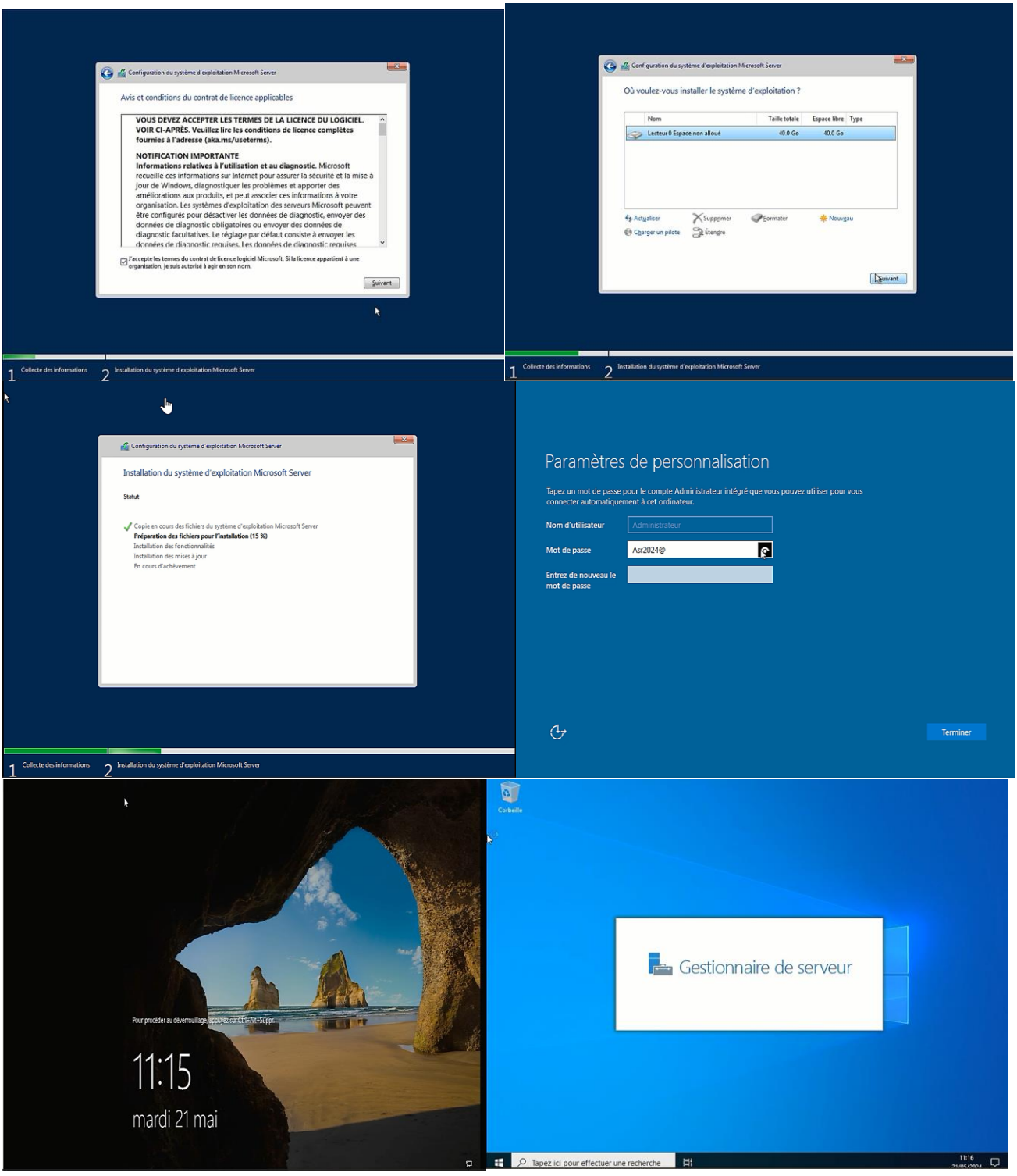

Figure 39 Etapes d'installation de Serveur 2022 (2)

2. Kali linux

Kali Linux est une autre distribution Linux basée sur Debian, développée par Offensive Security. Dans notre cas, nous avons utilisé ce système pour réaliser des tests de sécurité informatique et de pénétration afin d'évaluer les performances de notre solution SIEM et

IDS/IPS. Nous montrons les étapes d'importation de l'image Kali Linux sous VMware et les étapes d'installation de Kali Linux. (Figures 40 et 41).

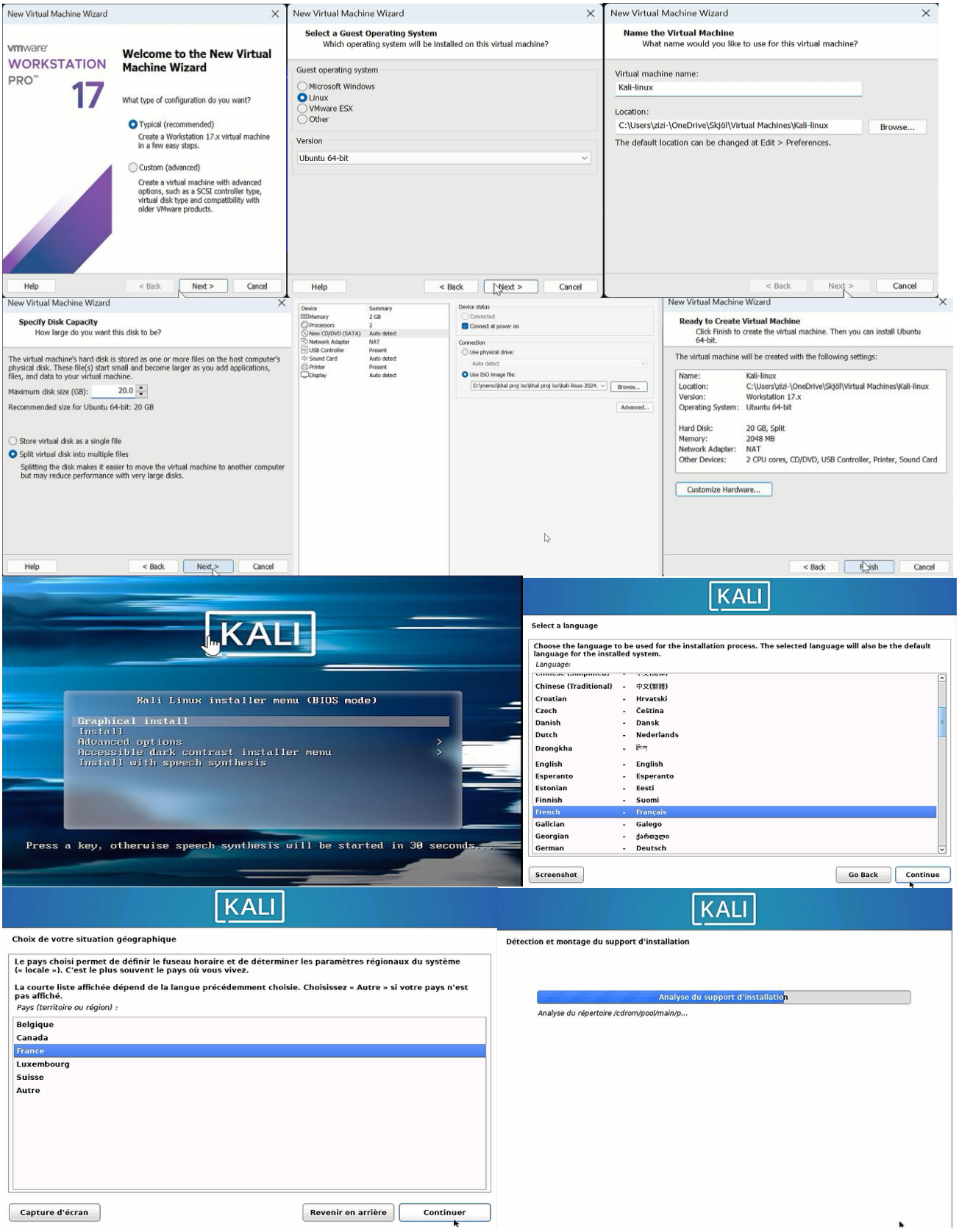

Figure 40 Etapes d'installation de Kali (1)

Annexe1

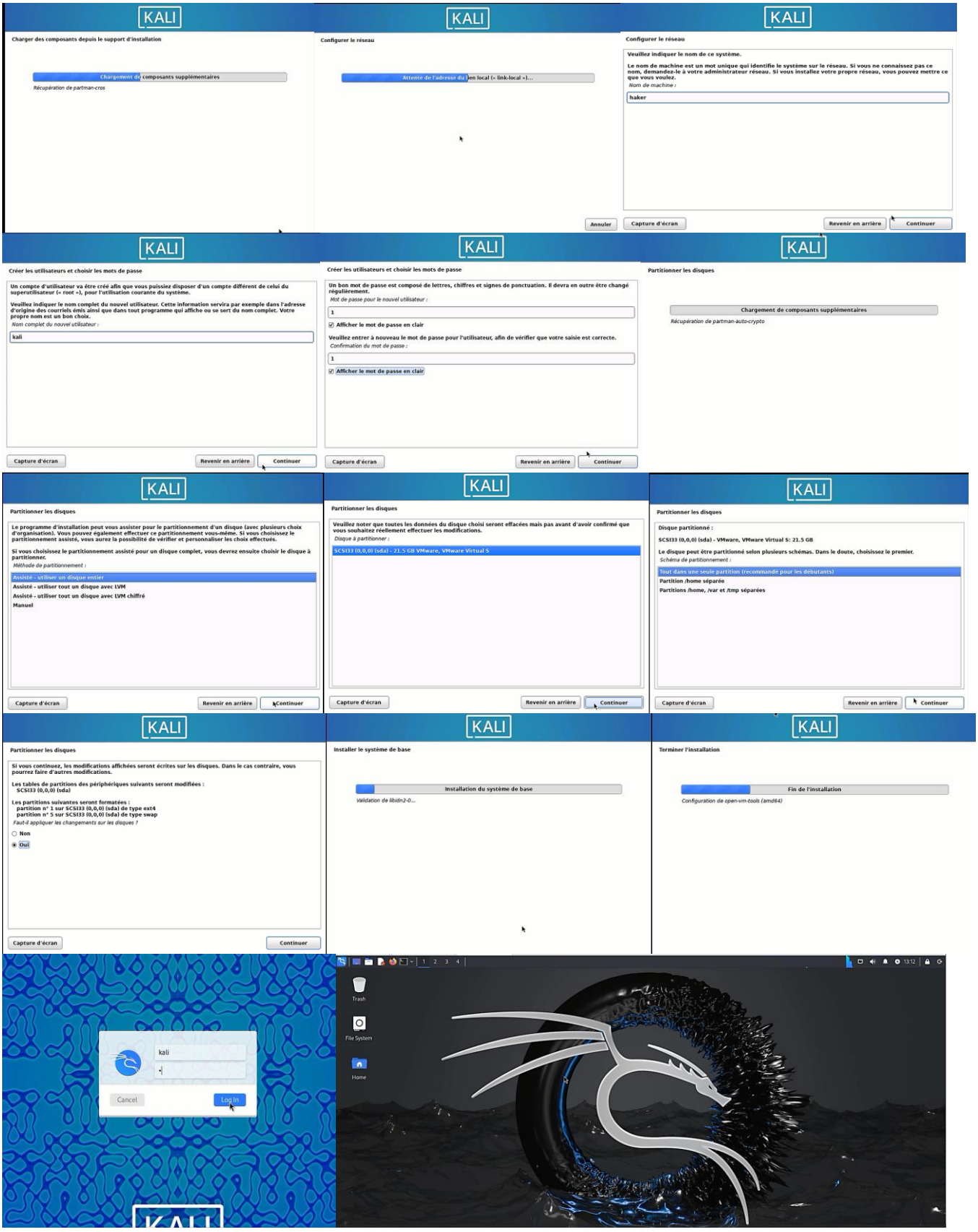

Figure 41 Etapes d'installation de Kali (2)

D. Pfsense

Nous avons intégré ce pare-feu (version 2.7.2) pour simuler de manière réaliste le contrôle du trafic réseau et pour y installer IDS/IPS (Snort) dans le but d'améliorer la sécurité du réseau. Son installation et sa configuration est illustrée dans les deux figures suivantes (42 et 43) :

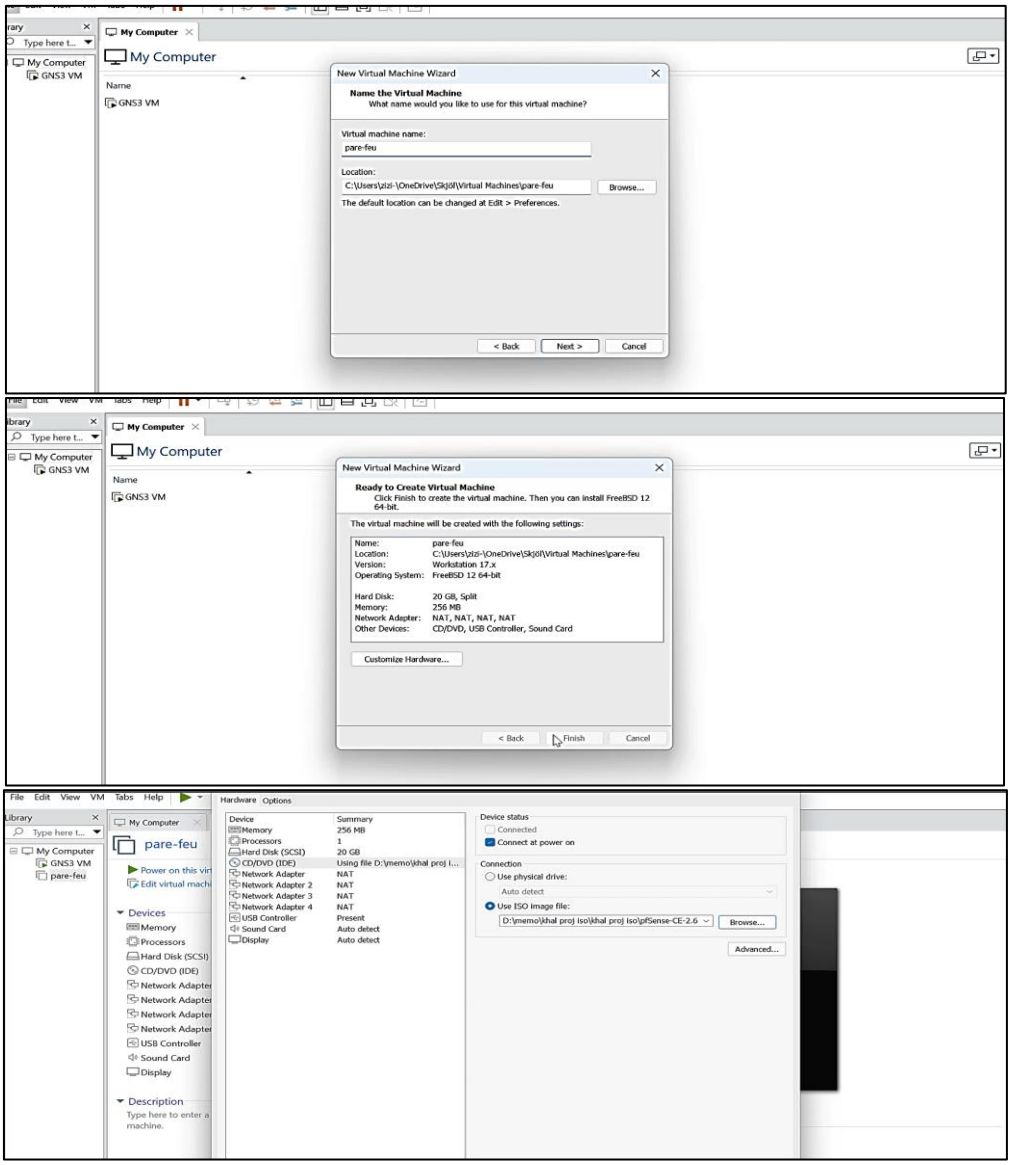

Figure 42 Etapes d'importation du Pfsense

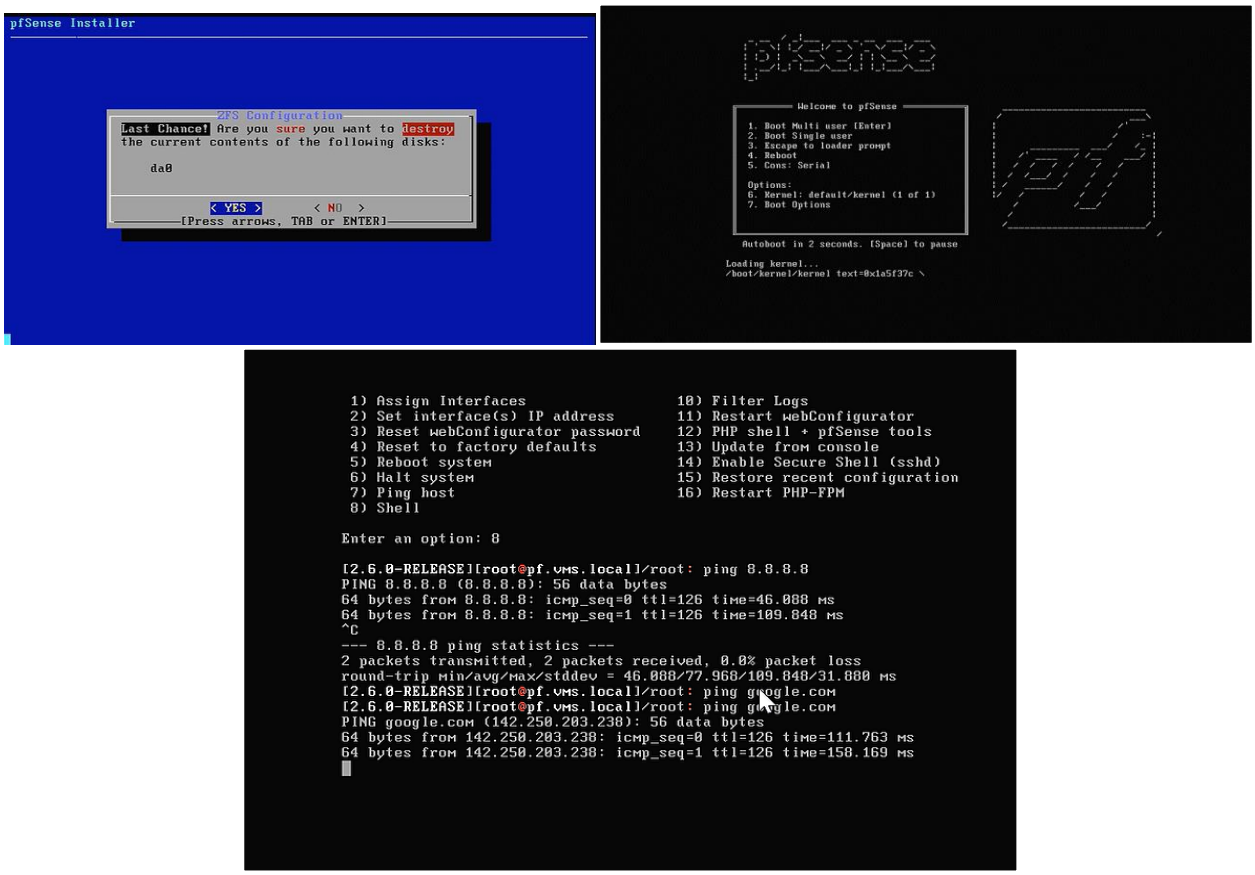

Figure 43 Configuration de Pfsense

Aller à google chrome puis taper adresse IP du Pfsense (192.168.1.1), et là c'est l'ouverture de Pfsense puis taper nom utilisateur et mot de passe, nous sommes dirigés vers une page d'accueil où nous pouvons configurer les éléments principaux comme suit :

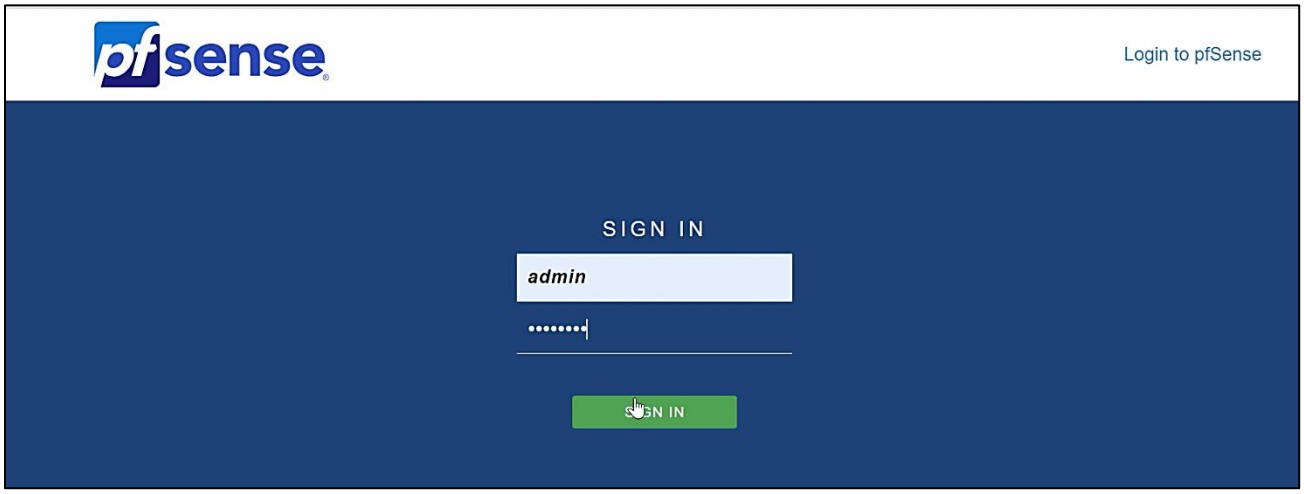

Figure 44 Interface connexion de Pfsense

Annexe1

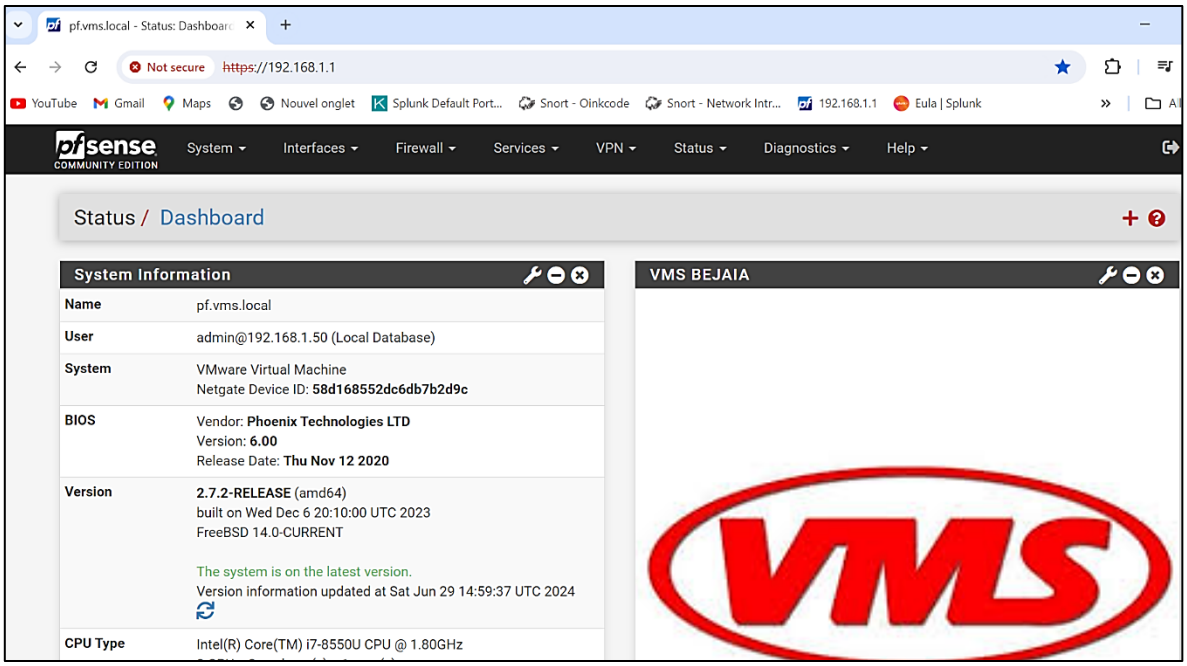

Figure 45 Interface ouverture Pfsense

Annexe 2

Planification de L'infrastructure

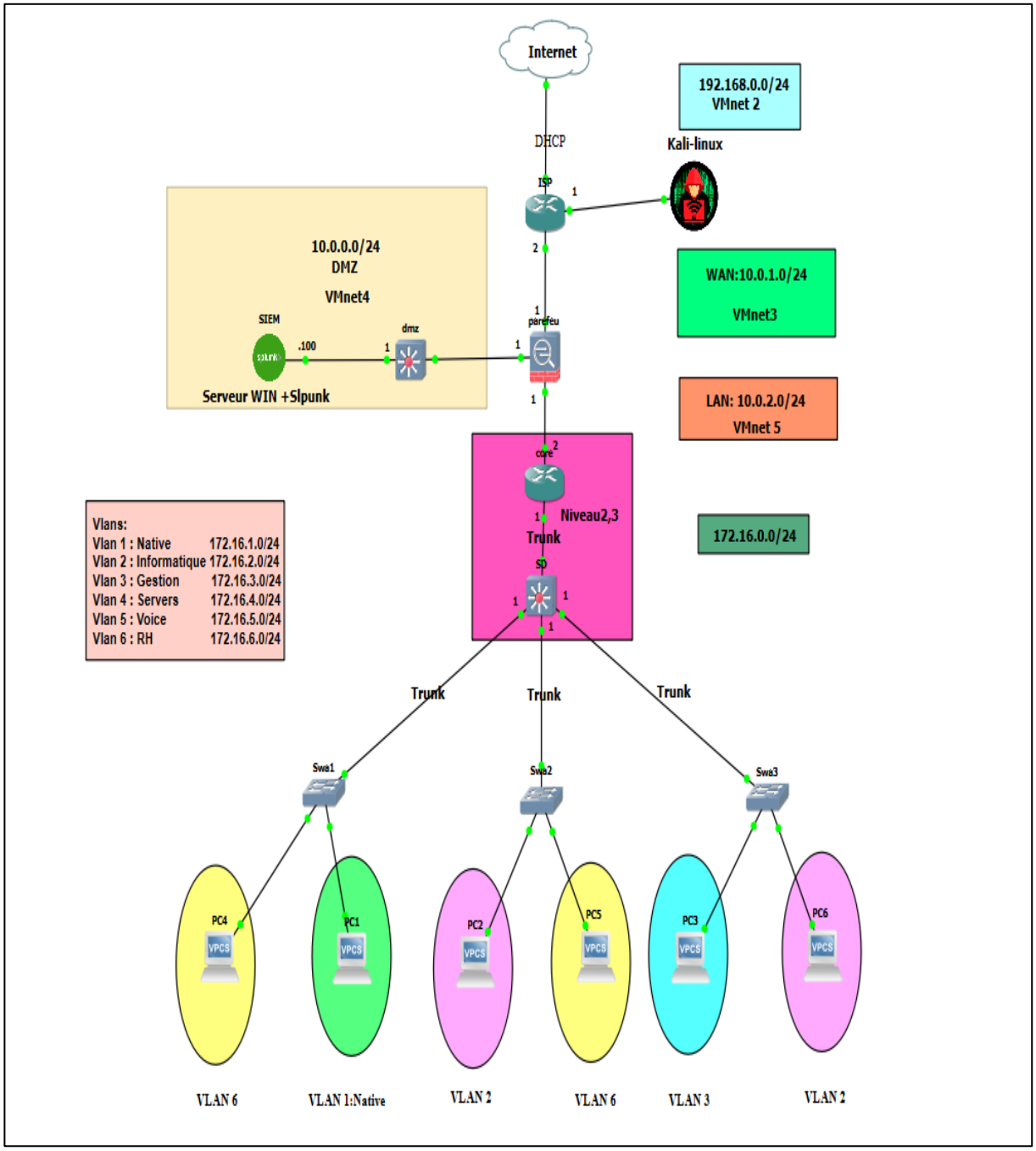

Figure 46 Infrastructure de réseau VMS Bejaia proposée

Annexe 3

I. Configuration des équipements de notreinfrastructure réseau

A. La configuration de base

Il est important d'effectuer les configurations de base (sécurisation des ports console, des lignes virtuelles et du mode enable) sur tous les commutateurs (accès et distribution) et routeurs avant de les déployer dans l'armoire de brassage. Cela permet de prévenir tout accès non autorisé, que ce soit pour la visualisation ou la modification des configurations.

B. Configuration du mode trunk

Il est nécessaire de configurer les interfaces des switches en mode trunk afin de permettre la transmission de plusieurs VLANs sur un seul lien physique et d'assurer la connectivité entre les différents VLANs reparties sur plusieurs switches. Les étapes de configuration du mode trunk sont représentés comme suit (figure 47) :

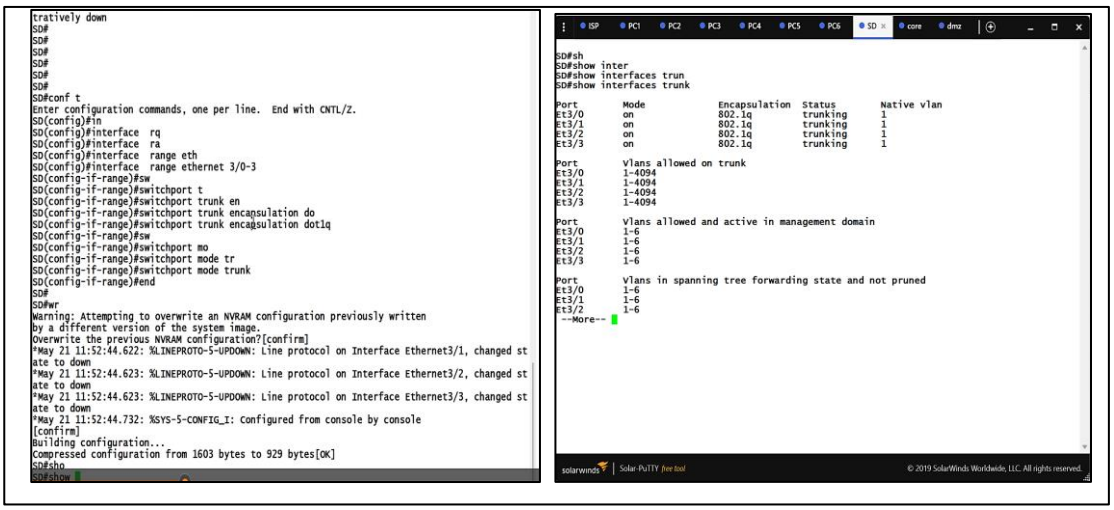

Figure 47 Exemple de configuration du mode trunk sur un switch distribution

Voici la vérification des interfaces en mode trunk en utilisant la commande 'show interface status' (figure 48)

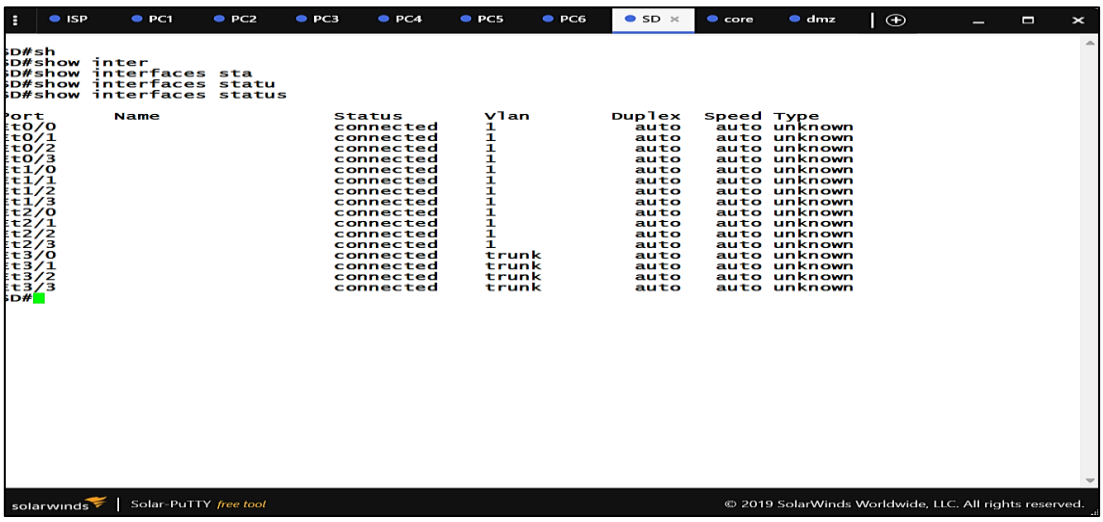

Figure 48 Vérification du mode trunk au niveau du Switch de distribution

C. Création des VLANS

Nous allons créer les VLANs à ce niveau switch distribution, comme le montre la figure 49 suivante :

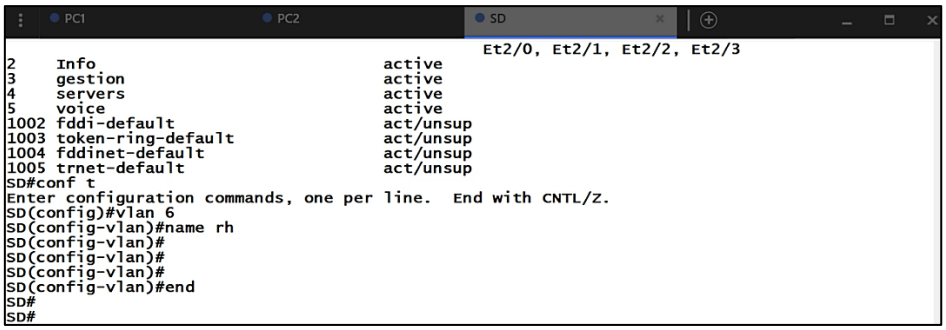

Figure 49 Création des Vlans au niveau du Switch

Afin de vérifier la propagation de la création des VLANs, nous avons utilisé la commande 'show vlan brief' (voir la figure 50) :

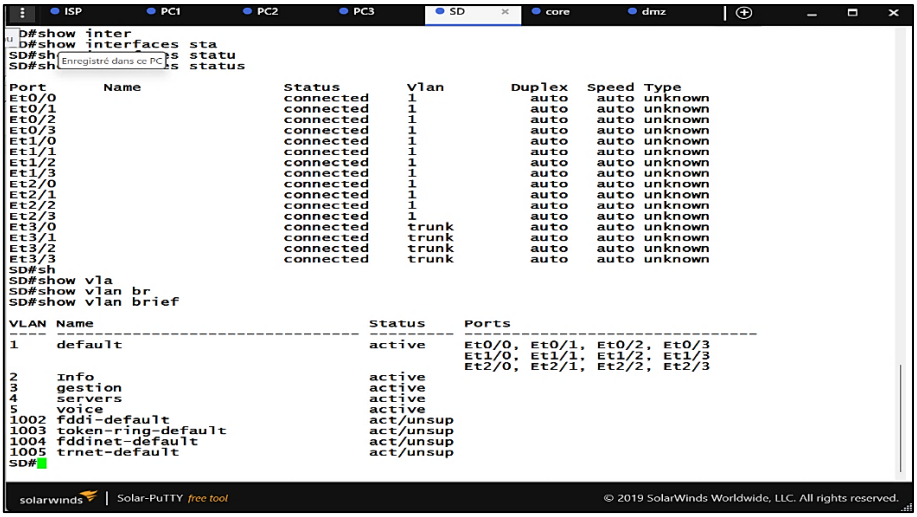

Figure 50 Vérification des VLANs

D. Activation des ports d'accès au VLAN

Tout périphérique branche sur un port physique configure en mode d'accès ne pourra communiquer qu'avec d'autres périphériques qui se trouvent dans le même VLAN. Dans la figure nous allons illustrer les étapes d'attribution de port d'accès au VLAN (figure 51).

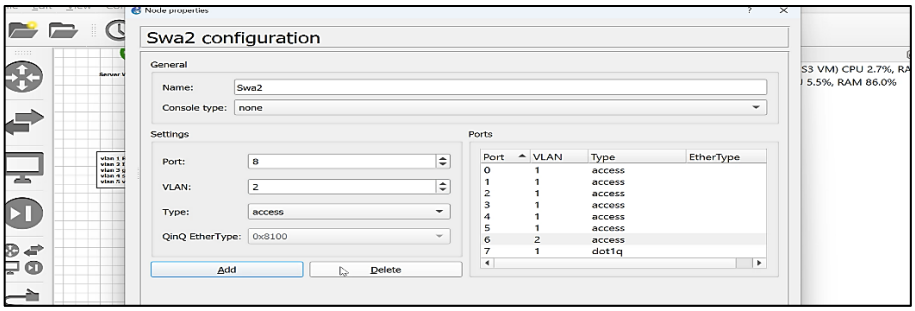

Figure 51 Activation du port d'accès au niveau du Switch 2

E. Configuration des routeurs (connecter à Internetet vers WAN)

Enfin, nous allons configurer l'interface WAN pour se connecter aux fournisseurs d'accès internet y compris les paramètres d'une configuration DHCP. De plus, nous allons configurer les protocoles de routage OSPF. Ensuite, nous allons spécifier et configurer le routeur connecte au réseau WAN, ainsi que configurer les interfaces WAN pour se connecter aux autres sites distants ou aux réseaux WAN(ISP). (Figures 52 et 53).

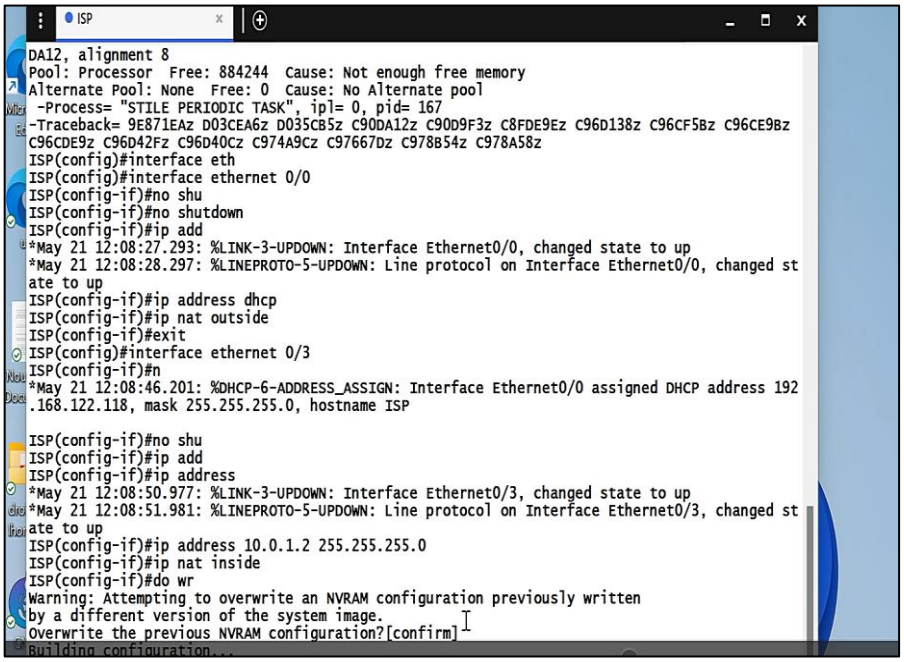

Figure 52 Configuration des interfaces Routeur WAN(ISP)

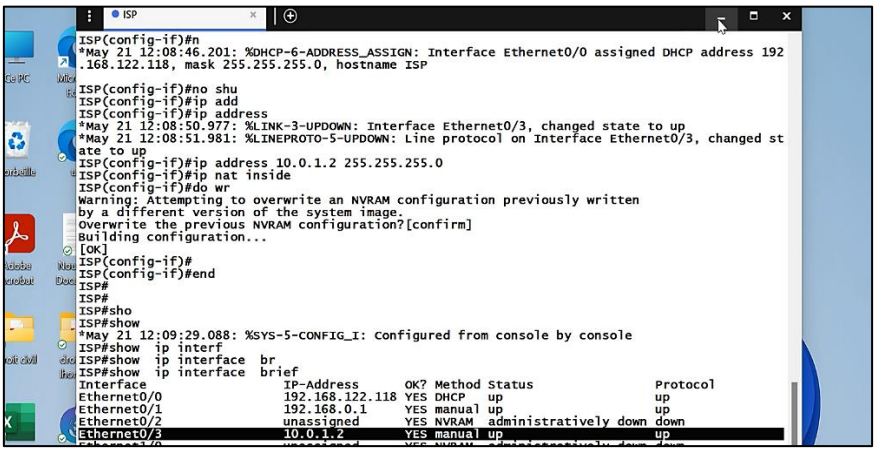

Figure 53 Vérification des interfaces Routeur WAN(ISP)

Annexe 4

I. Section2 : Le langage SPL

A. Introduction

Dans le cadre de la recherche et de l'extraction de données, ainsi que des statistiques selon nos besoins spécifiques, Splunk propose un langage de traitement étendu qui permet à un utilisateur de réduire et de transformer de grandes quantités de données d'un ensemble de données en informations spécifiques et pertinentes.

Dans cette partie, nous allons nous intéresser au langage SPL (Splunk Processing Language), à son format de base et aux différents types de commandes de recherche disponibles dans Splunk.

B. Définition de langage SPL

Le langage de traitement de recherche Splunk (SPL) est un langage contenant de nombreuses com- mandes, fonctions, arguments, etc., pour tirer au mieux parti des fonctions proposées par Splunk et de profiter pleinement de la puissance du moteur d'indexation.

C. Composants de SPL :

Le SPL comprend les composants suivants :

- **Termes de recherche :** Ce sont les mots-clés ou expressions que vous recherchez.
- **Commandes :** L'action que vous souhaitez effectuer sur le jeu de résultats, comme formater lerésultat ou le compter.
- **Clauses :** Comment regrouper ou renommer les champs dans le jeu de résultats.

D. Syntaxe

Toute requête SPL commence par la source, c'est-à-dire l'ensemble des événements étudiés, suivie d'une pipe ou barre verticale : « | ». On peut enchaîner plusieurs requêtes simplement en ajoutant une pipe au début de chacune.

Remarque : Les requêtes lancées, elles peuvent commencer par différents mots-clés tels que "chart"pour obtenir un graphe, "timechart" pour obtenir un graphe en fonction du temps, "top" pour obtenir les premiers résultats, et bien d'autres mots-clés encore. Voici les requêtes principales :

- **Demande de base :**

index=<nom-de-l'index> <recherche> **Clause de recherche :**

- **Clause de recherche**

  <champ>=<valeur>

- **Opérateurs de comparaison**

  <champ> <opérateur> <valeur>

- **Opérateurs logiques**

  <condition1> <opérateur-logique> <condition2>

- **Opérateurs logiques**

  <condition1> <opérateur-logique> <condition2>

- **Recherche par motif (wildcards)**

  <champ>=<valeur-avec-joker>

E. Commandes de transformation de recherche

- **Commande "stats" pour les statistiques**

  | stats <fonction>(<champ>) AS <nouveau-champ>

- **Commande "sort" pour le tri**

  | sort <champ> <ordre>

Bibliographie

[1] M.FARAH.Z, «Cours sécurité,» 2020/2021. [En ligne].

[2] M.DJEBBARI.N, «Sécurité,» 2019/2020. [En ligne].

[3] C.U.A.MILA, «SÉCURITÉ INFORMATIQUE,» 13 Fevrier 2023. [En ligne]. Available: https://elearning.centre-univ-mila.dz/a2024/pluginfile.php/91007/mod_resource/content/1/Chapitre%201.pdf. [Accès le 01 Juin 2024].

[4] Kincy, «Kincy: securite informatique,» [En ligne]. Available: https://kincy.fr/securite-informatique/.

[5] Nomios, «Nomios: Ingenierie sociale,» [En ligne]. Available: https://www.nomios.fr/ressources/ingenierie-sociale/. [Accès le Juin 2024].

[6] N. Ripoll, «Blog webidentity : importance de la securite informatique pour les entreprise,» 23 Janvier 2023. [En ligne]. Available: https://blog.webidentity.ch/importance-de-la-securite-informatique-pour-les-entreprise. [Accès le 07 Avril 2024].

[7] «Ninjaone.com,» [En ligne]. Available: https://www.ninjaone.com/fr/it-hub/endpoint-security/qu-est-ce-qu-une-liste-de-controle-d-acces-acl/. [Accès le 12 Juin 2024].

[8] «it-connect.fr,» [En ligne]. Available: https://www.it-connect.fr/les-listes-de-controle-dacces-acl-avec-cisco/. [Accès le 16 Juin 2024].

[9] P. Puteaux, «Analyse et traitement des images dans le domaine chiffré,» 9 Octobre 2020. [En ligne]. Available: https://theses.hal.science/tel-03117770v1/file/PPuteaux_These.pdf. [Accès le 12 Juin 2024].

[10] N. N. M. BOUDAOUD Fetta, «Sécurité informatiquebasé sur un cryptosystèmecas AES,» 2012/2013. [En ligne]. Available: https://dspace.ummto.dz/server/api/core/bitstreams/4f467bb2-32fb-40aa-b60a-e6a3ab7d5c36/content. [Accès le 18 Mars 2024].

[11] C. connecté, «IDS / IPS expliqués en dessins,» [En ligne]. Available: https://www.youtube.com/watch?v=bG8Xb02Lrs4&t=36s. [Accès le 25 Mars 2024].

[12] «SNORT-Protect your network with the world's most powerful Open Source detection software.,» [En ligne]. Available: https://www.snort.org/. [Accès le 25 Mars 2024].

[13] Splunk, «C'est quoi le SIEM,» 15 Decembre 2022. [En ligne]. Available: https://www.youtube.com/watch?v=ovNq9iuUkLs. [Accès le 01 Avril 2024].

[14] R. Mohanan, «Qu'est-ce que la gestion des informations et des événements de sécurité (SIEM) ? Définition, architecture, processus opérationnel et meilleures pratiques,» 24

Février 2022. [En ligne]. Available: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-siem/. [Accès le 27 Avril 2024].

[15] Splunk, «Splunk : Qu'est-ce qu'un SIEM?,» [En ligne]. Available: https://www.splunk.com/fr_fr/data-insider/what-is-siem.html. [Accès le 18 Mai 2024].

[16] W. Academy, «SIEM - Understanding How SIEM Works | SOC SIEM SOAR,» 23 Décembre 2019. [En ligne]. Available: https://www.youtube.com/watch?v=3JMp57jRd5Q&list=PLZg_TDpqoVKX6asnD5c6S6E0ASbPiKEp_. [Accès le 1 Avril 2024].

[17] M. A. Eddik, «Comprendre le fonctionnement d'un SIEM sous Logpoint,» Alphorm, 23 Janvier 2020. [En ligne]. Available: https://www.youtube.com/watch?v=c2RRs9cViuQ. [Accès le 28 Avril 2024].

[18] N. K. Pathi, «SIEM Architecture,» 14 Decembre 2015. [En ligne]. Available: https://fr.slideshare.net/slideshow/siem-architecture/56119394. [Accès le 28 Avril 2024].

[19] T. Z. ت. زين ,ا «Security Information and Event Management (SIEM) for Cyber Security شرح بالعربي للمهندس تامر زين,» 21 Novembre 2023. [En ligne]. Available: https://www.youtube.com/watch?v=CUWvm0YG_Aw. [Accès le 01 Avril 2024].

[20] ح. ص. مرشد, «SIEM (Security Information and Event Management : Digital Networks,» 17 Avril 2019. [En ligne]. Available: https://www.youtube.com/watch?v=jEBbIdlIBhU. [Accès le 27 Avril 2024].

[21] Meena, «What are Correlation Rules and How Do They Work In SIEM?,» [En ligne]. Available: https://luminisindia.com/cybersecurity-prism/363-what-are-correlation-rules-and-how-do-they-work-in-siem. [Accès le 16 Avril 2024].

[22] C. G. Matter, «SIEM, EDR, XDR, MDR & SOAR | Cybersecurity Tools and Services | Threat Monitoring,» 19 Avril 2022. [En ligne]. Available: https://www.youtube.com/watch?v=TAaRA4ctRL4. [Accès le 01 Avril 2024].

[23] CyberPlatter, «SIEM Interview Questions and Answers | Part 1 | Cybersecurity Interview Questions & Answers | SIEM,» 25 Aout 2023. [En ligne]. Available: https://www.youtube.com/watch?v=-HYD9mQl1zA. [Accès le 28 Avril 2024].

[24] D. CyberWox, «SIEM Capabilities for SOC Analysts, Threat Hunters, Detection Engineers & Incident Responders,» 22 Janvier 2024. [En ligne]. Available: https://www.youtube.com/watch?v=lXPtuSZ9P-A&t=661s. [Accès le 16 Avril 2024].

[25] S. Rai, «SIEM : Security Information and Event Management,» 29 Jaznvier 2022. [En ligne]. Available: https://fr.slideshare.net/slideshow/siem-security-information-and-event-management-251077906/251077906. [Accès le 28 Avril 2024].

[26] Imsnetworks, «SIEM : pourquoi et comment le mettre en place ?,» [En ligne]. Available: https://www.imsnetworks.com/ressources-et-actual/siem/. [Accès le 15 Avril 2024].

[27] «Security Information and Event Management (SIEM),» 7 Mars 2014. [En ligne]. Available: https://fr.slideshare.net/slideshow/security-information-and-event-management-siem/32046298. [Accès le 28 Arril 2024].

[28] Fortinet, «Qu'est-ce que le SIEM ?,» [En ligne]. Available: https://www.fortinet.com/fr/resources/cyberglossary/what-is-siem#:~:text=Les%20solutions%20de%20gestion%20des,conform%C3%A9ment%20%C3%A0%20des%20politiques%20pr%C3%A9d%C3%A9finies.. [Accès le 27 Avril 2024].

[29] IBM, «Qu'est-ce qu'un SIEM ?,» [En ligne]. Available: https://www.ibm.com/fr-fr/topics/siem#:~:text=La%20corr%C3%A9lation%20d'%C3%A9v%C3%A9nements%20a,la%20s%C3%A9curit%C3%A9%20de%20l'entreprise.. [Accès le 1 Avril 2024].

[30] «OPENVPN,» [En ligne]. Available: https://openvpn.net/. [Accès le 22 Mars 2024].

[31] OpenClassRooms, «OPENCLASSROOMS: Découvrez le fonctionnement d'un SIEM,» 15 Mars 2024. [En ligne]. Available: https://openclassrooms.com/fr/courses/1750566-optimisez-la-securite-informatique-grace-au-monitoring/7144273-decouvrez-le-fonctionnement-d-un-siem. [Accès le 28 Avril 2024].

[32] cloudflare, «Open System Interconnection,» [En ligne]. Available: https://www.cloudflare.com/fr-fr/learning/ddos/glossary/open-systems-interconnection-model-osi/. [Accès le 17 Mai 2024].

[33] «Microsoft : Qu'est-ce qu'un système SIEM ?,» [En ligne]. Available: https://www.microsoft.com/fr-fr/security/business/security-101/what-is-siem#:~:text=Un%20syst%C3%A8me%20de%20gestion%20des,elles%20ne%20perturbent%20leurs%20activit%C3%A9s.. [Accès le 1 Avril 2024].

[34] «Kiteworks.com,» [En ligne]. Available: https://www.kiteworks.com/fr/glossaire/quest-ce-que-les-systemes-de-detection-et-de-prevention-des-intrusions/. [Accès le 25 Mars 2024].

[35] «Juniper.com,» [En ligne]. Available: https://www.juniper.net/fr/fr/research-topics/what-is-ids-ips.html. [Accès le 25 Mars 2024].

[36] T. IPwithease, «IDS vs IPS vs Firewall #networksecurity #firewall #IPS #IDS,» 2023. [En ligne]. Available: https://www.youtube.com/watch?v=l7FeR1MIRFY. [Accès le 25 Mars 2024].

[37] G. Collins, «Cybersecurity Homelab - Detecting Cyber Threats (SIEM),» 07 Avril 2021. [En ligne]. Available: https://www.youtube.com/watch?v=_Xw43NLo2kg. [Accès le 01 Avril 2024].

[38] Exabeam, «Architecture SIEM : technologie, processus et données,» [En ligne]. Available: https://www.exabeam.com/explainers/siem/siem-architecture/. [Accès le 15 Avril 2024].

Résumé

Ce travail s'inscrit dans le cadre du projet de fin d'études à l'Université Abderrahmane Mira - Bejaïaen vue de l'obtention du diplôme de Master en Administration et Sécurité des Réseaux Informatiques.

Ce mémoire de fin d'études se concentre sur les principes fondamentaux du SIEM (Security Information and Event Management) et du IDS/IPS (Intrusion Detection System/Intrusion Prevention System), explore les différentes technologies et solutions de sécurité disponibles, et propose une approche pratique pour mettre en œuvre des solutions IDS/IPS et SIEM efficaces.

En résultat, nous avons réussi à implémenter les deux solutions essentielles : la plateforme SIEM Splunk pour la gestion avancée des informations de sécurité, et le système IDS/IPS Snort pour la détection et la prévention des intrusions. Cette étude explore diverses technologies de sécurité et propose une approche détaillée pour renforcer la sécurité des infrastructures informatiques contre les cybermenaces. Dans ce mémoire, nous détaillons la démarche de déploiement en expliquant en détaille les concepts, les outils utilises tout au long du processus.

Mots clés : SIEM, SIM, SEM, Splunk, Snort, log, IDS, IPS, Snort, cybermenaces.

Abstract

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

This thesis focuses on the fundamental principles of SIEM (Security Information and Event Management) and IDS/IPS (Intrusion Detection System/Intrusion Prevention System), explores various security technologies and solutions, and proposes a practical approach to implementing effective IDS/IPS and SIEM solutions.

As a result, we successfully implemented two essential solutions: the Splunk SIEM platform for advanced security information management, and the Snort IDS/IPS system for intrusion detection and prevention. This study explores diverse security technologies and provides a detailed approach to enhancing the security of IT infrastructures against cyber threats. In this thesis, we detail the deployment process, explaining the concepts and tools used throughout.

Keywords: SIEM, SIM, SEM, Splunk, Snort, log, IDS, IPS, cyber threats.

ملخص

يندرج هذا العمل في إطار مشروع التخرج بجامعة عبد الرحمن ميرة - بجاية، للحصول على شهادة الماستر في إدارة وأمن الشبكات المعلوماتية.

يركز هذا البحث على المبادئ الأساسية لإدارة معلومات وأحداث الأمن ونظام كشف ومنع التسلل، ويستعرض التقنيات والحلول الأمنية المختلفة المتاحة، ويقترح نهجًا عمليًا لتنفيذ حلول فعّالة لأنظمةIDS/IPS وSIEM

كجزء من النتائج، تمكنا من تنفيذ حلّين أساسيين:

SIEM Splunkمنصة لإدارة معلومات الأمن المتقدمة ,

وIDS/IPS Snort نظام للكشف عن التسللات ومنعها .

تستعرض هذه الدراسة تقنيات الأمن المختلفة وتقترح نهجًا مفصلاً لتعزيز أمن البنى التحتية المعلوماتية ضد التهديدات السيبرانية. نوضح في هذا البحث عملية النشر بشكل مفصل من خلال شرح المفاهيم والأدوات المستخدمة على مدار العملي.

الكلمات المفتاحية: SIEM ،SIM ،SEM ،Splunk ،Snort ،log ،IDS ،IP.تهديدات سيبرانية