République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire De Master

En vue d'obtention du diplôme de master en informatique spécialité :

Réseaux et Sécurité

Thème

Etude et mise en place d'un centre d'opération de sécurité

Réalisé par :

M. MAZARI Amar
M. ARIB Mouloud

Promotrice :

Mme. HOUHA Amel	**M.A. A**	**U. A. Mira Bejaïa.**
Les jurys :		
Président Mr. MOKTEFI Mohand	**M.C. B**	**U. A. Mira Bejaïa.**
Examinatrice Mme. BOUADEM Nassima	**M.C. B**	**U. A. Mira Bejaïa.**

Année universitaire 2022-2023

REMERCIMENTS

Nous remercions tout d'abord le bon dieu de nous avoir donné le courage et la patience pour mener à bien notre travail.

Nous tenons aussi à adresser nos vifs remerciements :

A notre promotrice Mme. HOUHA Amel pour ses précieux conseils, sa confiance et de nous avoir dirigé tout au long de ce travail.

Nous souhaitons formuler nos remerciements les plus affectueux à nos familles, nos amis qui nous ont toujours encouragés au cours de la réalisation de notre travail.

Dédicaces

Je dédie ce modeste travail à mes parents et toute ma famille pour leur soutien tout au long de mon parcours universitaire, et à tous mes amis.

Amar . M

Dédicaces

Je dédie ce modeste travail à mes parents et toute ma famille pour leur soutien tout au long de mon parcours universitaire, et à tous mes amis.

Mouloud . A

Table des matières

Liste des tableaux

Liste des figures

Liste des abréviations

AWS : Amazon Web Services

CLI : Command Line Interface

DDOS: Distributed Denial of Service

DHCP: Dynamic Host Configuration Protocol

DMZ: Demilitarized Zone

DOS: Denial of Service

GNS3: Graphical Network Simulator 3

HTTP: Hypertext Transfer Protocol

ICMP: Internet Control Message Protocol

IDS: Intrusion Detection System

IP: Internet Protocol

IPS: Intrusion Prevention System

ISP: Internet Service Provider

LAN: Local Area Network

NAT: Network Address Translation

NTS: Network Technologies Solution

OSSIM: Open Source Security Information Management

SEM: Security Event Management

SIEM: Security Information and Event Management

SIM: Security Information Management

SOC: Security Operations Center

SPL: Search Processing Language

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

UF: Universal Forwarder

VLAN: Virtual Local Area Network

VM: Virtual Machines

WAN: Wide Area Network

Introduction générale

Introduction générale

La sécurité informatique joue un rôle très important dans le développement technologique, cependant avec ce développement les problèmes de sécurité s'augmentent encore et encore, pour cela les entreprises et les organisations doivent protéger leur infrastructure informatique (données, machine, serveur, etc.) et améliorer leurs stratégies de sécurité informatique. Ce mémoire explore les différents aspects de sécurité, offrant un aperçu sur une problématique de sécurité cruciale dans les entreprise et les organisations ainsi sur une solution moderne face à cette problématique.

Les technologies de sécurité traditionnelles présentent des limitations importantes. Les attaquants utilisent des techniques avancées qui rendent leur détection difficile, voire impossible, pour les solutions conventionnelles. Cela crée une faille dans la défense des entreprises, qui peuvent ne pas être conscientes des activités malveillantes en cours sur leur réseau jusqu'à ce qu'il soit trop tard. De plus, ces technologies ont une capacité limitée à gérer efficacement les incidents de sécurité, ce qui rend la résolution des problèmes plus complexe et prolonge le temps de récupération après une cyberattaque. Pour répondre à ces défis, les entreprises ont besoin d'une approche plus proactive et réactive pour détecter et gérer les menaces de manière efficace, minimisant ainsi les perturbations potentielles.

Face à ces limitations, une solution moderne se présente sous la forme d'un Centre d'Opération de Sécurité (SOC). Un SOC est un élément centralisé et intégré du système de sécurité d'une entreprise ou d'une organisation, qui met l'accent sur la surveillance en temps réel, la détection proactive des menaces et la réponse rapide aux incidents de sécurité. Un élément clé d'un SOC est le Security Information and Event Management (SIEM), qui collecte et analyse les fichiers journaux et les événements de sécurité pour identifier les activités suspectes.

Le premier chapitre de ce mémoire donne une introduction générale aux éléments essentiels de la sécurité informatique ainsi les types des menace informatique est les solutions traditionnelles contre ces menaces.

Le deuxième chapitre se concentre sur la présentation de l'entreprise Campus NTS, ainsi un aperçu sur les problèmes de sécurités confronté par les clients de ce dernier et la solution pour contrer ces problèmes et améliorer leur sécurité.

Le troisième chapitre met en évidence l'importance d'un centre d'opération de sécurité (SOC) comme une solution moderne pour faire faces aux problèmes de sécurité dans les entreprises En se concentrant sur les technologies essentielles d'un SOC, telles que le Security

Information and Event Management (SIEM) et l'analyse des fichiers journaux, ce chapitre montre comment ces outils peuvent renforcer la capacité des organisations à détecter et à réagir rapidement face aux menaces.

Enfin, le dernier chapitre décrit en détail l'environnement de travail et l'architecture choisie. Il donne un aperçu sur les étapes d'installation des outils utilisés, les méthodes de collection et d'analyse des fichiers journaux, ainsi les méthodes de visualiser les données collectées (la création des tableaux de bords). Il présente également un test d'intrusion pour évaluer l'efficacité de la solution ainsi que la mise en œuvre des contre-mesures face à l'intrusion.

Chapitre 1
Généralité sur la sécurité informatique

1.1 Introduction

Un réseau a pour fonction de transporter les données entre les différents terminaux informatiques. Pour ce faire, un ensemble d'équipements et de processus sont nécessaires, allant de l'environnement matériel, utilisant des câbles ou des ondes radio, jusqu'à l'environnement logiciel constitué de protocoles, c'est-à-dire des règles permettant de décider de la façon de traiter les données transportées.

Dans ce chapitre nous allons exposer quelques concepts théoriques sur les réseaux informatiques et la sécurité afin de mieux comprendre leur fonctionnement. De ce fait, toutes les notions nécessaires seront présentées.

1.2 Définition de réseaux informatique

Un réseau informatique est une série d'équipement informatique interconnectés qui communiquent et partagent des ressources. Les réseaux informatiques peuvent être de différentes tailles et configurations, allant d'un petit réseau local reliant quelques ordinateurs dans un bureau à un réseau mondial tel qu'internet.

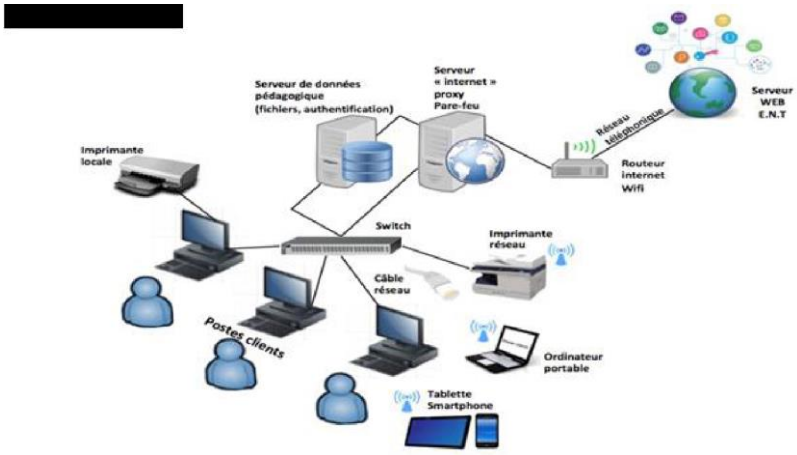


Figure 1-1 Réseau informatique

1.3 Définition de sécurité

La sécurité informatique est un ensemble de méthodes et stratégies utilisées pour protéger les systèmes informatiques et les données qu'ils contiennent et de faire face aux différentes menaces qui peuvent faire tomber le système. Ces mesures visent à détecter les accès non autorisés, les dommages causés par des logiciels malveillants, ainsi que les autres menaces

qui pourraient compromettre l'intégrité et la confidentialité des informations stockées sur les systèmes informatiques.

1.4 Objectifs de sécurité informatique

Généralement on trouve 3 principales objectifs qui sont présenter par : la confidentialité, l'intégrité et la disponibilité.

- **Confidentialité**

  L'objectif de la confidentialité est d'empêcher l'accès non autorisé aux données et informations sensibles. Les informations personnelles, financières, médicales ou les secrets commerciaux sont des exemples d'informations confidentielles. Le cryptage des données, l'authentification des utilisateurs, les pare-feu, les réseaux privés virtuels (VPN) et d'autres méthodes de sécurité peuvent être utilisés pour atteindre cet objectif.

- **Intégrité**

  L'intégrité a pour but de garantir que les données et les informations sont exactes, complètes et fiables, et qu'elles n'ont pas été altérées de quelque manière que ce soit. La validation des données, les journaux d'audit, la cryptographie et d'autres techniques de sécurité peuvent être utilisés pour atteindre cet objectif.

- **Disponibilité**

  L'objectif de la disponibilité est de s'assurer que les données et les informations sont disponibles et accessibles aux utilisateurs autorisés à tout moment. La sauvegarde des données, la redondance des systèmes, les plans de reprise après sinistre et d'autres mesures de sécurité peuvent être utilisés pour atteindre cet objectif.

1.5 Terminologies

Voici quelques exemples des termes fréquemment utilisés dans la terminologie de la sécurité sont présentés ci-dessous [9]

- **Un risque :** est la probabilité qu'une menace donnée puisse exploiter une vulnérabilité au système donné
- **Une vulnérabilité :** c'est une faiblesse ou une faille de sécurité dans un système informatique qui le rend vulnérable aux menaces aux niveaux suivants : système d'exploitation, applications, protocoles de communication, etc.

- **Une menace** : un danger qui existe dans un environnement indépendant des systèmes informatiques comme : criminel, pirate, employé mécontent, concurrent, agences gouvernementales.

  Un risque = Une vulnérabilité + Une menace
- **Contre-mesures :** ce sont les moyens de contrôle mis en place dans un système informatique pour minimiser ou éliminer les risques.

1.6 Politique de sécurité

La politique de sécurité informatique est un ensemble de règles, de procédures et de lignes directrices établies pour protéger les systèmes informatiques, les réseaux, les données et les informations contre les menaces et les risques liés à la sécurité. Elle décrit les mesures de sécurité à prendre pour assurer la confidentialité, l'intégrité et la disponibilité des ressources informatiques de l'entreprise. [1]

1.6.1 Eléments de politique de sécurité

- La politique de sécurité doit décrire explicitement les objectifs de sécurité de l'organisation, tels que la confidentialité, l'intégrité et la disponibilité des données, ainsi que la prévention des menaces.
- Les utilisateurs finaux, les agents de sécurité et les dirigeants de l'organisation doivent tous être tenus responsables de leur rôle et de leurs obligations au sein de l'organisation.

1.7 Attaques informatiques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

1.7.1 Définition de l'attaque

Une attaque est l'exploitation d'une faille d'un système informatique (système d'exploitation, réseau, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

1.7.2 Motivations des attaques

- Obtenir un accès au système.
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles.
- Glaner des informations personnelles sur un utilisateur ;

- Récupérer des données bancaires ;
- S'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- Troubler le bon fonctionnement d'un service ;
- Utiliser le système de l'utilisateur comme « rebond » pour une attaque.
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

1.8 Types d'attaques

Les attaques sont nombreuses donc il est très difficile de les citer tous. Alors ces dernières peuvent être classés en deux grandes catégories : [8]

1.8.1 Attaque passive

Ce genre d'attaques relèvent de l'écoute et de l'interception. L'attaquant collecte uniquement les informations échangées sans intention de les modifier, ce qui le rend particulièrement difficile à détecter.

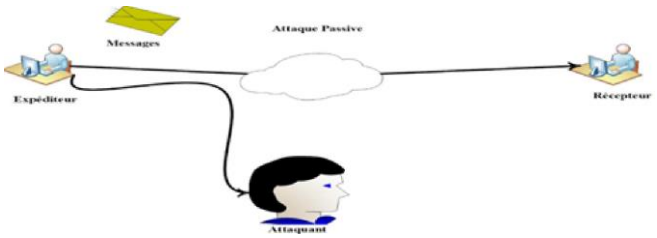


Figure 1-2 attaque passive

1.8.2 Attaque active

Elle consiste à manipuler ou modifier les données ou les ressources du système, ou à perturber leur bon fonctionnement de ce dernier.

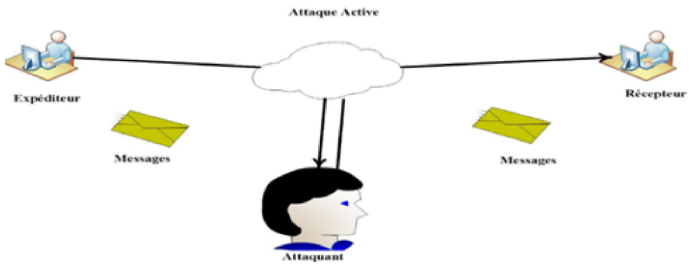


Figure 1-3 Attaque active

1.9 Description de quelques attaques

- **Attaques de phishing :** ces attaques visent à tromper les utilisateurs en leur faisant croire qu'ils communiquent avec une source de confiance, comme une banque ou un service en ligne, afin de les inciter à divulguer des informations personnelles.
- **Attaques de malware :** ces attaques utilisent des programmes malveillants pour infecter des systèmes informatiques, souvent en téléchargeant un logiciel malveillant qui peut prendre le contrôle de l'ordinateur.
- **Attaques de déni de service (DDoS) :** ces attaques visent à mettre un système informatique indisponible en envoyant une grande quantité de trafic, ce qui empêche les utilisateurs autorisés d'accéder aux ressources informatiques.
- **Attaques de force brute :** ces attaques visent à trouver les mots de passe en essayant toutes les combinaisons possibles jusqu'à ce que le bon mot de passe soit trouvé.
- **Attaques de réseau :** ces attaques tentent d'exploiter les vulnérabilités dans les protocoles de communication réseau afin d'accéder à des données sensibles ou prendre le contrôle de machines distantes.
- **Attaques de ransomwares :** l'objectif de ces attaques est de chiffrer les données d'un utilisateur et à demander une rançon pour les déchiffrer.
- **Attaques d'ingénierie sociale :** ces attaques consistent à manipuler les utilisateurs dans le but d'obtenir des informations sensibles ou accéder à des systèmes protégés.

- La politique doit établir les règles d'authentification et de contrôle d'accès, y compris les exigences en matière de mot de passe et les règles de création et de gestion des comptes d'utilisateurs.
- La politique doit contenir des méthodes pour sécuriser les données de l'organisation, telles que des procédures de sauvegarde et de récupération des données, de cryptage des données et de catégorisation des données sensibles.
- La politique doit contenir des méthodes pour faire face aux incidents de sécurité tels que les violations de données ou les attaques, ainsi que des moyens de surveiller l'environnement informatique et de détecter les activités suspectes.
- La politique doit couvrir les lois et les règlements applicables à l'organisation, tels que la confidentialité des données, la protection des consommateurs et le respect des normes industrielles.

- La politique devrait comporter des mesures visant à sensibiliser les utilisateurs finaux sur la sécurité informatique et à leur fournir une formation sur les meilleures pratiques en matière de sécurité.

1.10 Solutions de défense

1.Serveur proxy

Un serveur proxy est un système informatique qui agit comme un intermédiaire entre un client et un serveur cible dans une communication Web. Il permet de faciliter la communication entre ces deux systèmes sans modifier les requêtes ou les réponses. Lorsqu'un client demande une ressource auprès du serveur cible, le serveur proxy détourne la connexion et agit comme un client auprès du serveur cible, en demandant la ressource au nom du client. Si le serveur cible renvoie une réponse, le serveur proxy la renvoie au client, ce qui donne l'impression que la communication s'est déroulée directement entre le client et le serveur cible. Le serveur proxy est souvent utilisé pour améliorer la sécurité et les performances du réseau, ainsi que pour contourner les restrictions d'accès à certains sites Web.

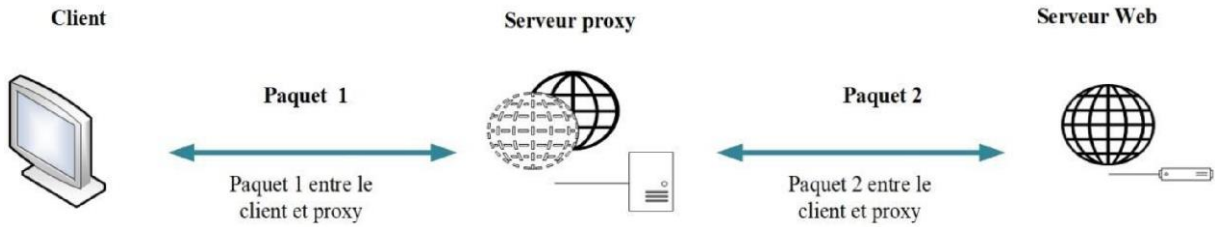


Figure 1-4 Proxy

2. VLANs

Sont des réseaux locaux virtuels qui permettent de regrouper des ordinateurs et des périphériques réseau en fonction de leur appartenance à un même groupe logique, indépendamment de leur position physique dans le réseau. Cette segmentation logique permet de limiter l'accès aux ressources réseau aux seuls utilisateurs et périphériques autorisés, et d'isoler les différentes parties du réseau les unes des autres pour empêcher la propagation des attaques. Les VLANs sont souvent utilisés pour améliorer la sécurité et la gestion du réseau dans les grandes entreprises et les environnements à haute densité de trafic réseau.

3.VPN (Virtual Private Network)

Le VPN permet de sécuriser les échanges de données entre deux ordinateurs à distance en établissant une connexion privée et cryptée, souvent via Internet. Cette technique de chiffrement permet de garantir la confidentialité et la sécurité des données échangées. En utilisant un VPN, les entreprises peuvent protéger leurs données sensibles contre les intrusions et les attaques malveillantes.

IDS (Intrusion Detection System)

Un système de détection d'intrusion qui surveille le réseau ou les systèmes informatiques pour détecter tout comportement suspect ou nuisible. L'objectif des systèmes de détection d'intrusion (IDS) est de détecter les tentatives d'attaque, les virus, les logiciels malveillants et autres menaces susceptibles de compromettre la sécurité du système. Il fonctionne en surveillant les activités du réseau ou du système informatique. Pour détecter les menaces, les IDS peuvent utiliser des signatures, des comportements ou des anomalies. [2][3]

1.Types d'IDS

- **IDS à base de signature**

Pour identifier les menaces, un IDS consulte une base de données de signatures reconnues. Les signatures sont des modèles distinctifs associés à des attaques reconnues. L'IDS génère une alerte lorsqu'un paquet correspond à une signature.

- **IDS basé sur les comportements**

Sont des systèmes de détection d'intrusion qui utilisent des modèles comportementaux pour détecter les activités absurdes du réseau ou du système. Ils collectent des données sur l'activité du réseau ou du système, puis les analysent pour trouver des modèles de comportement inhabituels.

- **IDS basé sur les anomalies**

Les systèmes de détection d'intrusion basés sur les anomalies détectent les comportements anormaux ou non autorisés d'un réseau ou d'un système en surveillant le trafic réseau ou le comportement du système pour détecter les actions qui ne correspondent pas au comportement autorisé ou attendu.

- **IDS hybride**

Ce système de détection des intrusions détecte les menaces à l'aide de signatures et de comportements. Il peut identifier des attaques connues à l'aide de signatures, mais il peut également détecter des attaques inattendues à l'aide de comportements.

IPS (Intrusion Prevention System)

Un système de prévention des intrusions (IPS) détecte et bloque les attaques sur un réseau ou un système informatique. Contrairement à l'IDS, qui se concentre sur l'identification des attaques, l'IPS prévient les menaces en temps réel. Pour identifier les menaces, l'IPS peut utiliser les mêmes techniques que l'IDS, telles que les signatures, les comportements et les anomalies. Lorsqu'une menace est découverte, les systèmes de prévention des intrusions (IPS) peuvent soit restreindre la communication avec la source de l'attaque, soit appliquer des règles de sécurité pour empêcher l'attaque de réussir. [2][3]

1.Types d'IPS

- **IPS à base de signature**

Pour détecter les attaques, cet IPS utilise une base de données de signatures reconnues. Les signatures sont des modèles uniques associés à des attaques reconnues. Lorsqu'un paquet correspond à une signature, l'IPS génère une alerte et interrompt le trafic.

- **IPS basé sur les comportements**

Cet IPS surveille l'activité typique du réseau ou du système informatique et utilise ces données pour détecter les activités anormales ou malveillantes. Certaines activités, telles que la création de comptes d'utilisateurs ou l'accès à des informations sensibles, peuvent être bloquées par l'IPS.

- **IPS basé sur les anomalies**

Ce système de prévention des intrusions (IPS) surveille le réseau ou les systèmes informatiques pour détecter tout comportement inhabituel. Il peut être configuré pour bloquer le trafic lorsqu'il détecte une augmentation du trafic, une utilisation inhabituelle de la bande passante ou toute autre action qui s'écarte du modèle de comportement attendu.

- **IPS hybride**

Pour détecter les menaces, cet IPS utilise à la fois des signatures et des comportements. Il peut détecter les attaques connues à l'aide de signatures, mais aussi les nouvelles attaques à l'aide de comportements. À l'aide de règles de sécurité, l'IPS hybride peut détecter et bloquer les menaces en temps réel.

Pare-feu

Définition

Un pare-feu est un système de sécurité réseau conçu pour surveiller et contrôler le trafic entrant et sortant d'un réseau. Son objectif principal est d'agir comme une barrière entre un réseau interne de confiance et un réseau externe non fiable. En inspectant le trafic réseau et en appliquant des règles de sécurité, un pare-feu peut contribuer à empêcher l'accès non autorisé au réseau, à protéger contre les logiciels malveillants et à garantir la confidentialité et l'intégrité des communications réseau. [4]

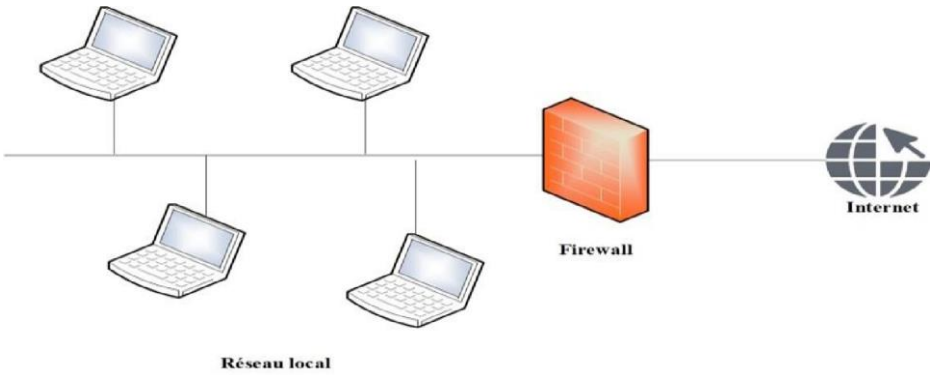


Figure 1-5 Pare-feu.

- **Rôle d'un pare-feu**

Le rôle principal d'un pare-feu est de protéger un réseau informatique en filtrant le trafic entrant et sortant et en mettant en œuvre un ensemble de règles de sécurité pour empêcher les connexions illégales. Un pare-feu joue plusieurs rôles importants, notamment : [5]

- **Définir une zone de sécurité**

  Un pare-feu crée une zone sécurisée au sein du réseau qui protège contre les dangers extérieurs tels que les attaques de pirates informatiques.

- **Contrôle d'accès**

  Un pare-feu peut être configuré pour restreindre l'accès en fonction des adresses IP ou des ports, ou pour refuser l'accès à certaines ressources ou à certains services du réseau.

- **Identifier et bloquer les menaces**

  Un pare-feu est capable de détecter et de prévenir les tentatives d'intrusion, les virus et les logiciels malveillants avant qu'ils n'atteignent le réseau.

- **Surveiller l'activité du réseau**

Un pare-feu peut être configuré pour enregistrer les événements et les activités du réseau, ce qui permet ensuite de détecter les comportements suspects et d'identifier les emplacements du réseau qui posent des problèmes de sécurité.

- **Améliorer la confidentialité**

  Un pare-feu peut être utilisé pour empêcher l'accès non autorisé aux données sensibles du réseau ou pour crypter les données en vue d'une transmission plus sûre.

2.Types de pare-feu

a. Pare-feu de proxy

Ce type de pare-feu agit comme un intermédiaire entre les clients et les serveurs en filtrant les données entrantes et sortantes du réseau. Il permet de renforcer la sécurité tout en ralentissant le trafic**.**

b. Pare-feu d'application

Ce type de pare-feu évalue les données de la couche d'application et utilise des règles spécialisées pour empêcher les attaques sur les faiblesses connues.

c. Pare-feu personnel

Ce type de pare-feu est destiné à empêcher les dangers extérieurs d'atteindre les ordinateurs individuels et les réseaux domestiques. Il peut être monté sur un PC ou un routeur.

d. Pare-feu de réseau

Il s'agit d'un pare-feu installé sur un dispositif réseau, tel qu'un routeur ou un commutateur, afin de protéger l'ensemble du réseau. Le pare-feu réseau est généralement configuré pour restreindre le trafic entrant illégal tout en autorisant le trafic sortant.

e. Pare-feu de Cloud

Ce type de pare-feu est hébergé dans le Cloud et protège les programmes et les données qui y sont stockés.

3.NGFW (Next-Generation Firewall)

Pare-feu de nouvelle génération en français. Il s'agit d'une évolution des pare-feu traditionnels qui offre des fonctionnalités de sécurité supplémentaires et plus avancées. [4] Quelques-unes des caractéristiques des NGFW :

- **Inspection approfondie des paquets**

Les NGFW peuvent analyser le trafic réseau à l'aide de techniques telles que l'inspection de la couche d'application, l'inspection SSL/TLS et la prévention des intrusions (IPS).

- **Filtrage basé sur les applications**

Les NGFW peuvent détecter et bloquer le trafic réseau en fonction de l'application ou du service qui le génère.

- **Contrôle d'accès avancé**

Les NGFW offrent des fonctionnalités de contrôle d'accès telles que la segmentation du réseau et la gestion des politiques d'accès.

- **Fonctionnalités de gestion des menaces**

Les NGFW sont dotés de fonctions avancées de gestion des menaces, telles que la détection des logiciels malveillants et la sécurité des réseaux de zombies.

- **Intégration de la sécurité avancée**

Les NGFW sont souvent équipés de fonctions de sécurité supplémentaires telles que des services VPN, des services de gestion de l'identité et de l'accès, ainsi que des capacités de gestion des événements et des informations de sécurité.

1.11 Sécurité des systèmes d'exploitation

1.11.1 Sécurité des systèmes Windows

Windows est le système d'exploitation le plus utilisé dans le monde avec une statistique de 75% des ordinateurs utilise Windows comme un système principal. Dans le but de protéger les utilisateurs contre les menaces en ligne et hors ligne, Windows a été conçu avec un ensemble de fonctionnalités de sécurité intégrées. Cette présentation se concentrera sur certains des aspects clés de la sécurité des systèmes Windows. [7]

- **Couches de sécurité dans Windows**

- **Première couche**

  Elle est constituée d'un pare-feu intégré. Ce pare-feu permet d'empêcher les accès non autorisés au système et peut être personnalisé pour n'autoriser que les connexions entrantes et sortantes spécifiques, ce qui permet de prévenir les attaques de logiciels malveillants et autres menaces.

- **Deuxième couche**

  Elle est constituée d'un système de protection antivirus. Les programmes antivirus ont pour objectif de repérer et supprimer les logiciels malveillants, y compris les virus, les chevaux de Troie et les logiciels espions. Il est crucial de choisir une solution antivirus de confiance parmi les nombreuses options proposées par les différents fournisseurs.

- **Troisième couche**

Elle est présentée par la sécurité des comptes des utilisateurs, en créant des comptes d'utilisateurs avec des mots de passe solides et en limitant les privilèges d'accès, nous pouvons réduire le risque d'accès non autorisé à votre système.

- **Quatrième couche**

  Elle occupe la sécurité des mises à jour. Pour maintenir la sécurité des systèmes et les protéger contre les dernières menaces, il est important de mettre à jour régulièrement le système d'exploitation et les programmes. Les mises à jour de sécurité régulières corrigent les vulnérabilités du système et garantissent sa protection.

1.11.2 Sécurité des systèmes UNIX/LINUX

UNIX/LINUX sont des systèmes d'exploitation open source développés dans les années 1960 pour les grands ordinateurs. Ils ont subi une évolution majeure pour devenir très populaires et largement utilisés de nos jours. Ce sont des systèmes modulaires, ce qui signifie que les utilisateurs peuvent personnaliser le système en ajoutant ou en supprimant des composants selon leurs besoins. Les systèmes UNIX/LINUX sont très sécurisés grâce à leur architecture de sécurité en couches qui offre une protection contre des menaces spécifiques. Cette architecture inclut des pare-feu, des contrôles d'accès, des mécanismes de chiffrement et d'autres fonctionnalités de sécurité.

Les systèmes UNIX/LINUX sont très personnalisables pour répondre aux besoins de sécurité spécifiques d'une entreprise ou d'une organisation. Les administrateurs peuvent ajuster les fonctionnalités, ajouter des modules de sécurité et appliquer des politiques de sécurité strictes. [6]

1.12 Conclusion

Au terme de ce chapitre, nous avons pu acquérir une compréhension générale des réseaux informatiques. Nous avons également abordé la sécurité informatique, en identifiant les attaques et les vulnérabilités auxquelles les systèmes informatiques sont exposés, ainsi que les mesures de sécurité essentielles pour protéger ces systèmes. Donc ce chapitre a posé les bases nécessaires pour comprendre l'importance et les enjeux liés aux systèmes informatiques et à leur sécurité. Dans le chapitre suivant on va entamer la présentation d'organisme d'accueille ainsi que la problématique de ce projet d'étude.

Chapitre 2

Présentation de l'organisme d'accueil

2.1 Introduction

Ce chapitre sera réservé à la présentation du campus NTS (New Technology § Solutions) où nous effectuerons 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'architecture réseau de cette entreprise et ses composantes afin de pouvoir suggérer d'éventuelles améliorations.

Partie 1 : Présentations de l'entreprise « Campus NTS »

2.2 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 ouzemour, 17 octobre...etc).
- SARL Alphas Bejaïa.
- Providentia Béjaïa.

2.3 Localisation de l'entreprise

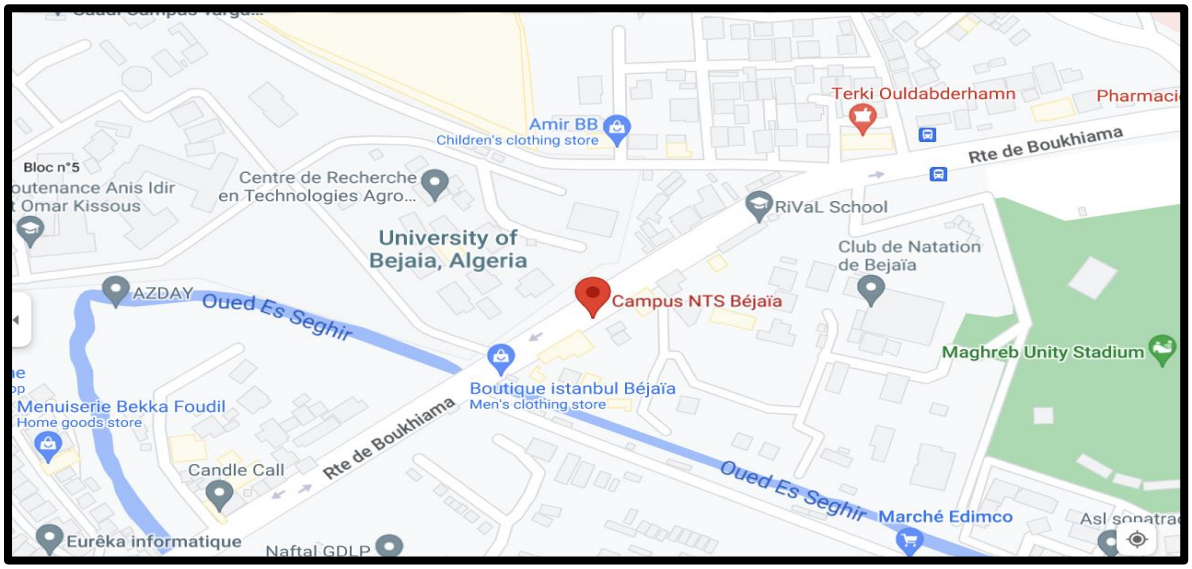


Figure 2-1 Localisation de l'entreprise NTS

2.4 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.

Dénomination	**Campus NTS**
Logo	
Siège	Bâtiment A les beaux quartiers Targa Ouzemour, Béjaïa 06000
Secteurs d'activités	Informatique et télécommunication
Numéros de FAX	044 204 400
Numéros de Téléphone	0770446101
Email	contact@campus-nts.com
Site Internet	http://www.campus-nts.com/

Tableau 2-1 Identification sur campus NTS

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

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

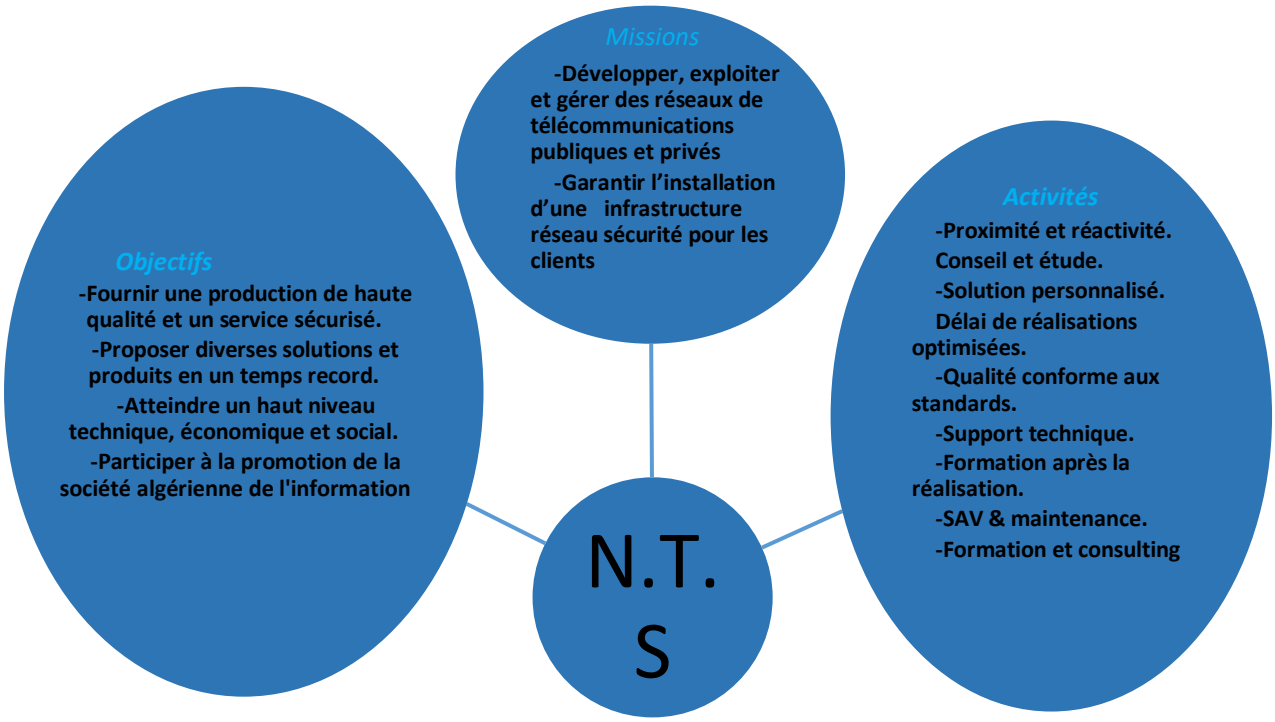


Figure 2-2 Objectifs, Missions et Activités de l'NTS.

2.6 Organigramme général de l'organisme d'accueil

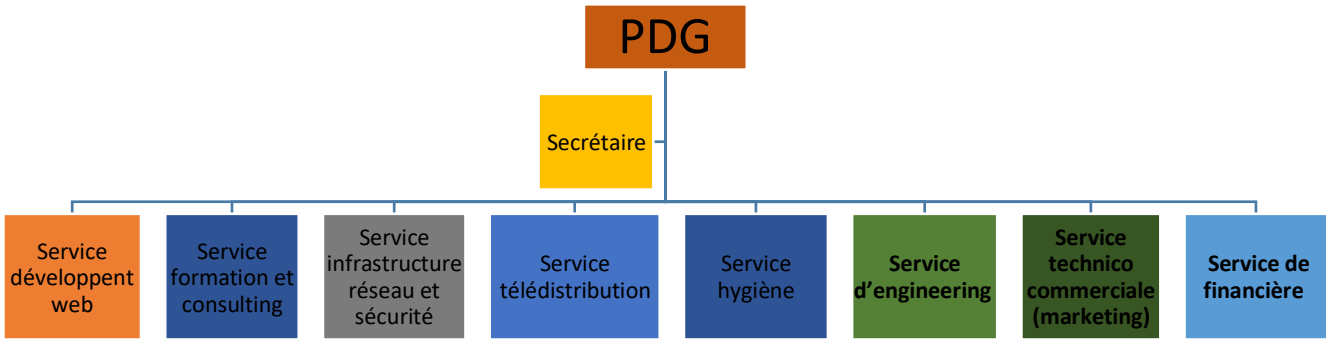


Figure 2-3 L'organigramme de campus NTS.

Nous allons nous contenter de présenter ci- dessous la description de l'organigramme du campus NTS (voir la figure 3) dans lequel cet apprentissage terminé 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 professionnels.
- Installation et configuration des caméras de surveillance analogique et numérique.
- Fibre optique : les réseaux d'accès FTTH/FTTX.
- Création de sites web.
- Programmation (C, C++, C#, Java, Python…etc.).
- Électricité Bâtiments et industriels.
- Formation Cisco CCNA, CCNP S&R.
- Virtualisation.
- Microsoft server, SQL.
- Cybersécurité.

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.

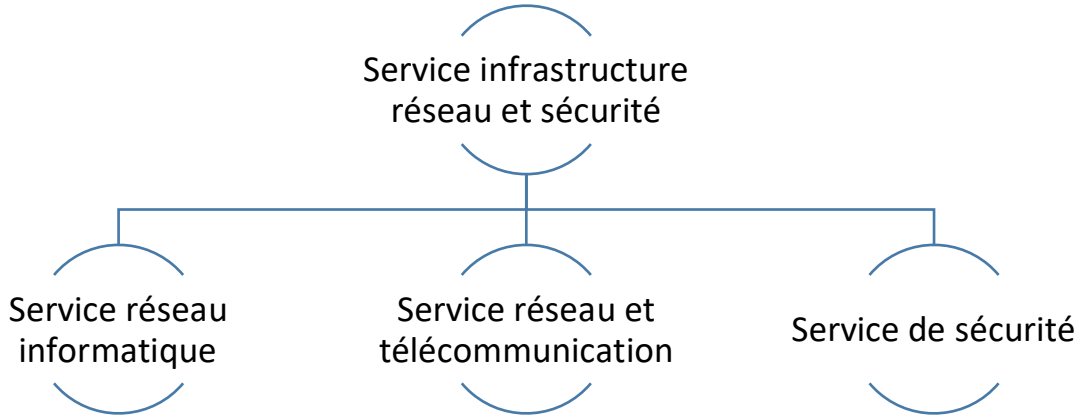


Figure 2-4 organigramme de service d'accueil

➢ **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'autres 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 collectives, 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 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 le suivi des budgets de fonctionnement et d'investissement.
- La préparation des états financiers.
- La gestion de la trésorerie et 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 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.

Partie 2 : Etat des lieux

2.7 Présentation du réseau campus NTS

L'entreprise a une architecture en couches et, pour assurer la communication entre ses différents services, elle connecte un LAN à une connexion FTTH fournie par un fournisseur d'accès Internet. Le schéma ci-dessous nous montre l'infrastructure du réseau NTS :

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

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

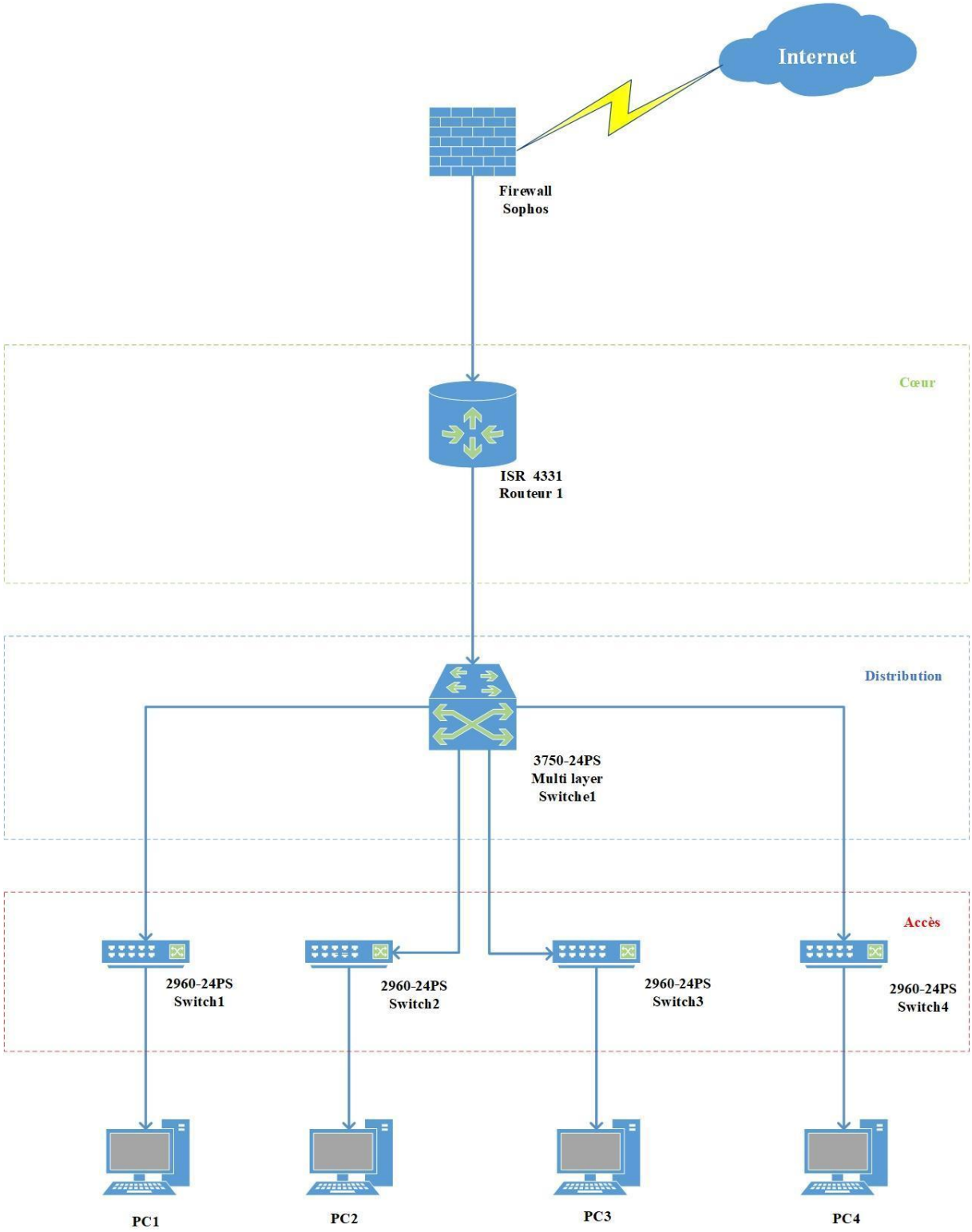


Figure 2-5 Architecture de réseau (NTS)

Partie 3 : Problématiques et Solutions proposées

2.8 Problématique

La sécurité informatique est devenue une préoccupation majeure pour les entreprises de toutes tailles et de tous secteurs. Dans ce contexte, notre mémoire de fin d'étude se concentre sur l'étude des problèmes de sécurité rencontrés par les clients de l'entreprise Campus NTS, Bejaia. Au cours de notre stage pratique au sein de cette entreprise, nous avons réalisé une recherche afin d'identifier les manques existants et les défis auxquels les clients sont confrontés en matière de sécurité informatique.

Au cours de notre étude, nous avons constaté que la majorité des clients de Campus NTS utilisent des méthodes et des concepts de sécurité similaires. Ces approches reposent principalement sur des technologies de sécurité traditionnelles telles que les pare-feu, les systèmes de prévention d'intrusion (IPS), les systèmes de détection d'intrusion (IDS), etc. Cependant nous avons identifié diverses limites associées à ces technologies.

Limitations des technologies de sécurité traditionnelles :

- Délais de réponse lents : Ces délais peuvent permettre aux attaquants de causer des dommages importants avant que des mesures de protection ne soient mises en place.
- Détection insuffisante des menaces : Les attaquants utilisent souvent des techniques avancées pour contourner les systèmes de sécurité traditionnels, rendant leur détection difficile voire impossible.
- Capacité limitée à gérer les incidents de sécurité : Cela peut rendre la résolution des problèmes plus complexe et augmenter le temps de récupération après une cyberattaque.

Solution

Solution envisagée pour renforcer la sécurité informatique des clients de Campus NTS, est la mise en place d'un Centre d'Opération de Sécurité (SOC).

Cette solution se résume en 4 partie :

- Implémentation d'une solution SIEM pour la surveillance en temps réel.
- Effectuer la génération, la collecte et l'analyse de journaux d'événements (logs).
- Création de visions d'événements personnalisées et sophistiquées.

- Intervention contre les menaces.

2.9 Conclusion

Ce chapitre est consacré à la présentation de l'entreprise campus NTS ainsi que les problèmes de sécurité de ces clients, afin de trouver des solutions efficaces pour eux. On a proposé notre solution dans le but de satisfaire leur besoin de sécurité. Dans le prochain chapitre, nous aborderons les éléments essentiels de notre solution.

Chapitre 3

Gestion des logs ,intégration du SIEM et présentation d'un SOC

3.1 Introduction

La sécurité informatique est devenue une priorité pour les entreprises dans le monde numérique d'aujourd'hui. Les menaces sont de plus en plus sophistiquées, ce qui rend la surveillance et la réponse aux incidents plus importantes que jamais. Les logs, les SIEM et le SOC sont des outils clés utilisés pour assurer la sécurité des entreprises. Dans ce chapitre, nous allons explorer l'utilisation de ces outils.

3.2 Fichiers journaux

3.2.1 Définition

Les fichiers journaux appelé aussi Log sont des fichiers qui permettent de stocker un historique des événements survenus sur un ordinateur, serveur ou une application. Contient généralement les informations suivantes :

- Les connexions d'utilisateurs
- Événement survenu
- Date et l'heure de l'événement
- Un identifiant (généralement une adresse IP)

Ces fichiers sont utilisés par des logiciels permettent la surveillance des activités des réseaux et systèmes d'informations.

3.2.2 Types des logs

- **Logs web serveur**

Les applications Web comme Apache et NGINX produisent des fichiers journaux de serveur Web qui fournissent une vue non filtrée du trafic du site Web. Les journaux Web enregistrent des détails tels que "qui" a visité votre site Web (adresse IP) et "quelles" pages ont été consultées (URL). En outre, vous pouvez repérer les pièges à araignées, les spams déposés par les pirates, les liens externes cassés, les mauvaises réponses du serveur et les tentatives d'exploitation.

- **Logs réseau**

En fonction de leur activité sur le réseau, les commutateurs, les routeurs, les pare-feu, les concentrateurs VPN et autres dispositifs connectés fournissent divers journaux. Les tentatives non autorisées d'exécution de processus ou d'accès à des données verrouillées peuvent être trouvées, les tentatives de connexion d'utilisateurs ayant échoué peuvent être enregistrées, et bien plus encore dans un journal de réseau.

- **Logs applicatifs**

Les enregistrements des actions consignées par les applications logicielles sont stockés dans les fichiers journaux des applications. Vous pouvez les utiliser pour le dépannage, le diagnostic et l'audit. Ils vous fournissent une multitude d'informations sur les performances d'une application, telles que les avertissements relatifs à l'espace disque, les opérations terminées, les problèmes qui empêchent le démarrage de l'application, l'audit des connexions réussies et l'audit des échecs de connexion.

- **Logs systèmes**

Les fichiers journaux du système, également appelés "journaux du serveur", contiennent des informations complètes sur le système d'exploitation, le système de fichiers, les programmes en cours d'exécution et les identifiants de connexion. Ils permettent aux administrateurs de vérifier la présence de problèmes tels que des erreurs système, des avertissements, des messages de démarrage, des modifications du système, des arrêts inattendus, etc. pour voir si les processus système se chargent correctement ou s'il y a des problèmes.

- **Logs de base de données**

Les logs de base de données (ou logs de transactions) sont des enregistrements détaillés de toutes les opérations effectuées sur une base de données. Les logs de base de données contiennent généralement des informations telles que :

-L'heure et la date de l'opération

-L'utilisateur ou l'application qui a effectué l'opération

-Le type d'opération effectuée (INSERT, UPDATE, DELETE, SELECT, etc.)

- **Logs de trafic http(s)**

Les logs du trafic http(s) sont des enregistrements de toutes les transactions HTTP effectuées entre un client (tel qu'un navigateur web) et un serveur web. Ces logs contiennent des informations détaillées sur chaque transaction. Telles que :

-L'adresse IP du client et du serveur

-La date et l'heure de la transaction

-La méthode HTTP utilisée (GET, POST, etc.)

- **Logs de sécurité**

De nombreux périphériques conservent des informations de journal de sécurité qui vous permettent de voir les types de trafic réseau qui sont autorisés ou non sur votre réseau. Par exemple, les journaux d'audit et les contrôles d'accès peuvent être utilisés pour trouver les utilisateurs suspects qui abusent de leurs droits d'accès et peut-être arrêter une attaque potentielle par force brute.

Les fichiers journaux d'authentification qui enregistrent les tentatives d'accès des utilisateurs à une ressource du réseau en sont une autre illustration. Ce faisant, les problèmes d'accès sont corrigés et les règles d'authentification sont modifiées. Les événements de sécurité de haut niveau sont également enregistrés à des fins d'audit.

3.2.3 Format d'un log

Le format d'un log peut varier selon le type de système, d'application ou de service qui le génère. Cependant, la plupart des logs suivent un format standard qui inclut les informations suivantes :

Timestamp (horodatage) : la date et l'heure à laquelle l'événement a été enregistré.

Source : l'adresse IP ou le nom d'hôte de la source de l'événement.

Destination : l'adresse IP ou le nom d'hôte de la destination de l'événement.

Type d'événement : une description de l'événement qui s'est produit, généralement sous la forme d'un code ou d'un libellé.

Sévérité : le niveau de gravité de l'événement, généralement indiqué par un code numérique ou un libellé.

Exemples d'un format d'un log :

```
Jun 14 21:59:06 10.10.1.1 date=2023-06-14 time=13:59:05 devname="FortiGate0
1" devid="FGVMEVWZSKGMY_BF" eventtime=1686776344812287391 tz="-0700" logid
="0001000014" type="traffic" subtype="local" level="notice" vd="root" srcip=
127.0.0.1 srcport=21712 srcintf="root" srcintfrole="undefined" dstip=127.0.
0.1 dstport=9980 dstintf="root" dstintfrole="undefined" srccountry="Reserve
d" dstcountry="Reserved" sessionid=734 proto=6 action="close" policyid=0 ser
vice="tcp/9980" trandisp="noop" app="tcp/9980" duration=1 sentbyte=1349 rcvd
byte=1079 sentpkt=5 rcvdpkt=5 appcat="unscanned"
host = 10.10.1.1 | source = fortigate | sourcetype = fortigate_traffic
```

FIGURE 12 : Exemple d'un log

3.2.3.1 Explication des champs

Ce journal d'événement (log) est généré par un pare-feu FortiGate. Il enregistre un événement de trafic réseau avec les informations suivantes :

- Jun 14 21:59:06 : Date et heure de la récupération de l'événement, qui est le 14 juin à 21h59m06s.
- 10.10.1.1 : Adresse IP de l'hôte ou de l'interface concernée par l'événement.
- date=2023-06-14 : Date de l'événement, qui est le 14 juin 2023.
- time=13:59:05 : Heure de l'événement, qui est 13h59m05s.
- devname="FortiGate01" : Nom du périphérique FortiGate, qui est "FortiGate01".
- devid="FGVMEVWZSKGMY_BF" : Identifiant unique du périphérique.
- logid="0001000014" : Identifiant du journal (log) spécifique.
- type="traffic" : Type d'événement, qui est lié au trafic réseau.
- level="notice" : Niveau de gravité de l'événement, qui est "notice" indiquant une information.
- vd="root" : Nom de la partition virtuelle du périphérique, qui est "root".
- srcip=127.0.0.1 : Adresse IP source du trafic, qui est 127.0.0.1 (localhost).
- srcport=21712 : Numéro de port source du trafic, qui est 21712.
- dstip=127.0.0.1 : Adresse IP de destination du trafic, qui est 127.0.0.1 (localhost).
- dstport=9980 : Numéro de port de destination du trafic, qui est 9980.
- srccountry="Reserved" : Pays d'origine du trafic, qui est "Reserved" (réservé).
- dstcountry="Reserved" : Pays de destination du trafic, qui est "Reserved" (réservé).
- sessionid=734 : Identifiant de session pour le trafic.
- proto=6 : Protocole utilisé pour le trafic, qui est le protocole TCP (6).
- action="close"` : Action prise sur le trafic, qui est "close" (fermé).

3.2.4 Serveur/Client log

Les fichiers journaux sont généralement utilisés dans les environnements de serveur/client pour surveiller l'activité de l'infrastructure informatique d'une organisation et pour enregistrer les événements qui se produisent sur les serveurs et les clients.

Dans les environnements serveur, les logs servent à suivre les connexions entrantes et sortantes, les activités des utilisateurs, les erreurs système, etc. En outre, les fichiers journaux

peuvent être utilisés pour surveiller les activités des utilisateurs sur un système informatique et repérer tout comportement anormal ou mauvais. Ils peuvent être utilisés pour repérer des comportements potentiellement dangereux ou négatifs.

Dans les environnements client, les logs peuvent être utilisés pour surveiller et enregistrer les erreurs système, les activités des applications, etc. En outre, les fichiers journaux peuvent être utilisés par les administrateurs pour diagnostiquer les problèmes de performance et de sécurité, ainsi que par les utilisateurs pour résoudre les difficultés qu'ils peuvent rencontrer.

3.2.5 Intérêt d'utiliser les fichiers journaux

- Suivre les différents comportements des utilisateurs, dans le cas d'un site web, le serveur peut garder la trace des temps de connexion, de l'emplacement de l'utilisateur et des pages qu'il a visitées.
- L'expérience de l'utilisateur peut être améliorée en analysant les données analytiques du site web, comme les visites de pages et le temps passé sur une page.
- Identifier et anticiper les fraudes à venir, notamment dans le secteur bancaire ou en e-commerce grâce au traçage des données.
- Utiliser le suivi des données pour identifier et prévoir les fraudes, notamment dans les secteurs de la banque ou du E-commerce.
- La surveillance des Logs permettra aux administrateurs et aux équipes de sécurité au sein d'une organisation de recevoir des notifications lorsque le serveur est hors service.
- Les administrateurs système peuvent identifier les causes profondes des défaillances et des pannes du système en utilisant les fichiers journaux pour résoudre les problèmes.
- Les fichiers journaux peuvent contribuer à détecter les activités malveillantes et les tentatives d'intrusion au sein d'une organisation ou une entreprise en surveillant les activités de l'infrastructure par l'enregistrement des tentatives de connexion, les modifications des fichiers, etc.

Les fichiers journaux peuvent être utilisés pour découvrir les goulets d'étranglement et optimiser les configurations afin d'analyser les performances des systèmes informatiques

3.3 SIEM (Security Information and Event Management)

3.3.1Définition du SIEM

SIEM (Security informations and Event Management) est une solution permet la gestion des informations(SIM) et la gestion des événements de sécurité(SEM) au sein d'une entreprise. Il offre une surveillance totale du réseau et traite un grand volume de données, détecter et signaler les comportements inhabituels en un temps fini. le SIEM offre une vision globale de la posture de sécurité de l'organisation et permet aux organisations de réagir rapidement aux menaces détectées à l'aide des alertes générer lorsqu'il identifié des problèmes essentiels. [11] [12]

Figure 3-1 fonctionnement du SIEM [26]

3.3.2 Fonctionnement des SIEMs

Les outils SIEM collectent les logs et les données des événements générés par les applications, les équipements et les systèmes hôtes des organisations. Ils rassemblent toutes les informations nécessaires et les classent dans des catégories ce qui permet aux équipes de sécurité de détecter et bloquer les attaques entrantes.

- **Agrégation des logs** : le processus de rassembler plusieurs logs qui ont le même type dans un seul log à l'aide des critères définis. Cette fonctionnalité permet de réduire le nombre des logs et les événements dans le SIEM, la capacité d'accélération des recherches et facilite les tâches de surveillance dans les organisations. L'agrégation présente un inconvénient qui est la mauvaise adaptation des règles d'agrégation qui peut causer la perte des informations importantes.

- **Corrélation** : la corrélation utilise des critères définis par les règles de corrélation pour analyser les événements détectés par le SIEM. L'objectif de cette fonctionnalité est d'implémenter des liens entre événements, et de créer des alertes de corrélation, des rapports d'activités. La corrélation varie de plusieurs manières :

- **Auto-apprentissage et connaissances rapportées :**Les moteurs de corrélation exigent des informations sur les réseaux et les systèmes de l'infrastructure qui vont permettre le bon fonctionnement de cette fonctionnalité. Les informations de moteurs de corrélation sont collectées automatiquement ou manuellement
- **Temps réel et données retardées :** Dans certains cas, les événements bruts forgés sont envoyés directement pour une corrélation en temps réel. Dans d'autres situations, les événements sont d'abord stockés, puis envoyés après un traitement initial. Ensuite, leur envoi peut être ajusté.

  Corrélation active et passive :

  - **Active** : a la capacité d'améliorer les événements reçus en recueillant des informations supplémentaires pour prendre des décisions.
  - **Passive** : une corrélation qui ne peut pas interagir avec son environnement.
- **Les rapports :** possèdent un résumé des alertes générées et exemple de la sécurité du système à l'instant T.
- **Tableaux de bord** : les données liées aux événements sont traitées par le SIEM afin de les transforment en graphe informatifs pour permettre aux équipes de sécurité voire les activités qui sont pas habituelles.
- **Alertes :** le SIEM offre une analyse de corrélation automatique des événements et de créer des alertes pour notifier les destinataires des problèmes urgents.

3.3.3 Rôle de SIEM dans les entreprises

Aujourd'hui les organisations continuent à s'augmenter, d'être complexes et difficiles à gérer. L'infrastructure informatique est souvent divisée en plusieurs équipes, telles que l'équipe des serveurs, l'équipe des ordinateurs de bureau, le centre d'opérations réseau et le centre d'opérations de sécurité. Une solution SIEM offre aux équipes de sécurité dans les organisations et entreprises de rassembler et d'analyser les données à l'échelle de toute l'entreprise, ce qui favorise une coopération efficace entre les équipes dans les très grandes organisations.

3.3.4 Comparaison entre le SIM, SEM & SIEM

- **SIEM :** il est composé de deux concepts qui sont : SEM (gestion des événements de sécurité) et le SIM (gestion des informations de sécurité). Ils combinent ces deux concepts pour bien surveiller l'infrastructure informatique et pour un rendement maximisé.
- **SEM :** Il a la mission de s'assurer la surveillance de la sécurité, la corrélation des événements et la réponse aux incidents, il analyse en temps réel les données des journaux et des événements provenant des systèmes et des applications des dispositifs de le composent qui a la mission de traiter les données et celle des événements des dispositifs de sécurité.
- **SIM :** Il offre la sécurité, les dispositifs de réseau, la gestion des journaux, la collecte de données, la création de rapports et l'analyse à partir des systèmes et applications hôtes. Il facilite l'établissement de rapports sur la conformité réglementaire, la gestion des menaces internes et la surveillance de l'accès aux ressources. SIM gère les tâches de surveillance des utilisateurs privilégiés et de l'accès aux ressources, ainsi que les exigences de rapports des organismes d'audit interne et de conformité.

Dans le tableau le suivant nous avons fait une comparaison entre SIEM, SIM et SEM avec des exemples de chaqu'un :

	Gestion des information de sécurité (SIM)	**Gestion des événement de sécurité (SEM)**	**Gestion de l'information et des événements de sécurité (SIEM)**
Aperçu	Collecte et analyse des données relatives à la sécurité à partir des logs.	Analyse, visualisation et réponse aux incidents en temps réel.	SIEM, comme son nom l'indique combine les capacités SIM et SEM
Caractéristique	Facilite le déploiement Capacité de gestion des journaux	Plus complexe à déployer Supérieur dans la surveillance en temps réel.	Plus complexe à déployer/ Fonctionnalité complète
Exemple d'outils	OSSIM ALIEN VAULT OSSIM	Sentinelle NetlQ NetIQ.	SolarWinds solarwinds

Tableau 3-1 Tableau de comparaison SIM, SEM, SIEM

3.3.5 Avantages et inconvénients des SIEMs

SIEM présente et offre plusieurs avantages à tous les types d'organisations. Parmi ces avantages :

- La détection, identification et réponse aux menaces en temps réel.
- Rapports et audits de conformité réglementaire
- La gestion des événements.
- Respecte les obligations de conformité d'une entreprise.
- Fournir une vue d'ensemble du réseau.

En outre, il simplifie la gestion de la sécurité pour les entreprises en gérant facilement et filtrant la quantité massive des données des entreprises et organisations.

Les outils SIEMs facilitent beaucoup le travail des équipes de sécurité au sein des entreprises et organisations, donc ces outils sont indispensables dans les entreprises.

Les SIEM présentent toutefois certains inconvénients, dont les suivants :

- La complexité des configurations dans quelques outils SIEMs.
- Les coûts élevés de déploiement.
- Beaucoup d'alerte à gérer et à surveiller.
- Manque de capacité de détecter les vulnérabilités dans les systèmes.
- Aucune information sur le degré de sensibilité des données.

Les outils SIEM dépendent généralement de règles pour analyser toutes les données enregistrées. Le problème, c'est que le réseau d'une entreprise génère un grand nombre d'alertes généralement 10 000 par jour qui peuvent être positives ou non. Difficile, dans ces conditions, d'identifier les attaques potentielles en raison du nombre de journaux non pertinents. [14]

3.3.6 Solutions SIEM

On trouve plusieurs solutions SIEM proposées dans le marché. Certaines sont payantes comme SPLUNK, IBM QRadar, McAfee, etc. il existe d'autres solutions open source (FREE) comme ELK Stack, OSSIM, Graylog, etc.

Figure3-2 Classement des solutions SIEM en 2022 [12]

Avant de sélectionner la solution optimale pour notre projet, nous allons procéder à une présentation de diverses options.

3.3.6.1 Solutions Open Source

a. **ELK Stack :** ELK (Elasticsearch, Logstash, Kibana) est une plateforme libre et gratuite qui permet aux organisations de collecter, d'analyser et de visualiser les données qui peut être utilisée pour la gestion des événements et des informations de sécurité (SIEM). ELK Stack est composé de trois éléments principaux : Elasticsearch, Logstash et Kibana.

- **Elasticsearch :** est une base de données qui stocke et recherche les données et de sécurité.
- **Logstash :** collecte et analyse les données.
- **Kibana :** fournit une interface utilisateur graphique pour visualiser les données.

b. **OSSIM** : OSSIM (Open Source Security Information Management) développé par AlienVault propose plusieurs caractéristiques comme la surveillance de la sécurité réseau, la détection d'intrusion, la gestion des vulnérabilités, la surveillance des journaux, etc. OSSIM permet de rassembler, analyser et corréler les données de sécurité provenant de divers systèmes de sécurité. [16]

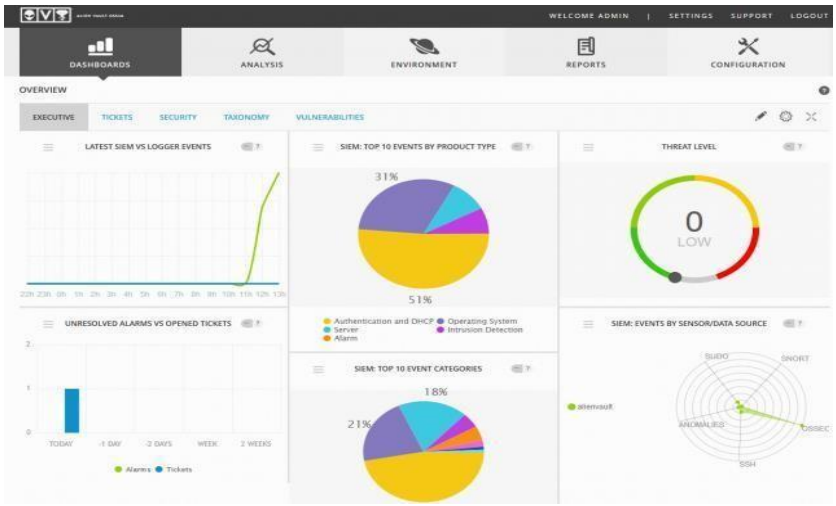


Figure 3-3 OSSIM [16]

f. **Security Onion :** est une solution open source SIEM basée sur Ubuntu Linux a comme objectif d'aider les entreprises à renforcer leur dispositif de sécurité. Security Onion est conçue pour collecter, agréger, analyser et corréler les données de sécurité provenant de différents systèmes de sécurité. [17] [19]

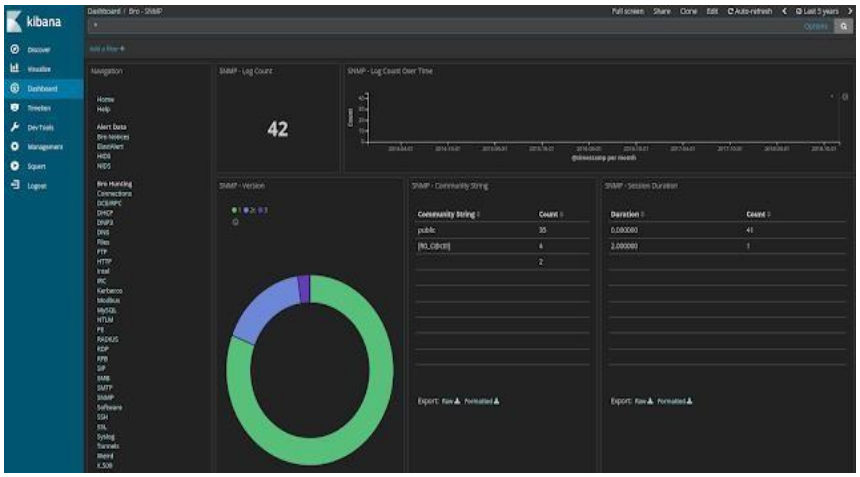


Figure 3-4 Security Onion [17]

3.3.6.2. Solutions payantes

a. Splunk Enterprise Security

Est une solution SIEM très puissantes, permet aux organisations de collecter, d'analyser et de répondre aux événements de sécurité et menaces en temps réels. Cet outil permet de collecter et récupérer des informations de diverses sources comme les

dispositifs réseau, les serveurs etc. ensuite Splunk regroupe toutes les informations dans une seule plateforme et les analysées à l'aide des algorithmes d'apprentissage automatique et d'autres outils d'analyses pour identifier les événements de sécurité tels que les comportements anormaux, les tentatives d'intrusion, et d'autres activités suspectes. La technologie de Splunk fournit des outils de visualisation et de reporting qui permet aux équipes de sécurité au sein d'une organisation de surveiller plus d'avantages la posture de sécurité et d'être capable d'intervenir rapidement en cas de problème. [21]

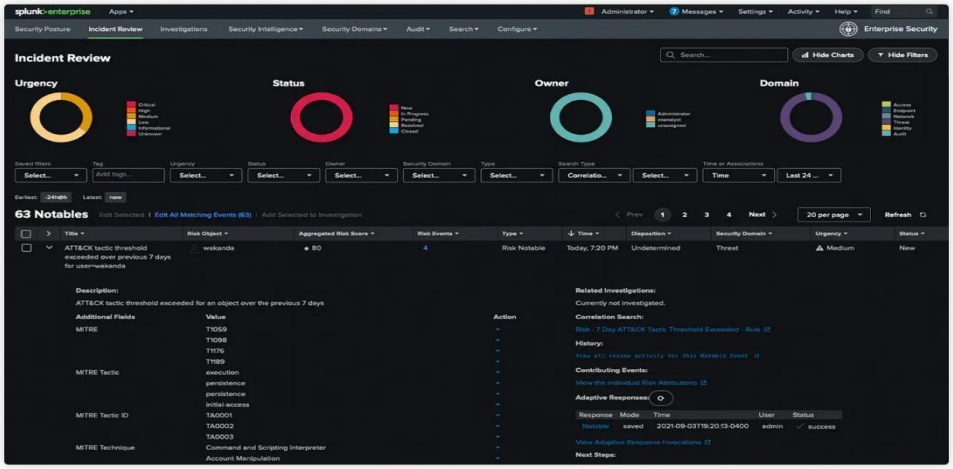


Figure 3-05 Splunk [21]

b. IBM QRadar

Est une solution SIEM permet aux entreprises de surveiller en temps réel et de détecter les menaces de sécurité potentielles. QRadar utilise l'analyse comportementale pour détecter les anomalies et les activités suspectes. Cette solution recueille, organise et stocke toutes les données de sécurité dans un même endroit pour faciliter leur recherche et leur analyse ultérieures. [15]

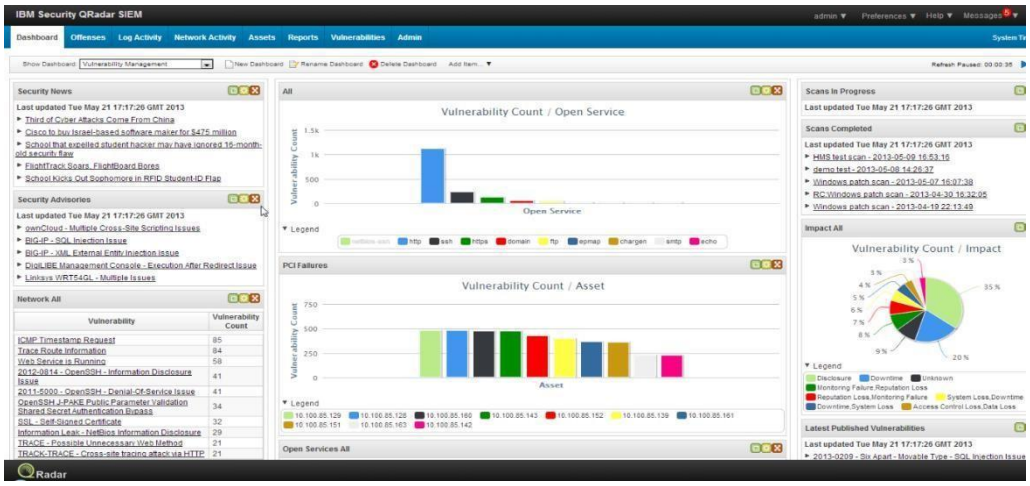


Figure 3-6 IBM QRadar [15]

c. LogRhythm

Est une solution SIEM qui surveille les données de sécurité réseau, les journaux d'événements et les flux de données en utilisant une analyse comportementale pour identifier les activités suspectes et les anomalies qui pourraient indiquer une menace pour la sécurité. La solution permet également de rassembler, d'indexer et de stocker toutes les données de sécurité dans une base de données centrale, ce qui facilite la recherche et l'analyse ultérieures. [20]

Figure 3-7 LogRhythm [20]

d. Microsoft Sentinel

Est une solution SIEM développée par Microsoft qui s'agit d'une plateforme de sécurité basée sur le Cloud. Cette solution de sécurité peut récupérer, étudier et comparer les informations de sécurité en provenance de plusieurs sources, telles que les journaux d'activité, les événements de sécurité et les alertes de sécurité.

e. Rapid7 Insight

Cette solution de sécurité utilise une technique appelée analyse comportementale pour détecter les risques potentiels et donne une vue globale de la sécurité de l'entreprise. Elle possède également une fonctionnalité qui permet de détecter les attaques en temps réel et une interface utilisateur facile à utiliser pour surveiller la sécurité de l'entreprise.

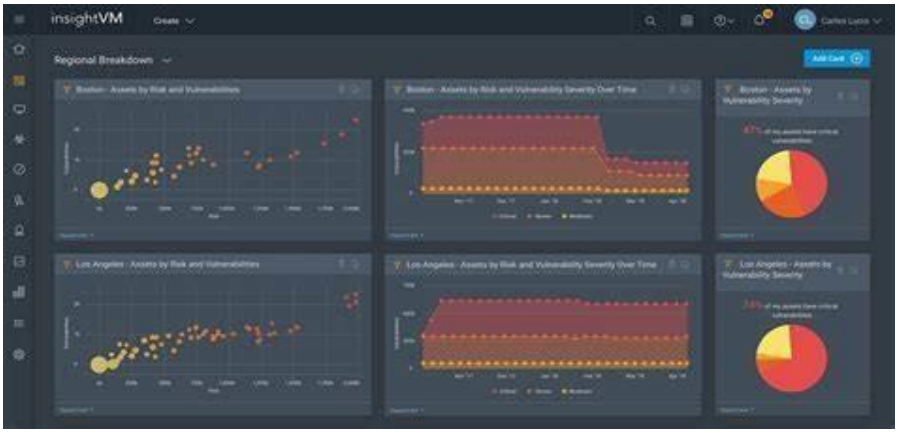


Figure 3-8 Rapid7 Insight [14]

f. FortiSIEM

Est une solution de SIEM proposée par Fortinet. Cette solution est conçue pour rassembler et analyser les données de sécurité qui appartiennent à diverses sources, comme celle des dispositifs réseau, les serveurs, les périphériques terminaux dans l'objectif d'avoir une vue globale de comportement de sécurité d'une organisation. FortiSIEM permet la détection des menaces en temps réel, la génération de rapports de conformité et plusieurs autres avantages.

Figure 3-9 FortiSIEM

3.3.6.3 Schéma de l'ensemble de solution SIEM

Figure 3-10 schéma récapitulatif des solutions

3.3.6.4 Comparaison des solution SIEM

Voici un tableau de comparaison des solutions SIEM :

Solution SIEM	Meilleur pour	Plateforme OS	Déploiement	Caractéristiques principale	Essai gratuit
SolarWinds	Petites, moyennes et grandes entreprises.	Windows, Linux, Mac, Solaris.	Sur site et dans le cloud	-Interface de recherche -Détection des activité suspectes au moment de l'événement	30 jours
Splunk	Petites, moyennes et grandes entreprises.	Windows, Linux, Mac, Solaris.	Sur site et SaaS	-Collecte, indexation et analyse de données massives	Splunk Enterprise : 60 jr Splunk Cloud : 15jr Splunk Light: 30 jr Splunk Free: échantillon gratuit pour la plateforme d'entreprise principale.
Datadog	Petites, moyennes et grandes entreprises.	Windows, Mac, Linux, Debian, Ubuntu, CentOS, RedHat.	Sur site et SaaS.	- Surveillance de la sécurité et des performances	Disponible
IBM QRadar	Grandes entreprises	Linux	Sur site, Cloud	Corrélation d'événements en temps réel	Oui, version limitée
LogRhythm	Moyennes à grandes entreprises	Windows, Linux	Sur site	Gestion complète des opérations de sécurité	Oui, version limitée
Security Onion	Petites à moyennes entreprises	Linux	Sur site	Surveillance réseau et détection d'intrusions	Oui, version limitée

Tableau 3-2 Tableau de comparaison des SIEM

3.3.7 Solution SIEM choisie

Après avoir comparé les différentes solutions SIEM disponibles on a opté pour le Splunk vu les avantages et les caractéristiques qu'il contient, dans ce qui suit nous allons faire une présentation de Splunk.

3.3.7.1 Splunk

Définition

Splunk est un logiciel qui exploite les données informatiques pour les suivre, les analyser et les afficher en temps réel. Il surveille et lit les données stockées sous forme d'événements d'indexation et de plusieurs types de fichiers journaux, ce qui nous permet d'examiner les données sous de nombreuses formes de tableaux de bord. Grâce à une modélisation correcte des données, il examine les données semi-structurées et les journaux créés par de nombreuses activités. Les données sont générées par l'utilisateur au moyen d'applications web, de capteurs ou d'ordinateurs, et il existe des capacités intégrées pour définir les types de données, les séparateurs de champs et l'optimisation du processus de recherche. [26] [25]

Figure 3-11 l'écosystème de Splunk[25]

3.3.7.2 Avantages de Splunk

- Visibilité de l'écran en temps réel.
- Splunk offre une meilleure interface.
- Il permet de gagner du temps en offrant des résultats instantanés.
- C'est le moyen le plus efficace pour déterminer les causes fondamentales des problèmes.
- Splunk permet de générer des graphiques, des avertissements et des tableaux de bord.
- Il nous permet d'améliorer les performances en dépannant toute situation de défaillance.
- Il vous permet de surveiller et de prendre des décisions appropriées concernant tous les paramètres de l'entreprise.
- Splunk permet d'intégrer l'intelligence artificielle dans la stratégie de données.

- Il vous aide à obtenir des informations opérationnelles importantes à partir des données de votre système.
- Splunk nous permet de reconnaître n'importe quel type de données tel que .csv, json, les formats de log, etc.
- Splunk permet également aux clients de rechercher, d'analyser et de visualiser les données.

3.3.7.3 Versions de Splunk

Il existe trois versions essentielles de Splunk « Splunk Enterprise, Splunk Light, Splunk Cloud » [21] [25]

a) Splunk Enterprise

Splunk Enterprise Version est utilisé par les grandes organisations informatiques. L'outil Splunk permet de collecter et d'analyser des données provenant de téléphones mobiles, de sites web et d'applications.

b) Splunk Light

La version gratuite de Splunk Illumination. Elle vous permet d'analyser, d'enregistrer et de modifier vos données de connexion. Elle possède moins de fonctionnalités que les autres versions.

c) Splunk Cloud

Splunk Cloud est le site web d'hébergement. Il offre les mêmes fonctionnalités que la version professionnelle. On peut y accéder en utilisant Splunk ou la plateforme cloud AWS.

3.3.7.4 Caractéristiques de Splunk

a) Collecte de données

Splunk nous permet d'importer ou d'insérer des données à partir d'une variété de types de données, y compris JSON, XML, les weblogs et les journaux d'application, y compris les données système non structurées. Les données non structurées peuvent être modélisées dans une structure de données selon les besoins du client.

b) Indexation des données

Splunk indexe les données ingérées afin d'améliorer les performances de recherche et d'interrogation dans divers scénarios.

c) Recherche de données

Splunk indexe les données ingérées afin d'améliorer les performances de recherche et d'interrogation dans divers scénarios.

d) Utilisation d'alertes

Utilisé pour envoyer des courriels ou des flux RSS lorsqu'une exigence spécifique est trouvée dans les données examinées.

e) Tableaux de bord

Lorsque nous recherchons quelque chose, les résultats sont affichés dans le tableau de bord sous forme de cartes, de rapports, de tableaux croisés dynamiques, etc.

f) Modèle de données

En fonction de l'expertise du domaine, les données indexées peuvent être modélisées en un ou plusieurs ensembles de données. Cela facilite la navigation pour les utilisateurs finaux qui analysent les cas d'affaires sans comprendre les stratégies linguistiques utilisées par Splunk pour traiter les données.

3.3.7.5 Composants de Splunk

- **Indexer**

Les indexeurs Splunk traitent et stockent les données locales et distantes et servent de référentiel de données Splunk principal.

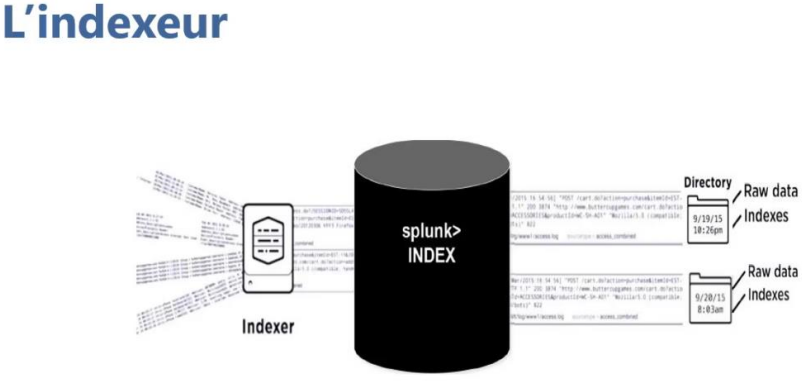


Figure 3-12 Indexeur [25]

- **Search Head**

Search Head est une instance Splunk Enterprise qui distribue les recherches aux indexeurs (appelés dans ce contexte "pairs de recherche"). Selon qu'elles indexent ou non, les têtes de recherche peuvent être dédiées ou non. Outre les index internes standard, les têtes de recherche dédiées n'ont pas d'index propres. Au lieu de cela, elles regroupent et affichent les résultats des pairs de recherche distants. [25]

Figure 3-13 Search Head [25]

- **Forwarder**

Les forwarders sont des instances Splunk qui envoie des données à des indexeurs distants pour traitement et stockage. Dans la plupart des cas, ils n'indexent pas eux-mêmes les données. [25]

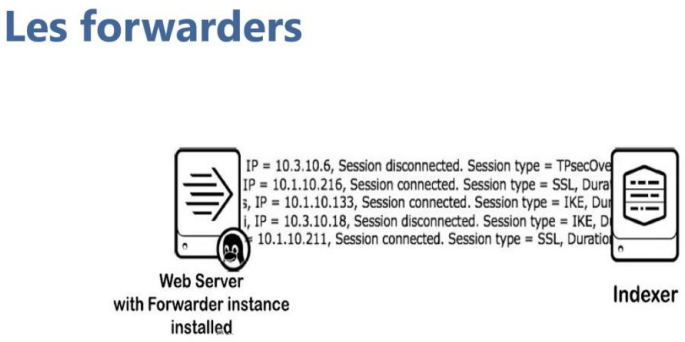


Figure 3-14 Forwarders [25]

3.4 SOC (Security Operations Center)

3.4.1 Définition SOC

Un centre des opérations de sécurité (SOC) est une base de commande pour les professionnels de la sécurité informatique, qui surveille en temps réel l'ensemble de

l'infrastructure d'une entreprise, afin de détecter les événements de cyber sécurité et faire face aussi rapidement et efficacement que possible.

Figure 3-15 Centre d'opération de sécurité [24]

3.4.2 Fonctionnement du SOC :

Le SOC fonctionne à l'aide d'un ensemble d'outils avancés en sécurité informatique et les compétences des professionnels de ce domaine, le SOC remplit les fonctions principales suivantes [22] [24] :

- Surveillance, détection, investigation et filtrage des alertes des événements de sécurité.
- Gestion des réponses aux incidents de sécurité, notamment l'analyse des malwares.
- Gestion des renseignements sur les menaces (ingestion, production, curation et diffusion).
- Gestion des vulnérabilités basée sur les risques (notamment, la priorisation des correctifs).
- Traque des menaces.
- Gestion et maintenance des dispositifs de sécurité.
- Développement de données et d'indicateurs pour le rapport/la gestion de la conformité.

3.4.3 Liste de rôles et de missions générales pour un SOC (Centre d'Opérations de Sécurité)

Les rôles et missions du SOC sont multiples, voici quelques exemples :

1. **Surveillance continue** : le SOC permet constamment de surveiller les activités sur le réseau informatique de l'entreprise en utilisant des outils de sécurité tels que des pare-feu, des IDS (systèmes de détection d'intrusion) et des SIEM (systèmes de gestion des informations de sécurité). Il gère également les mises à jour et les configurations de ces outils.
2. **Détection des incidents de sécurité :** lorsqu'une menace de sécurité est détectée, le

   SOC réagit rapidement pour l'isoler et la neutraliser. En examinant les alertes de sécurité et les événements suspects pour évaluer la gravité de la menace, identifier les impacts potentiels et déterminer les actions à prendre.

3. **Réponse aux incidents de sécurité** : Le SOC lance des mesures d'intervention en cas de problème de sécurité pour contrôler la situation et minimiser les dommages. La suppression de logiciels malveillants, le bannissement d'adresses IP suspectes, la réinitialisation de mots de passe, etc. sont quelques exemples d'actions.
4. **Gestion des vulnérabilités** : le SOC évalue constamment les vulnérabilités des systèmes informatiques de l'entreprise et propose des mesures de sécurité pour les corriger. Des correctifs de sécurité peuvent également être déployés par le SOC pour remédier aux vulnérabilités connues.
5. **Gestion des identités et des accès** : L'accès aux ressources informatiques de l'entreprise est contrôlé par le SOC, qui gère les comptes utilisateurs, les mots de passe et les certificats et s'assure que les utilisateurs ont les bonnes autorisations. Il est également attentif à tout comportement inhabituel des utilisateurs.

6. **Gestion des politiques de sécurité :** le SOC met en place des politiques de sécurité pour l'entreprise. Il établit des normes de sécurité, des procédures de sécurité et des règles d'utilisation des ressources informatiques de l'entreprise.

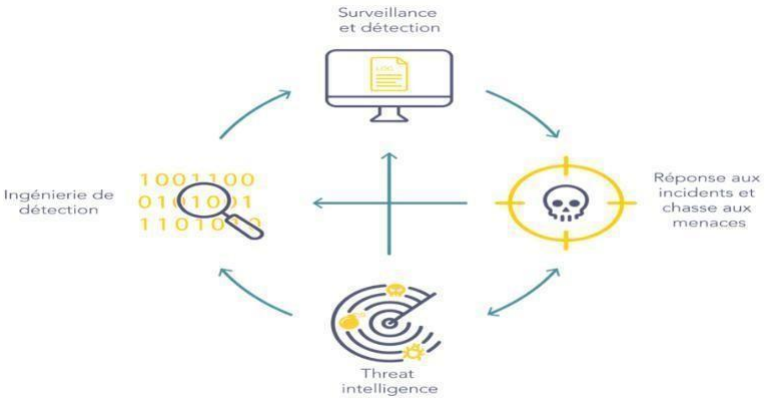


Figure 3-16 Rôle du SOC

3.4.4 Outils SOC

- **SIEM (Security Information and Event Management)**

Un SIEM est un système de gestion des événements de sécurité qui est une technologie qui permet la collecte et analyse les données de sécurité provenant de différentes sources telles que les journaux d'événements, les systèmes de détection d'intrusion et les pare-feu. Il permet aussi de générer des alertes en cas d'activité suspecte ou malveillante.

- **Pare-feu**

Sont des dispositifs de sécurité matériels ou logiciels qui contrôlent le trafic réseau en autorisant ou en bloquant l'accès en fonction de règles de sécurité définies. Ils permettent également de surveiller les activités réseau et de bloquer les tentatives d'intrusion.

- **Systèmes de détection d'intrusion (IDS)**

Est un outil de sécurité informatique qui surveille le trafic du réseau ou des systèmes informatiques pour détecter les tentatives d'intrusion ou d'attaque. Il s'agit d'un composant important d'une architecture de sécurité complète.

- **EDR (Endpoint Detection & Response)**

C'est un antivirus de nouvelle génération qui analyse les données serveurs et les terminaux, puis détecte des séquences de comportements malveillants.

- **NDR (Network Detection & Response)**

C'est un outil est complémentaire au SIEM et à l'EDR qui englobe les réseaux et établit des liens entre les hôtes, cependant il ne surveille pas les terminaux. L'utilisation d'un NDR permet d'avoir un contexte de détection plus large, qui peut révéler toute l'étendue d'une attaque et permettre des actions de réponse plus rapides et mieux ciblées.

- **XDR (eXtended Detection & Response)**

Le XDR corrèle les données de l'EDR avec les autres informations du réseau (Cloud, Active

Directory…) pour détecter les menaces plus rapidement. Une plateforme XDR ne surveille pas seulement les terminaux, mais aussi les e-mails, les serveurs et le Cloud.

- **Open XDR**

C'est une plateforme qui permet de centraliser et de corréler les données de sécurité provenant de différentes sources pour améliorer la détection et la réponse aux menaces de sécurité.

- **MDR (Managed Detection & Response**

Le MDR est un service qui collecte un maximum d'informations contextualisées pour gérer des incidents de sécurité. Les solutions sont opérées par un SOC, interne ou externalisé, et permettent d'adresser de bout en bout les menaces.

3.4.5 Avantage du SOC

Dans une entreprise le SOC représente un élément très important de la sécurité informatique de l'entreprise par rapport aux services qui fournit, parmi ces avantages on a :

- Il permet de réduire les risques de sécurité pour l'entreprise en identifiant et en répondant rapidement aux menaces de sécurité.
- Il offre une surveillance 24h/24 et 7j/7 de l'infrastructure informatique de l'entreprise
- Il offre une visibilité complète de l'environnement informatique de l'entreprise, ce qui permet de mieux comprendre les risques de sécurité et de prendre des mesures nécessaires. [25]

3.4.6 Mode de déploiement d'un SOC

Le mode de déploiement d'un SOC est la façon dont une entreprise peut acquérir des capacités de cyber sécurité pour surveiller et détecter les menaces sur son réseau. Il y a trois modèles de déploiement courants :

- **SOC Interne**

Une entreprise expérimentée dans le domaine de la sécurité informatique, peut créer son propre SOC interne dédié pour surveiller son réseau 24/24 et 7j/7. Ceci permet d'avoir une vue d'ensemble complète et de répondre rapidement aux incidents. Mais peut être coûteux et nécessite un investissement important en temps et en ressources humaines.

- **SOC, MSSP, et MDR managés**

Pour les entreprises qui ont des limites financières ou des compétences limitées, il est recommandé de choisir un SOC géré par une entreprise externe, dans le but d'effectuer des opérations de surveillance et de détection de haut niveau. Les avantages sont une mise en œuvre plus économique et une expertise supplémentaire de l'entreprise externe.

- **Hybride**

Un modèle hybride combine entre un petit SOC interne avec des experts externes, pour offrir une approche sécurisée de la détection et de la réponse aux menaces. Cela permet une détection et une réponse rapides, mais il peut être coûteux à maintenir sur le long terme.

Enfin chaque modèle a ses avantages et ses inconvénients en termes de coûts, de rapidité et de ressources humaines nécessaires pour le mettre en place

3.4.6 Défis d'un SOC

Le soc a plusieurs défis à réaliser au sein d'une entreprise afin d'assurer son bon fonctionnement et parmi ces défis en trouve :

- Installation, mise à jour et dépannage des logiciels d'application.
- Surveillance et gestion des systèmes de pare-feu et de prévention des intrusions.
- Analyse et remédiation des solutions antivirus, des logiciels malveillants et des ransomwares.
- Gestion du trafic e-mail, voix et vidéo.
- Gestion des correctifs et liste blanche.
- Analyse approfondie des données des journaux de sécurité provenant de diverses sources.
- Application des politiques et procédures de sécurité.
- Sauvegarde, stockage et récupération des données.

3.5 Conclusion

Dans le cadre de ce chapitre, nous avons présenté les différentes technologies indispensables dans un SOC pour assurer la sécurité des entreprises. En combinant le SOC, le SIEM et l'analyse des fichiers log, les organisations peuvent renforcer leur posture de sécurité, améliorer leur capacité à détecter les menaces et à réagir de manière prompte et efficace. Dans le prochain chapitre on va explorer la configuration et la mise place d SOC.

Chapitre 4

Mise en place et configuration du SOC

4.1Introduction

Le présent chapitre décrit la mise en œuvre de notre solution proposée pour renforcer la sécurité informatique d'un client spécifique. Notre solution consiste à la mise en place d'un Centre d'Opération de Sécurité (SOC) au sein de l'entreprise cliente, afin de surveiller, détecter et gérer les incidents de sécurité de manière proactive. Ce chapitre détaillera les étapes clés de déploiement du SOC, les outils et les ressources utilisés, ainsi que les avantages attendus pour l'entreprise cliente.

4.2 Partie 1 : Présentation de notre environnement de travail

Dans cette étape, nous allons présenter l'environnement de développement qui est constitué de deux parties, nommées environnement matériel et environnement logiciel.

4.2.1Environnement matériel :

Nous avons utilisé un ordinateur portable qui a les caractéristiques suivant :

Processeur	Intel(R) Core(TM) i7-7300HQ CPU @ 2.5GHz 2.5
Mémoire RAM	16 Go
Type du Système	Système d'exploitation 64 bits
Système d'exploitation	Windows 10
type de disque dur	SSD de 250 Go

Tableau 4-1 Caractéristiques techniques

4.2.2Environnement logiciel

- **GNS3 :** GNS3 est un émulateur d'équipements réseau, notamment des équipements Cisco. Cet outil permet de charger un véritable système d'exploitation Cisco IOS (Internetwork Operating System) et de l'utiliser pour simuler complètement un réseau sur un seul ordinateur. Il offre la possibilité aux machines virtuelles de se connecter aux hyperviseurs tels que VMware ou Virtualbox. GNS3 est largement utilisé par les ingénieurs réseaux du monde entier pour émuler, configurer, tester et dépanner des réseaux virtuels et réels. Il permet la conception et la simulation de réseaux simples ou complexes. GNS3 est un logiciel gratuit qui fonctionne sur plusieurs plateformes, dont Windows, Linux et MacOS. Il prend en charge les systèmes d'exploitation Cisco IOS, Juniper, MikroTik, Arista, Vyatta, et bien d'autres.

- **VMware Workstation :** repose sur une virtualisation complète, ce qui lui permet d'être compatible avec la majorité des systèmes d'exploitation, sans nécessiter de spécifications matérielles particulières. De plus, la version 6 de VMware Workstation offre la prise en charge de la para-virtualisation lorsqu'elle est utilisée avec des systèmes Linux invités qui intègrent un noyau étendu avec les fonctionnalités VMware VMI

(Interface de Machine Virtuelle). Cette fonctionnalité améliore significativement les performances de la virtualisation**.**

- **FortiGate :** est une marque de pare-feu (firewall) et de sécurité réseau développée par la société Fortinet. Les appareils FortiGate offrent des fonctionnalités avancées de sécurité, telles que la détection des intrusions, la prévention des menaces, la gestion unifiée des menaces, le filtrage du contenu, la protection contre les attaques de déni de service (DDoS), la gestion de la bande passante, la VPN (réseau privé virtuel) et bien plus encore. Les solutions Fortinet sont conçues pour les entreprises de toutes tailles, offrant une protection globale et une gestion centralisée des politiques de sécurité. Grâce à leurs performances élevées, leur évolutivité et leur large éventail de fonctionnalités, les pare-feu FortiGate sont largement utilisés pour sécuriser les réseaux d'entreprise.
  Windows 10 : est le dernier système d'exploitation développé par Microsoft, combinant les meilleures caractéristiques de Windows 7 et Windows 8. Il propose une interface conviviale, un menu Démarrer amélioré, la possibilité de créer des bureaux virtuels et une intégration avec le Windows Store. Compatible avec une variété d'appareils, Windows 10 prend en charge les applications universelles et offre des fonctionnalités de sécurité avancées telles que Windows Defender. C'est un système d'exploitation moderne et polyvalent, offrant aux utilisateurs une expérience utilisateur riche et sécurisée.
- **Windows Serveur 2022 :** est la dernière version du système d'exploitation serveur développé par Microsoft, offrant des améliorations majeures en termes de performances, de sécurité et de gestion. Cette plateforme solide prend en charge une variété de charges de travail, allant des serveurs traditionnels aux déploiements de cloud hybride et aux conteneurs. Doté de fonctionnalités avancées de sécurité telles que la protection contre les ransomwares et l'authentification renforcée, Windows Server 2022 simplifie la gestion des politiques de sécurité. Avec sa gestion simplifiée et ses améliorations de performances, il répond aux besoins évolutifs des infrastructures informatiques modernes.
- **Ubuntu :** est une distribution Linux réputée pour sa convivialité et sa facilité d'utilisation, en particulier dans un environnement de bureau. L'installation d'Ubuntu est simple et ses mécanismes de mise à jour témoignent d'une grande maturité et d'une simplification remarquable, rivalisant ainsi avec les produits propriétaires concurrents. La distribution est également réputée pour sa sécurité robuste et son optimisation efficace des ressources.
- **Kali Linux :** est une distribution Linux spécialisée dans la sécurité informatique et les tests de pénétration. Elle est largement utilisée par les professionnels de la sécurité et les chercheurs en sécurité pour évaluer les vulnérabilités des systèmes informatiques. Kali Linux est basée sur Debian et offre un large éventail d'outils d'hacking et de sécurité réseau préinstallés. Ces outils permettent aux utilisateurs d'effectuer des tests de sécurité avancés, d'identifier les failles de sécurité et de protéger leurs systèmes contre les attaques potentielles. Kali Linux est appréciée pour sa stabilité, sa flexibilité

et sa documentation complète, ce qui en fait un choix populaire parmi les professionnels de la sécurité informatique.

4.3Architecture choisie

Pour réaliser notre mise en place, nous a pris une architecture d'un des clients de campus NTS. Nous a fait les installations et les configurations nécessaires pour tous les équipements de cette architecture. Et après le test de connexion nous avons commencé notre mise en place de notre solution.

Au niveau de notre DMZ nous avons ajouté un serveur Splunk entreprise qui est installer sur le Windows serveur 2022, pour qu'il collecte des logs et aussi pour nous permettre la visualisation en temps réel de tous les évènements qui se présente au niveau des machine client (Windows, Ubuntu) à l'aide des Forwarder qui sont installés au niveau de ces dernières.

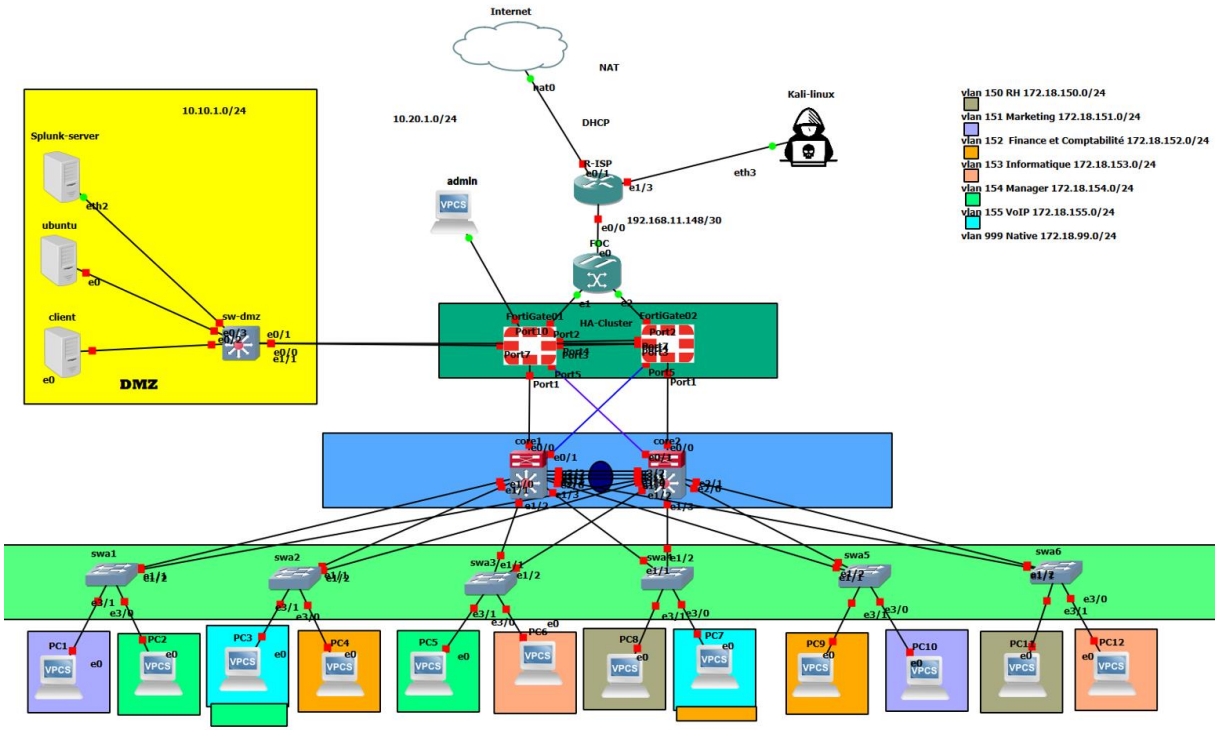


Figure 4-1 L'architecture choisie.

4.4 Tableaux d'adressage

Le plan d'adressage des sous réseaux « VLANs »

Nom du VLAN	ID du VLAN	Adresse du sous-réseau	Passerelle du sous-réseau

VLAN RH	150	172.18.150.0/24	172.18.150.1
VLAN Marketing	151	172.18.151.0/24	172.18.151.1
VLAN Finance	152	172.18.152.0/24	172.18.152.1
VLAN Informatique	153	172.18.153.0/24	172.18.153.1
VLAN Manager	154	172.18.154.0/24	172.18.154.1
VLAN VoIP	155	172.18.155.0/24	172.18.155.1
VLAN Native	999	/	/

Tableau 4-2 Adressage des VLANs

Le plan d'adressage des équipements d'interconnexion

Equipements	**Interface réseau**	**Adresse IP**
Pare-feu(FortiGate)	**Inter-vlan1 (port1)** **Internet (port2)** **DMZ**	**0.0.0.0/0** **192.168.11.149/30** **10.10.1.1/24**
Router(R-ISP)	**Internet (Eth0/0)** **FortiGate (Eth0/1)** **LAN-2 (Eth1/3)**	**DHCP (192.168.80.142/24)** **192.168.11.150/30** **10.11.1.1/24**
Ubuntu	**Eth0**	**10.10.1.115/24**
Windows 10	**Ethernet 0**	**10.10.1.111/24**
Windows server 2022(Splunk)	**Ethernet 0**	**10.10.1.100/24**
Kali linux (Hacker)	**Eth0**	**10.11.1.12/24**
PC 1	**Ethernet 0**	**DHCP (VLAN 151)**
PC 2	**Ethernet 0**	**DHCP (VLAN 154)**
PC 3	**Ethernet 0**	**DHCP (VLAN 155)**
PC 4	**Ethernet 0**	**DHCP (VLAN 152)**
PC 5	**Ethernet 0**	**DHCP (VLAN 154)**
PC 6	**Ethernet 0**	**DHCP (VLAN 153)**
PC 7	**Ethernet 0**	**DHCP (VLAN 155)**
PC 8	**Ethernet 0**	**DHCP (VLAN 150)**
PC 9	**Ethernet 0**	**DHCP (VLAN 152)**
PC 10	**Ethernet 0**	**DHCP (VLAN 151)**

PC 11	**Ethernet 0**	**DHCP (VLAN 150)**
PC 12	**Ethernet 0**	**DHCP (VLAN 153)**

Tableau 4-3 Table d'adressage des équipements

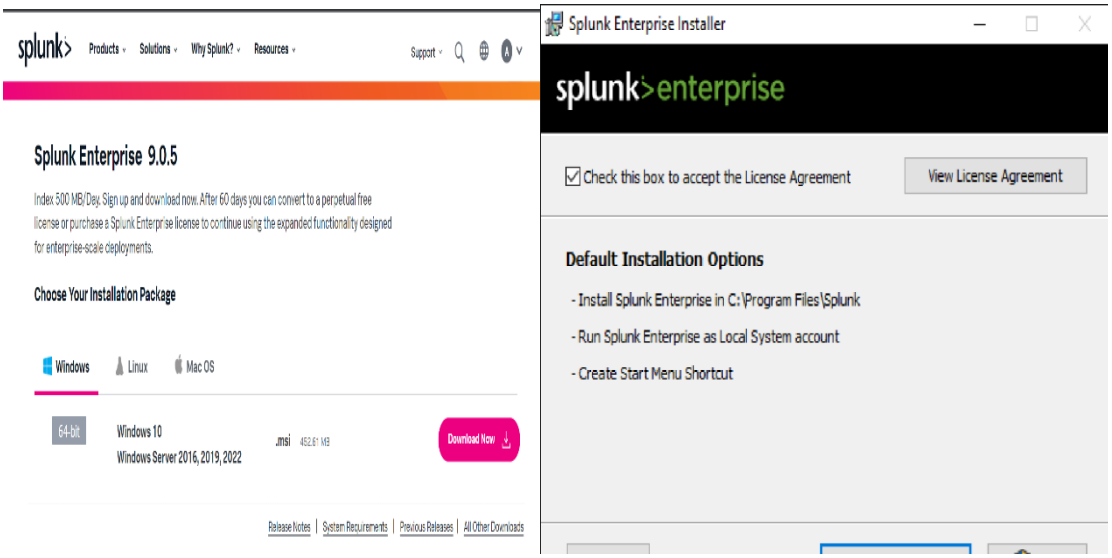
Partie 2 : Mise en œuvre de la solution

4.5 Installation du serveur Splunk entreprise

4.5.1 Installation sous Windows serveur 2022

Pour installer Splunk entreprise sur Windows serveur 2022 nous devons d'abord téléchargez le fichier d'installation de Splunk Enterprise pour Windows à partir du site officiel de Splunk après avoir créé un compte sur leur site web, ensuite nous exécutons le fichier d'installation et suivre les instructions à l'écran et aussi nous devront créer un compte administrateur et on Accepte les termes du contrat de licence.

Les figures suivantes montrent les étapes de l'installation :



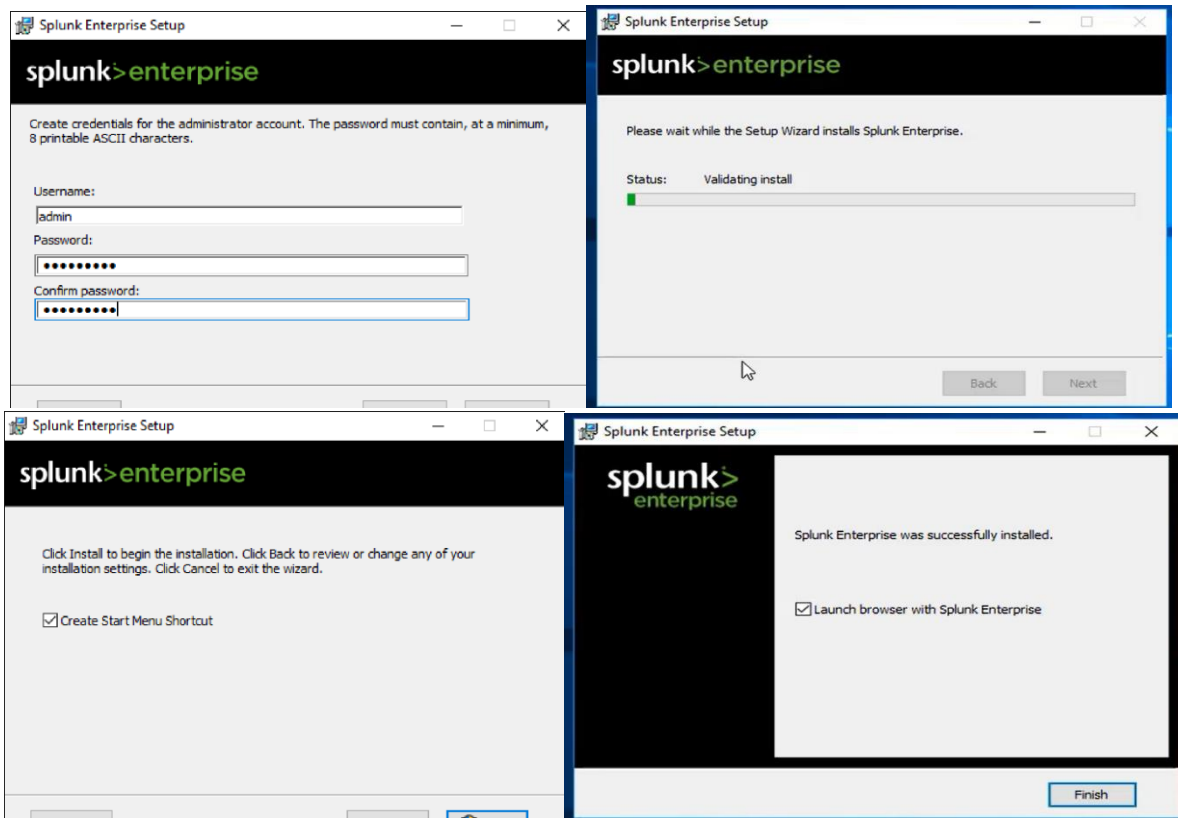
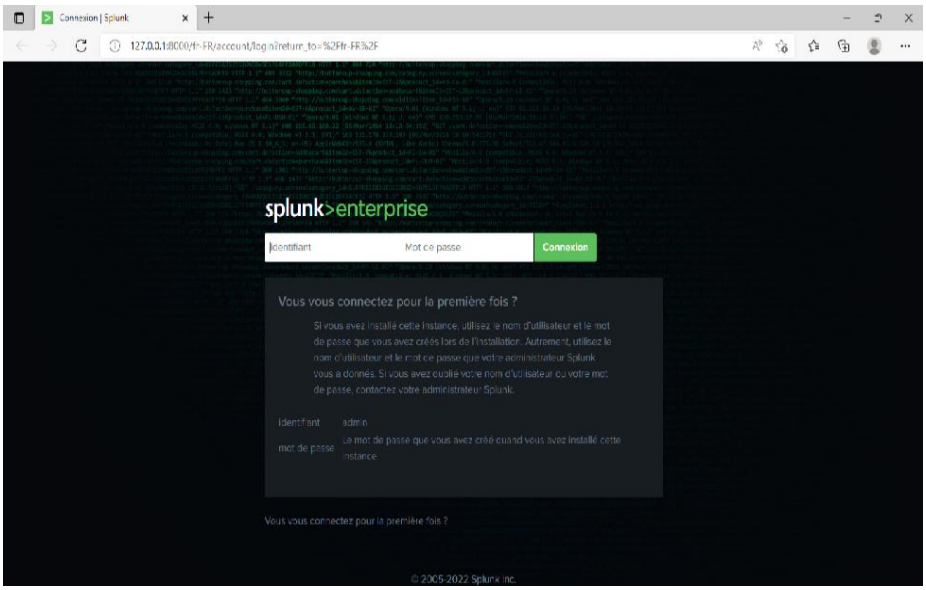


Figure 4-2 Les étapes d'installations de Splunk entreprise

Une fois l'installation terminée, Splunk Enterprise devrait être prêt à être utilisé sur notre Windows Server 2022, nous allons accéder à son interface graphique à l'aide d'un navigateur.

Les figures suivantes montrent l'interface graphique de notre Splunk.



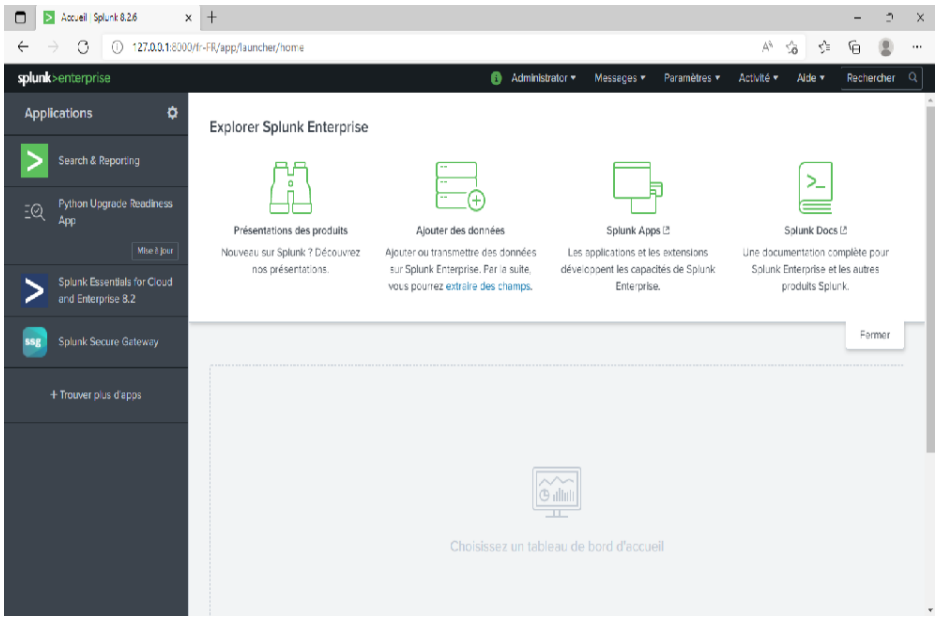
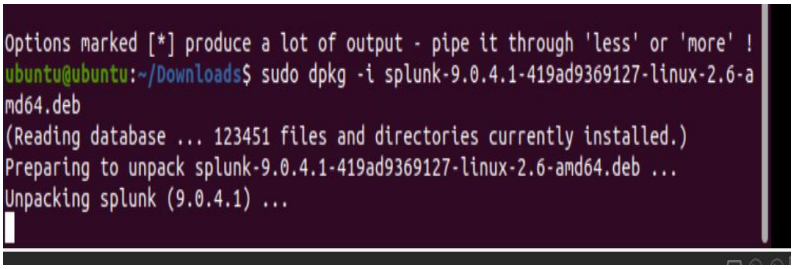


Figure 4-3 L'interface graphique de Splunk Enterprise.

4.5.2 Installation sous linux (Ubuntu)

Pour installer Splunk Enterprise sur Ubuntu nous devront d'abord télécharger le fichier d'installation de Splunk Enterprise avec le format Deb pour Linux à partir du site officiel de Splunk après avoir créé un compte sur leur site web. Nous ouvrons le terminal et nous accédons au répertoire téléchargement afin de lancer son installation à l'aide des commandes.

Les figures suivantes montrent les étapes d'installations :



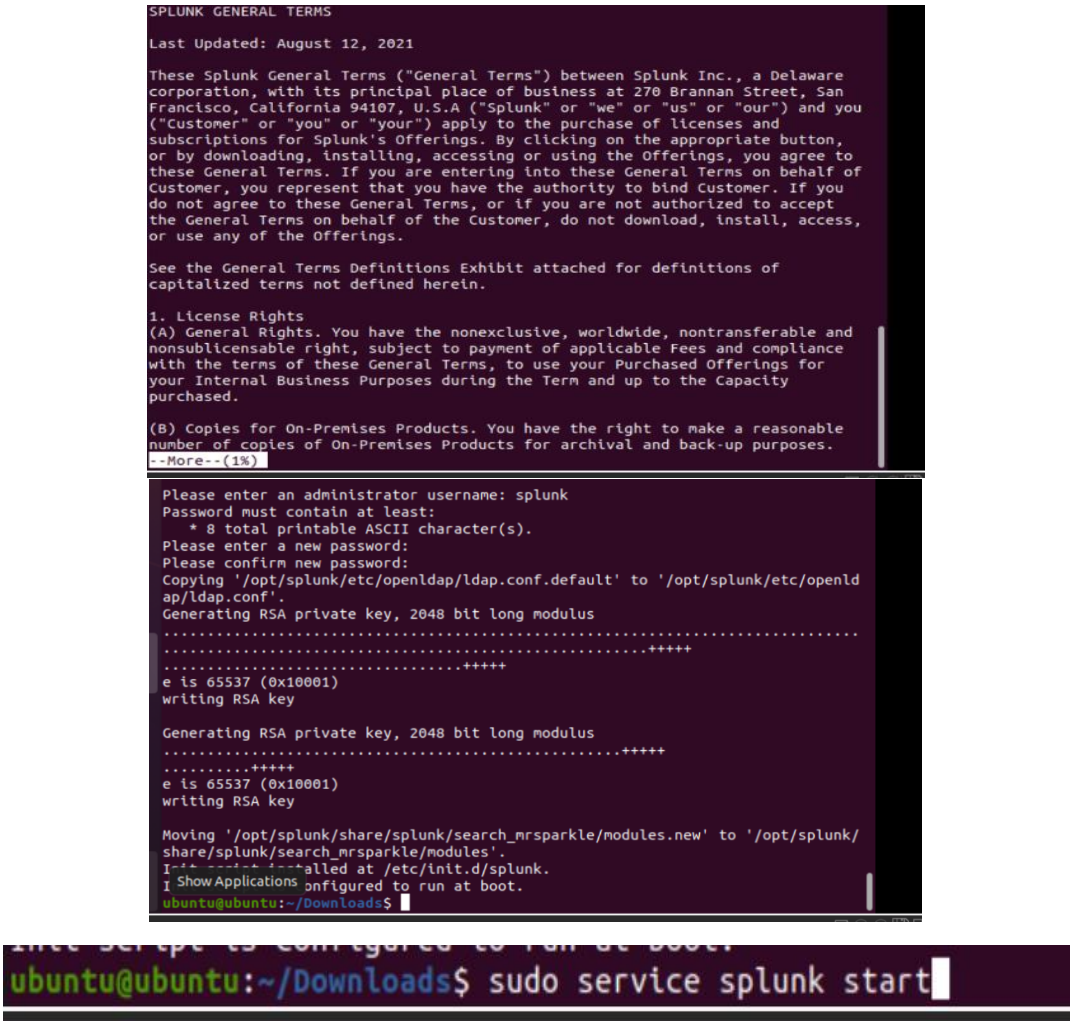


Figure 4-4 Les étapes d'installation de Splunk sur Ubuntu.

Une fois l'installation terminée, Splunk Enterprise devrait être prêt à être utilisé sur notre Ubuntu, nous va accéder à son interface graphique à l'aide d'un navigateur.

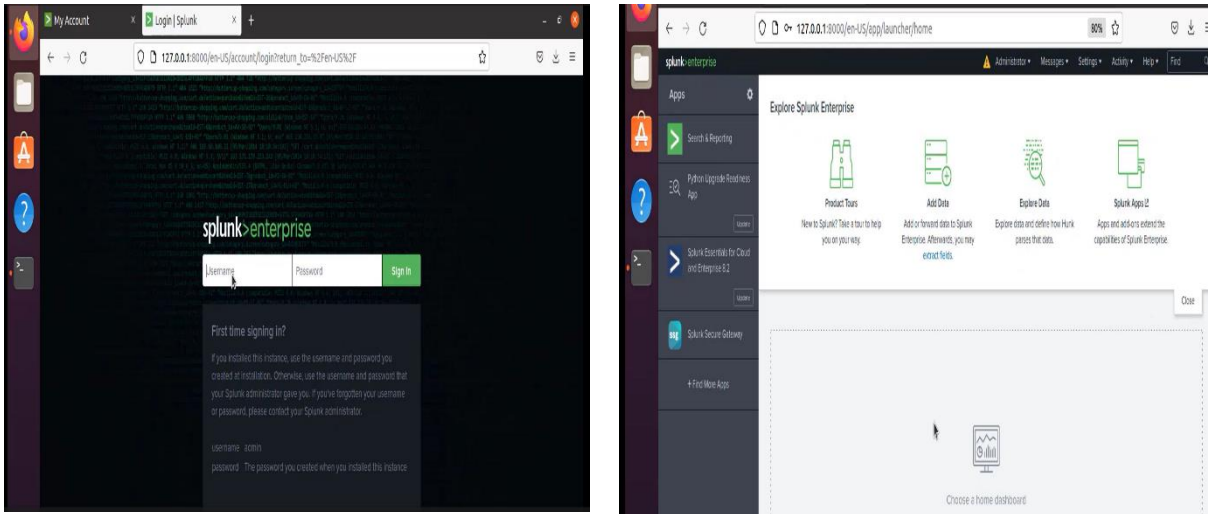


Figure 4-5 L'interface graphique de Splunk sur Ubuntu

4.6 Récupération et l'analyse des Logs

Afin de collecter et analyser les fichiers journaux nous devons premièrement installer Universal SplunkForwader sur les différentes machines clientes (Ubuntu, Windows 10).

Pour effectuer l'installation des UF nous devons d'abord télécharger les fichiers d'installation du Forwarder Splunk pour Windows (avec l'extension MSI) et Ubuntu (avec l'extension DEB) depuis le site officiel de Splunk.

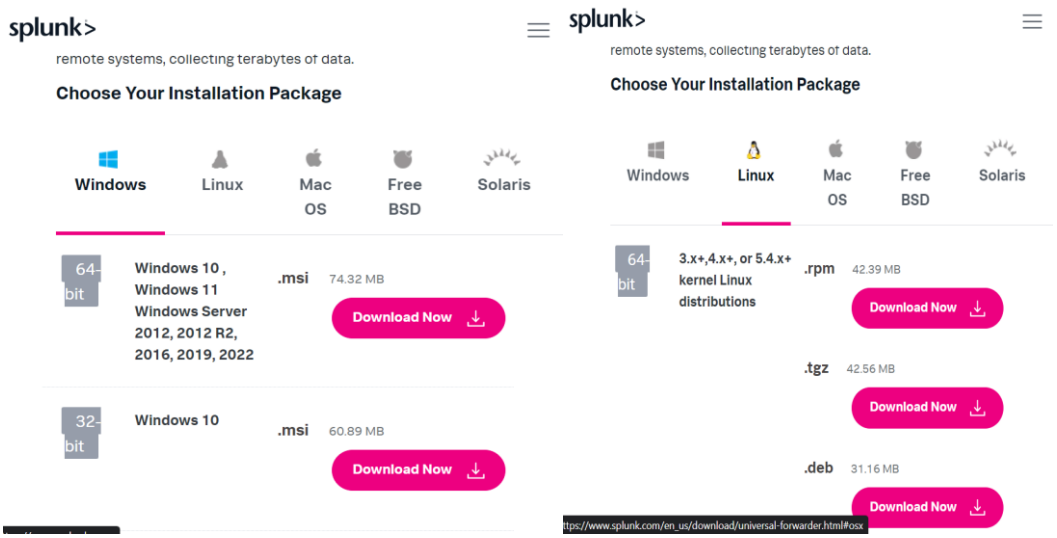


Figure 4-6 Les fichiers d'installation des UFs

4.6.1 Installation de SplunkForwader au niveau de Windows 10

- Téléchargement du fichier d'installation d'UF pour Windows 10 depuis le site officiel de Splunk.
- Nous exécutons le fichier d'installation et nous allons suivre les instructions à l'écran.
- Configurez les paramètres de connexion au serveur Splunk en spécifiant l'adresse IP du serveur Splunk et le port de réception des données (par défaut, c'est le port 9997).
  Une fois l'installation terminée, le Forwarder Splunk devrait être prêt à transmettre les données au serveur Splunk.

Les figures suivantes montrent les étapes d'installation :

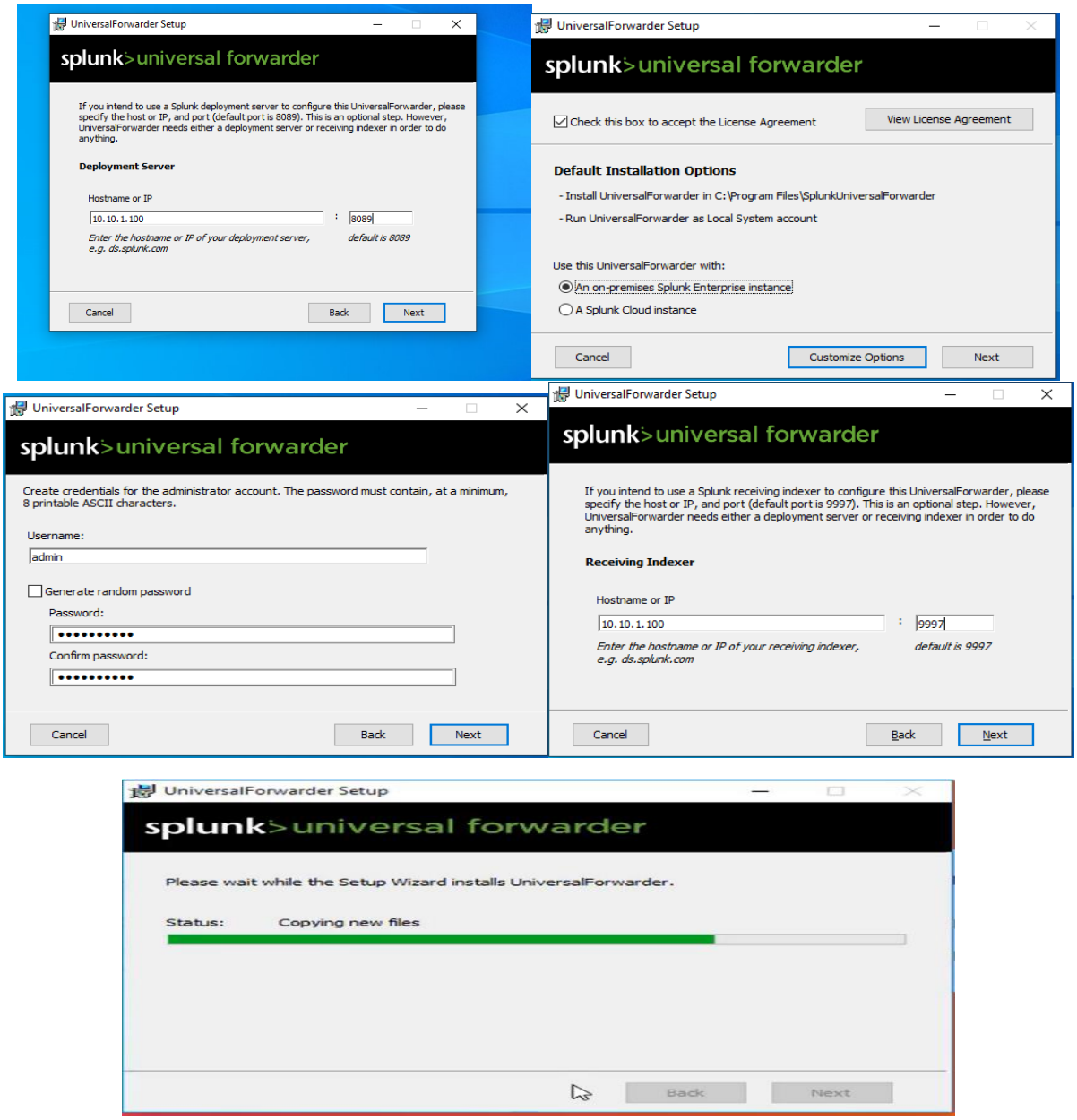


Figure 4-7 L'installation de Splunk Forward sur Windows 10.

4.6.2 Installation de SplunkForwader au niveau de Ubuntu

Pour Ubuntu, nous allons suivre une procédure similaire, en téléchargeant le fichier d'installation du Forwarder Splunk pour Linux (format DEB) depuis le site officiel de Splunk et en l'installant sur le système Ubuntu en utilisant les commandes appropriées.

Les figures suivantes montrent les étapes d'installations :

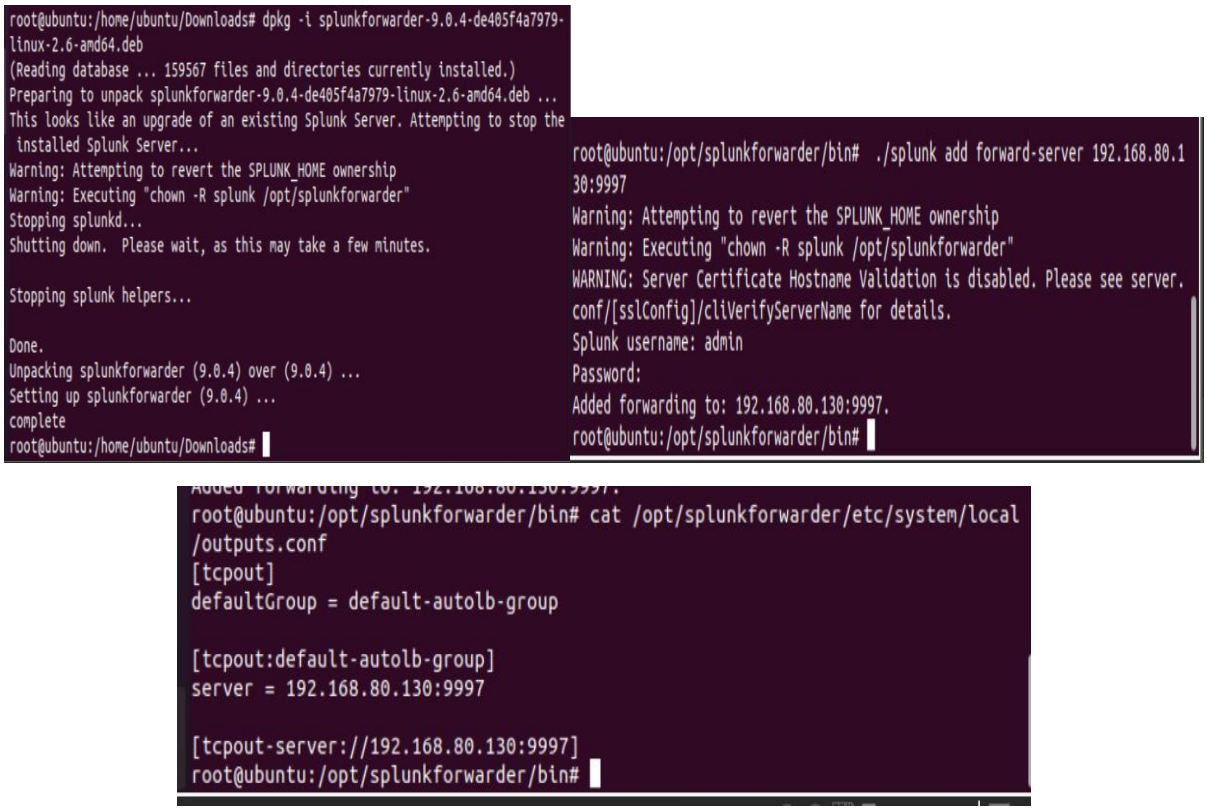


Figure 4-8 L'installation de Splunk Forwarder sur Ubuntu.

4.6.3 Collecte des logs

Pour collecter les logs sur notre serveur Splunk nous devons aller sur le tableau de bord d'accueil de Splunk, cliquer sur "Settings" (Paramètres) dans la barre de navigation supérieure, puis sélectionner "Forwarding and Receiving" (Transfert et réception) dans la section "Data" (Données).

Dans la section "Receiving"(Réception), nous cliquons sur « nouveau port de réception » et ajouter le port 9997 puis cliquez sur enregistrer.

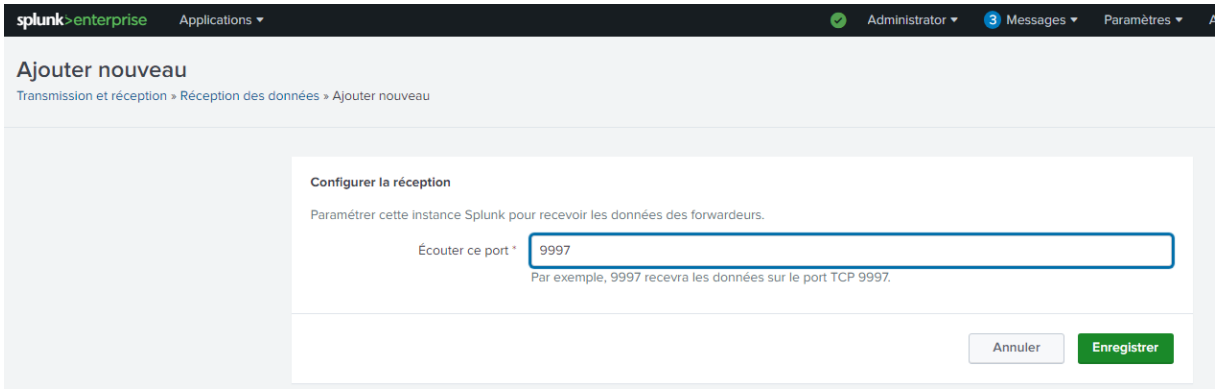


Figure 4-9 Configuration du port de réception

Pour permettre la transmission et la réception des logs entre les machines clientes et Splunk serveur nous doit ouvrir(autoriser) les ports au niveau du pare-feu, comme il est montré sur la figure suivante :

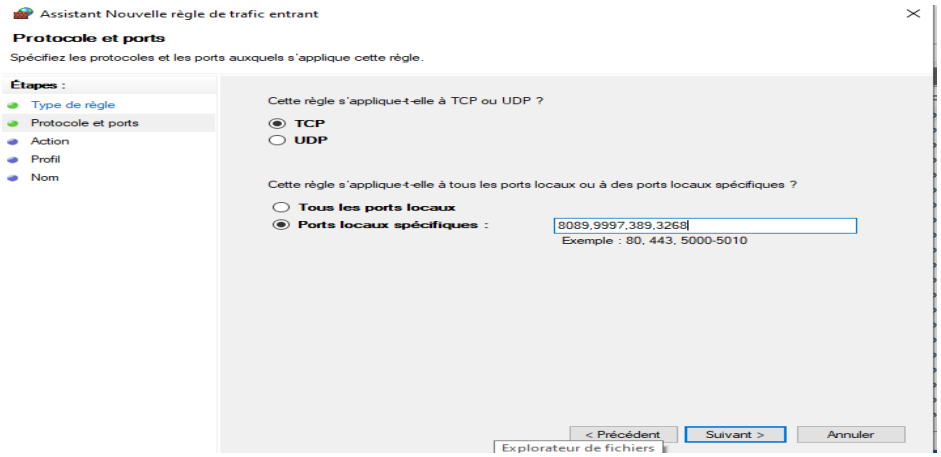


Figure 4-10 L'autorisation des ports

4.6.4 Configuration d'envoi des logs de Windows 10 vers Splunk serveur

- Autoriser les ports 9997,8089 sur le pare-feu de Windows 10.
- Au niveau Splunk serveur, nous allons cliquer sur « ajouter des données » qui se trouve dans « Paramètre », puis nous cliquons sur « Transmettre »
- Après l'affichage de la liste des machines clientes disponibles, nous avons sélectionné celles dont nous souhaitions récupérer les logs. Ensuite, nous avons précisé le nom de la classe serveur, qui regroupe plusieurs hôtes, puis nous avons cliqué sur le bouton "Suivant" pour poursuivre la configuration. Comme le montre les deux figures suivantes :

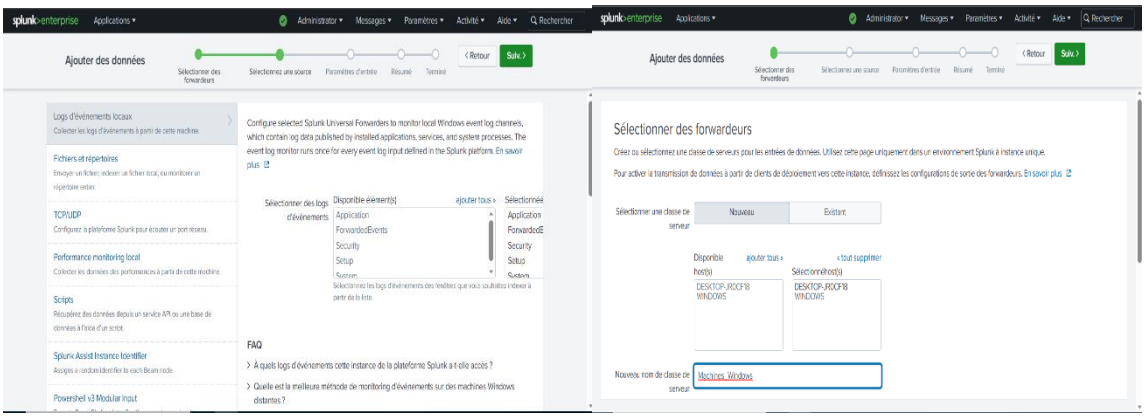


Figure 4-11 Configuration de la réception des logs

- Création d'un index pour cette machine surnommé « windows_index » comme le montre la figure suivante

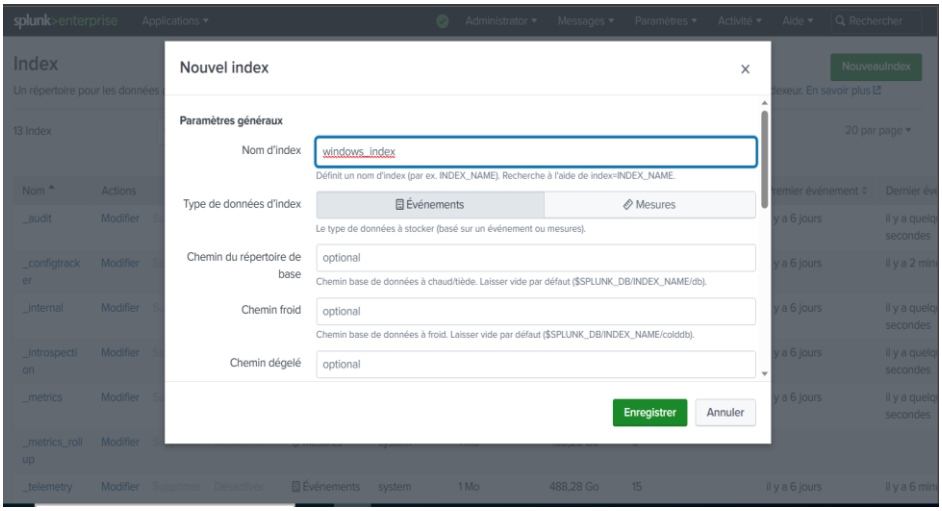


Figure 4-12 Création d'index

Après avoir terminé nos configurations du Forwarder de Windows 10 en passe vers la recherche de ces logs avec l'index que nous avons créée comme le montre la figure suivante :

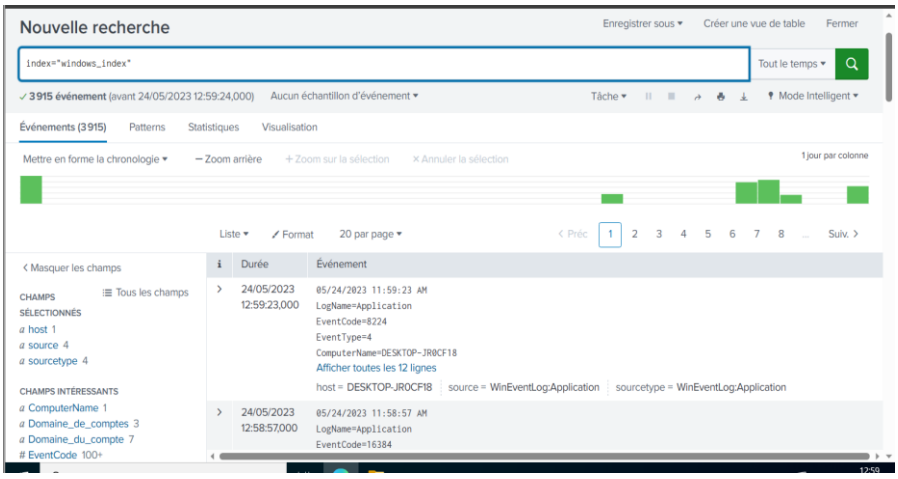


Figure 4-13 Recherche des logs sur Windows.

4.6.5 Configuration d'envoi des logs d'Ubuntu vers Splunk serveur

Avec La commande suivante « sudo ./splunk add monitor /var/log » nous allons ajouter le répertoire /var/log » en tant que source de surveillance dans Splunk. Cela signifie que Splunk va surveiller les fichiers journaux présents dans ce répertoire pour permettre la recherche et l'analyse ultérieures, Comme illustré dans figure ci-dessous :

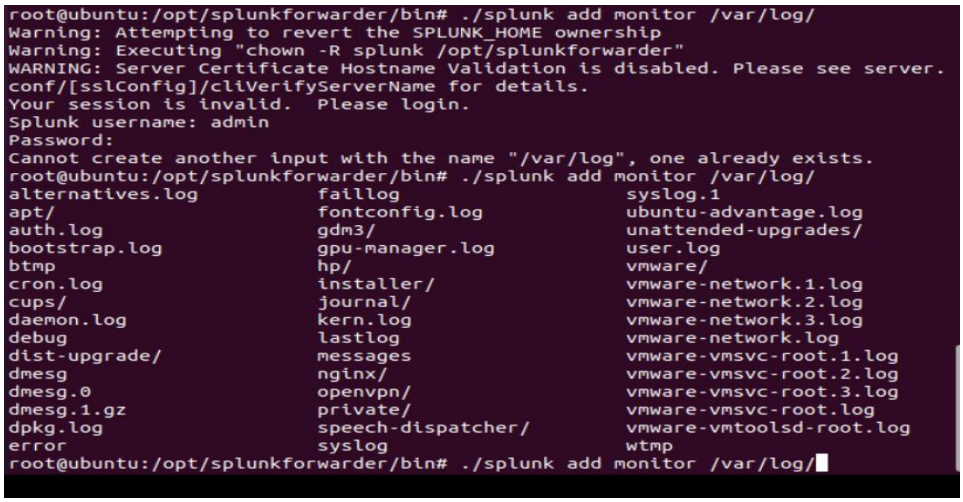


Figure 4-14 Surveillance d'Ubuntu.

Dans la figure suivante en montre notre recherche sur logs collecté à partir de la machine Ubuntu.

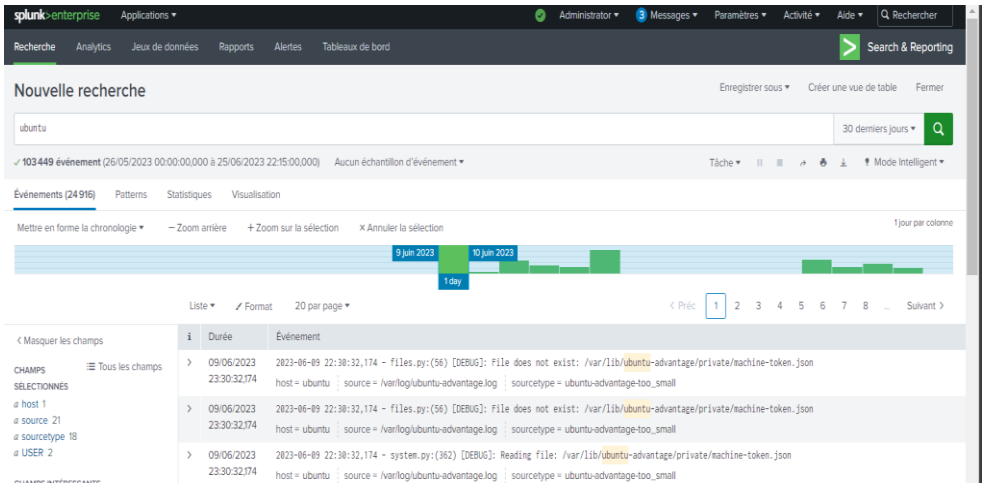


Figure 4-15 Logs Ubuntu.

4.6.6 Surveillance du serveur web Nginx

Ce serveur est présent sur notre machine Ubuntu, qui est responsable de la gestion du trafic web de l'entreprise, ce qu'il le rend un élément essentiel et qu'nous doit surveiller.

Pour cela nous devons créer un index au niveau des Splunk pour qu'il nous aide dans la recherche de log du serveur, cela est illustré dans le figure suivante :

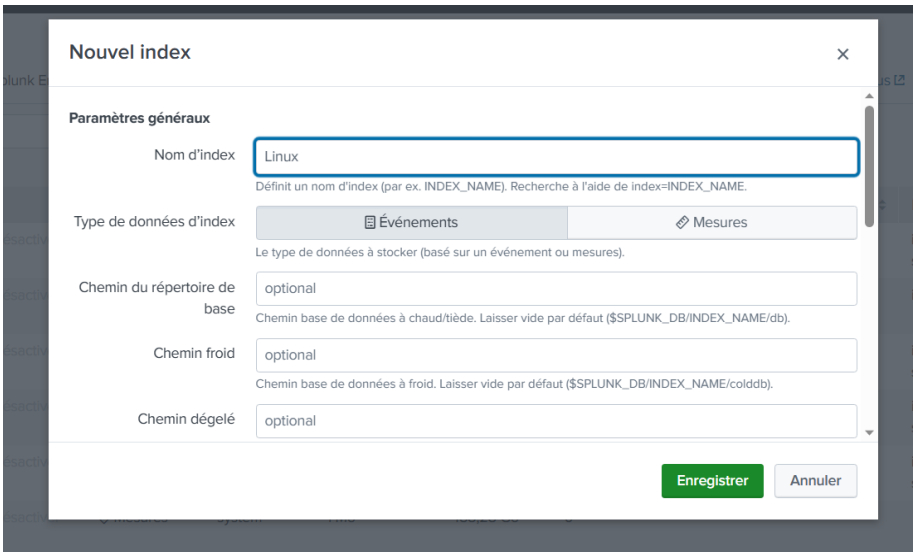


Figure 4-16 La création d'index Nginx

Après nous devons entrer la commande « sudo ./splunk add monitor /var/log/nginx/access.log –index linux » pour récupérer les logs de nginx.

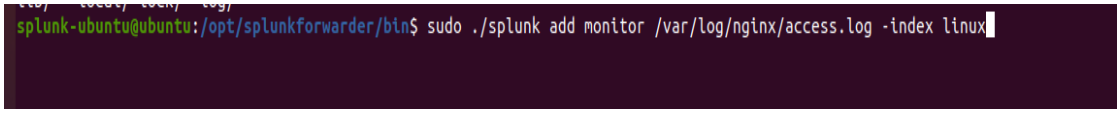


Figure 4-17 Surveillance de Nginx

Dans la figure suivante en montre notre recherche sur logs collecté à partir de serveur Nginx.

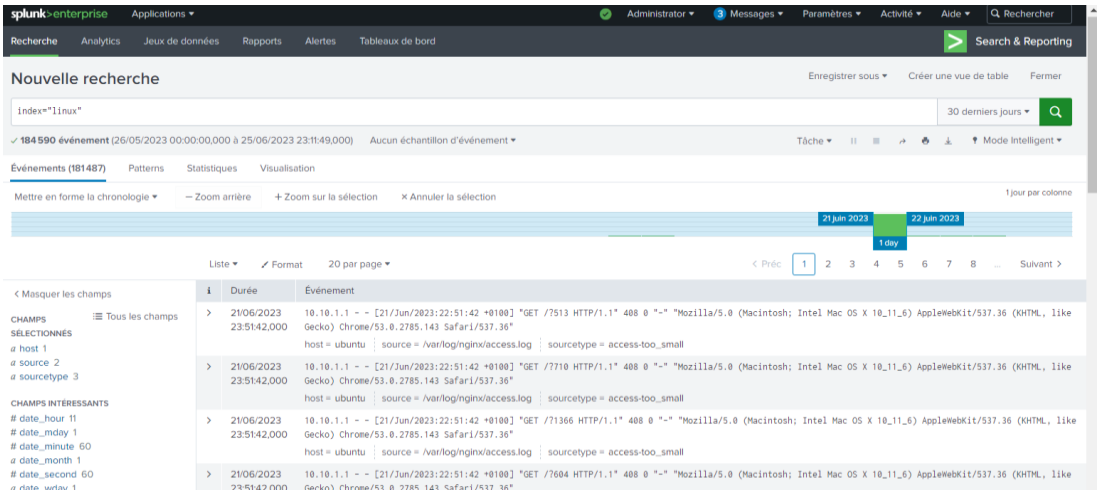


Figure 4-18 Logs Nginx

4.6.7 Surveillance et collection des logs de FortiGate

Pour surveiller et collecter les logs de FortiGate sur Splunk, nous devons suivre les étapes suivantes :

- Configuration de FortiGate :

  Nous accédons à l'interface graphique de notre pare-feu à l'aide de son adresse IP, et nous cliquons sur « Log&Repport » puis sur « Log setting », activer l'envoie des logs vers SysLog nous ajoutons l'adresse IP de serveur Splunk comme le montre la figure suivante :

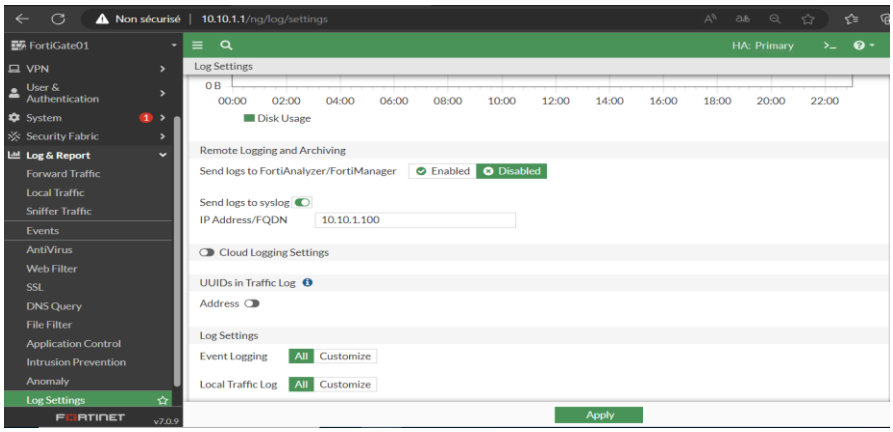


Figure 4-19 Activation d'envoi de syslog.

En suite en passe à la configuration de gestion des logs et du serveur de syslog dans CLI de FortiGate comme illustré dans la figure suivante :

```
FortiGate01 # config log syslogd setting

FortiGate01 (setting) # set status enable

FortiGate01 (setting) # set port 1514

FortiGate01 (setting) # set server 10.10.1.100

FortiGate01 (setting) # end
Port 1514 is different from default port 514.
Confirm to use port 1514 instead?
Do you want to continue? (y/n)y

Port set to 1514

FortiGate01 #
```

Figure 4-20 Configuration des logs FortiGate

- Installation de l'application Splunk Add-on for Fortinet :

  Sur la page de gestion de Splunk, en clique sur "Apps" dans le menu supérieur ensuite "Browse more apps" pour accéder à Splunkbase. Dans la barre de recherche de Splunkbase en tape " Splunk Add-on for Fortinet" et appuyer sur Entrée, après sur le bouton "Download" pour télécharger le package d'installation de l'application.

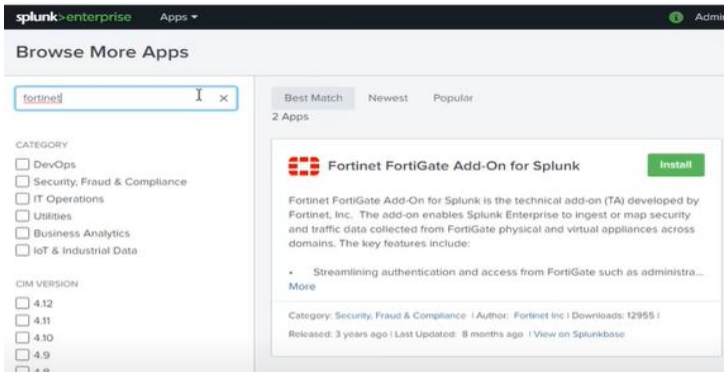


Figure 4-21 Splunk Add-on for Fortinet

- Configuration de l'entrée de logs FortiGate dans Splunk : Dans Splunk, nous accédons à l'interface de configuration des inputs (Données d'entrée) pour configurer une nouvelle source de logs pour FortiGate. Sélectionne l'option appropriée dans l'add-on Splunk for Fortinet pour spécifier que vous collectez des logs de FortiGate.

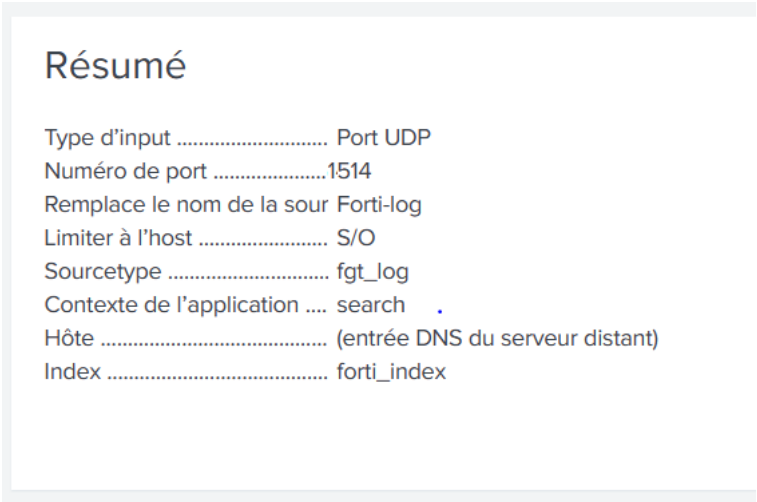


Figure 4-22 L'entrée de logs FortiGate dans Splunk.

- Recherche et analyse des logs : Une fois que les logs de FortiGate sont collectés dans Splunk, en lance notre recherche.

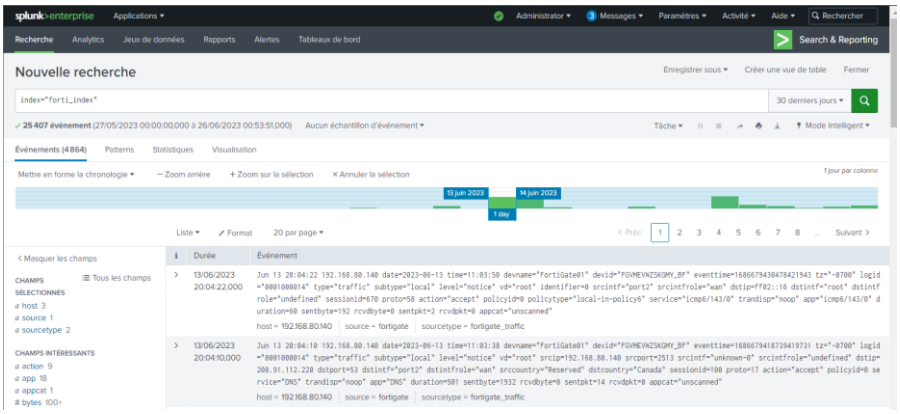


Figure 4-23 Log FortiGate

4.6.8 Surveillance et collection des logs de router Cisco :

Pour surveiller et collecter les logs du routeur (R-ISP) sur Splunk, nous devons suivre les étapes suivantes :

- Configuration de syslog au niveau du routeur : nous accédons à la CLI pour activer le syslog pour qu'il génère les logs et les envoyer à Splunk.

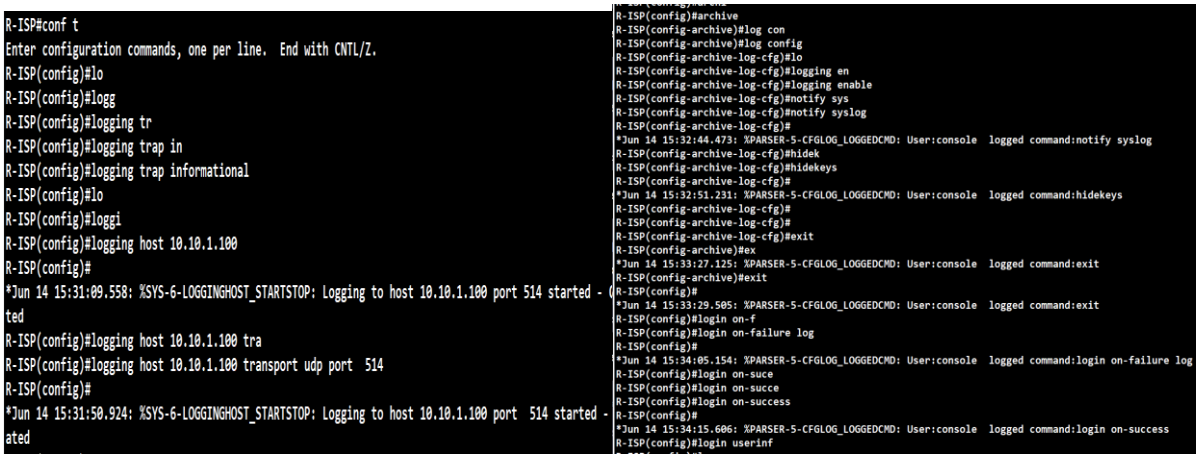


Figure 4-24 Configuration de syslog router R-ISP

- Installation de l'application Cisco Networks Add-on for Splunk : Sur la page de gestion de Splunk, nous cliquons sur "Apps" dans le menu supérieur ensuite "Browse more apps" pour accéder à Splunkbase. Dans la barre de recherche de Splunkbase en tape "Cisco Networks Add-on" et appuyez sur Entrée, après sur le bouton" Télécharge " pour télécharger le package d'installation de l'application.

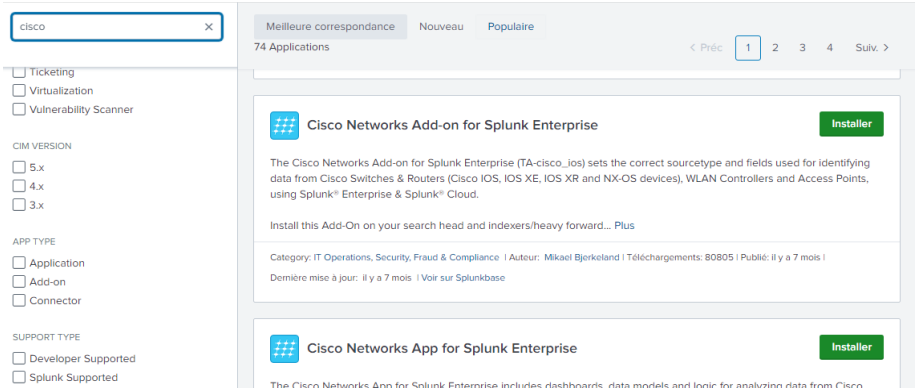


Figure 4-25 L'application Cisco Networks Add-on for Splunk

- Configuration de l'entrée de logs Cisco dans Splunk : Dans Splunk, nous accédons à l'interface de configuration des inputs (Données d'entrée) pour configurer une nouvelle source de logs pour FortiGate. Sélectionne l'option appropriée dans l'add-on Splunk for Fortinet pour spécifier que vous collectez des logs de FortiGate.

Figure 4-26 Résumé de la configuration du log

L'entrée de logs Cisco dans Splunk.

- Recherche et analyse des logs : Une fois que les logs de Cisco sont collectés dans Splunk, en lance notre recherche.

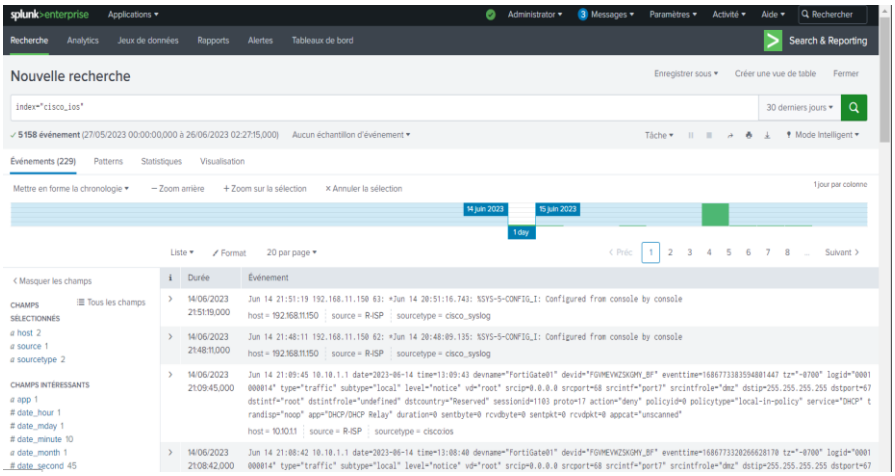


Figure 4-27 Log Cisco

4.7 Création des tableaux de bord (Dashboard)

Splunk permet une visualisation générale des événements d'une façon personnalisée et organiser à l'aide de la création des tableaux de bord.

Pour créer cela, d'abord nous devons s'exposer à une notion qui est intitulé « langage SPL ».

4.7.1 Définition de langage SPL

Le langage SPL (Search Processing Language) est utilisé pour extraire les données et créer les requêtes nécessaires pour alimenter nos tableaux de bord. Voici quelques éléments du langage SPL utilisés dans les tableaux de bord Splunk.

Stats : Utilisée pour calculer des statistiques et agréger les données

Count : utilisée pour compter le nombre d'événements

Table : Utilisée pour afficher les résultats sous forme de table

Where : Utilisée pour filtrer les résultats en fonction de conditions spécifiques.

AND, OR : combiner des conditions lors de la recherche et du filtrage des données.

Top : utilisée pour obtenir les valeurs les plus élevées d'un champ spécifié.

Showperc : Affiche également le pourcentage de chaque valeur par rapport au total.

Source : fait référence à un champ spécifique qui contient des informations sur la source des données.

4.7.2 Tableau de bord FortiGate

A l'aide de l'application Splunk Add-on for Fortinet nous peut générer directement le tableau de bord de notre pare-feu FortiGate en suivant les étapes suivantes :

- Accéder à l'application puis en cliquant sur modifier pour compléter nos champs avec les requête SQL comme le montre l'exemple dans les figures suivantes :

Figure 4-28 Exemple d'ajout de requête

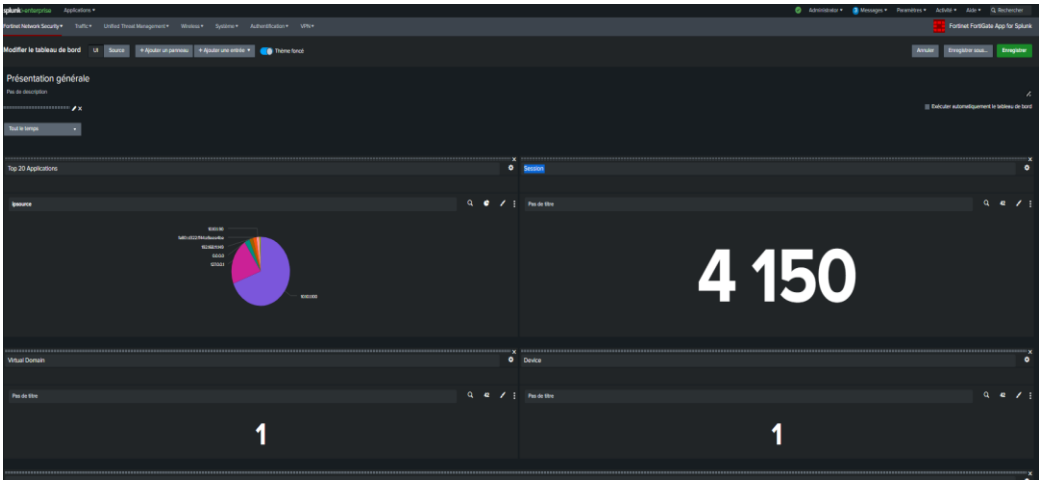


Figure 4-29 Tableau de bord FortiGate.

A l'aide de ce tableau nous pouvons suivre les différents évènements qui se déroule au niveau de notre pare-feu.

4.7.3 Tableau de bord de routeur Cisco

A l'aide de l'application Cisco Networks Add-on for Splunk, nous pouvons directement générer le tableau de bord de notre routeur Cisco en suivant les étapes suivantes :

- Nous accédons à notre application et nous remplissons le champ Product (avec IOS) et ont choisi une période de temps (tous les temps) ensuite soumettre.

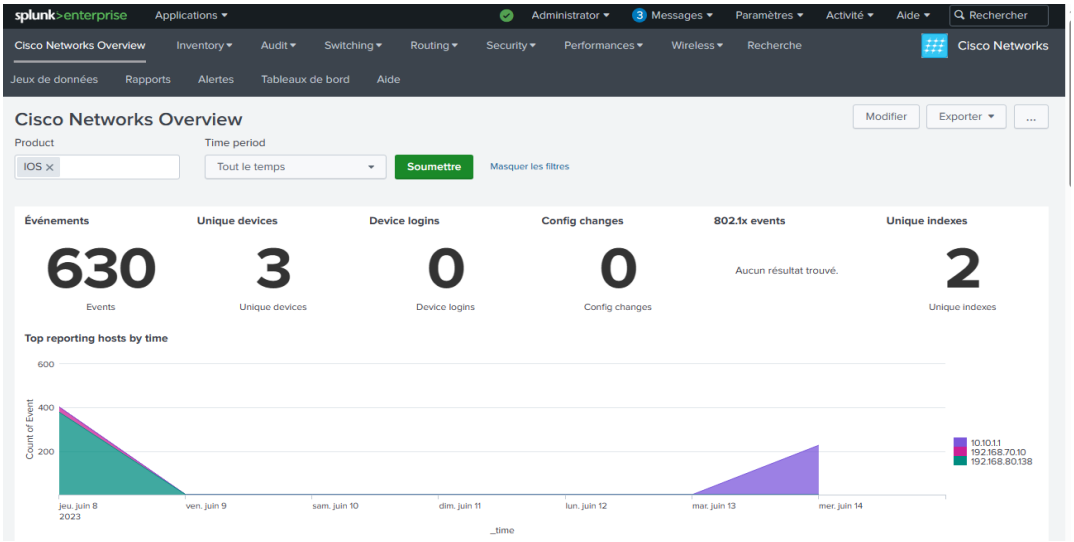


Figure 4-30 Tableau de bord router Cisco (R-ISP)

Partie 3 : Test

Dans le cadre de simuler le teste de notre solution (test d'intrusion), nous supposons que notre machine attaquante kali linux a un accès direct au réseau de l'entreprise comme il est illustré sur la topologie, et nous devons prendre la machine Ubuntu comme machine cible.

4.8 Etapes d'attaque

- Nous commençons par scanner la machine cible afin de détecter les ports ouverts avec leurs services en utilisant la commande « nmap –sV –O 10.10.1.115 », comme illustré la figure suivante :

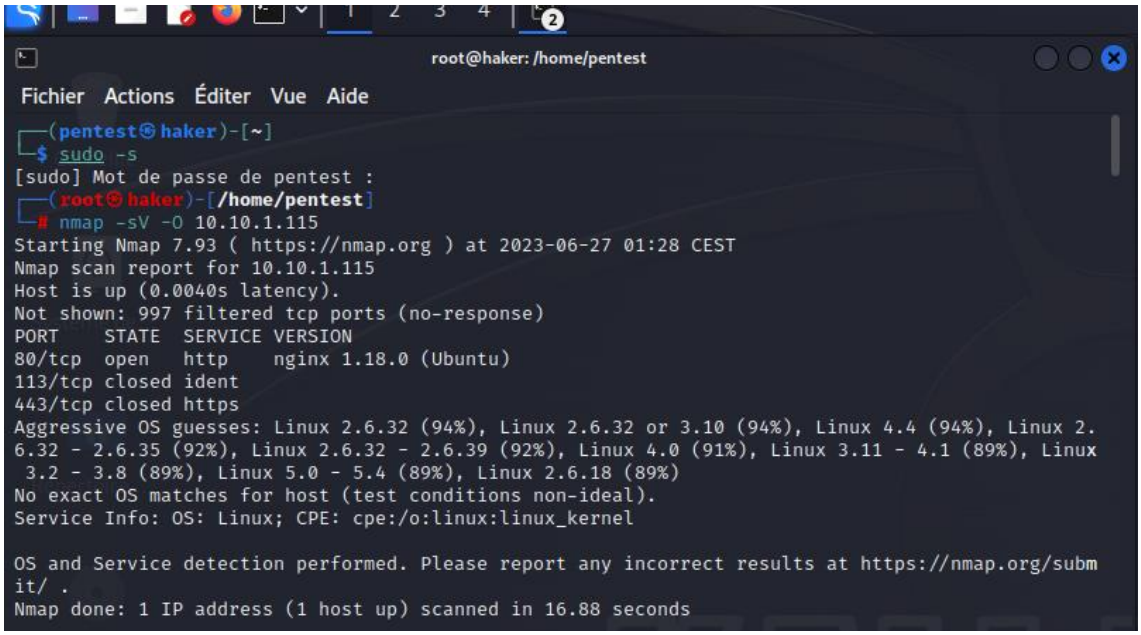


Figure 4-31 Scan de la machine (avec nmap)

- en lance notre attaque DOS sur la machine cible avec l'utilisation de l'outil **hping3**

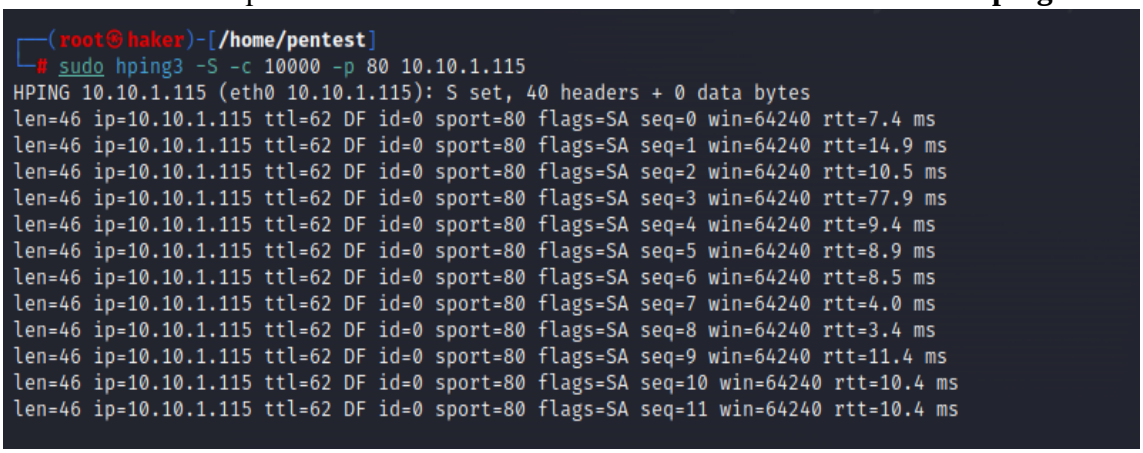


Figure 4-32 Attaque DDOS

4.9 Détection de l'attaque

A l'aide des logs collecté au niveau de Splunk nous avons remarqué qu'il existe des logs qui signifient qu'une attaque DDoS est encore de d'exécution, comme le montre le log suivant :

4.9.1 Au niveau de FortiGate

Figure 4-33 logs collecter pare FortiGate

Ces logs fournissent des détails sur une communication bloquée par le pare-feu FortiGate01, avec des informations sur les adresses IP source et destination, les ports, les interfaces, les actions prises et d'autres attributs associés à la communication.

L'explication de chaque partie du Log

- "srcip-10.10.1.100" : C'est l'adresse IP source mentionnée dans le log.

- "srcport-54642" : C'est le port source associé à l'adresse IP source.

- "srcintf "port"" : Il s'agit de l'interface source associée à l'événement, dans ce cas "port".

- "dstip 10.10.1.1" : C'est l'adresse IP de destination mentionnée dans le log.

- "dstport-53" : C'est le port de destination associé à l'adresse IP de destination.

- "action"deny"" : Cela indique que l'action prise pour ce trafic est "deny" (refusé ou bloqué).

Ces informations spécifiques montrent qu'il y a eu une tentative de connexion refusée depuis l'adresse IP source 10.10.1.100 vers l'adresse IP de destination 10.10.1.1 sur le port 53, qui est généralement utilisé pour les requêtes DNS.

4.9.2 Au niveau d'Ubuntu

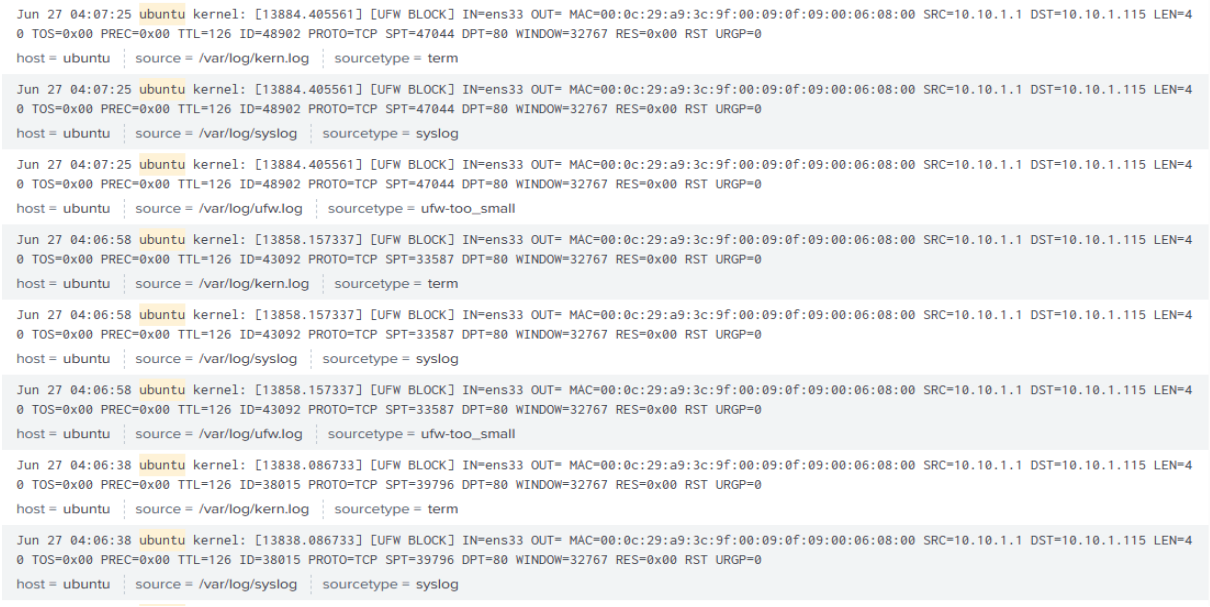


Figure 4-34 logs collecter pare Ubuntu

Ce log indique qu'un paquet TCP provenant de l'adresse IP source 10.10.1.1 avec un port source de 47044 a été bloqué par le pare-feu lorsqu'il était destiné à l'adresse IP de destination 10.10.1.115 sur le port 80. Le paquet contenait le flag RST, indiquant une demande de réinitialisation de la connexion TCP.

L'explication de chaque partie du Log

- "[UFW BLOCK) IN ens33 OUT MAC-00:0c:29:9:30:57:00:09:07:09:00:06:08:00" : Cela indique qu'un événement de blocage a été enregistré par UFW (Uncomplicated Firewall) sur l'interface réseau "ens33". Le blocage a été effectué sur la base de l'adresse MAC source ("MAC-00:0c:29:9:30:57") et de l'adresse MAC de destination ("MAC-00:09:07:09:00:06:08:00").

- "SRC-10.10.1.1" : C'est l'adresse IP source mentionnée dans le log, indiquant l'origine de la tentative de communication.

- "DST-10.10.1.115" : C'est l'adresse IP de destination mentionnée dans le log, indiquant la cible de la tentative de communication.

- "PROTO-TCP" : Cela indique que le protocole utilisé pour la tentative de communication était TCP.

- "SPT-47044" : C'est le port source associé à la tentative de communication, indiquant le port à partir duquel la communication a été initiée.

- "DPT-80" : C'est le port de destination associé à la tentative de communication, indiquant le port sur lequel la communication était destinée à se connecter (port 80 correspondant généralement au protocole HTTP).

- "RST" : Cela indique que le paquet de réinitialisation (RST) a été émis pour bloquer la tentative de communication.

4.9.3 Au niveau routeur Cisco

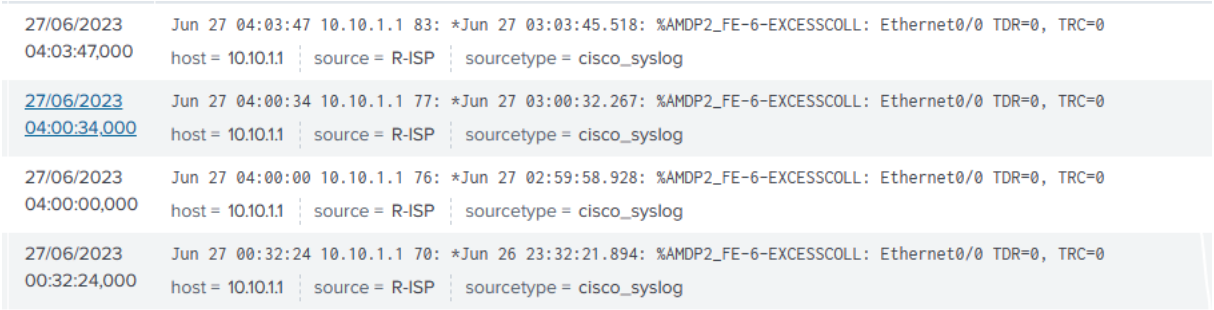


Figure 4-35 logs collecter pare router R-ISP

Ces logs indiquent qu'une collision excessive a été détectée sur l'interface Ethernet 0/0 du périphérique ayant l'adresse IP 10.10.1.1. Les collisions se produisent lorsque plusieurs périphériques tentent de transmettre des données en même temps sur le même segment de réseau. Cela peut indiquer un problème de congestion ou de connectivité sur le réseau.

L'explication de chaque partie du Log

- "XAMDP2_FE-6-EXCESSCOLL" : C'est le code d'événement spécifique qui indique la détection d'un nombre excessif de collisions sur l'interface Ethernet0/0.

- "Ethernet0/0" : C'est le nom de l'interface réseau concernée par l'événement, où les collisions ont été détectées.

4.10 Contre mesure

4.10.1 Activation des alertes au niveau de Splunk

Afin de réagir rapidement en cas d'événement suspect (comme une attaque), nous avons configuré Splunk pour qu'il nous envoie des alertes de notification sur notre email.

La configuration d'une alerte dans Splunk est démontrée dans les figures suivantes :

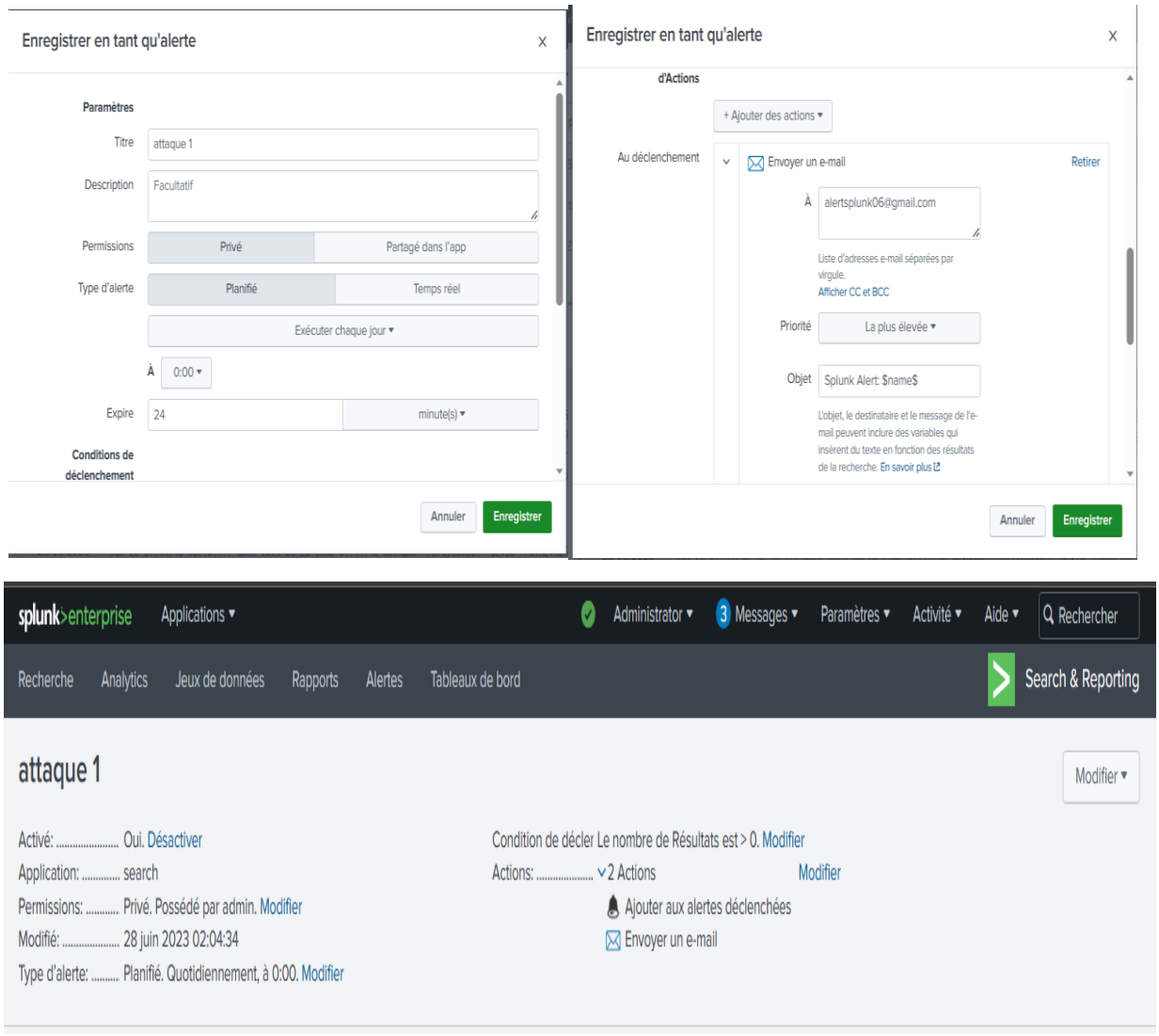
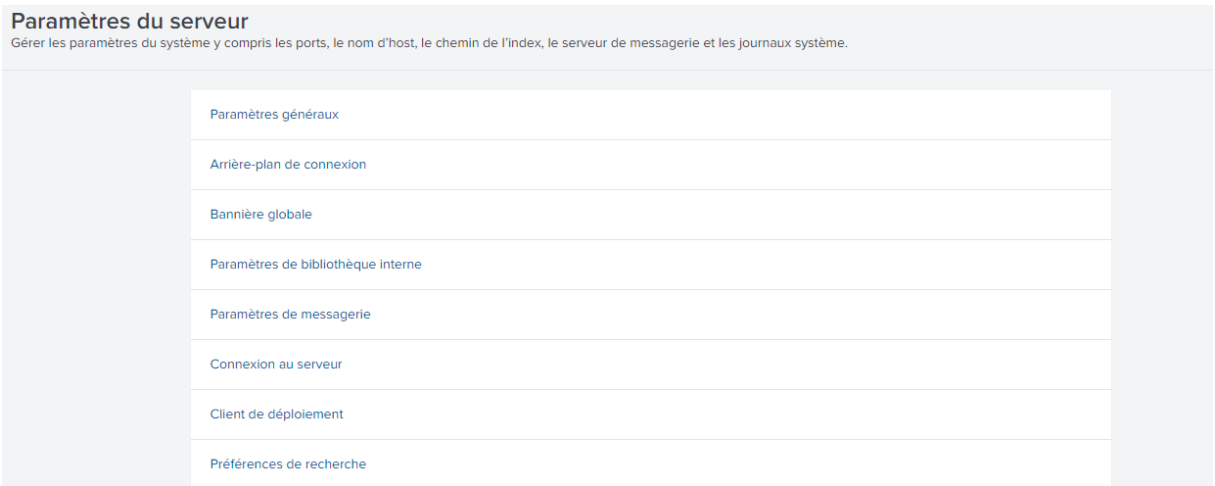


Figure 4-36 Création d'alertes



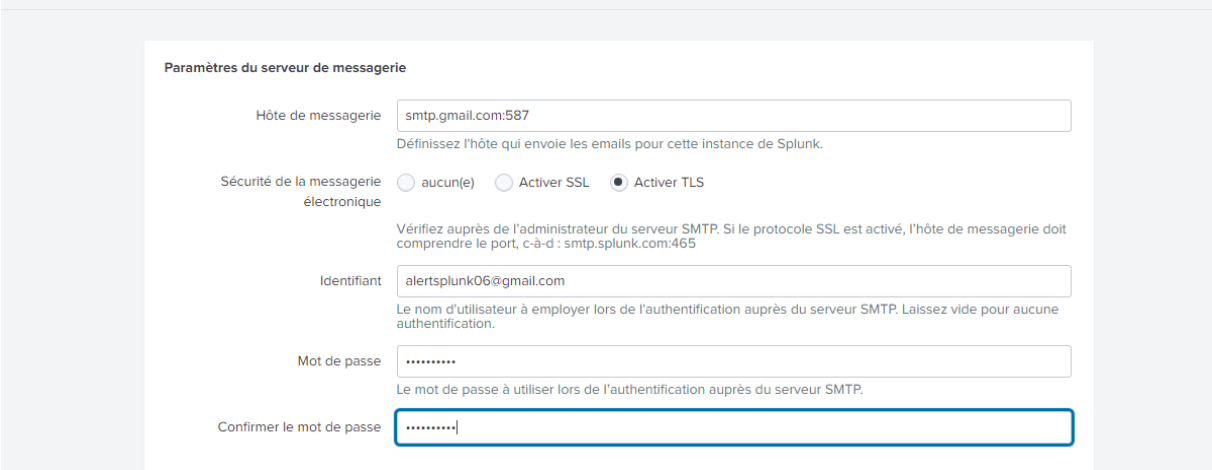
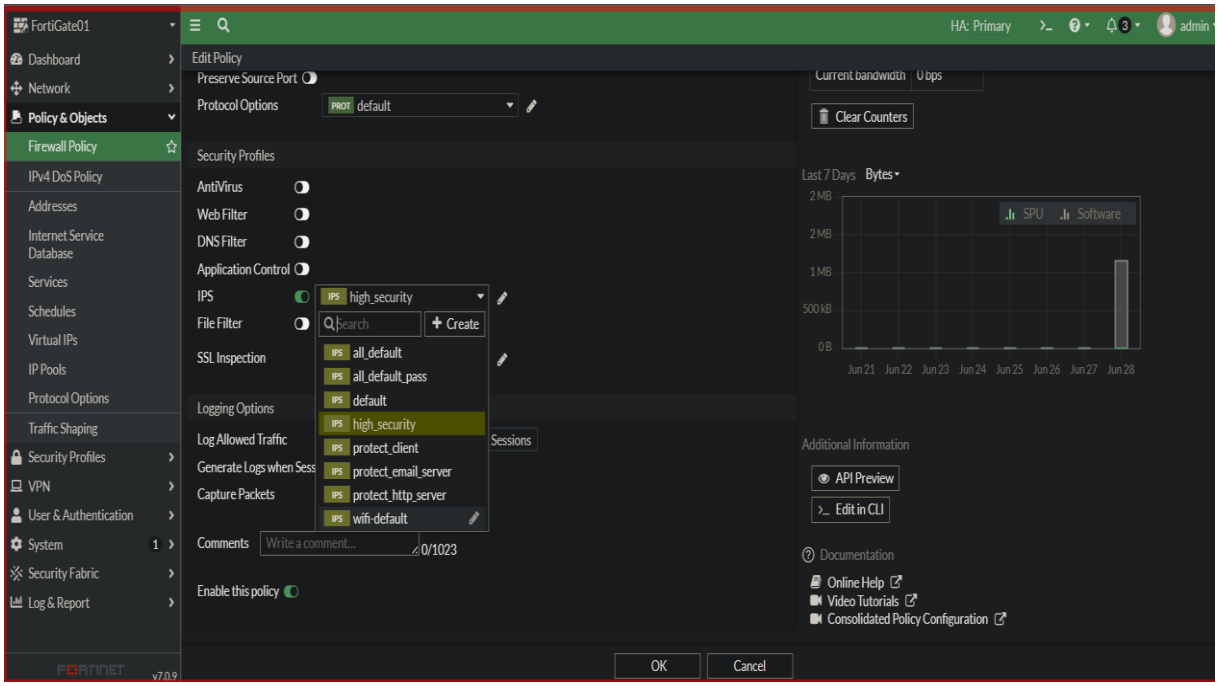


Figure 4-37 Configuration l'email

4.10.2 Configuration du pare-feu FortiGate

- Activation de l'IPS pour permettre le blocage et la réponse contre les attaques en temps réel avec l'utilisation du mode high security.
- Activation de filtre DNS qui va nous permettre de bloquer les requêtes suspectes, de limiter le trafic malveillant, de détecter les attaques et les atténuer.



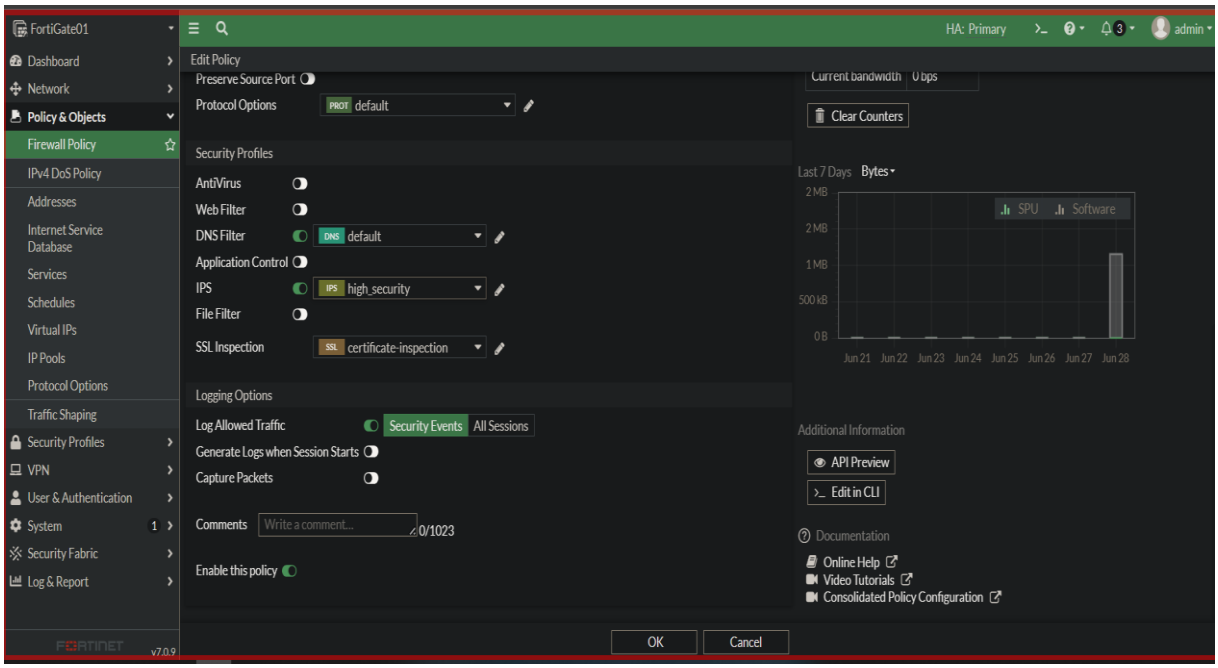


Figure 4-38 Activation d'IPS et DNS Filter

Conclusion

Au cours de ce chapitre, nous avons exposé les éléments essentiels de notre environnement de travail. Nous avons décrit la procédure d'installation, déploiement et de configuration de notre outil de surveillance. Nous avons également abordé la collecte et l'analyse des Log, ainsi que la création de tableaux de bord. Enfin, nous avons mis à l'épreuve notre solution de surveillance en effectuant un test d'intrusion, et nous avons simulé une démarche d'équipe de SOC pour contrer une attaque en mettant en place des contre-mesures.

Conclusion générale

En conclusion de ce mémoire de fin d'étude, nous avons exploré divers aspects cruciaux liés aux réseaux informatiques et à leur sécurité. Le premier chapitre nous a permis d'acquérir une compréhension générale des réseaux, en examinant leurs différents types et en soulignant l'importance des mesures de sécurité pour les protéger des attaques et des vulnérabilités. Ce fondement nous a préparés à aborder les défis spécifiques rencontrés par l'entreprise Campus NTS dans le deuxième chapitre, où nous avons proposé des solutions efficaces pour répondre à leurs besoins de sécurité.

Le troisième chapitre s'est concentré sur les technologies essentielles d'un SOC (Security Operations Center) pour assurer la sécurité des entreprises. Nous avons mis en avant l'intégration du SOC, du SIEM (Security Information and Event Management) et de l'analyse des fichiers log, soulignant ainsi comment ces combinaisons peuvent renforcer la posture de sécurité des organisations et améliorer leur capacité à détecter et à réagir rapidement et efficacement aux menaces. Dans notre étude, nous avons choisi Splunk comme solution SIEM qui offre une plateforme puissante qui permet la collecte, l'agrégation et l'analyse des données de sécurité provenant de diverses sources, ce qui permet une détection proactive des menaces et une réponse rapide aux incidents de sécurité.

Enfin, dans le dernier chapitre, nous avons décrit notre environnement de travail et l'architecture choisie pour notre étude. Nous avons expliqué en détail les étapes d'installation des différents outillages utilisés, ainsi que la collecte et l'analyse des fichiers journaux. Nous avons également créé des tableaux de bord pour visualiser les données collectées et nous avons effectué des tests pour évaluer l'efficacité de la solution en termes de détection et de prévention des attaques.

Pour conclure, cette étude a permis de mettre en évidence l'importance cruciale de la sécurité des réseaux informatiques et des entreprises. Les connaissances acquises tout au long de ce mémoire offrent une base solide pour poursuivre les travaux futurs dans ce domaine. Il reste encore des défis à relever et des avancées à réaliser, mais nous espérons que ce mémoire contribuera à stimuler davantage la recherche et l'innovation en matière de sécurité des réseaux informatiques et à fournir des solutions toujours plus robustes et efficaces.

Bibliographie

Bibliographie

[1]https://www.eccouncil.org/cybersecurity-exchange/network-security/understand-design-implement-network-security-policies/ consulté le 10/05/2023

[2]https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html consulté le 15/03/2023

[3]https://www.comparitech.com/net-admin/ids-vs-ips/ consulté le 15/03/2023

[4]https://www.forcepoint.com/cyber-edu/firewall consulté le 25/03/2023

[5]https://www.techtarget.com/searchsecurity/feature/The-five-different-types-of-firewalls consulté le 26/04/2023

[6] https://phoenixnap.com/kb/linux-security consulté le 01/04/2023

[7]https://learn.microsoft.com/en-us/windows/security/operating-system consulté le 04/04/2023

[8] PILLOU, Jean-François ; BAY, Jean-Philippe. Tout sur la sécurité informatique. Livre. Dunod, 2020.

[9] Berkani, D., & Bouzeria, M. (2021/2022). Mémoire de fin d'étude sur le thème "Étude et mise en place d'une infrastructure réseau sécurisée". Université Abderrahmane Mira de Béjaïa

[10] ACISSI, Marion ; AGÉ, Sébastien ; BAUDRU, Robert ; CROCFER, Franck ; EBEL, Jérôme ; HENNECART, Sébastien ; LASSON, David PUCHE. Sécurité informatique et Ethical Hacking : Apprendre l'attaque pour mieux se défendre. Livre. Éditions ENI, 20 octobre 2009.

[11] https://www.microsoft.com/fr-fr/security/business/security-101/what-is-siem consulté le 12/05/2023

[12] https://www.logpoint.com/fr/comprendre/c-est-quoi-le-siem consulté le 12/05/2023

[13] Karun Subramanian. Practical Splunk Search Processing Language: A Guide for Mastering SPL Commands for Maximum Efficiency and Outcome. Springer, 2020 consulté le 16/05/20223

[14] https://itsocial.fr/tribunes/tribunes-par-thematique/ae-cybersecurite/comprendre-les-avantages-et-limites-du-siem/ consulté le 16/05/20223

[15] https://www.ibm.com/topics/siem consulté le 19/05/2023

[16] https://www.alienvault.com/products/ossim.3/5 consulté le 19/05/2023

[17] https://securityonion.net/3/5 consulté le 19/05/2023

Bibliographie

[18] https://www.elastic.co/what-is/elk-stack3/5 consulté le 20/05/2023

[19] https://securityonionsolutions.com/software/3/5 consulté le 20/05/2023

[20] https://logrhythm.com/solutions/siem/ consulté le 21/05/2023

[21] https://www.splunk.com/en_us/products/splunk-security-operations-suite consulté le 21/05/2023

[22] https://www.logpoint.com/fr/blog/security-operations-center-soc/ consulté le 23/05/2023

[23] https://www.advens.fr/ consulté le 24/05/2023

[24] https://www.logpoint.com/fr/blog/security-operations-center-soc consulté le 24/05/2023

[25] https://www.alphorm.com / consulté le 02/06/2023

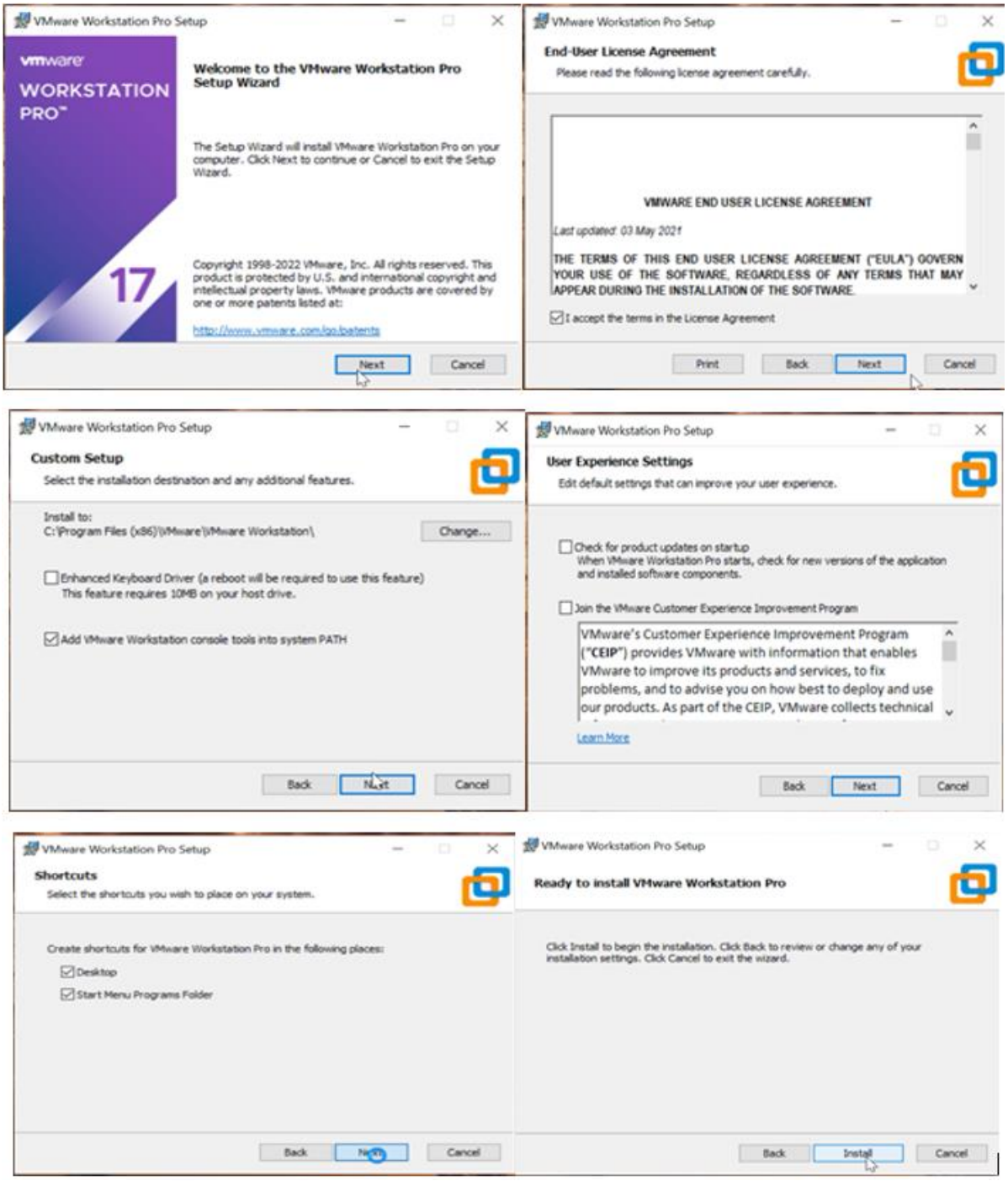
[26] https://www.splunk.com/en_us/blog/learn/what-splunk-does.html consulté le 26/05/2023

Annexe

Annexe

Installation de VMware Workstation

VMware nous Permet de créer et de gérer des machines virtuelles sur un seul ordinateur physique, voilà ces étapes d'installation :



Annexe

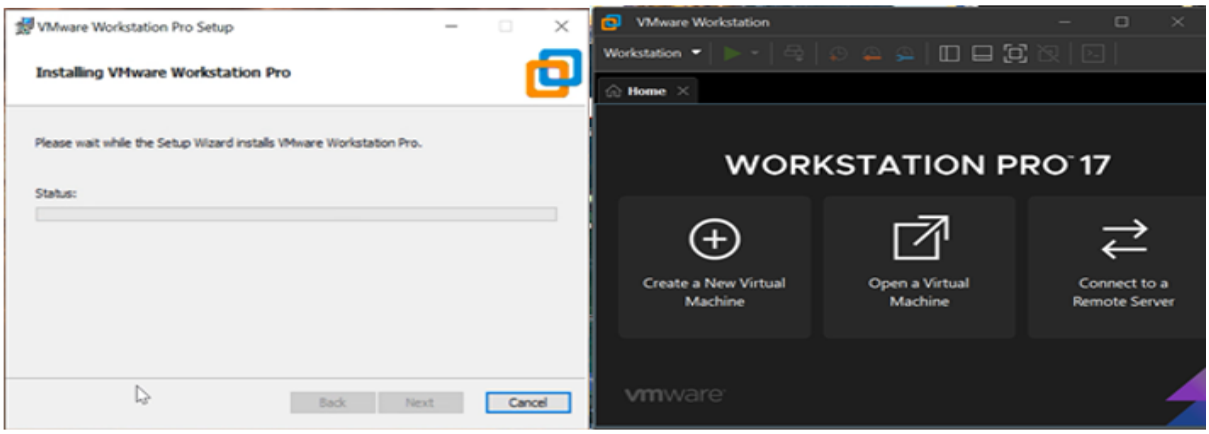
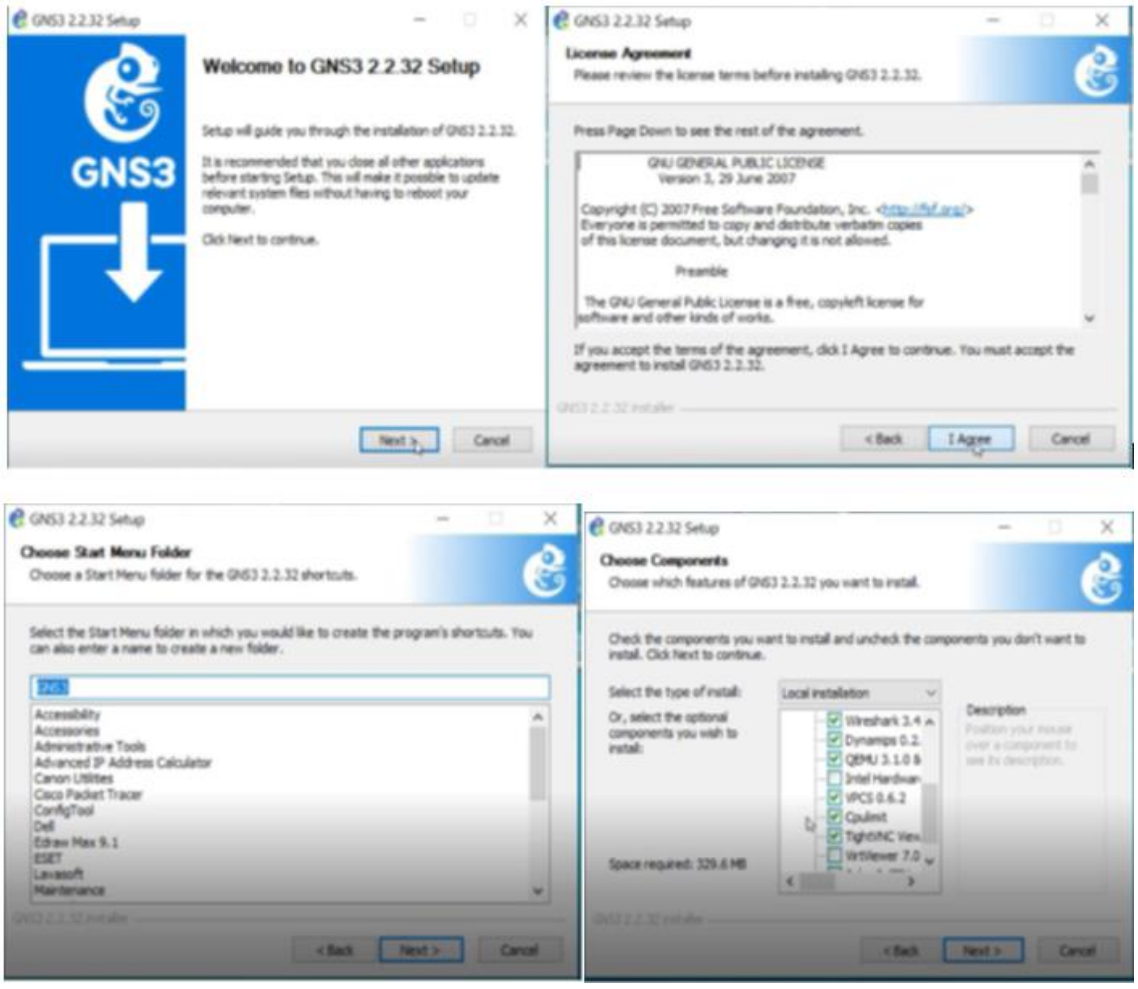


Figure 0-39 Installation de VMware

Installation de GNS3

L'installation de GNS3 est assez simple. Après avoir le télécharger en lance l'installation, la fenêtre de configuration apparaît et nous suivons les instructions ci-dessous :



Annexe

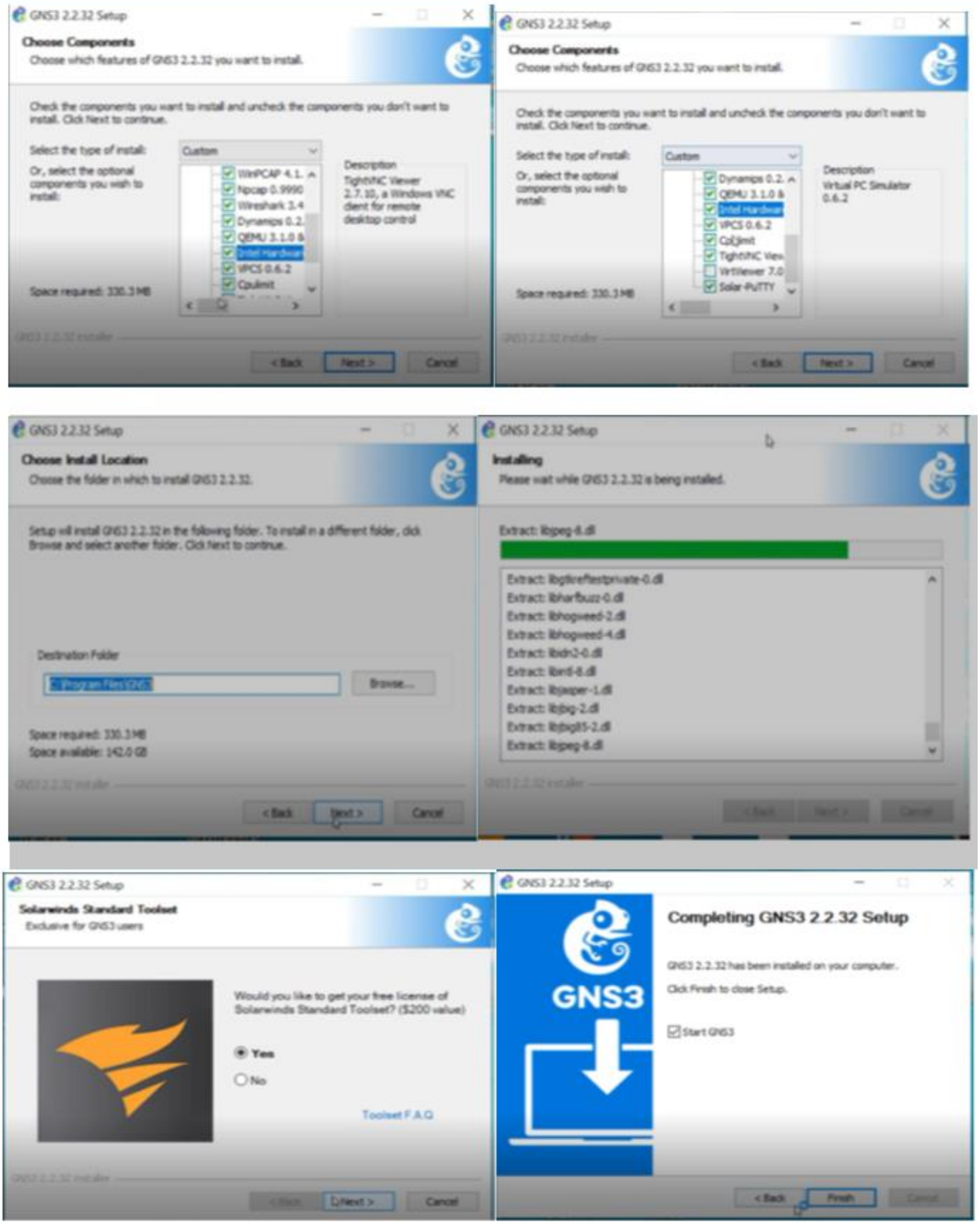


Figure 4-40 Installation de GNS3

Annexe

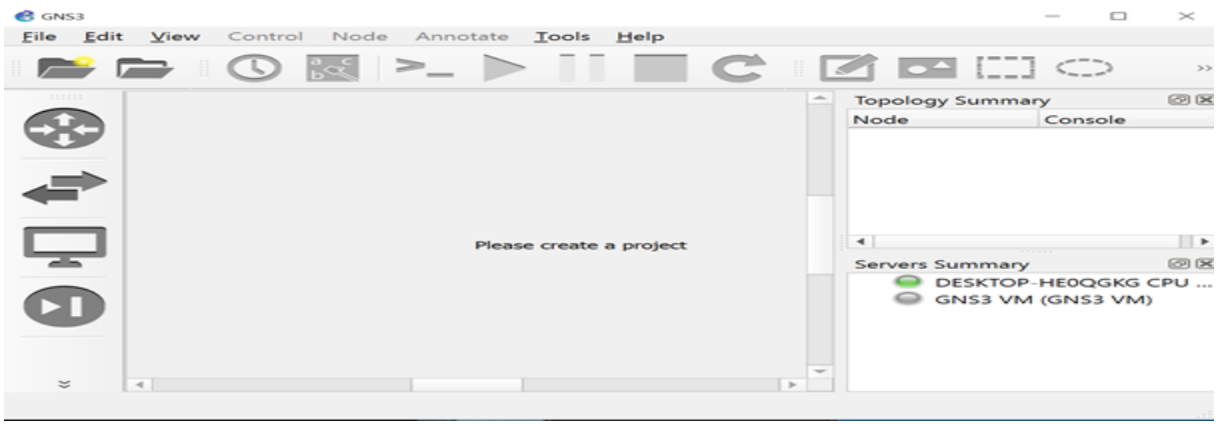
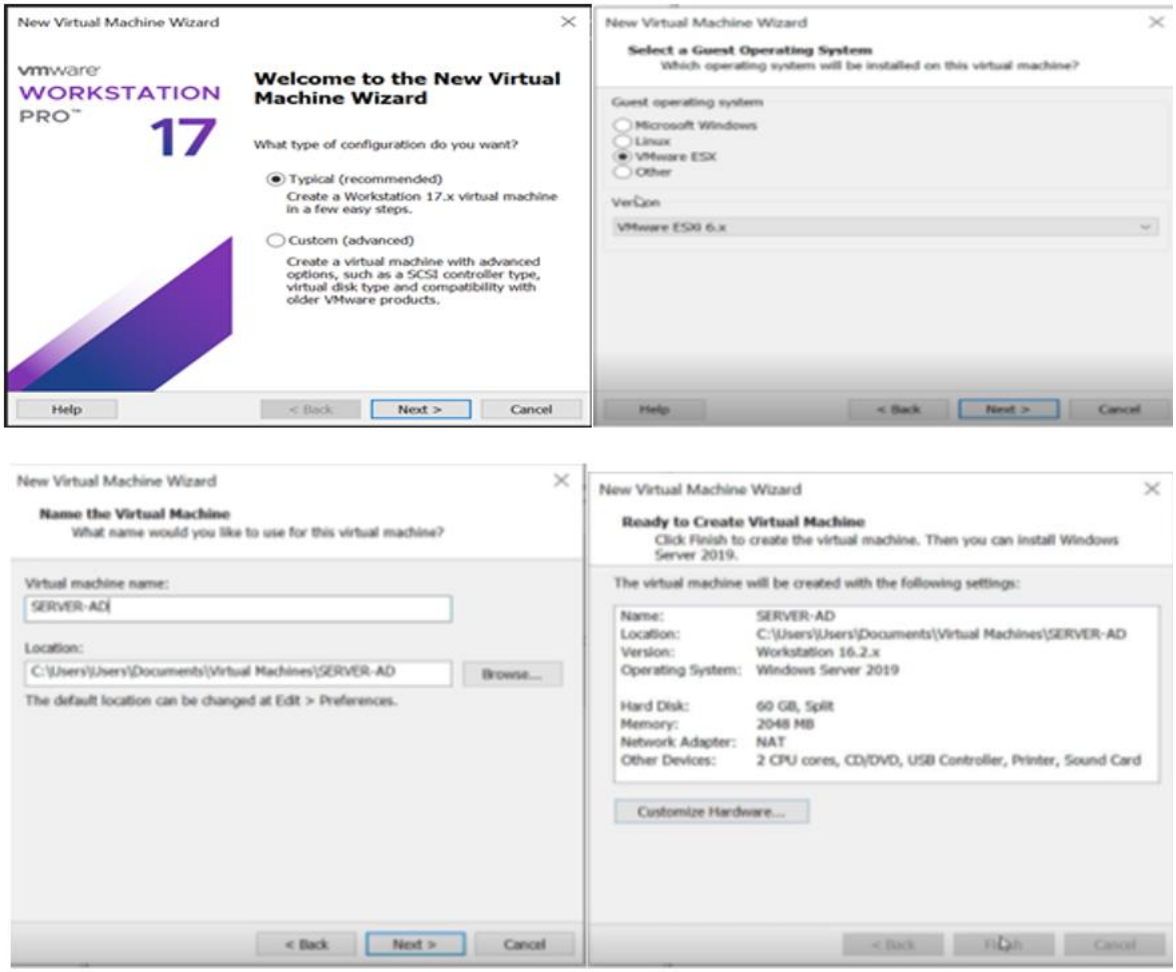


Figure 4-41 L'interface de GNS3

Installation Windows Serveur 2022

Dans cette section, nous aborderons les différentes étapes de l'installation de Windows Server 2022.



Annexe

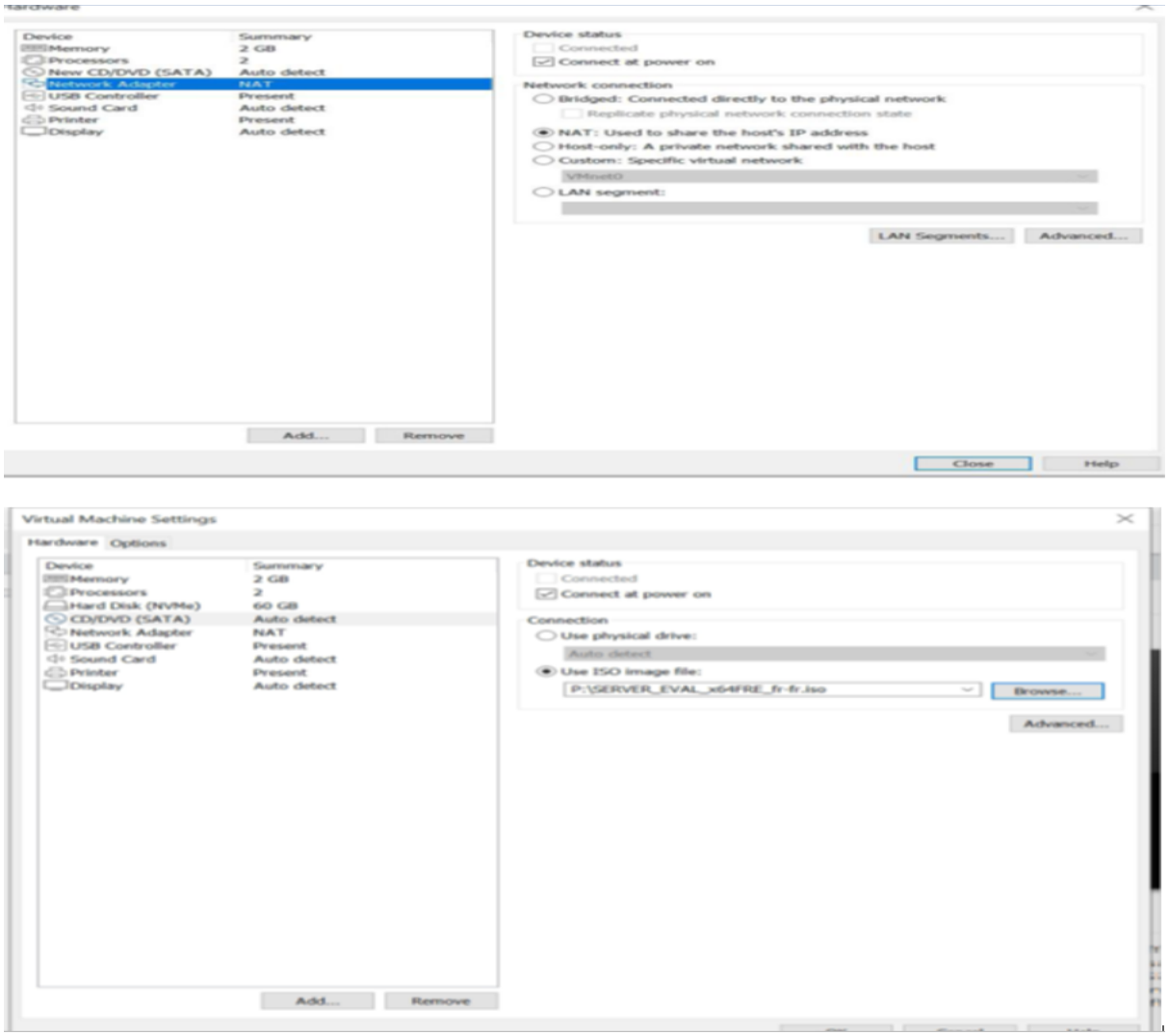


Figure 4-42 Installation de Windows serveur 2022 sous VMware

Annexe

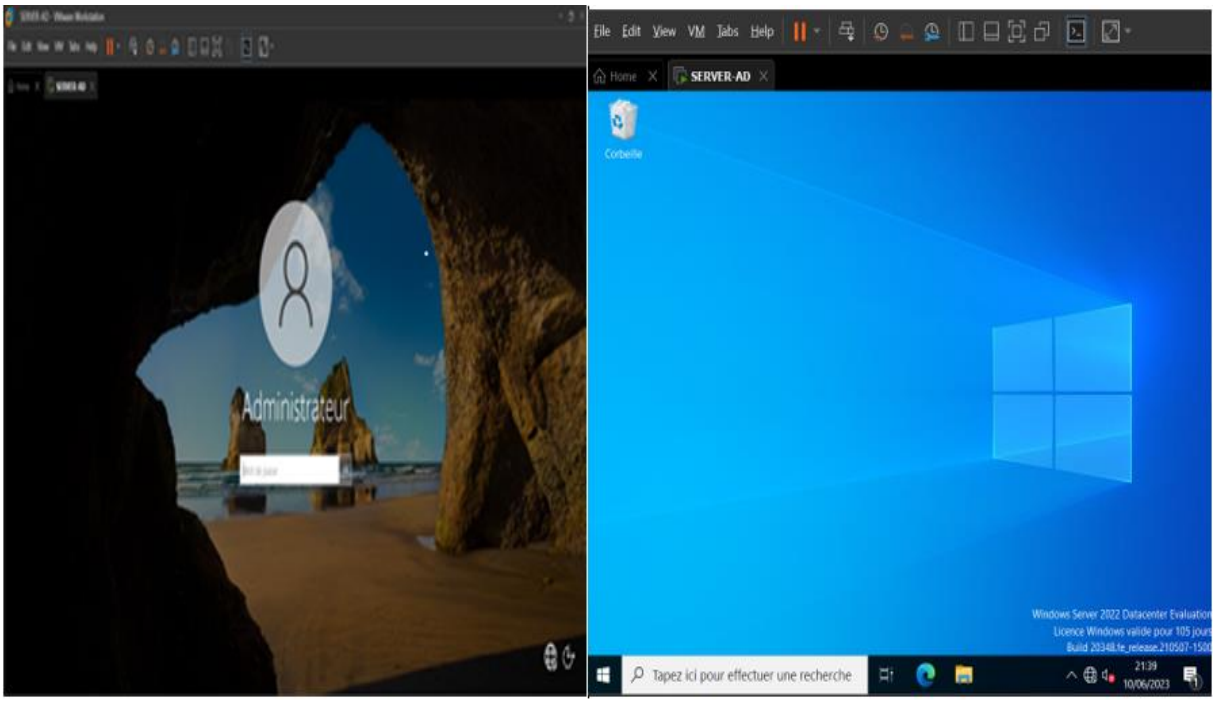


Figure 4-43 l'interface Windows serveur 2022

Installation de la machine Ubuntu

Dans cette partie, nous allons voir les différentes étapes d'installations d'Ubuntu :

- Télécharger le fichier iso d'Ubuntu dans le site officiel d'Ubuntu.
- Suivez les étapes montrées dans les figures suivantes

Annexe

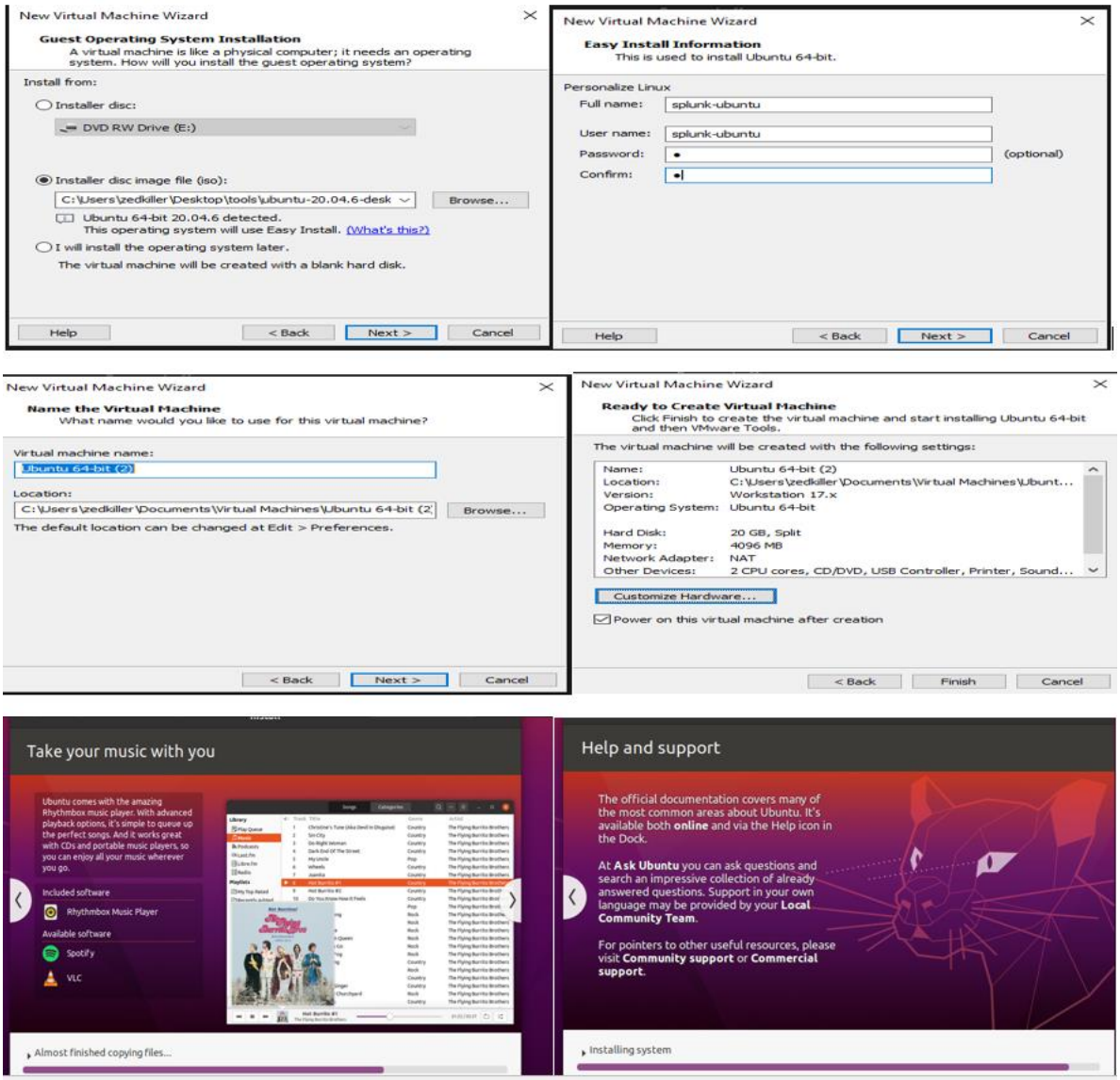


Figure 4-44 L'installation d'Ubuntu

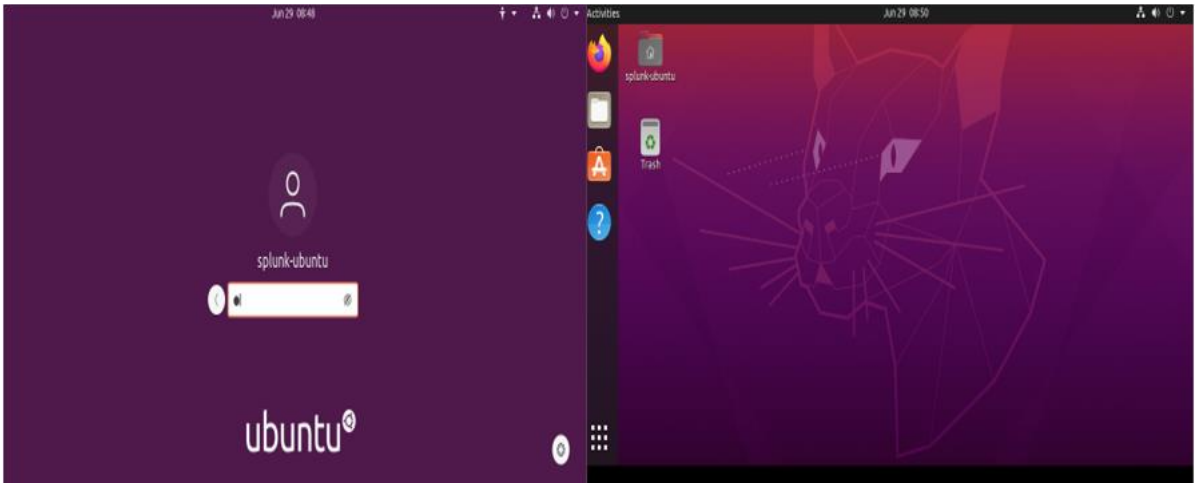
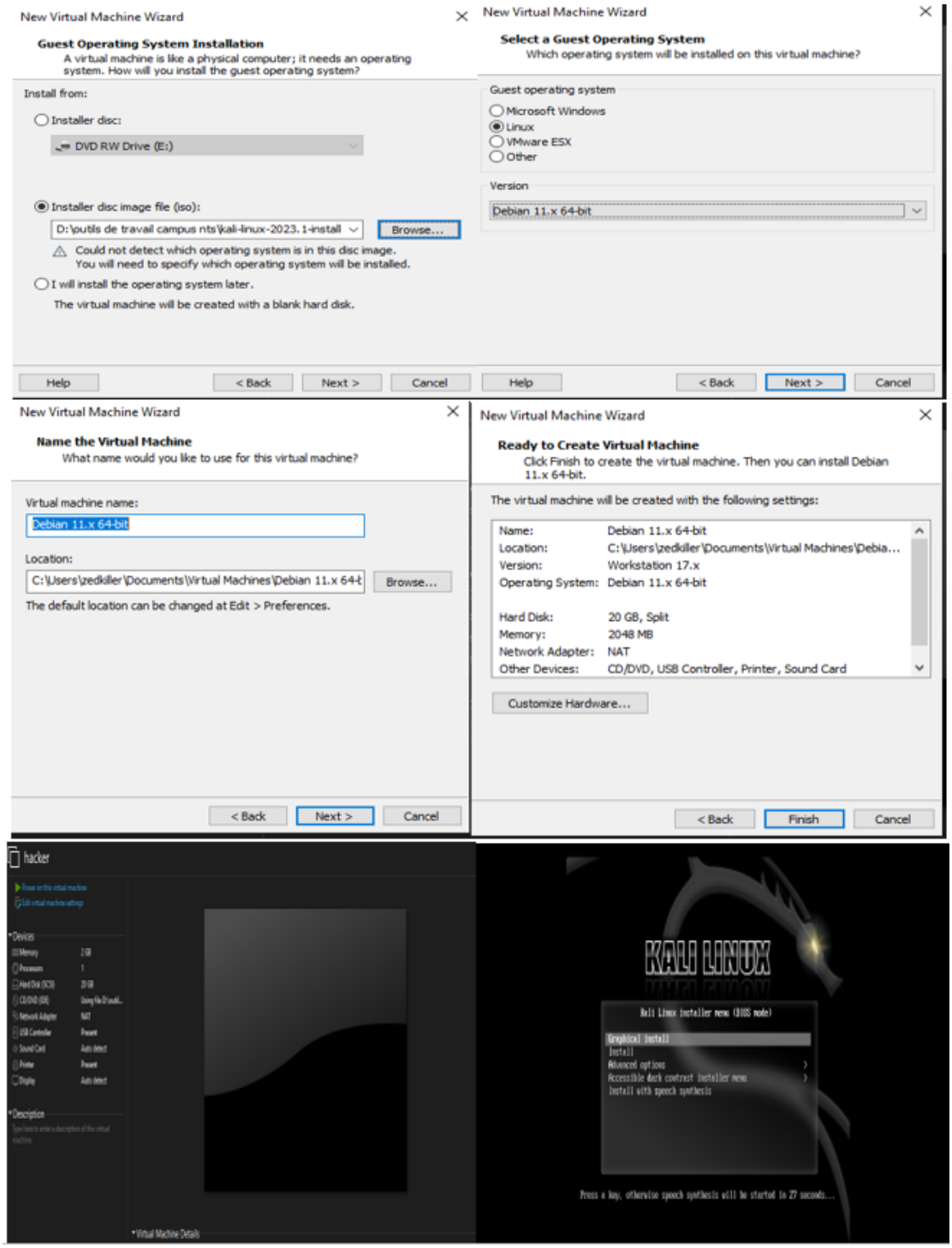


Figure 4-45 Interface Ubuntu

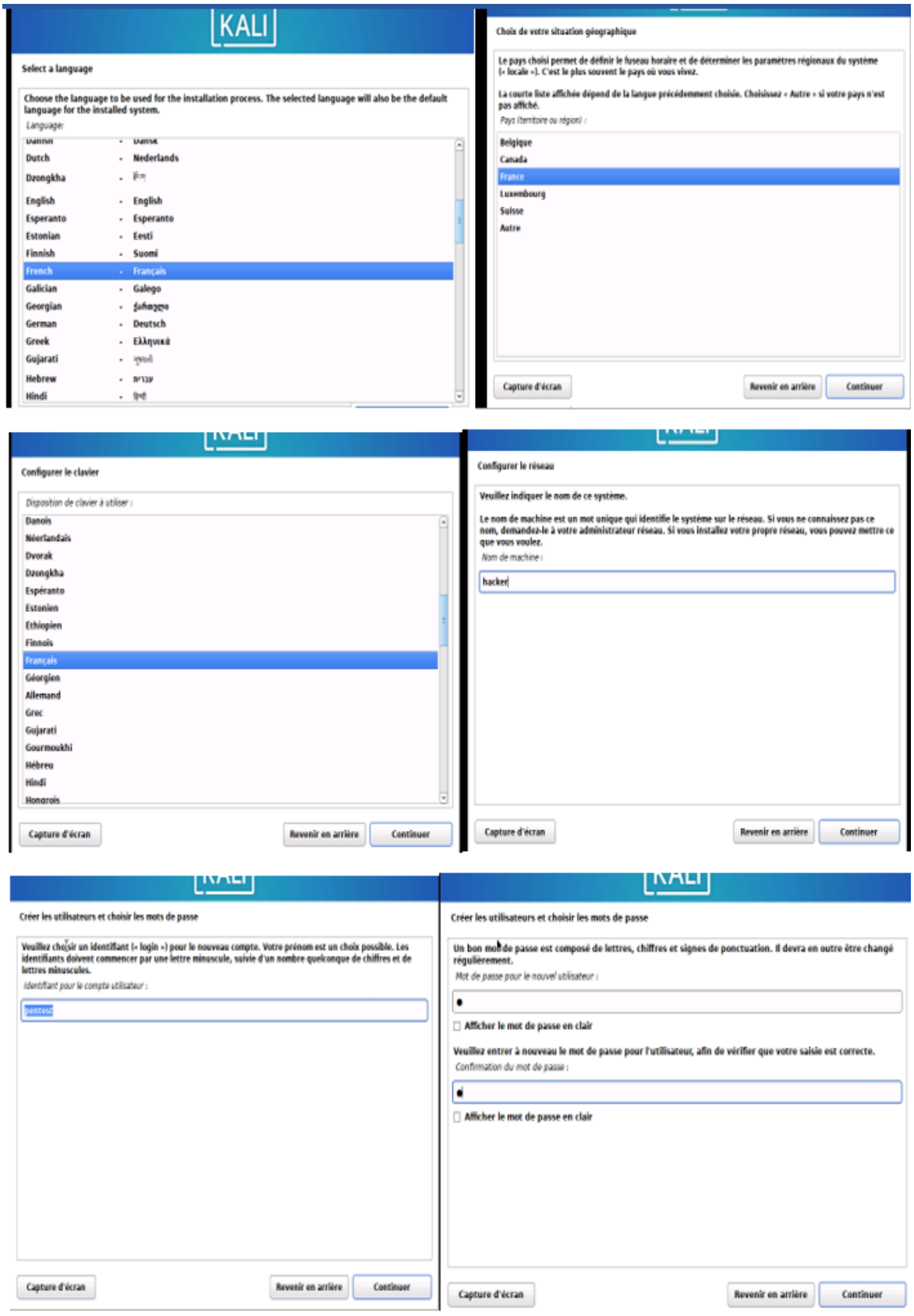
Annexe

Installation de la machine kali linux

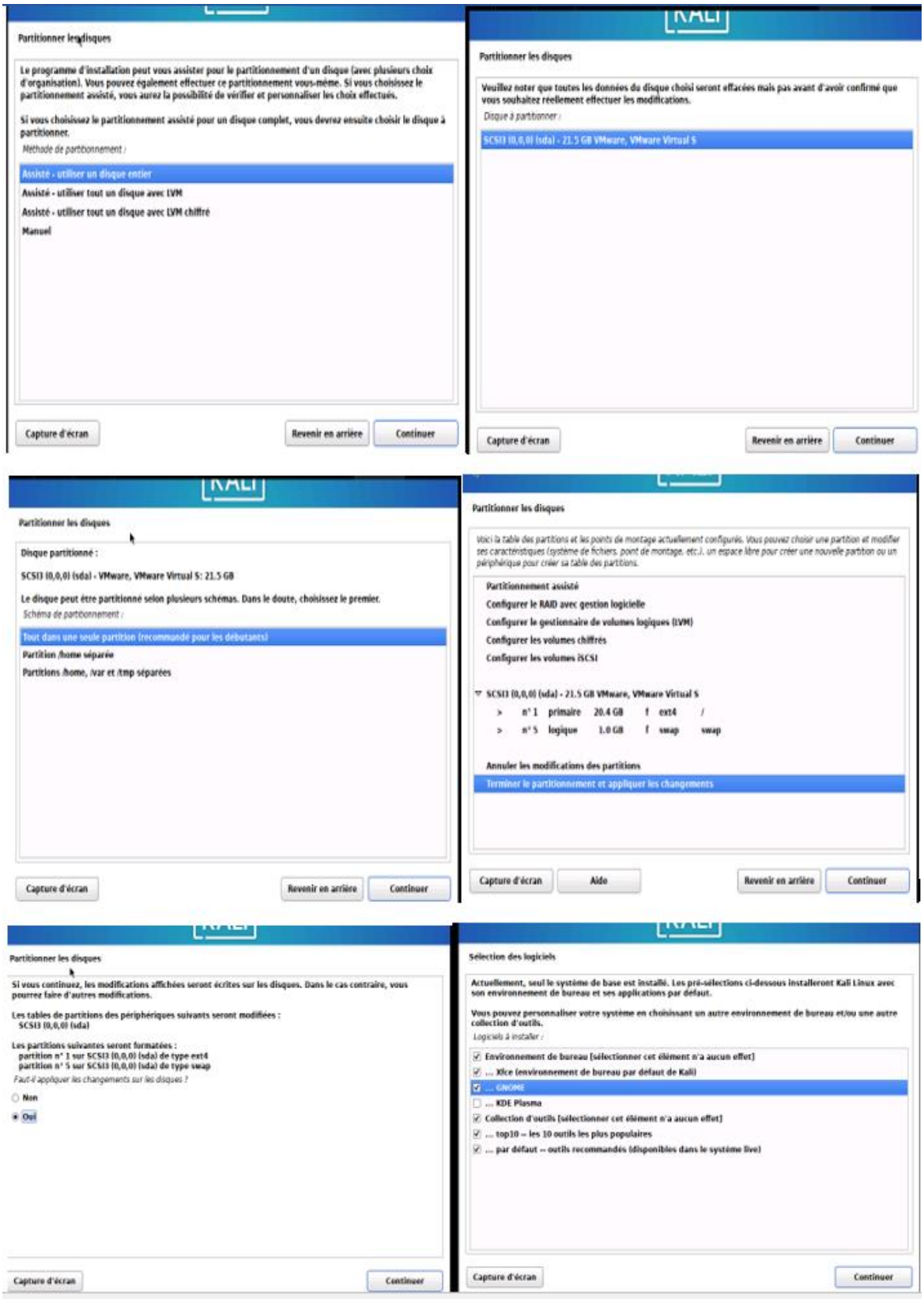
Dans les figures suivantes, nous allons voir les différentes étapes d'installations de kali linux



Annexe


KALI
Select a language
Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.
Language:
Dutch - Nederlands
Dzongkha -
English - English
Esperanto - Esperanto
Estonian - Eesti
Finnish - Suomi
French - Français
Galician - Galego
Georgian -
German - Deutsch
Greek - Ελληνικά
Gujarati -
Hebrew -
Hindi -
Choix de votre situation géographique
Le pays choisi permet de définir le fuseau horaire et de déterminer les paramètres régionaux du système (« locale »). C'est le plus souvent le pays où vous vivez.
La courte liste affichée dépend de la langue précédemment choisie. Choisissez « Autre » si votre pays n'est pas affiché.
Pays (territoire ou région) :
Belgique
Canada
France
Luxembourg
Suisse
Autre
Capture d'écran
Revenir en arrière
Continuer
Configurer le clavier
Disposition de clavier à utiliser :
Danois
Néerlandais
Dvorak
Dzongkha
Espéranto
Estonien
Éthiopien
Finnois
Français
Géorgien
Allemand
Grec
Gujarati
Gourmoukhi
Hébreu
Hindi
Hongrois
Configurer le réseau
Veuillez indiquer le nom de ce système.
Le nom de machine est un mot unique qui identifie le système sur le réseau. Si vous ne connaissez pas ce nom, demandez-le à votre administrateur réseau. Si vous installez votre propre réseau, vous pouvez mettre ce que vous voulez.
Nom de machine :
hacker
Créer les utilisateurs et choisir les mots de passe
Veuillez choisir un identifiant (« login ») pour le nouveau compte. Votre prénom est un choix possible. Les identifiants doivent commencer par une lettre minuscule, suivie d'un nombre quelconque de chiffres et de lettres minuscules.
Identifiant pour le compte utilisateur :
pentest
Créer les utilisateurs et choisir les mots de passe
Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.
Mot de passe pour le nouvel utilisateur :
Afficher le mot de passe en clair
Veuillez entrer à nouveau le mot de passe pour l'utilisateur, afin de vérifier que votre saisie est correcte.
Confirmation du mot de passe :
Afficher le mot de passe en clair

Annexe


Partitionner les disques
Le programme d'installation peut vous assister pour le partitionnement d'un disque (avec plusieurs choix d'organisation). Vous pouvez également effectuer ce partitionnement vous-même. Si vous choisissez le partitionnement assisté, vous aurez la possibilité de vérifier et personnaliser les choix effectués.
Si vous choisissez le partitionnement assisté pour un disque complet, vous devrez ensuite choisir le disque à partitionner.
Méthode de partitionnement :
Assisté - utiliser un disque entier
Assisté - utiliser tout un disque avec LVM
Assisté - utiliser tout un disque avec LVM chiffré
Manuel
Capture d'écran
Revenir en arrière
Continuer
Partitionner les disques
Veuillez noter que toutes les données du disque choisi seront effacées mais pas avant d'avoir confirmé que vous souhaitez réellement effectuer les modifications.
Disque à partitionner :
SCSI3 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S
Capture d'écran
Revenir en arrière
Continuer
Partitionner les disques
Disque partitionné :
SCSI3 (0,0,0) (sda) - VMware, VMware Virtual S: 21.5 GB
Le disque peut être partitionné selon plusieurs schémas. Dans le doute, choisissez le premier.
Schéma de partitionnement :
Tout dans une seule partition (recommandé pour les débutants)
Partition /home séparée
Partitions /home, /var et /tmp séparées
Capture d'écran
Revenir en arrière
Continuer
Partitionner les disques
Voici la table des partitions et les points de montage actuellement configurés. Vous pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique pour créer sa table des partitions.
Partitionnement assisté
Configurer le RAID avec gestion logicielle
Configurer le gestionnaire de volumes logiques (LVM)
Configurer les volumes chiffrés
Configurer les volumes iSCSI
SCSI3 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S
n° 1 primaire 20.4 GB f ext4 /
n° 5 logique 1.0 GB f swap swap
Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements
Capture d'écran
Aide
Revenir en arrière
Continuer
Partitionner les disques
Si vous continuez, les modifications affichées seront écrites sur les disques. Dans le cas contraire, vous pourrez faire d'autres modifications.
Les tables de partitions des périphériques suivants seront modifiées :
SCSI3 (0,0,0) (sda)
Les partitions suivantes seront formatées :
partition n° 1 sur SCSI3 (0,0,0) (sda) de type ext4
partition n° 5 sur SCSI3 (0,0,0) (sda) de type swap
Faut-il appliquer les changements sur les disques ?
Non
Oui
Capture d'écran
Continuer
Sélection des logiciels
Actuellement, seul le système de base est installé. Les pré-sélections ci-dessous installeront Kali Linux avec son environnement de bureau et ses applications par défaut.
Vous pouvez personnaliser votre système en choisissant un autre environnement de bureau et/ou une autre collection d'outils.
Logiciels à installer :
Environnement de bureau (sélectionner cet élément n'a aucun effet)
... Xfce (environnement de bureau par défaut de Kali)
... GNOME
... KDE Plasma
Collection d'outils (sélectionner cet élément n'a aucun effet)
... top10 -- les 10 outils les plus populaires
... par défaut -- outils recommandés (disponibles dans le système live)
Capture d'écran
Continuer

Annexe

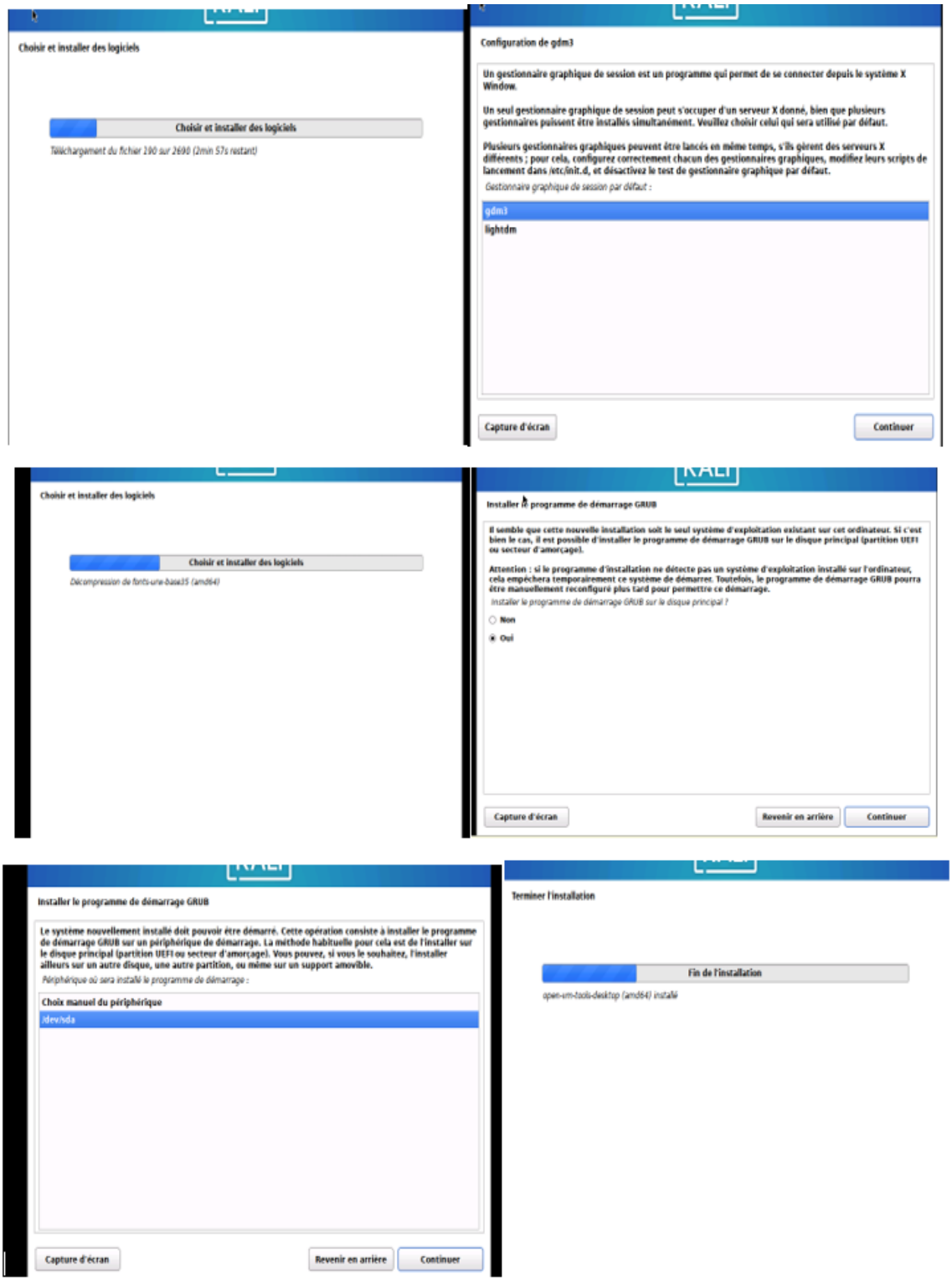


Figure 4-46 installation kali linux

Annexe

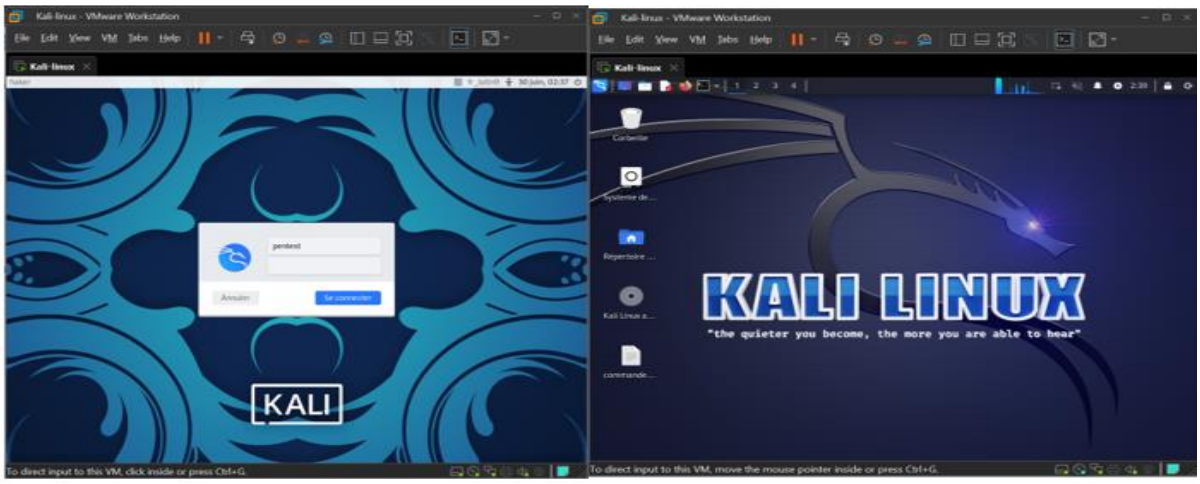
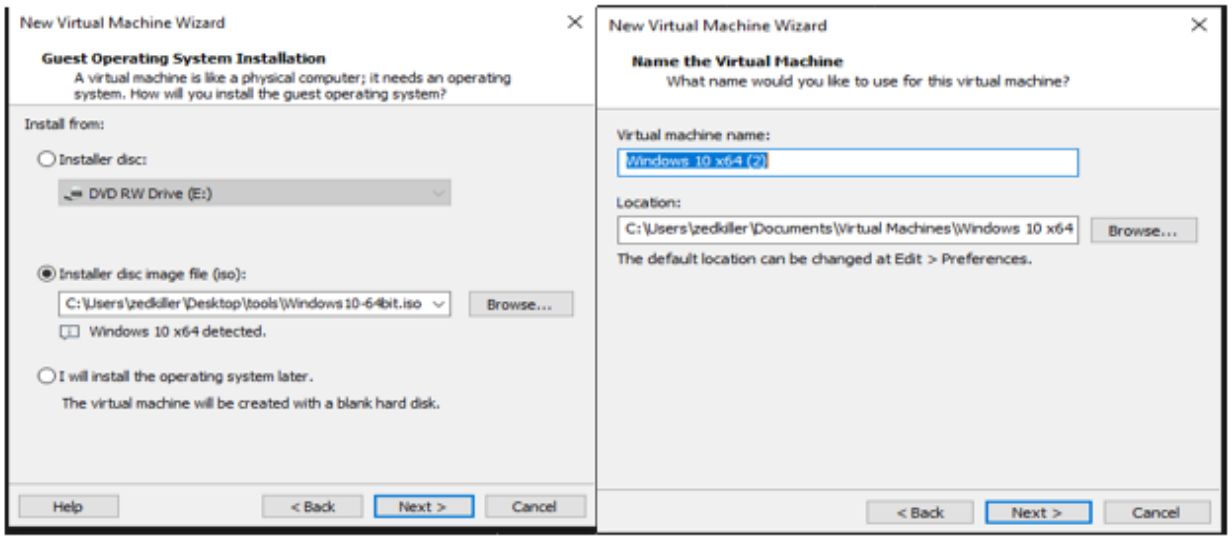
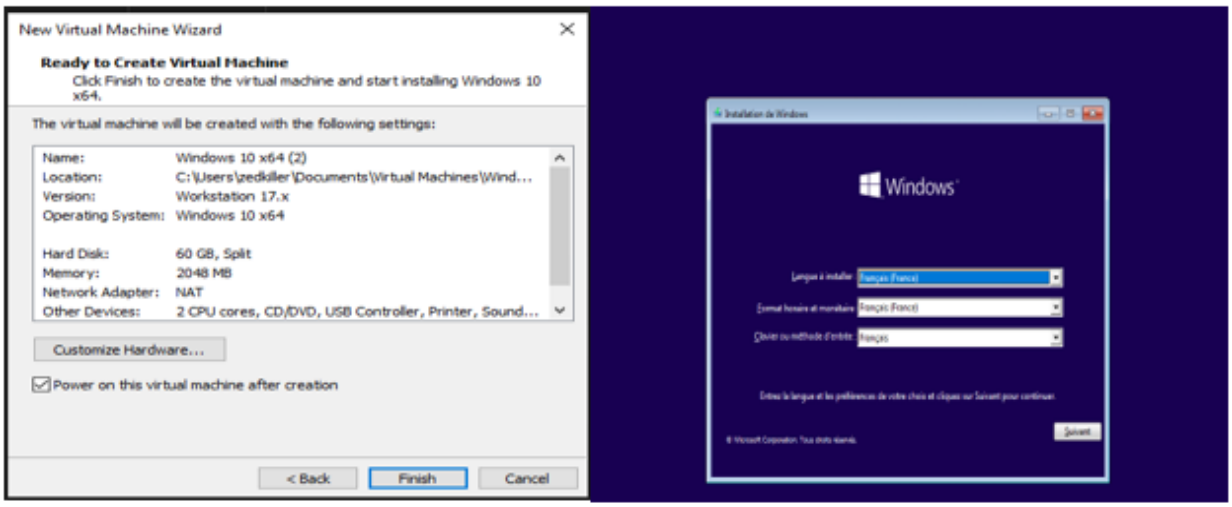


Figure 4-47 interface kali linux

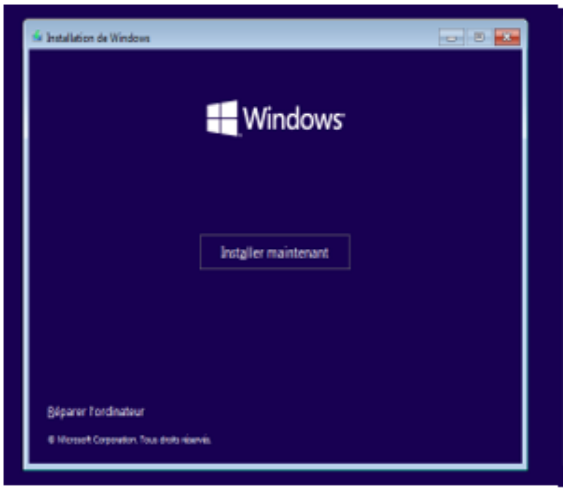
Installation de la machine Windows 10

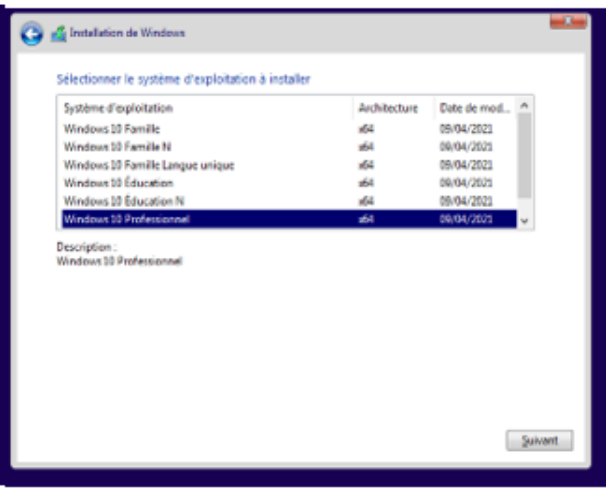
Dans les figures suivantes, nous allons voir les différentes étapes d'installations de Windows 10

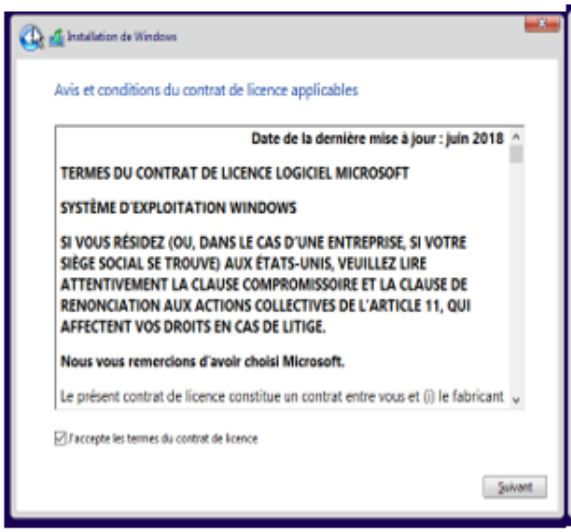


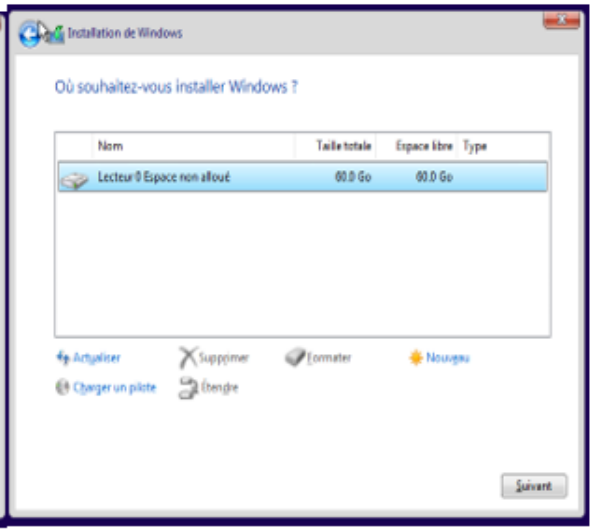


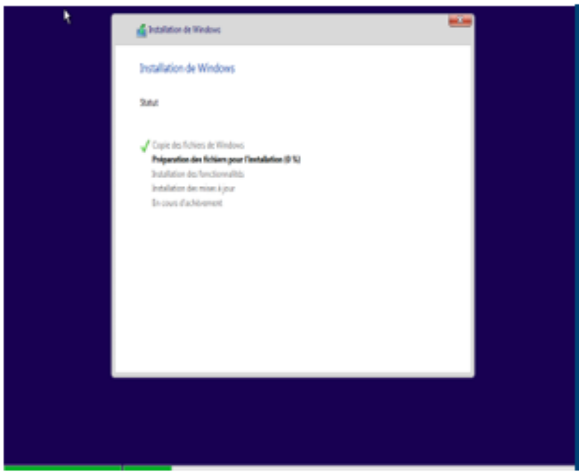
Annexe

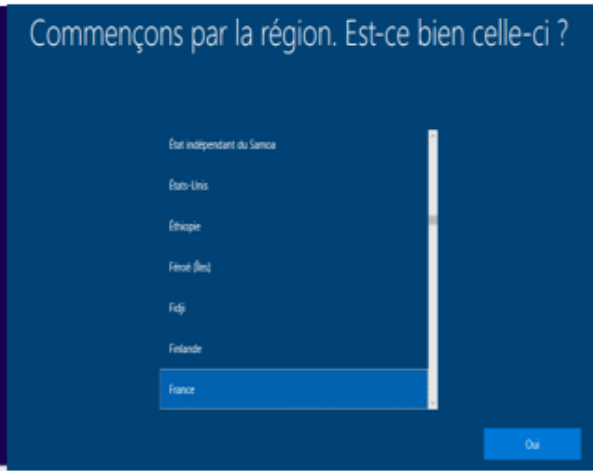

Installation de Windows
Windows
Installer maintenant
Réparer l'ordinateur


Installation de Windows
Sélectionner le système d'exploitation à installer
Système d'exploitation
Architecture
Date de modi...
Windows 10 Famille
Windows 10 Famille N
Windows 10 Famille Langue unique
Windows 10 Éducation
Windows 10 Éducation N
Windows 10 Professionnel
Description :
Windows 10 Professionnel
Suivant


Installation de Windows
Avis et conditions du contrat de licence applicables
Date de la dernière mise à jour : juin 2018
TERMES DU CONTRAT DE LICENCE LOGICIEL MICROSOFT
SYSTÈME D'EXPLOITATION WINDOWS
SI VOUS RÉSIDEZ (OU, DANS LE CAS D'UNE ENTREPRISE, SI VOTRE SIÈGE SOCIAL SE TROUVE) AUX ÉTATS-UNIS, VEUILLEZ LIRE ATTENTIVEMENT LA CLAUSE COMPROMISSOIRE ET LA CLAUSE DE RENONCIATION AUX ACTIONS COLLECTIVES DE L'ARTICLE 11, QUI AFFECTENT VOS DROITS EN CAS DE LITIGE.
Nous vous remercions d'avoir choisi Microsoft.
Le présent contrat de licence constitue un contrat entre vous et (i) le fabricant
J'accepte les termes du contrat de licence
Suivant


Installation de Windows
Où souhaitez-vous installer Windows ?
Nom
Taille totale
Espace libre
Type
Lecteur 0 Espace non alloué
60.0 Go
60.0 Go
Actualiser
Supprimer
Formater
Nouveau
Charger un pilote
Étendre
Suivant


Installation de Windows
Installation de Windows
Statut


Commençons par la région. Est-ce bien celle-ci ?
État indépendant du Samoa
États-Unis
Éthiopie
Féroé (îles)
Fidji
Finlande
France
Oui

Annexe

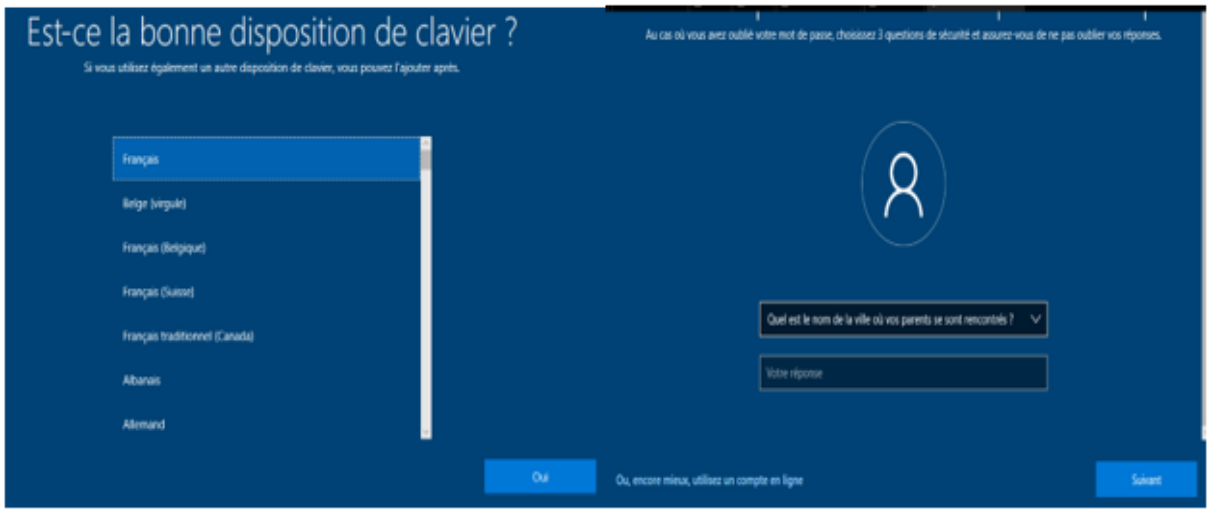


Figure 4-48 installation Windows 10

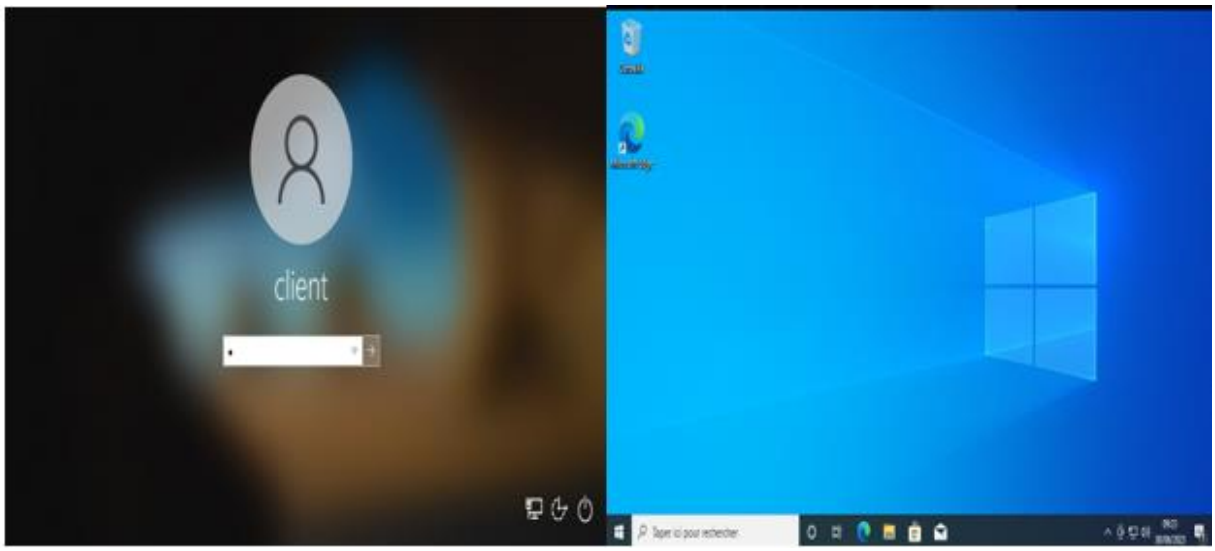


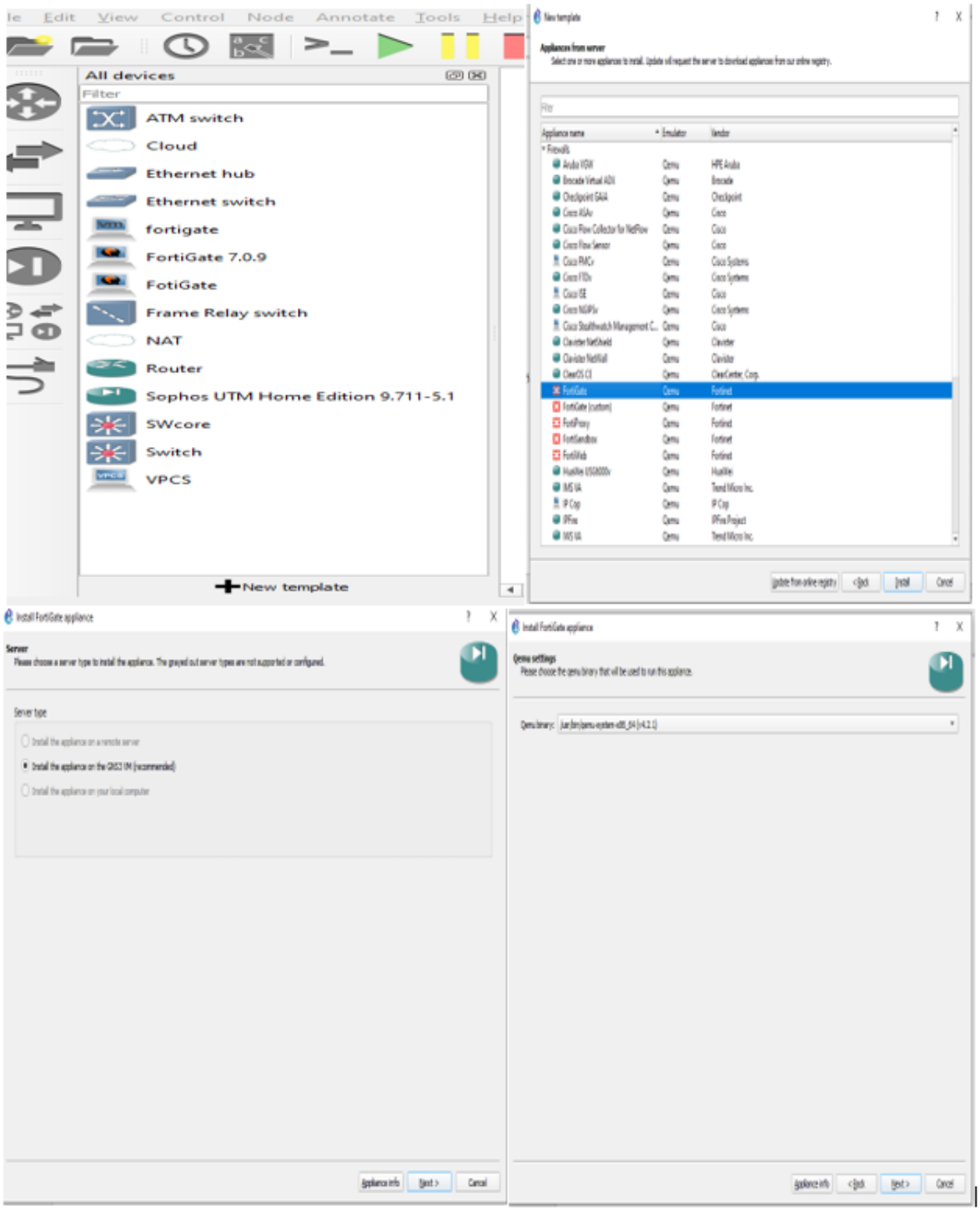
Figure 4-49 Interface Windows 10

Installation de FortiGate

Les étapes d'installation de FortiGate dans GNS3

- Il faut avoir l'image de FortiGate en l'achetant.
- Accéder à GNS3 et cliquer sur « browser all devices ».
- Cliquer sur « new Template » et suivez les étapes illustrées dans les figures

Annexe


Edit
View
Control
Node
Annotate
Tools
Help
All devices
Filter
ATM switch
Cloud
Ethernet hub
Ethernet switch
fortigate
FortiGate 7.0.9
FotiGate
Frame Relay switch
NAT
Router
Sophos UTM Home Edition 9.711-5.1
SWcore
Switch
VPCS
New template
Appliances from server
Server
Qemu settings

Annexe

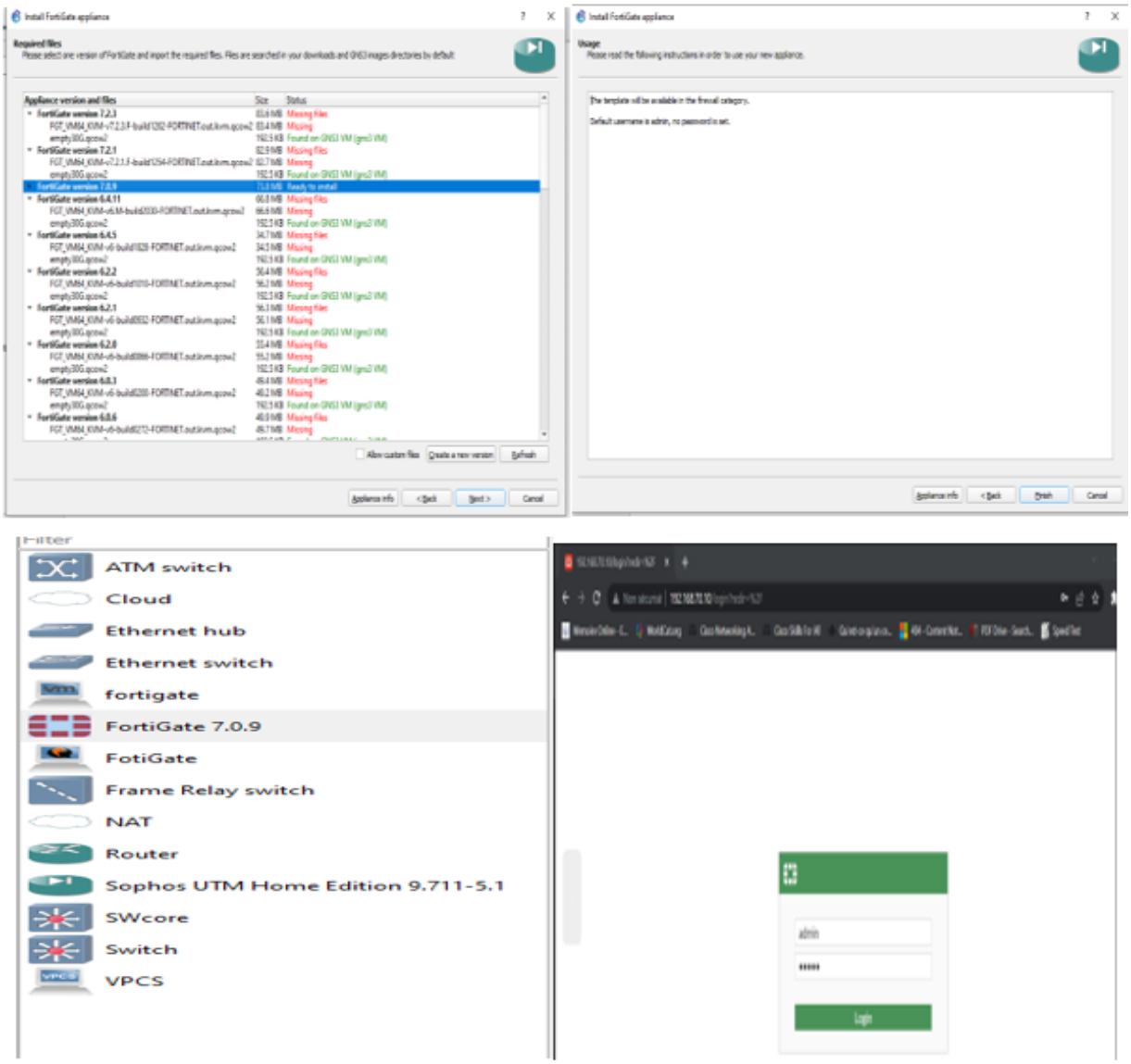


Figure4-50 Installation de FortiGate

Résumé

Ce mémoire se concentre sur la sécurité informatique et présente le centre d'opération de sécurité comme une solution pour faire face aux problèmes de sécurité dans les entreprises et les organisations. Il explore les différents aspects de la sécurité informatique, en mettant en évidence les menaces et les solutions traditionnelles. Il met également en avant l'importance d'un centre d'opération de sécurité (SOC) et montre comment les technologies telles que le Security Information and Event Management (SIEM) et l'analyse des fichiers journaux renforcent la capacité des organisations à détecter et à réagir rapidement aux menaces. Enfin, il décrit l'environnement de travail, les étapes d'installation des outils, les méthodes de collecte et d'analyse des fichiers journaux, ainsi que les méthodes de visualisation des données collectées. Ce mémoire met en évidence l'importance cruciale de la sécurité des réseaux informatiques et offre une base solide pour la recherche future et l'innovation dans ce domaine.

Mots clés : Log, SIEM, SOC, SI, détection, analyse d'événements, indexation, alerte, tableau de bord, recherche et filtrage, Splunk, Attaque et défense, Scan.

Abstract

This thesis focuses on computer security and presents the Security Operations Center (SOC) as a solution to address security issues in businesses and organizations. It explores various aspects of computer security, highlighting threats and traditional solutions. It also emphasizes the significance of a Security Operations Center and demonstrates how technologies such as Security Information and Event Management (SIEM) and log file analysis enhance organizations' ability to detect and respond quickly to threats. Furthermore, it describes the working environment, tools installation steps, log file collection and analysis methods, as well as data visualization techniques. This thesis underscores the critical importance of network security and provides a solid foundation for future research and innovation in this field.

Keywords : Log, SIEM, SOC, SI, detection, event analysis, indexing, alert, dashboard, search and filtering, Splunk, Attack and defense, Scan.