REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR

ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE SAAD DAHLAB DE BLIDA 1

FACULTE DES SCIENCES

PROJET DE FIN D'ETUDE

POUR L'OBTENTION DU DIPLOME DE MASTER EN INFORMATIQUE

SPECIALITE : SECURITE DES SYSTEMES D'INFORMATION

THEME

Mise en Place d'une Solution de Gestion des Informations et des Evènements de Sécurité Security Information & Event Management « SIEM »

Mémoire présenté par :

GADI HASSIBA

Promotrice: Professeur GHEBGHOUB YASMINE
Co-promotrice: SAIDIA Siham

Année Universitaire : 2019- 2020

REMERCIEMENT

Je remercie tout d'abord

ALLAH le tout puissant qui m'a donné la force de mener à bon terme ce modeste travail.

Je tiens à remercier sincèrement toutes

les personnes qui ont apporté leur contribution à l'aboutissement de ce projet.

Je remercie ma promotrice Mlle GHABGHOUB pour son soutien et ses précieux conseils.

Je remercie aussi tous les enseignants de département d'informatique pour les efforts consacrés pour nous transmettre le savoir.

En fin, je tiens à remercier les membres de jury

qui vont faire l'honneur d'apprécier ce travail

Dedicas

Je dédie ce modeste travail à :

** Mes parents qui m'encouragent toujours.*

**Mes frères et soeur.*

(MOHAMED- NAWEL-CHOUKRI- SEDAM)

et

Ma chère

Anfel Yara

** Tous mes amis.*

Ainsi qu'à toutes les personnes

qui m'ont encouragé surtout ***Mr DAHLEB.***

Hassiba

Sommaire

CHAPITRE 3 : CONCEPTION DE LA SOLUTION CIBLE

CHAPITRE 4 : MANAGEMENT DE LA SOLUTION

PARTI 1 : EMULATION DE LA TOPOLOGIE DE LA SOLUTION

LISTE DES FIGURES

LISTE DES TABLEAUX

INTRODUCTION GÉNÉRALE

De nos jours, l'information est devenue pour 1'entreprise une ressource essentielle qu'elle soit privée ou publique. Cette évolution rend la sécurité informatique de plus en plus importante puisque les réseaux d'entreprises sont confrontés à toutes sortes d'attaques informatiques.

Les attaques peuvent être classées en deux catégories : externes (menées par des hackers ou des entreprises concurrentes via le réseau Internet) ou internes (menées par les employés au sein de 1'entreprise elle-même qui cherchent prouver leurs efficacité). La mondialisation a poussé les entreprises à se délocaliser, les collaborateurs et les employés sont devenus ainsi de plus en plus mobiles, ce qui a mené les entreprises à se doter d'un certain nombre de réseaux intranet et extranet nationaux (voir même mondiaux), avec un grand nombre de réseaux d'accès variés.

De ce fait. la tâche de protection et de prévention contre les attaques informatiques est devenue complexe et coûteuse. En effet, une entreprise qui cherche à se protéger doit déployer plusieurs dispositifs de défense et d'outils d'observations performants pour détecter les éventuelles failles. Les responsables sécurité doivent disposer donc d'outils parfaitement opérationnels et sécurisés, qui assure la gestion du réseau et l'information (gestion des alertes, suivi des pannes, gestion des données de configuration et maintenance...) par la collecte des alertes provenant de tous les équipements (détecteurs d'intrusion, firewalls, serveurs, systèmes d'exploitation...) et les traiter et classer par priorité en éliminant les alertes inutiles et en se basant sur des algorithmes de corrélation d'alertes.

Ces algorithmes permettent d'identifier les attaques réelles à partir d'un ensemble d'alertes. Ces alertes sont ensuite affichées via une interface graphique où elles sont étiquetées et résolues soit automatiquement à travers des recommandations déjà prédéfinies, soit manuellement par l'administrateur.

Le présent projet consiste à étudier la gestion sécurité information ainsi les différentes solutions **SIEM** (Security Information and Event Management) présentes sur le marché et à mettre en place une solution adaptée aux spécificités et aux contraintes du réseau de DIRECTION GENERAL NAFTIL (NAFTAL).

Le plan envisagé dans le reste de ce document adopte une démarche répartie en quatre modules :

1. En premier lieu, le rapport s'ouvrira sur une présentation détaillée de l'entreprise ainsi que du sujet de stage. Il sera clôturé par une étude de l'existant afin de dévoiler les entraves que rencontre l'opérateur. Finissant par la solution proposée

2. Le deuxième chapitre présente des concepts de base et quelques termes primordiaux de la supervision des systèmes d'informations et de l'administration des réseaux, puis une

description générale de la sécurité informatique, ensuite nous enchainerons avec les différents plateformes open source existantes dans le domaine de la surveillance réseau .

3. Le troisième chapitre portera sur l'étude de concept de centralisation et d'analyse des journaux des équipements « la solution S1EM open source ELK » cette partie sera valorisée par une étude comparative des systèmes SIEM de centralisation des journaux existant, finissant par le choix opté pour notre solution.

4. Le quatrième chapitre mise en place d'un Système SIEM par l'implémentation d'un serveur de journalisation et d'analyse de log des équipements réseaux cœur de **NAFTAL** ainsi qu'une confirmation du bon fonctionnement de cette solution à travers des tests.

- Nous clôturons le rapport par une conclusion générale traçant les grandes lignes de notre travail suivie par des perspectives que nous désirons accomplir dans un travail futur.

Chapitre I

CADRE GENERALE DU PROJET

ETUDE DE L'EXISTANT

Ce chapitre présente, d'une manière générale, le contexte du travail afin de fixer les objectifs de ce projet de fin d'études.

I.1 Introduction

Dans ce chapitre. Nous présentons d'abord l'entreprise d'accueil au sein duquel notre stage a été accompli, par une description générale, domaine d'activité, ensuite nous allons étudier les problématiques posées. Enfin nous présenterons la solution adoptée pour ces derniers.

I.2 Présentation De Direction Générale NAFTAL :

Issue de SONATRACH, l'entreprise ERDP a été créée par le décret N° 80/101 du 06 avril 1981. Entrée en activité le 1er janvier 1982, elle est chargée du raffinage et de la distribution des produits pétroliers. En Août 1987, l'activité raffinage est séparée de l'activité distribution et dévolue à une nouvelle entité NAFTEC.NAFTAL est désormais chargée uniquement de la commercialisation et de la distribution des produits pétroliers et dérivés. En 1998, elle change de statut et devient Société par actions filiale à 100% de SONATRACH.

NAFTAL a pour mission principale, la distribution et la commercialisation des produits pétroliers sur le marché national.
Elle intervient dans les domaines :

- de l'enfûtage des GPL
- de la formulation de bitumes de la distribution, stockage et commercialisation des carburants, GPL, lubrifiants, pneumatiques,
- GPL/carburant, produits spéciaux.
- du transport des produits pétroliers.

➢ Organigramme DG NAFTAL :

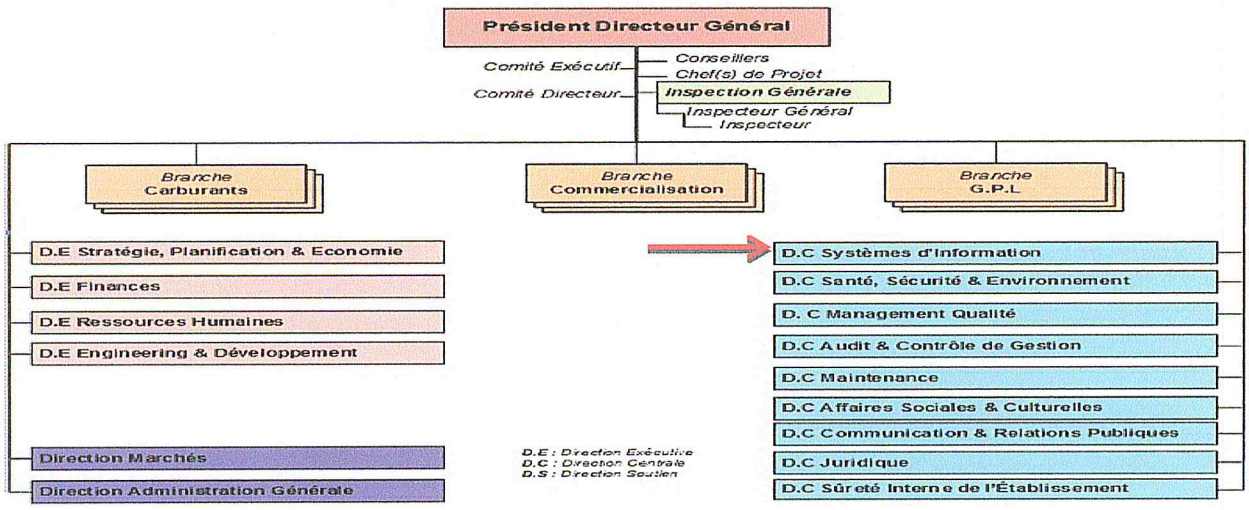

Figure 1.1 : organigramme DG NAFTAL

I.3 Direction Générale Des Systèmes D'information

Compose de deux sous-direction 'voir l'organigramme Figure I.2' sa mission principale est de garantir l'alignement du système d'information sur la stratégie de l'établissement, elle est responsable de la conception de la mise en œuvre et du maintien en condition opérationnelle du système d'information, de sa sécurité et de qualité

Elle fixe et valide les grandes évolutions de l'informatique de l'entreprise. Elle anticipe les évolutions nécessaires en fonction de la stratégie de l'établissement et en maitrise les couts

Elle détermine les investissements en fonction des sauts technologiques souhaites elle s'assure de l'efficacité et de la maitrise des risques liés au système d'information.

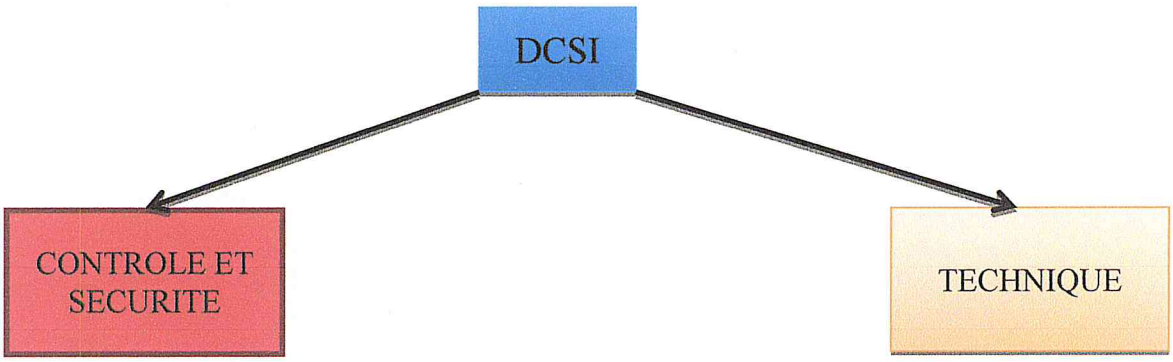

Figure 1.2 : Organigramme DCSI

I.3.1 Missions Des Différents Sous Directions De La DCSI

- **TECHNIQUE** : Garantir La Disponibilité, la fiabilité et le niveau de performance adéquat de l'ensemble des moyens techniques et infrastructures de **NAFTAL** (réseaux, systèmes, matériels).
- **CONTROLE ET SECURITE SI** : Elle a pour mission de définir la politique de sécurité et veiller à son application.

Principales activités :

- Définir les objectifs et les besoins en termes de sécurité des systèmes d'information de **NAFTAL**
- Définir l'organisation de la sécurité de l'établissement.
- Définir et mettre en place les politiques et procédures liées à la sécurité des SI.
- Piloter l'évolution des risques SI et de sécurité SI, les menaces et les conséquences.
- Valider le choix des outils de sécurité.

I.5.1 Modèle conceptuel de la solution de journalisation

Avec révolution flagrante des architecture réseaux et le trafic très critique qu'elles génèrent (trafic financier, trafic bancaire, trafic Datacenter..), la supervision reste un élément insuffisant vue qu'on n'aperçoit l'incident que lorsqu'il se produit.

C'est pour cela que cette partie de notre projet détermine des lignes directrices pour le choix d'une solution de collecte et d'analyse des journaux des équipements réseaux de « NAFTEL » permettant à l'administrateur réseaux de détecter les incidents suspects et de réagir d'une façon proactive face à ces incidents qui peuvent provoque un arrêt de système.

Donc l'objectif principal de cette partie est de refléter l'importance qui réside sur la collecte et l'analyse des événements des équipements réseaux avec un système centralisé et les corréler pour générer des alertes afin de suivre efficacement tout état de cause dans le réseau dans un délai nécessaire.

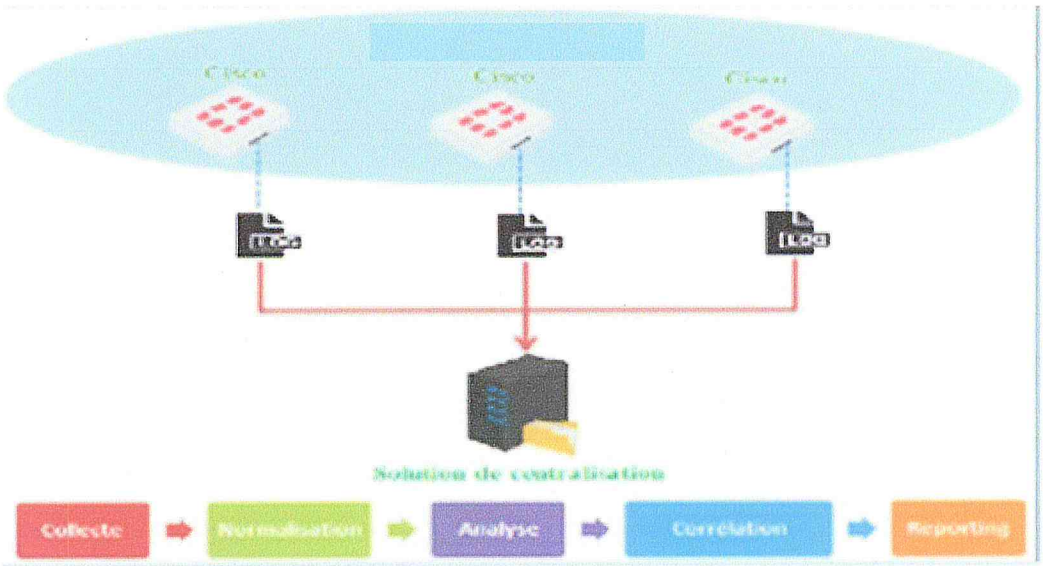

Figure 1.3 : Architecture de solution de journalisation

On parle céans de la mise en place d'un système **SIEM** (Security Information and Event Management) qui permet à raide de la réception des journaux de la part de différents équipements existant dans l'infrastructure réseaux de l'entreprise de :

- Contrôler les vulnérabilités de l'infrastructure réseaux de l'entreprise
- Détecter d'une manière précoce les cyberattaques en maintenant une surveillance permanente
- Réagir pro-activement face aux incidents qui peuvent se produire (Ex : si on détecte une mauvaise qualité de lien entre deux routeurs, on peut régler le problème avant qu'il provoque l'échec de service de routage).

Comme il est montré dans la figure de la solution, le principe de fonctionnement d'un système **SIEM** est réparti en cinq principales phases :

- **La collecte :** consiste à recueillir des journaux système provenant des différentes sources (routeur, pare-feu ,serveur ...)
- **La normalisation :** permet de convertir les logs originaux collectés dans un format universel et de les classer dans des catégories utiles. (ex : modifications d'une configuration, accès aux fichiers ou encore attaque par surcharge de tampon)
- **Analyse :** permet d'analyser les journaux à partir de requêtes paramétrables
- **La corrélation :** les règles de corrélation permettent d'identifier un événement qui a causé la génération de plusieurs autres (ex : un hacker qui s'est introduit sur le réseau puis a manipulé tel équipement...)
- **Reporting** : sert à la création des rapports standards et planifiés qui prendront en compte toutes les vues historiques des données recueillies par le produit **SIEM**

I.6 Conclusion

Ce chapitre a été conçu pour familiariser l'environnement de travail en présentant l'entreprise d'accueil et l'architecture réseaux dont elle dispose. Les problèmes que rencontre NAFTAL se sont Imposés suite à l'étude de l'existant et à sa critique. Pour finir par la proposition de la solution qui répond aux exigences cités tout en détaillant son modèle conceptuel et son architecture ciblé, dans le deuxième chapitre, On va .définir les concepts de base et quelques termes primordiaux de la supervision des systèmes d'informations et de l'administration des réseaux, puis une description générale de la sécurité informatique, ensuite nous enchainerons avec les différents plateformes open source existantes dans le domaine de la surveillance réseau .

Chapitre II

Etat de l'art

II.1 Introduction

L'information est aujourd'hui, la sève de l'entreprise. C'est ce qui fait à la fois sa force et son existence. Fichiers, bases de données, méthodes de travail et de fabrication, fiches des salariés et informations industrielles. Il s'agit là de son capital intellectuel ou plutôt capital informationnel.

Toute perte d'information peut porter un coup fatal à une entreprise ou même à une nation. Si ces informations venaient à être perdues, volées ou à tomber dans les mains d'une autre entreprise, la donnée n'aurait plus de raison d'exister car elle ne serait plus exclusive. L'information a aujourd'hui, de la valeur par son côté unique et exclusif pour une entreprise. Il est donc dans l'intérêt de l'entreprise de protéger son patrimoine informationnel [**B2**].

II.2 Définition d'un système d'information :

Un système d'information (SI) est un ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de collecter, regrouper, classifier, traiter et diffuser de l'information sur un environnement donné. Un système d'information est une partie intégrante de l'organisation [**B3**].

II.3 Définition de la sécurité informatique :

La sécurité informatique se réfère aux processus et méthodologies conçus et mis en œuvre pour protéger toute forme d'information ou de données confidentielles, privées et sensibles contre tout accès non autorisé, utilisation, divulgation, destruction, modification ou interruption [**B4**].

II.4 Objectifs de la sécurité informatique :

Les trois objectifs de la sécurité imposés par les normes sont : la confidentialité, l'intégrité et la disponibilité de l'information (CIA: Confidentiality, Integrity, Availability). Auxquels s'ajoutent d'autres objectifs notamment : l'identification, l'authentification et la non répudiation [B5], que nous allons détailler. Ces objectifs sont présentés dans la figure II.1.

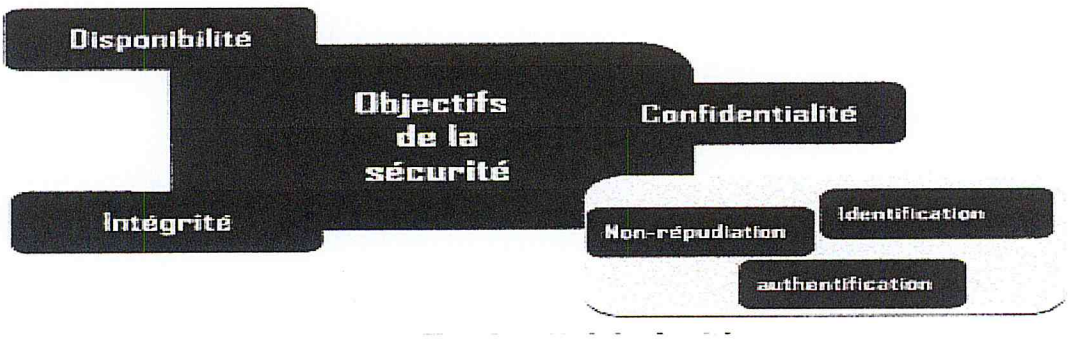

Figure II.1 : Objectifs de la sécurité

II.4.1 Confidentialité

La confidentialité des données est le maintien des informations contre tout accès non autorisé. C'est la propriété qu'une information ne soit pas révélée à des utilisateurs non autorisé à la connaitre .Cela signifie que le système informatique doit empêcher les utilisateurs de lire une information confidentielle s'ils n'y sont pas autorisés [**B5**].

II.4.2 Intégrité

La propriété qu'une information ne soit pas altérée, Cela signifie que le système informatique doit empêcher une modification indue de l'information, c'est-à-dire une modification par des utilisateurs non autorisée ou modification incorrecte par des utilisateurs autorisés [**B5**].

11.4.3. Non répudiation

Permet de garantir qu'une transaction ne peut être niée, et qu'aucun des correspondants ne pourra nier la transaction [**B5**].

11.4.4. Authentification

Permet de vérifier l'identité d'une entité, afin d'autoriser l'accès de cette entité à des Ressources. L'authentification protège de l'usurpation d'identité [**B6**].

II.4.5 Disponibilité

Consiste à s'assurer que l'accès à l'information est continuellement disponible aux utilisateurs autorisés [**B7**]. En d'autre terme cet aspect permet de garantir qu'un objet soit accessible et utilisable sur demande par une entité autorisée.

II.5 Principes de déploiement de la sécurité :

Afin de sécuriser un système, il est nécessaire de :

- Identifier les menaces, les risques, les acteurs malveillants ainsi que leurs motivations. Il faut prévoir la façon dont ils procèdent pour s'en protéger et limiter les risques intrusion.
- Instaurer les bonnes pratiques de sécurité qui doivent être mises en place pour les différents services.
- Auditer le système pour connaître son niveau de sécurité réel. Pour cela, un test d'intrusion est réalisé, mené par les professionnels de la sécurité ou par les chapeaux blancs. Ces derniers sont des pirates qui ont comme finalité d'aider à la sécurisation du système, sans en tirer profit de manière illicite.

II.6 Normes de sécurité de l'information

Les normes de sécurité de l'information sont des ouvrages publiés par diverses organisations

Professionnelles qui tentent de résumer les directives nécessaires à la sécurité d'un système informatique. Des normes différentes sont applicables à différents secteurs, tels que les cartes de paiement et les soins de santé, mais couvrent généralement l'ensemble des composants liés au système, tels que les périphériques réseau, les stations de travail, les serveurs, les logiciels, les interactions utilisateur avec les systèmes, les interactions de processus système, les données, transmission et stockage.

Le tableau II.1 détaille quelques normes populaires utilisées dans le monde entier:

Norme	Description
ISO 27001 et 27002	Un ensemble d'exigences qui fournissent un cadre à une organisation pour planifier et évaluer sa sécurité.
HIPPA (*Health Insurance Portability and Accountability Act)*	La loi HIPAA définit les normes américaines pour la gestion électronique de l'assurance maladie, la transmission des feuilles de soins électroniques et tous les identifiants nécessaires au programme de dématérialisation des feuilles de soins pour l'assurance-maladie.
PCI DSS (Payment Card Industry Data Security Standard)	La norme DSS (PCI Data Security Standard) fournit un cadre de travail pour développer un processus de sécurité des données de carte de paiement, qui inclut la prévention, la détection et la réaction aux incidents de sécurité.

Tableau II.1 : Norme populaire dans la sécurité informatique

II.7 .Termes et définitions lié à la sécurité informatique

Le domaine de sécurité informatique contient plusieurs termes et définition Nous allons définir certains :

II.7.1 Mesure de sécurité ou contre-mesure :

Moyens de gestion des risques, comprenant les politiques, les procédures, les lignes directrices, les pratiques ou l'organisation, qui peuvent être de nature administrative ,technique, managériale ou juridique [**B8**].

II.7.2 Vulnérabilité :

Faille dans un actif, ou dans une mesure de sécurité qui peut être exploitée par une menace [**B8**].

II.7.3 Menace :

Cause potentielle d'un incident indésirable, qui peut nuire à un système informatique ou une organisation [**B9**].

II.7.4 Incident

Un ou plusieurs évènements intéressant la sécurité de l'information, indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les

opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information[**B9**].

II.7.5 Intrusion

L'intrusion est le fait, pour une personne ou un objet, de pénétrer dans un espace (physique, logique, relationnel) défini où sa présence n'est pas souhaitée [**B10**].

II.7.6 Attaque :

Une tentative d'obtenir un accès non autorisé à des services, des ressources ou des informations du système, ou une tentative de compromettre l'intégrité, la disponibilité ou la confidentialité du système [**B11**].

II.7.7 Risque

Un risque est un danger éventuel, plus ou moins prévisible, inhérent à une situation ou à une activité. Le risque en terme de sécurité est généralement caractérisé par l'équation suivant : « **Risque = menace * vulnérabilité * impact** »[**B12**].

II.8 Principales Attaque :

- **virus** :

Les virus est un exécutable qui va exécuter des opérations plus ou moins destructrices sur la machine Sur internet, les virus peuvent contaminer une machine de plusieurs manières :

- Téléchargement des logiciels puis exécution de celui- ci sans précautions.
- Ouverture sans précaution de documents contenant des macros
- Ouverture d'un courrier au format HTML contenant du JavaScript exploitant une faille de sécurité du logiciel de courrier….

- **Déni De Service (DOS) :**

Le but d'une telle attaque n'est pas de dérober des informations sur une machine distante, mais de paralyser un service ou un réseau complet. Les utilisateurs ne peuvent plus alors accéder aux ressources' exemple principal, est le « Ping flood » ou l'envoi massif des courriers électroniques pour saturer la boîte aux lettres.

La meilleure parade est le Firewall ou la réparation des serveurs sur un réseau sécurisé

.

- **Ecoute De Réseau (Sniffer) :**

Il existe des logiciels qui, à l'image des analyseurs du réseau, permettent d'intercepter certaines informations qui transitent sur un réseau local, en retranscrivent les trames dans un format plus lisible (network paquet Sniffing) .de plus l'utilisateur n'a aucun moyen de savoir qu'un pirate a mis son réseau en écoute.

L'utilisation de switchers (commutateurs) réduits les possibilités d'écoute , mais la meilleure parade reste l'utilisation de mot de passe, de carte à puce ou de calculette à mot de passe.

- **L'intrusion**

L'intrusion dans un système informatique a généralement pour but la réalisation d'une menace est donc une attaque. le principal moyen pour prévenir les intrusions et les coupe- feu (Firewall) Une politique de gestion efficace des accès, des mots de passe et l'étude des fichiers « log »

- **Cheval De Trois (Trojan)**

Le pirate, après avoir accéder au système, installe un logiciel qui va lui transmettre par internet les informations des disques durs. La meilleure mesure de protection face à ces attaques, et de sécuriser au maximum l'accès à la machine et de mettre en service un antivirus régulièrement mis a jours.

II.9 Dispositifs de sécurité

Pour implémenter la sécurité, les administrateurs de sécurité informatique disposent de nombreux outils cités dans le **tableau II.2** :

Dispositifs	Définition
Antivirus	Un programme capable de détecter la présence des malwares sur un hôte et, dans la mesure du possible, de le désinfecter.
Serveur mandataire (proxy)	Une machine faisant fonction d'intermédiaire entre deux extrémités. Il offre plusieurs fonctionnalités telles que le cache, le filtrage, le NAT (Network Adress Translation), l'authentification, les logs utilisateurs ...etc.
VPN sécurisé	Les VPN (Virtual Private Network) sont utilisés principalement pour répondre aux besoins des entreprises en matière de sécurisation des échanges via des réseaux publics.
Pare feu	Une entité matérielle ou logicielle conçue pour créer une ligne de défense claire entre deux réseaux. Il représente le premier rempart de la protection des environnements informatiques des menaces extérieures.

Tableau II.2 : Dispositifs de la sécurité

II.10 Concept De Supervision Et Administration Des Réseaux

La supervision d'un système d'information a pour vacation de collecter des informations sur l'état d'une infrastructure et des entités qui y sont liées, de les analyser, et de les organiser.

Elle peut ainsi se définir comme étant l'utilisation de ressources réseaux adaptés afin d'obtenir des informations sur l'utilisation et sur l'état des réseaux et de leurs composants.

Ces informations peuvent servir d'outils pour gérer de manière optimale le traitement des pannes et les problèmes de surcharge du réseau

II.10.1 Supervision Des Systèmes D'Information

Le système d'information est devenu l'épine dorsale de l'entreprise puisqu'il joue le rôle important de la surveillance e la sécurité des infirmations et des activités internes de l'entreprise.

La supervision est un activité de surveillance et de suivi de l'état d'un service ou d'un processus telles que le taux de transfert des fichiers, le niveau de la disponibilité des services etc…

II.10.2 Niveau de supervision dans un système d'information:

Afin d'améliorer le fonctionnement de notre système d'information', il est commandé de diviser la gestion de ce système en des niveaux de surveillance appropriés, compte tenu de leurs domaine d ' utilisation, nous distinguons alors:

- **La supervision réseau** : elle s'occupe essentiellement des équipements constituant le réseau tels que: les serveurs: par la mesure de disponibilité, la vérification de l'interconnexion' au réseau, l'analyse des flux d'entrée et de sortie, le contrôle de débit…

- **La supervision système** : il s'agit des évaluations et des mesures faites sur les ressources système du parc informatique tels que: les processus: par la mesure du taux d'utilisation instantanés, de la charge moyenne pendant une telle période, la connaissance du nombre de processus en cours de fonctionnement, mesure du temps de réponse…

- **La supervision des applications et services:**
  - Vérification de la taille de processus
  - Suivi de la liste des utilisateurs présents dans le réseau
  - Statistique que le taux d'utilisation des protocoles et services par les utilisateurs du système.

II.11 Etude De Différentes Solutions Open Source De Surveillance Réseau

Il existe des solutions de supervision libres et professionnelles. L'avantage de ces logiciels libres est la gratuité, la disponibilité du code source et la liberté d'étudier et de modifier le code selon nos besoins et de le diffuser

De plus, il existe une communauté importante d'utilisateurs et de développeurs qui participent à l'amélioration des logiciels et apportent une assistance par la mise en ligne des documentations et des participations aux forums.

Parmi les plus répandues, reconnues du moment nous pouvons citer Nagios, ZABBIX, EYES·OF- NETWORK et FAN

II.11.1 Nagios

Anciennement (Net saint) est un logiciel de supervision de réseaux créé en 1999 par « Ethan Galstad ». Il est considéré comme étant la référence des solutions de supervision Open Source. C'est un outil très complet pouvant s'adapter à n'importe quel type d'utilisation avec des possibilités de configuration très poussées. La modularité et la forte communauté (> 250 000) qui gravite autour de Nagios (en participant au développement de nombreux plugins et addons) .

offrent des possibilités en terme de supervision qui permettent aujourd'hui de pouvoir superv iser pratiquement n'importe quelle ressource. [**B13**]

➢ **Avantages**

- La supervision à distance peut utiliser SSH ou un tunnel SSL (notamment via un agent NRPE).
- Les plugins sont écrits dans les langages de programmation les plus adaptés à leurs tâches :scripts shell (Bash,ksh, etc.), C++,Perl,Python, Ruby,PHP, C#.
- La remontée des alertes est entièrement paramétrable grâce à l'utilisation de plugins (alerte par courrier électronique ,SMS, etc...).

➢ **Inconvenient**

- Difficile à Installer et à configurer
- Dispose d'une interface compliquée
- Ne permet pas d'ajouter des hosts via Web
- Besoin d'un autre outil comme CACTI pour faciliter sa configuration Pas de représentations graphiques
- Les mises à jour de la configuration se font en mode « ligne de commande » et elles doivent être réalisées côté supervision comme côté équipement à superviser.

II.11.2 Zabbix

Figure II.2 : LOGO ZABBIX

C'est un outil de supervision ambitionnant de concurrencer NAGIOS et MRTG il fait la Supervision technique et applicative, il offre des vues graphiques (générés par RRDtool) et des alertes sur seuil. C'est une solution de monitoring complète embarquant un front -end web, un ou plusieurs serveurs distribués, et des agents multiplateformes précompilés (Windows, Linux, AIX,Sotaris). Il est également capable de faire du monitoring SNMP et IPMI ainsi que de la découverte de réseau. Il repose sur du C/C++, PHP pour la partie front end et MySQL/PostgreSQL/Oracle pour la partie BDD.[**B14**]

➢ **Avantages**

- Richesse des sondes et tests possibles (supervision d'applications Web, par exemple).
- Réalisation de graphiques, cartes ou screens.
- Configuration par la GUI(interface graphique) .
- Mise à jour de la configuration via l'interface Web de Zabbix.
- Serveur Proxy Zabbix.
- Surveillances des sites web:temps de réponse, vitesse de transfert.

➢ **Inconvénients**

- Interface est un peu vaste, la mise en place des Template n'est pas évidente au début : petit temps de formation nécessaire.
- lL'agent zabbix communique par défaut en clair les informations, nécessité de sécuriser ces données (via VPN par exemple).

II.11.3 Check_MK

C'est une solution de supervision open source développée par Mathias KITTNER en 2008. En réalité c'est une extension de Nagios, qui est l'outil de monitoring le plus connu et le plus utilisé dans les entreprises. [**B15**]

Figure II-3 : Logo Check-mk

➢ **Avantages**

- Installation et configuration facile
- Interface Web est beaucoup plus intuitive et elle intègre des outils ,comme PNP4 NAGIOS et RRDTtool.
- Interface Permet une configuration entièrement graphique.
- Check_MK est capable de réaliser un inventaire automatique des services disponibles sur un hôte à superviser.
- Pas besoin redéveloppé des sondes.

➢ **Inconvénients**

- Offre plus de services sur l'environnement Unix

II.11.4 Eyes-Of-Network

Figure II-4 : Logo Eyes-of–network

Eyes Of Network « EON ,. est une solution complète de supervision, basée sur la distribution GNU/Linux CentOS, gérée et administrée via une interface web,qui est accessible par tousles acteurs d'un système d'informations avec une vue correspondant à chacun de leur métier.[**B16**]

EON est open source et sous licence GPL2, qui englobe plusieurs outils de supervision monitoring et de gestion, chacun d'eux est spécialisé pour effectuer une tache spécifique de supervision :

NAGIOS : Gestion des incidents et des problèmes
CACTI : Gestion des performances
WEATHERMAP : Cartographie de la bande passante
BACKUP MANAGER : Outil de sauvegarde de la solution

➢ **Avantages**

- Interface de configuration web
- Permet de faciliter le déploiement des outils de supervision
- Noyau linux solide et fiable.

➢ **Inconvénients**

- Une configuration en interface web qui ne supporte pas la navigation sécurisée (HTIPS).

II.12 Etude Comparatif

La Comparaison générale des outils de supervision à base open source précédemment cités a été étudiée en premier lieu avec un diagramme radar en fonction de :

- ➢ Dynamisme.
- ➢ Ressource.
- ➢ Souplesse et extensibilité
- ➢ Socle technique.
- ➢ Périmètre fonctionnel.
- ➢ Notoriété Actuelle.

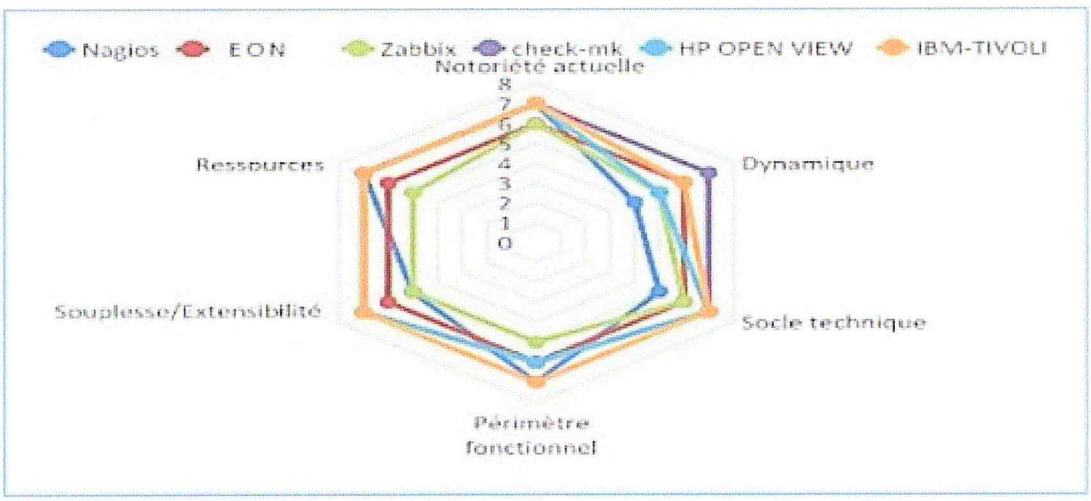

Figure II-5: Diagramme Radar

En deuxième lieu pour mieux enrichir notre étude comparative, nous donnons le tableau comparatif ci-dessous qui résume les différentes caractéristiques des outils de supervision open

source précédemment cités, qui présentent les points faibles et les points forts de ces derniers. Ce qui nous aide bien évidemment à prévoir le meilleur choix de la solution adoptée pour la phase de supervision.

Critère Fonctionnels	EON	Nagios	Zabbix	Check_MK
Environnement de L'installation	Linux CentOS	Unix	Unix	Unix
Base de donné	MYSQL	C++	PHP, C	Python
Protocole	SNMP	SNMP, ICMP	HTTP, FTP	SNMP
Gestion d'authentification et des rôles	OUI	OUI	OUI	OUI
Création des graphes simple à partir des mesures	OUI	NON	OUI	OUI
Utilisation d'agents sur les machines cibles	OUI	OUI	Agent Windows/Unix	Check-mk win
Installation et configuration simple	OUI	NON	OUI	OUI
Intégration simple des nouvelles host à superviser	OUI	NON	OUI	OUI
Possibilité de mettre en place une supervision centralisée entre plusieurs sous réseaux	OUI	NON	OUI	OUI
Compatibilité avec la plateforme de virtualisation VMware)	OUI	OUI	OUI	NON
Possibilité d'ajouter les plugins	OUI	OUI	OUI	NON
Générer des alertes	OUI	OUI	OUI	OUI
Générer des rapports	OUI	OUI	NON	NON

Tableau II-3 : Tableau comparative des outils de supervision open source

II.13 Défis des solutions de sécurité actuelles :

La sécurisation du système d'information est un enjeu clé pour les directions des entreprises. Dans ce contexte, de nombreux dispositifs de protection cohabitent (firewall, sonde de détection, IPS, ...) avec comme unique objectif de réduire « le niveau d'exposition » au risque du SI.

Les défis des solutions de sécurités actuelles sont :

- Conçues pour surveiller et protéger uniquement un segment spécifique de l'infrastructure informatique. Exemple, les pare-feu ne concernent que le filtrage du trafic réseau, tandis que les logiciels antivirus s'attachent à éliminer les applications indésirables et malveillantes des systèmes. Ces deux solutions, présentes dans la plupart des systèmes, opèrent souvent sans se rendre compte de l'existence de l'autre.
- L'impossibilité de détecter (sans coopération) les méthodes d'attaque moderne telle que les menaces persistantes avancées (APT), qui utilisent des vecteurs et des schémas d'attaque variée,
- La génération d'un nombre important de fichier logs,
- Le personnel de sécurité informatique a beaucoup de difficulté à analyser, comprendre et à faire le lien entre les données remonté par ces solutions de sécurité.
- Les entreprises doivent mettre en place une organisation défensive qui doit s'appuyer à la fois sur la prévention, sur la mise en place de moyens de détection et sur des capacités de réaction [**B17**].

II.14 Conclusion

Les mécanismes de sécurité cités dans ce chapitre, qui sont considérés comme classiques et de base, attient leurs limites face aux attaques modernes. En contrepartie il existe des solutions de renforcement très efficace et d'actualité telle que la mise en place d'un SIEM (**Security Information & Event Management**).

Dans le chapitre suivant, nous allons décrire conception de la solution cible **SIEM** (**Security Information & Event Management**)et considéré « **ELK** » comme solution décentralisation des journaux et les conditions que doit remplir un SIEM pour pouvoir surmonter ces défis.

Chapitre III

CONCEPTION DE LA SOLUTION CIBLE

III.1 Introduction

Le but de cette deuxième partie et de définir la notion de « centralisation des journaux », ainsi que présenter les techniques et les recherches actuelles qui sont utilisée et développées dans le domaine de la gestion des journaux, comment ces outils sont utilisés pour analyser ces fichiers journaux.

Elle développera également la comparaison des outils de centralisation des journaux actuellement disponibles par rapport à la fonctionnalité désirée pour arriver à la solution la plus appropriée

III.2 Centralisation des journaux

III.2.1 Logs

Un log, aussi appelé journal d'événement, est la notification d'un événement envoyé par une application, un système, un service ou une machine sur le réseau. La résolution des pannes nécessite en général d'étudier les logs des applications, équipements réseaux ou autres, ils permettent donc de comprendre ce qu'il s'est passé et de pouvoir retracer les actions d'un système. Ils sont donc très importants en informatique, car ils peuvent donner des explications sur une ou plusieurs erreurs, sur un crash ou une anomalie. Ils nous permettent de comprendre certains fonctionnements d'un système par exemple, ils retracent la vie d'un utilisateur, d'un paquet ou d'une application sur le réseau et peuvent aussi notifier une action quelconque. Les logs sont donc indispensables pour bien comprendre d'où proviennent certains dysfonctionnements. **[B18]**

III.2.2 Journalisation locale

De nombreux serveurs et systèmes d'exploitation des clients, des commutateurs de réseau, routeurs, pare-feu, et d'autres équipements de réseau ont la capacité de produire des journaux en les envoyant à travers le réseau. En fonction de la taille et de la complexité de l'infrastructure informatique comme on peut le voir dans la fiigure ci- dessous

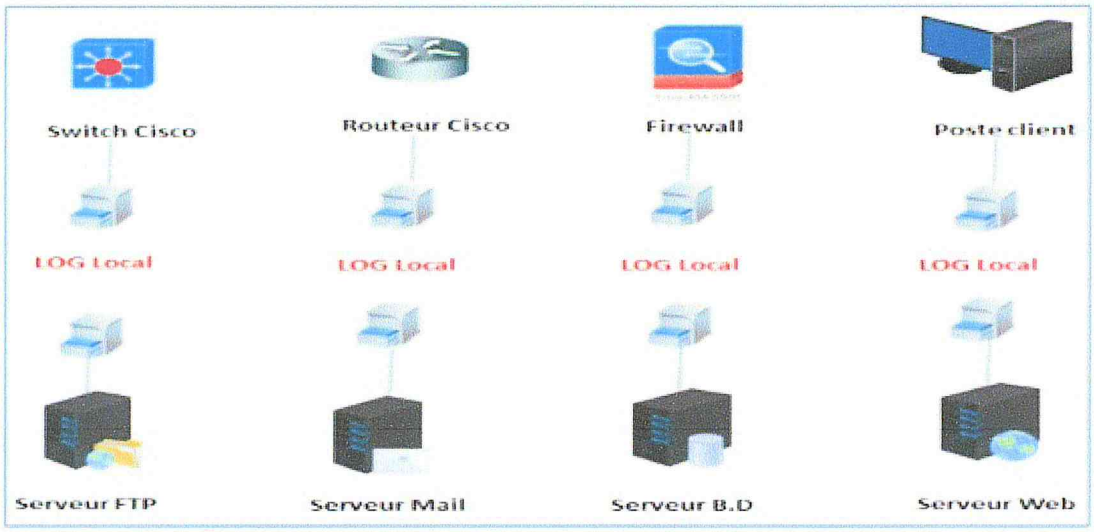

Figure 1I1- 1: Architecture log local

Ces événements journaux varient en importance, mais sont tous nécessaires pour obtenir une image complète de ce qui se passe dans le réseau et à l'intérieur des systèmes d'exploitation des nœuds.

Par défaut, les journaux sont stockés localement, ce qui entraîne de nombreux Inconvénients. Tout d'abord, il est très complexe de gérer chaque équipement de l'infrastructure séparément. Deuxièmement, les journaux stockés peuvent être supprimés ou modifiés localement .Si une attaque s'infiltre dans un périphérique réseau ou un serveur, les journaux, y compris les dossiers sur la violation de la sécurité pourraient être modifiés ou supprimés. Dans ce cas, l'attaque ne serait même pas remarquée. En troisième lieu, si une mémoire de l'appareil est endommagée, les journaux locaux pourraient ne pas être accessibles. Dans ce cas, il devient impossible de trouver la raison de ce dysfonctionnement. Donc a gestion du journal central et le système d'alerte d'événement peut aider à résoudre ces problèmes.

III.2.3 Centralisation des journaux :

Le fait de centraliser les logs permet de sécuriser le réseau, d'avoir la meilleure gestion du système d'information possible et d'avoir une vue d'ensemble de tous les éléments importants sur le réseau. Certains messages sont anodins, tandis que d'autres peuvent être très importants, c'est pour cela que la centralisation va faciliter la recherche et l'analyse, qui pourront ainsi être à la fois très précises et concises sur les activités de plusieurs systèmes, car tout se trouvera au même endroit. De plus, la centralisation sera utile pour détecter les événements anormaux sur le réseau ou sur les systèmes de tout type en utilisant les logs.

Ils pourront retracer le parcours d'une attaque plus facilement car ils seront d'une part tous regroupés et d'autre part exportés de la zone d'effet de l'attaquant, il sera donc difficile pour le pirate de supprimer les logs pour effacer ses traces. la centralisation permet également de garantir la pérennité des logs, il est nécessaire de ne pas les stocker sur un système en production qui peut tomber à tout instant car s'il devient injoignable,

sur un système en production qui peut tomber à tout instant car s'il devient injoignable, la récupération des logs devient plus compliquée alors que, s'ils sont exportés sur une machine disponible, la vitesse de récupération de ces derniers sera beaucoup plus rapide et le problème sera traité plus facilement.

Donc, il est d'une importance cruciale pour un service informatique d'une organisation pour être en mesure de suivre efficacement tout état de cause dans le réseau dans un délai nécessaire par la mise en œuvre d'un système de gestion des évènements « SIEM » qui permet d'envoyer tous les journaux dans un serveur central.

III.3 Système De Gestion Des Evènements

Actuellement, il existe trois types d'environnements définis sur les systèmes de gestion des événements:[B19]

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

III.3.1 SEM (Gestion des événements de sécurité)

Ces produits offrent une gestion des événements, une analyse des menaces en temps réel, une visualisation, une billetterie, une réponse aux incidents et des opérations de sécurité. Ils sont généralement basés sur des bases de données SQL d'entreprise telles qu'Oracle.

III.3.2 SIM (Gestion de l'information de sécurité)

Security Information Management, un type de logiciel qui automatise la collecte des données du journal des événements à partir des dispositifs de sécurité, tels que les pare-feu, les serveurs proxy, les systèmes de détection d'intrusion (IPS,IDS) et les logiciels antivirus.

III.3.3 SIEM (Informations sur la sécurité et gestion des événements)

Ces produits combinent des capacités SIM et SEM ,les produits SIM sont simples à déployer et à utiliser, tandis que les produits SEM sont plus complexes.

La technologie SIEM fournit une analyse en temps réel des alertes de sécurité générées par le matériel et les applications réseau. Les solutions SIEM sont fournies sous forme de logiciels d'Appliance ou de services gérés. Elles sont également utilisées pour consigner les données de sécurité et générer des rapports à des fins de conformité.

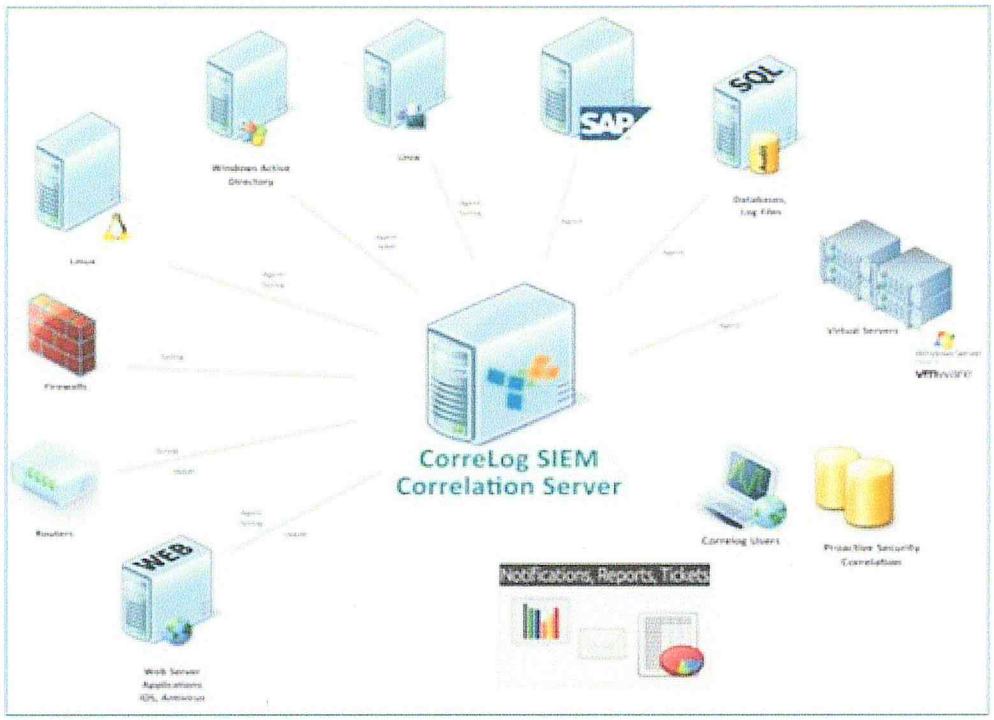

Figure III- 2 : Architecture SIEM

SIEM décrit les capacités du produit de rassembler, analyser et présenter l'information des dispositifs de :

- Réseau et sécurité.
- Applications de gestion d'identité et d'accès.
- Outils de gestion de la vulnérabilité et de conformité aux politique
- Systèmes d' exploitation.
- Bases de données.
- Journaux d'application.
- Données sur les menaces externes.

Un objectif clé de SIEM est de surveiller et d'aider à gérer les privilèges des utilisateurs et des services, les services d'annuaire et d'autres changements de configuration du système; ainsi que fournir l'audit et l'examen de journal et la réponse aux incidents.

III.4 Produit SIEM

Il existe un certain nombre d'outils SIEM sur le marché, à la fois open source et commercial. Avec la montée en puissance de DevOps, de conteneurs et d'autres méthodes de développement d'applications modernes, les solutions Open Source connaissent un regain d'intérêt. Jetons un coup d'œil sur certains des meilleurs outils SIEM open source

.

III41 Graylog

Graytog est un logiciel libre développé et écrit en langage Ruby et Java par Lennart Koopmann en mai 2010, qui permet de centraliser tous les logs d'un parc informatique sur une seule plateforme, avec des modules de traitements et de mise en page. [B20]

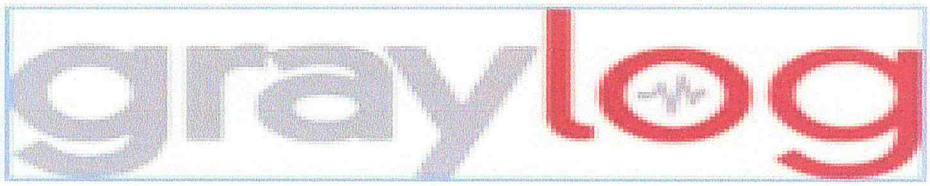

Figure 1I1-3: Logo Grayfog

Une importante communauté s'est fondée autour de cette solution, grâce au suivie régulière des développeurs. Actuellement la version 2.0 est sortie en Avril 2016. Son but est de pouvoir répondre rapidement en cas de problème sur le parc informatique. Ila une plage d'action large. Il peut prévenir l'apparition d'un problème, nous prévenir lorsqu'un problème survient, et il permet d'analyser les derniers logs de la machine si elle s'est éteinte subitement. La suite Graylog est alors composée de quatre parties :

- Elasticsearch permettant le stockage des logs et la recherche textuelle.
- Mongo DB qui assure la gestion des métadonnées.
- Le serveur Graytog qui va recueillir les logs sur différents protocoles: UDP, TCP
- L' interface web de Graylog, qui permettre de consulter les logs

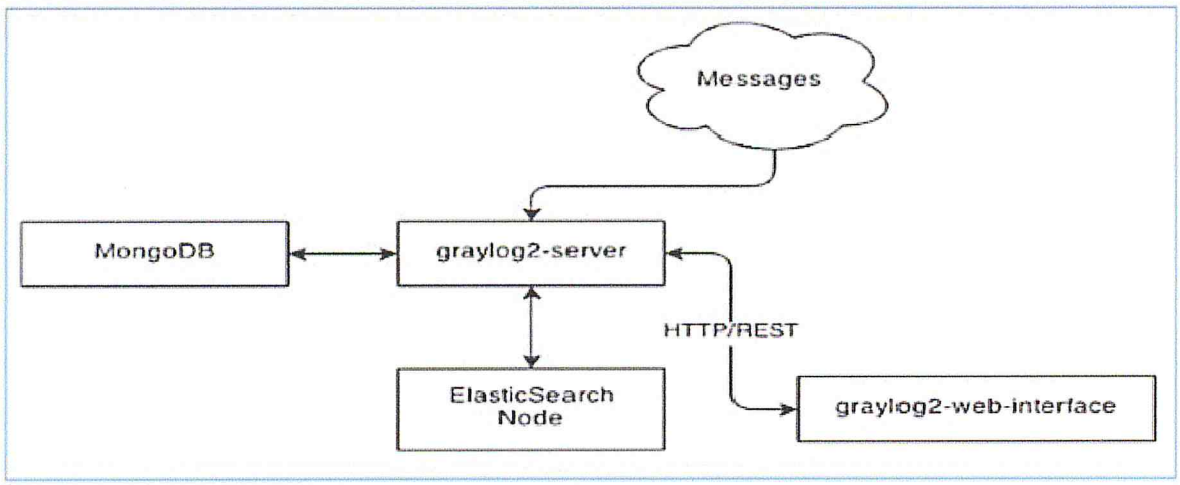

Figure II1-4: Architecture Graylog

III.4.2 Fluentd

Fluentd est un outil open source permettant de collecter des événements et des journaux .Son architecture permet de collecter facilement les journaux provenant de différents sources d'entrée et de les rediriger vers différents récepteurs de sortie.

Certains exemples d'entrée sont des journaux HTIP, syslog ou apache, et certains puits de sortie sont des fichiers, du courrier et des bases de données (aussi bien SGBDR que NoSQL). Aussi il permet d'analyser les logs et d'extraire seulement les parties significatives de chacun d'eux; La sauvegarde de ces informations structurées sur une base de données permet une recherche et une analyse beaucoup plus simples. **[B21]**

Figure III- 5 : Logo Fluentd

Fluend se compose de trois éléments de base

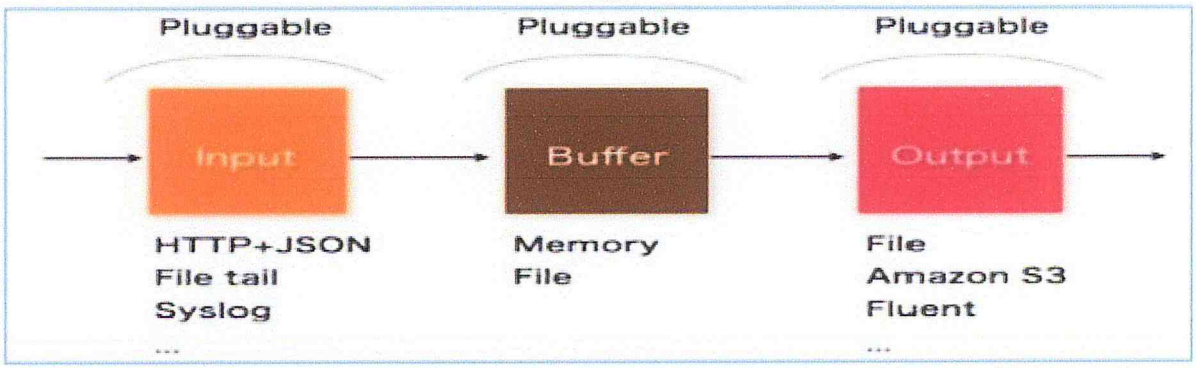

Figure III- 6 : architecture fluend

- **Input:** Recevoir et extraire les journaux de la source de données.
- **Buffer:** Assure la fiabilité .Lorsque la sortie échoue, les événements sont conservés par la mémoire Buffer et automatiquement rejugé.
- **Output:** Transmettre les journaux d'évènement vers le service de stockage.

III.4.3 ELK stack

ELK stack est une solution de centralisation et d'analyse de journaux, proposée par l'entreprise Elastlc. ELK stack se compose des trois logiciels suivants : **Elasticsearch, Logstash et Kibana. [B22]**

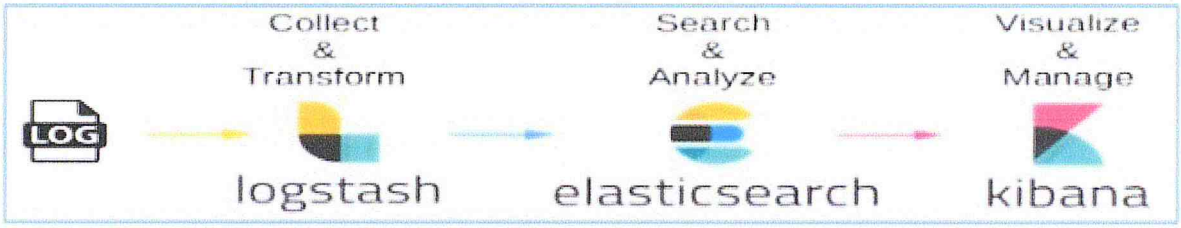

Figure III- 7 : ELK - Stack

- **logstash**

Est un outil de gestion des logs. Il prend en charge pratiquement tous les types de journaux y compris les journaux système, les journaux d'erreurs et les journaux d'applications personnalisées. Il peut recevoir des journaux provenant de nombreuses sources, y compris syslog, messagerie (par exemple, rabbitmq) et jmx, et il peut produire des données de différentes manières, y compris par courrier électronique, websockets et Elasticsearch.

- **Elasticsearch**

Est un moteur de recherche et d'ana lyse en texte intégral et en temps réel qui stocke les données de journal indexées par Logstash. Il est construit sur la bibliothèque du moteur de recherche Apache Lucene et expose les données via les API REST et Java. Elastlcsearch est évolutif et est conçu pour être utilisé par les systèmes distribués.

- **Kiabana**

Est une interface graphique basée sur le Web permettant de rechercher, d'analyser et de visualiser les données du journal stockées dans les index Elasticsearch.Il utilise l'interface REST d'Elasticsearch pour extraire les données, aussi il permet aux utilisateurs de créer des vues de tableau de bord personnalisées de leurs données, mais leur permet également d'interroger et de filtrer les données de manière ad hoc.

III.5 Analyse comparative :

La comparaison des plateformes de centralisation et d'analyse des journaux a base open source précédemment cités a était étudiés par deux tableaux comparatif dont le but est de mieux choisir la plateforme la plus adopté pour notre solution

III.5.1 Caractéristiques

Le premier tableau comparatif ci-dessous a *été* effectué en fonction de caractéristiques.

Plateforme	ELK-Stack	Graylog	Fluentd
Langage	JavaScript	Java / Ruby	Rubis
Licence	Apache 2.0	GPLv3	Apache 2.0
Protocole	UDP BSD Syslog, UDP syslog IETF, IETF TCP, GELF	BSD et syslog IETF, FAES, GELF via Http AMQP	HTTP, AMQP, OMQ Kafka
Stockage	Elastic-Search	Elastic-Search , MongoDB	Elastic-Search
Indexation	Elastic-Search	Elastic-Search	Elastic-Search
Transport	TCP, UDP	TCP, UDP	TCP, UDP

Tableau III-1 : Tableau comparatif SIEM – caractéristique

III.5.2 Fonctionnement

On vous présente simultanément, un deuxième tableau, qui réalise une comparaison en terme de :

- INSTALLATION
- CONFIGURATION
- FONCTIONALITES

III.6 Choix de plateforme

En partant de l'étude comparative énoncée au paragraphe précédent, nous avons décidé de choisir la solution ELK Dans la section suivante nous réaliserons une étude détaillée sur cette dernière.

III.6.1 Présentation générale de la solution ELK stack

ELK stack est une solution open source complète, ou plutôt plateforme complète d'administration des réseaux et du management du système informatique.

ELK stack utilise plusieurs produits issus de la même stratégie (Open Source) afin d'y intégrer une infrastructure de monitoring en temps réel de la sécurité du réseau d'où l'intérêt de mettre en place des outils d'analyse des logs applicatifs comme la suite ElasticSearch.

ElasticSearch, Logstash et Kibana : ces trois outils ont chacun un rôle bien précis dans le workflow permettant de passer des logs bruts au format fichier à des Dashboard avec graphiques et statistiques, qui montreront de manière synthétique le contenu des logs.

C'est une plateforme d'administration et supervision réseau,de management de la société de l'informatique et de la gestion instantanée des activités et des événements survenues sur le réseau informatique.

ELK stack assure les fonctionnalités d'un SIEM :

- La collecte des Logs
- L'agrégation,
- La normalisation
- La corrélation
- Le reporting
- L'archivage
- Le rejoue des évènements

III.6.2 Le principe technique de la solution ELK stack

La stack ELK transforme des flux de données brutes en un ensemble de données structurées. Cela inclut donc bien plus que des logs d'erreurs : on peut aussi l'utiliser pour vérifier le bon fonctionnement de son application en analysant ses propres fichiers de logs.

Les différentes étapes de la transformation par le serveur sont :

1. La réception du flux d'informations brutes provenant des fichiers de logs
2. L'analyse du f lux à l'aide d'un filtre présent sur le serveur
3. Le découpage de chaque ligne selon un pattern grok défini dans le filtre
4. Le stockage des informations structurées dans Elasticsearch.

III.6.3 Architecture d ' ELK-stack

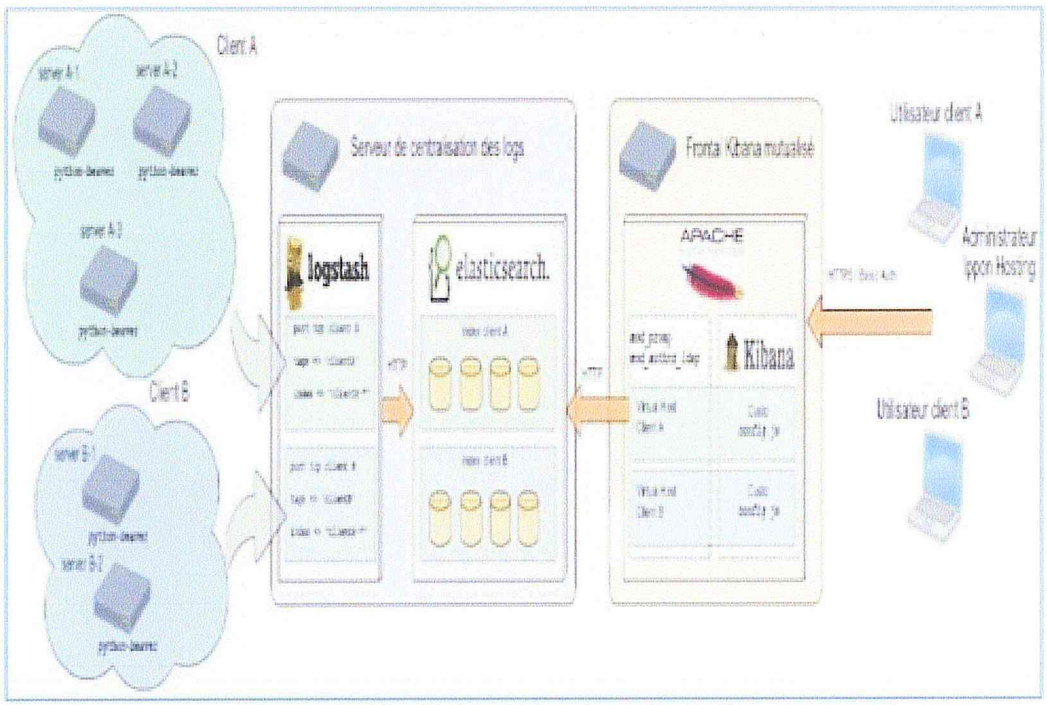

Figure III- 8 : Architecture ELK-Stack

L'architecture de la stack est assez simple : des shippers s'occupent de récupérer les logs, un ou plusieurs nœuds Logstash découpent les logs en éléments sémantiques (un timestamp, un serveur, une action, un résultat, un code de retour,...) et le transmettent à Elasticsearch, un ou plusieurs nœuds Elasticsearch indexent et stockent, Kibana gère la présentation en se basant sur les données lues dans Elasticsearch **[B23]**

III.6.4 Les composants d'ELK stack

III.6.4.1 ElasticSearch

III.6.4.1.1 Présentation d'Elast cSearch

Elastlcsearch est un moteur de recherche et d'indexation Open Source nouvelle génération. Basé sur la librairie Apache Lucene, ce moteur de recherche offre des fonctionnalités avancées telles que les recherches par coordonnées géographiques, l'analyse et la catégorisation par agrégations, le filtrage de résultats ou encore la recherche sur plusieurs index et types de documents différents. Taillé pour le Cloud, ElasticSearch a été spécialement conçu pour indexer de très gros volumes de données tout en assurant une montée en charge performante et une forte tolérance aux pannes.

III.6.4.1.2 Moteur de recherche et moteur d'indexation

Si nous parlons de moteurs de recherche, nous citons certainement Google, Bing.... qui sont des applications web permettant de retrouver des liens, des images...

Cependant, pour pouvoir donner des résultats pertinents, un moteur de recherche doit savoir à l'avance où sont les ressources que nous pourrions lui demander. Pour le savoir, de nombreux moteurs de recherche ont des robots qui parcourent Internet à la recherche de nouvelles ressources. Ils se basent donc sur des moteurs d'indexation, dont le rôle est de collecter des ressources, et d'extraire les mots-dés les plus significatifs. Un moteur d'indexation n'est donc qu'un sous ensemble du moteur de recherche.

Tandis que les géants du Web utilisent des moteurs d'indexation propriétaires, dans le monde de l'open source, Apache Lucene, une bibliothèque d'indexation développée en Java s'est fait une grosse réputation, et est devenue aujourd'hui le standard sur lequel se basent les meilleurs moteurs d'indexation. C'est le cas d'Elasticsearch lui aussi basé sur Apache Lucene, qui est aujourd'hui un des meilleurs moteurs d'indexation du marché.

III.6.4.1.3 Les fonctionnalités d'ElasticSearch

- **LA réplication des données**

Dans un cluster Elasticsearch, lorsque vous avez plusieurs nœuds, les données stockées sur ces derniers sont répliquées entre elles. Ceci permet entre autres de conserver l'intégralité des données en cas de perte d'un nœud.

La réplication est faite de manière automatique. Rajouter un nœud ou un shard déclenche la réplication automatique.

➢ **La recherche en temps réel et contextuelle**

La recherche dans Elast csearch est l'une des plus performantes du marché. Nous parlons de recherche distribuée. Quand nous lançons une recherche sur le nœud principal, ce dernier va renvoyer la recherche sur les autres nœuds et les résultats seront renvoyés au demandeur.

L'une des particularités du moteur est qu'il regroupe les éléments indexés en rapprochant selon le contexte de la donnée.

➢ **Les facettes**

Elasticsearch supporte les facettes, qui sont des regroupements de résultats de recherche. Ce qui permet aux utilisateurs d'avoir une vue agrégée de leurs données. Il existe plusieurs types de facettes disponibles dans Elasticsearch, parmi lesquelles :

- Filter : renvoie le nombre de hits correspondant à un filtre.
- Geo distance : regroupe les données par intervalle de distance géographique.
- Query : renvoie le nombre de hits correspondant à une requête.
- Terms : renvoie les termes les plus fréquents.
- Statistical : permet de calculer les données de type somme, minimum, moyenne, maximum, variance, etc. sur des données de type numériques.

III.6.4.2 Logstash

III.6.4.2.1 Présentation de Logstash

Cet outil permet de mettre en place l'analyse des logs. Les points d'entrée (Input) utilisés pour aller chercher L'information sont définis via un fichier de configuration. Plusieurs types de point d'entrée peuvent être choisis, notamment les fichiers : dans ce cas, on indique à Logstash l'emplacement où aller lire les fichiers de log. Logstash lit ensuite ces fichiers ligne par ligne. Il est alors possible d'appliquer certains "filtres" sur ces lignes : il ne s'agit pas seulement de sélectionner certaines informations et d'en écarter d'autres, mais également de faire des opérations plus complexes, comme du mapping. Par exemple dans le cas d'un log avec UID, il est possible de résoudre 1'1D en "Nom, Prénom" en faisant un appel externe. Il est également possible d'extraire des informations spécifiques et les stocker dans des champs spécifiques, ou encore d'exécuter du code Ruby. Autre exemple : le filtre GROK permet d'extraire desinformations à l'aide de RegEx (expressions régulières) pour matcher certains patterns, comme un numéro de version.

Une fois que les points d'entrée et les filtres sont définis, on indique à Logstash où envoyer les résultats :plusieurs points de sortie, ou adaptateurs, peuvent être définis.

Le plus utilîsé est Elasticsearch, mais il pourrait s'agir d'une BDD, ou d'un fichier... Logstash est bien un ETL (Extract Transform Load,des entrées, des sorties, un traitement entre les deux).

III.6.4.2.2 Principe de fonctionnement de Logstash

lLogstash fonctionne sur un principe simple, un peu comme un routeur de messages. Il est possible de parler de chaînes de liaisons entre ces différents composants.

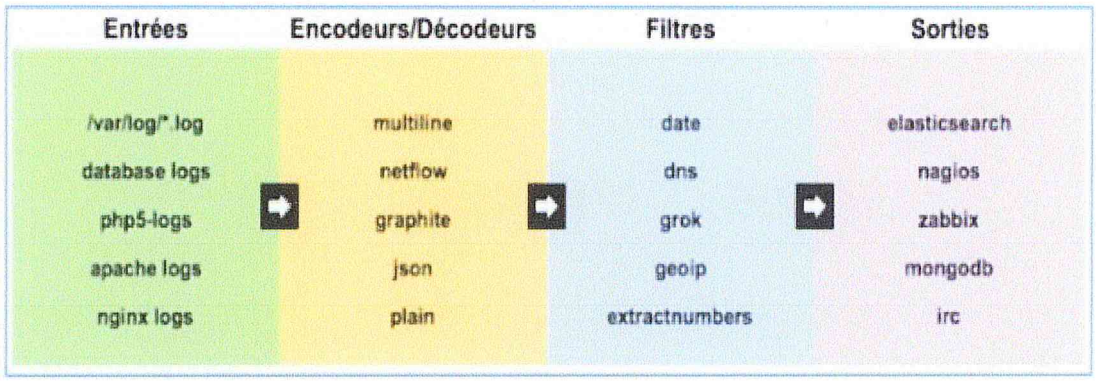

Figure III- 9 :Principe de fonctionnement Logstash

Tous les différents éléments que nous allons détailler sont implémentés sous forme de plugins ce qui rend très facile d'ajouter des possibilités à Logstash. La liste de ces plugins ne cesse d'ailleurs de croître.

- **Les entrées**

Logstash accepte à peu près tout ce qui peut être représenté sous forme de chaîne de caractères en entrée; texte, nombre, date.... La liste des entrées disponibles est impressionnante et couvre des plugins particuliers pour Collectd, Graphite, websocket, les interruptions SNMP et même l'IRC.

Des plugins plus génériques sont bien sûr disponibles comme Syslog,AMQP pour recevoir des messages depuis ce genre de bus messages.

- **L es encodeurs/décodeurs**

Les codecs sont arrivés pour pouvoir normaliser et packager un ensemble de filtres . Il existe de nombreux codecs dont Graphite pour encoder/décoder le format natif des métriques Graphite ou encore Netflow, qui permet l'encodage, décodage des flux Netflow, très utilisé pour la supervision réseau.

➢ **Les filtres**

Les filtres permettent de triturer tout message arrivant dans Logstash. Par triturer, nous entendons découper un message en plusieurs parties et Inversement, formater les dates normaliser le nom des champs mais pas seulement. Au programme, des filtres pour créer des sommes de contrôles, extraire des nombres, supprimer des messages avant stockage et bien sur Grok.

Grok est sûrement l'un des plus puissants et permet de structurer n'importe quel message, comme des logs Apache 2 par exemple. Sa force réside dans sa capacité à construire des expressions complexes à partir d'expressions régulières plus simples.

%{SYSLOGHOST;syslog_ hostname}

Dans l'exemple ci-dessus, SYSLOGHOST est une expression Grok qui permet de capturer une partie du message correspondant aux expressions régulières nécessaires pour reconnaître un nom d'hôte FQDN.

➢ **Les sorties**

Une fois que Logstash a opéré sur les messages, ceux-ci peuvent désormais être routés vers les plugins de sortie qui permettent d'envoyer les messages vers un bon paquet d'outils tierces,en plus de la sortie de Logstash, à savoir Elasticsearch.

III.6.4.3 Kibana

III.6.4.3.1 Présentation de Kibana

Kibana est le dernier outil de notre suite destinée à l'analyse des logs applicatifs : les données brutes sont analysées dans logstash, stockées dans Elasticsearch, mais ne sont pas encore exploitables.

Kibana qui est une interface homme machine permettant de consulter les documents d'une base Elasticsearch et d'en sortir des tableaux de bords, qui nous permettent de juxtaposer les visualisations que nous avons créées

III.6.4.3.2 Principe de fonctionnement de Kibana

Kibana est une interface Web qui se connecte au cluster Elasticsearch, et permet de faire des requêtes en mode texte pour générer des graphiques (histogrammes, barres, cartes...), ou des statistiques. De nombreux composants graphiques sont disponibles pour donner une dimension visuelle aux données stockées dans Elasticsearch. La création de tableaux de bord est intuitive grâce à une interface WYSIWYG (pas de code à créer). es tableaux de bord ainsi générés sont exploitables par les développeurs, les profils techniques, mais aussi par les interlocuteurs du métier ou les managers.

III.7 Conclusion

Ce chapitre, a été consacrée pour la définition des systèmes SIEM et de la notion de centralisation des journaux, ainsi que la réalisation d'une étude comparative entre les produits SIEM les plus utilisés, finissant par le choix de la solution Appropriée à l'accomplissement du notre projet.

Tout le long de ce chapitre, on a mis le point sur les éléments les plus importants de notre projet, nous passerons dans le prochain chapitre à la simulation de quelques méthodes Implémentées dans la solution envisagée.

Chapitre IV

MANAGEMENT DE LA SOLUTION

Parti 1 : Emulation de le protocole de la solution

Partie2 : Mise en place de serveur de centralisation des journaux

Parti 1 : Emulation de le protocole de la solution

IV.1 Introduction

Apres une présentation de solution propose des différents outils utilisés pour la centralisation des journaux pour fournir une étude théorique sur le projet, nous allons attaquer dans ce chapitre la phase de simulation de la topologie cible du projet, en simulant le réseau **NAFTAL** en utilisant des réseaux GNS3

IV.2 Environnement de simulation

➢ Prérequis matériels

Pour réaliser cette partie , nous avons utilisés un ordinateur portable présentant les caractéristiques suivantes :
Processeur : intel « core 15 cpu »
Mémoire installe : (RAM) 8g
Type de système d'exploitation : 64 bits
Système d exploitation : win7

➢ Prérequis logiciel

Nous avons une multitude d'outils de simulation de réseaux , quoi qu'une minorité prenne en charge la mise en œuvre de MPLS , c'est pour cette raison que nous avons choisi GNS3,en effet ce dernier présente plusieurs avantages .parmi lesquels nous citons :

- Il s'agit d'un logiciel open source et multiplateformes supportant MPLS et (VPN/VRF)
- Il peut être lie aux logiciels permettant l'émulation de machines telle que virtualbox et vmware et il supporte la connexion aux réseaux physiques.
- Il charge de véritables images IOS des routeurs Cisco dans un environnement virtuel

En fin il est nécessaire d'insister sur le terme émulation dans la mesure ou GNS3 s'appuie sur de véritable IOS téléchargeables et leur l'intégralité des fonctionnalités d'origine contrairement aux autres outils qui sont des simples simulateurs limites aux fonctionnalités implémentées par les développeurs de ces outils

Figure IV.1 : Logo GNS3

GNS3 (Graphical Network Simulator) est un simulateur d'équipements Cisco libre qui fonctionne sur de multiples plateformes indurant Windows, linux , et Mac.. GNS3 est capable de faire fonctionner des routeurs Cisco Virtuellement les rendant totalement réels, le contact avec le routeurs doivent avoir un système d'exploitation appelé IOS, contrairement à certains autres produits comme le paquet tracer propose par l équipements cisco, l'un des avantages de GNS3 c'est qu'on peut capturer er sniffer le trafic transitant sur une interface à l'aide de wireshark [**B24**]

IV.3 PRESENTATION DE LA TOPOLOGIE

Avant de commencer l'implémentation de la topologie sous **GNS3,** Nous allons évoquer la maquette de simulation. Pour des raisons liées aux performances de la machine physique, nous avons réduit la maquette afin de mener notre simulation dans de bonnes conditions, la figure ci-dessous montre la topologie.

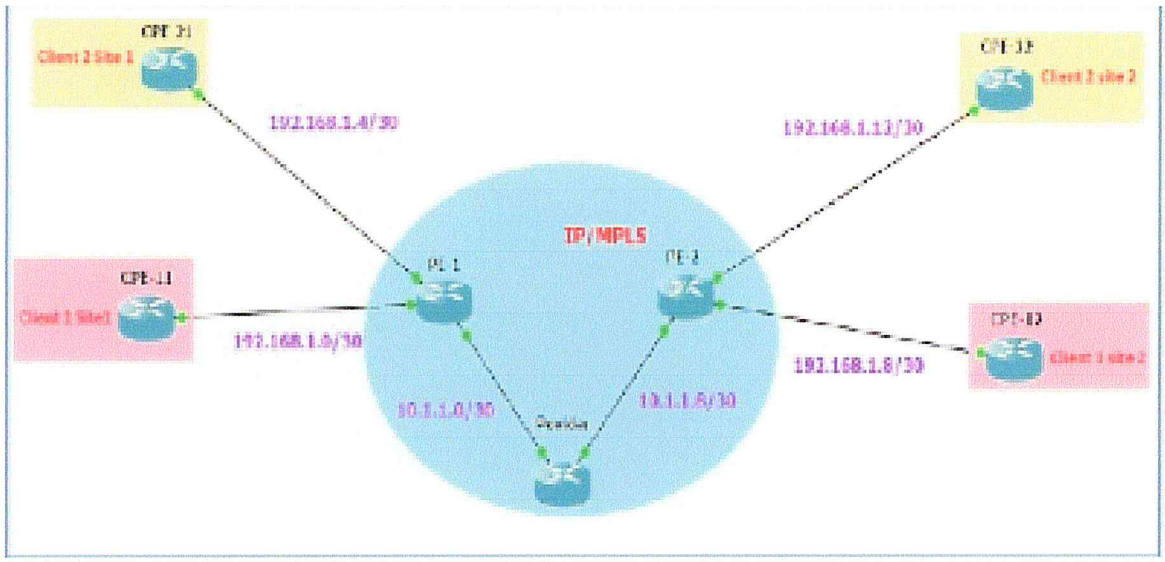

Figure IV.2 : Maquette de simulation

Comme il est montre par la figure, l'architecture de notre maquette comporte 3 routeurs 1 provider « P » et 2 provider Edge (PE1 et PE2). ainsi que 4 clients (CPE11 ,CPE12 ,CPE21 ,CPE22) pour la connexion des clients.

CPE i,j :(i : représente le client et j : représente le numéro de site)

Tous les routeurs sont de type cisco, la gamme 7200 utilisant comme image IOS « c7200- advipervicesk 9-mz-152-4 .55 bins supportant la technologie

IV.4 Table d'adressage

La table ci-dessous récapitulera l'adressage des différentes interfaces des routeur implemente

Routeur	Interface	Adresse IP
CPE11	G0/0 Connect to PE1	192.168.1.2/30
	Loopback0	172.16.11.11/32
CPE12	G0/0 Connect to PE2	192.168.1.10/30
	Loopback0	172.16.12.12/32
CPE21	G0/0 Connect to PE1	12.168.1.6/30
	Loopback0	172.16.21.21/32
CPE22	G0/0 Connect to PE2	192.168.1.14/30
	Loopback0	172.16.22.22/32
PE1	Loopback0	1.1.1.1/32
	G0/0 Connect to Provider	10.1.1.1/30
	G1/0 Connect to CPE21	192.168.1.5/30
	G2/0 Connect to CPE11	192.168.1.1/30
PE2	Loopback0	2.2.2.2/32
	G0/0 Connect to Provider	10.1.1.10/30
	G1/0 Connect to CE12	192.168.1.9/30
	G2/0 Connect to CE22	192.168.1.13/30
Provider	Loopback0	3.3.3.3/32
	G0/0 connect to PE1	10.1.1.2/30
	G1/0 connect to PE2	10.1.1.19/30

Tableau IV.1 : Adressage de la maquette

- **Configuration des interfaces**

  Dans cette étape nous devons configurer les différentes interfaces des routeurs à utiliser ci-dessous, un exemple de configuration de quelque interface du routeur PF1 (**Est illustre Annexe 1+2**)

Partie 2 : Mise en place de serveur de centralisation des journaux

IV.1 Introduction

La réponse à l'obsession des administrateurs réseaux précédemment posée, est articulée dans celle deuxième partie de la phase Management de notre solution. Ou nous mettrons en place un serveur de collecte et d'analyse des journaux d'évènements appelé « **ELK-STACK** » qui permet d'identifier et de régler les anomalies qui peuvent provenir sur les équipements, avant qu'elles provoquent des erreurs de production de l'architecture réseaux du **NAFTAL.**

IV.2 Mise en place de l'environnement

La solution de centralisation L'ELK-Stack peut être installée en utilisant une variété de méthodes et sur un large éventail de systèmes d'exploitation et d'environnements différents

Notre choix a été arrêté sur l'installation de la pile sur une machine virtuelle récipient le système d'exploitation Ubuntu version 18.04 LTS, une distribution s'inscrivant sous la fondation linux on a opté pour cette version de système d'exploitation pour sa convivialité, stabilité et sa communauté très active.

IV.2.1 Installation De La Machine Virtuelle

En utilisant la plateforme des virtualisation des systèmes d'exploitation Vmware Workstation pro 12, nous avons créé une machine virtuelle contenant le système d'exploitation **Ubuntu** 18.04 LTS

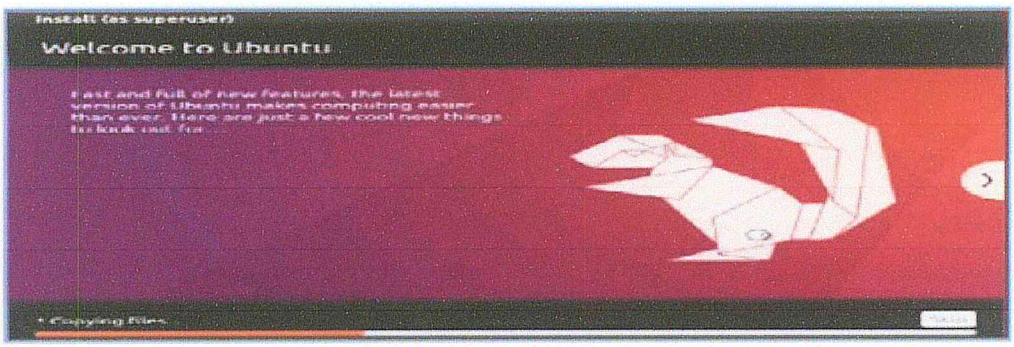

Figure IV- 3 : Processus d'installation d'Ubuntu 1804

IV.2.2 Connexion Gns3 - Machine virtuelle :

Pour rétablir la connexion entre réseau **NAFTAL** et le serveur Elk, Dans une première étape, nous allons créer une lnteface entre notre machine virtuelle et GNS3, et ce en ajoutant une 2ème carte réseau virtuelle « Vmnet10 » appartenant la plage publique 192.168.72.0 tel que montre la figurre suivante :

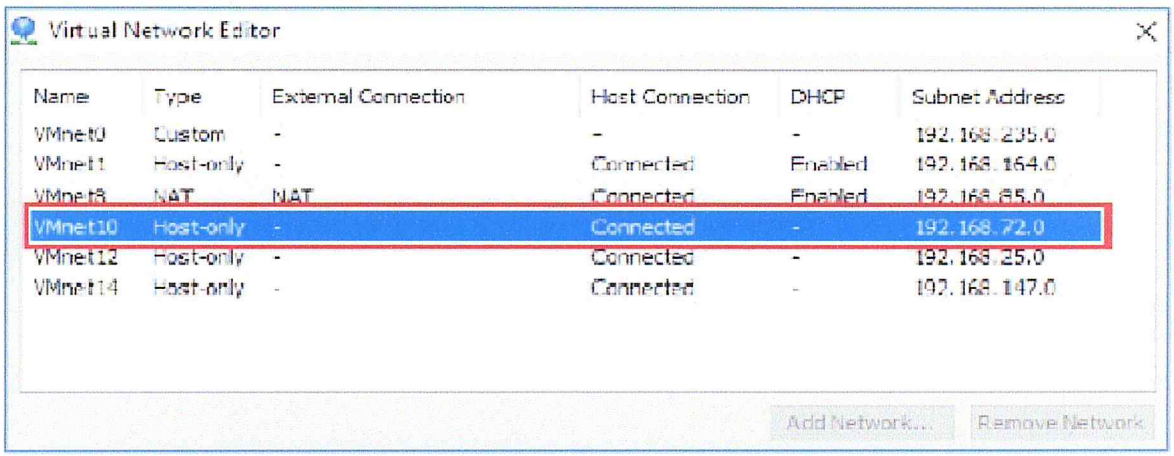

Figure IV- 4 : Ajout d'interface virtuelle

Il faut relancer le processus net working avec la commande « /etc/init.d/networking restart » pour que la nouvelle interface soit prise en compte. On arrive enfin à visualiser l'adresse IP de cette interface en palpant la commande « ip adress show » dans le terminal de la machine virtuelle. Le résultat est donne par la **Figure IV.6**

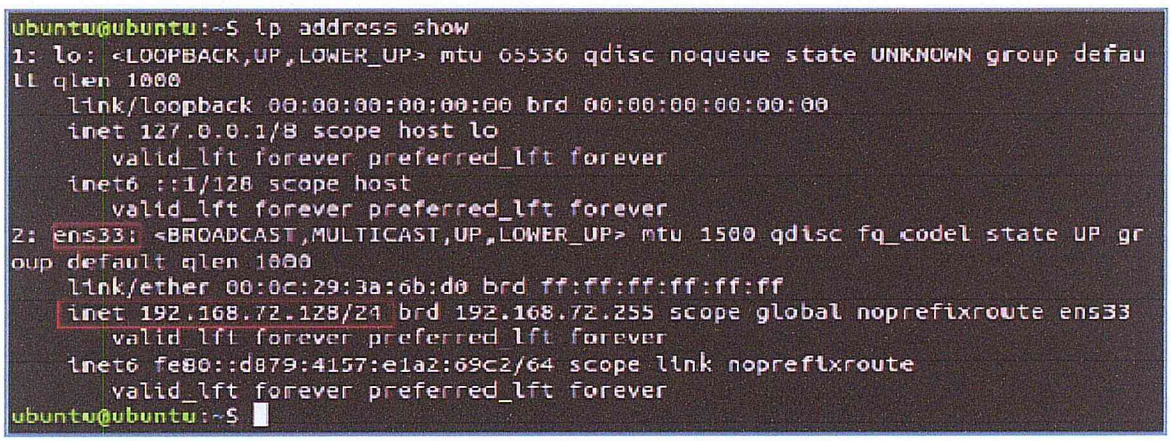

Figure IV. 5 : Adresses IP de l'interface de la machine hébergeant le serveur ELK

Par la suite nous avons lié notre zone réseau **NAFTAL** dans la maquette sous GNS3, via un cloud connecté directement à la même interface virtuelle déjà accordée dans la machine virtuelle hébergeant la pile ELK Comme i1 est montré dans la figure ci-dessous.

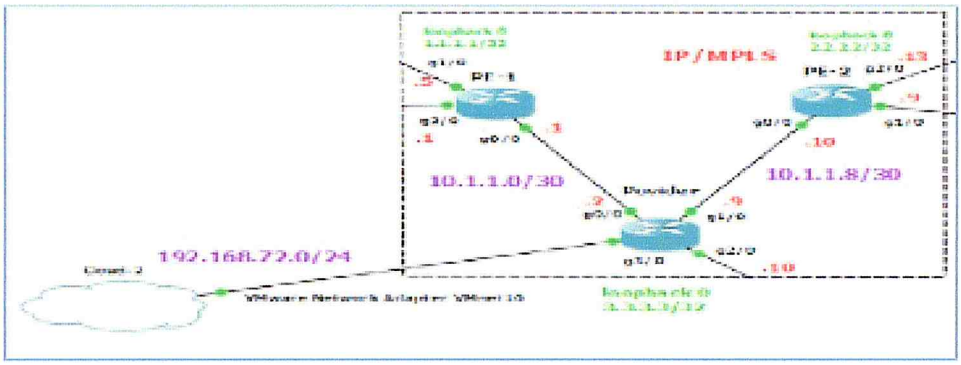

Figure IV- 6 : Couplage réseau NAFTAL -ELK

Afin de vérifier la connectivité entre la machine virtuelle hébergeant ELK-stack et les différents équipements réseaux de la zone réseau **NAFTAL**, il est nécessaire d'exécuter un Ping de la console d'Ubuntu vers les interfaces Loopback des routeurs par la commande « ping _ l'adresse loopoock du routeur »

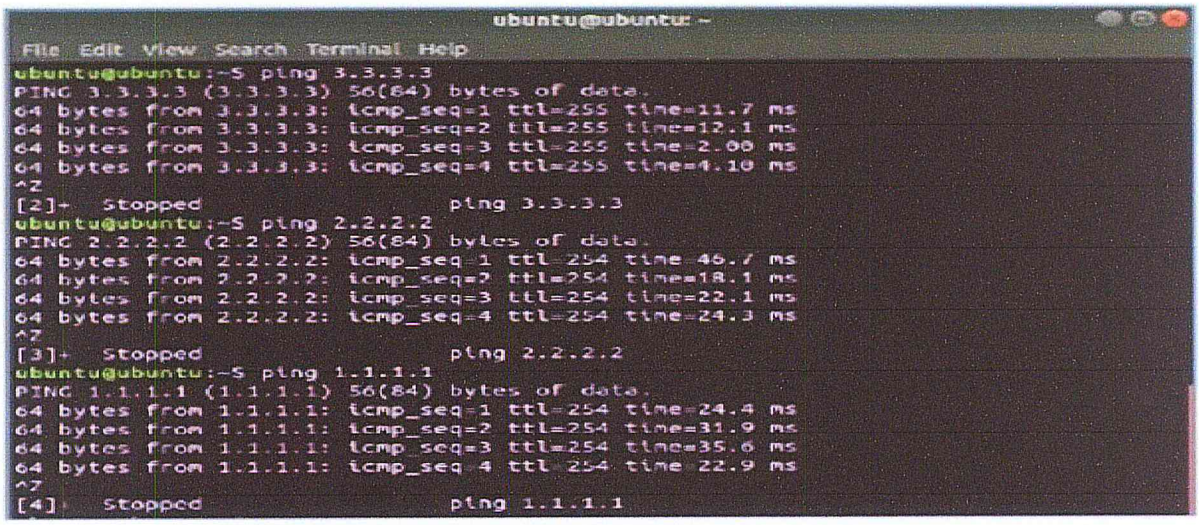

Figure IV- 7 : Test de connectivite réseau Naftal- ELK

On peut constater que la connectivité entre le serveur ELK et tous les routeurs du réseau a été rétablie avec succès.

IV.3 Installation de la pile ELK·stack

Après Avoir installé la machine virtuelle Ubuntu 18.04 et réalisé le couplage entre la dite machine et notre réseau, nous passerons en revue tous les éléments nécessaires pour créer la pile. Fonctionnelle. ELK-stack [**B25**]

- **Logstash** : composant responsable de traitement des journaux entrants.
- **Elasticsearch** : composant responsable de stocke et d'analyse des journaux
- **Kibana** : l'interface Web responsable de la recherche el la visualisation des journaux

IV.3.1 Insta11ation de Java 8

Elastlcsearch et Logstash nécessitent Java, nous allons donc installer une version récente d'Oracle Java 8 car c'est ce que recommande Elasticsearch Il devrait cependant fonctionner correctement avec OpenJDK.

L'installation de java est repartie en quatre étapes, en premier lieu on doit ajouter le référentiel Oracle Java dans la base de paquet APT système

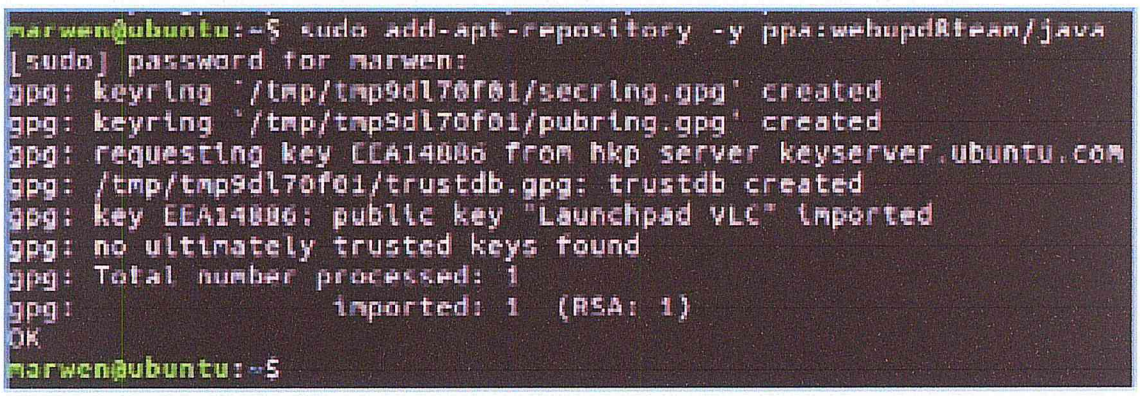

Figure IV.8 : Ajout d'un référentiel oracle java

Par la suite, il faut mettre à jours la base de données des paquets APT pour la prise en compte de la modification apportée

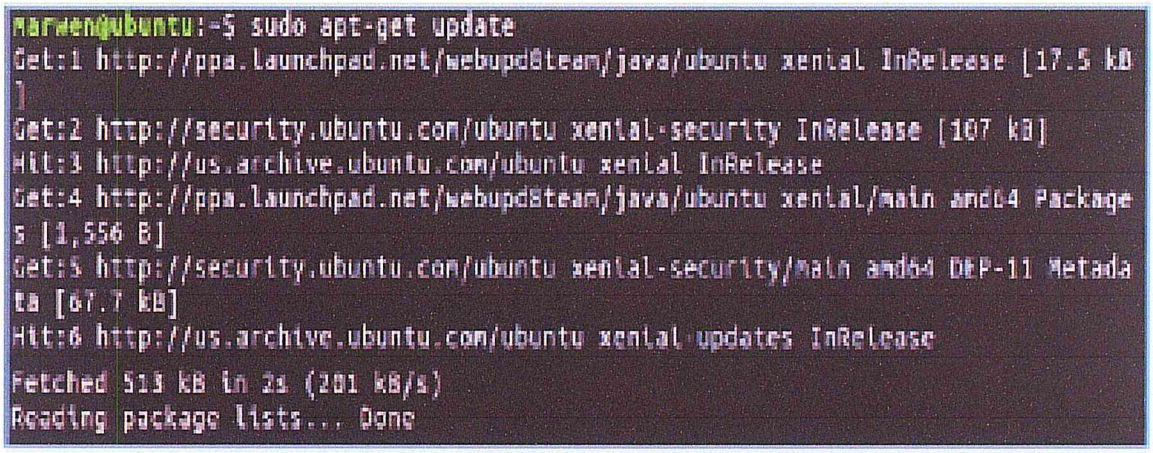

Figure IV- 9 : Mise à jour de base de données de paquets APT

Ensuite, on doit installer la dernière version stable d'oracle java 8 comme il est montre dans la figure suivante :

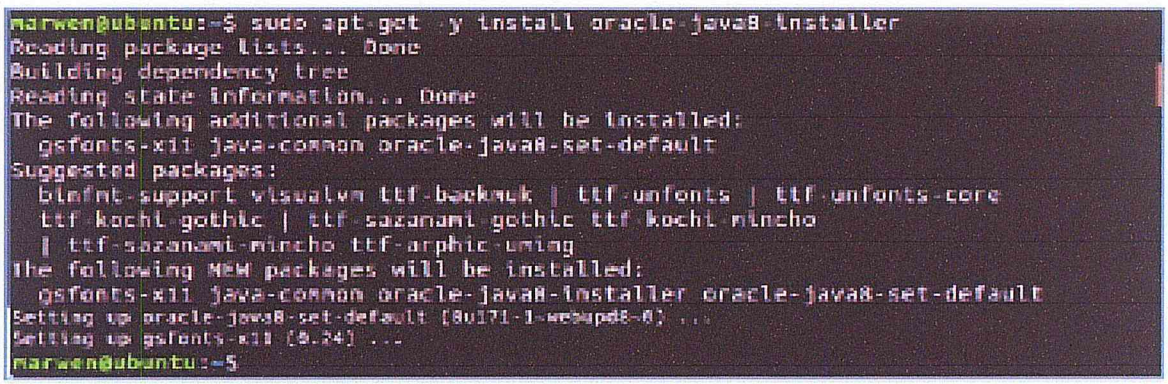

Figure IV-10 : Installation java8

Et finalement, il ne reste que vérifier la bonne installation et version java.

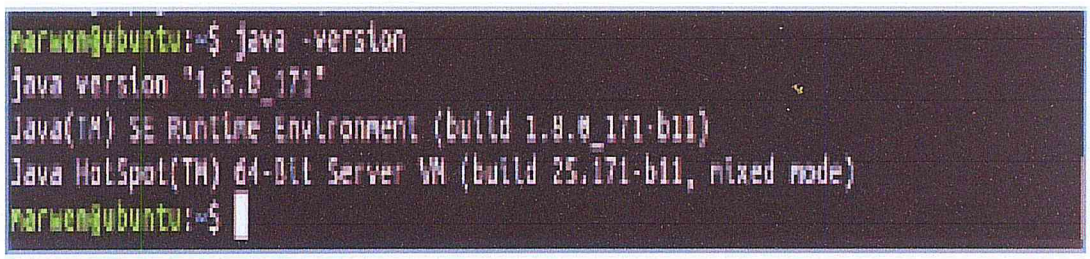

Figure IV-11 : Version java

IV.3.2 Installation d'Elasticserach

Elasticserach peut être installé avec un gestionnaire de paquets en ajoutant la liste des sources de paquets d'Elastic.

D'abord. On doit ajouter la clé de signature d'Elasric : pour que le paquet téléchargé puisse être vérifie

Figure IV-12 :clé de signature d'elastic

L'étape suivante consiste à ajouter la définition du référentiel dans le système avec la commande suivante

Tous ce qui reste à faire, est de mettre à jour des référentiels et installer elasticsearch

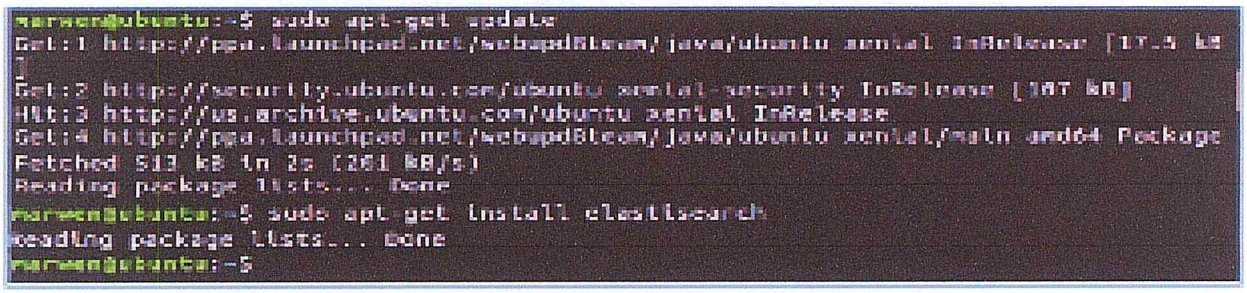

Figure IV- 13: Installation d'Elasticserach

IV.3.3 Installation de Logstash

Arrivant maintenant à l'installation de logstash, le package logstash .Est disponible dans le même référentiel qu'ElaticsParch, et puisque nous avons déjà installé cette clé publique, il ne reste que créer la liste source logstash par la commande suivante :

```
marwen@ubuntu:~$ echo "deb http://packages.elastic.co/logstash/2.2/debian stable
main" | sudo tee /etc/apt/sources.list.d/logstash-2.2.x.list
```

On doit maintenant Mettre à jour la base de données de paquets apt et installer logstash en utilisant les dites commandes suivante :

```
marwen@ubuntu:~$ sudo apt-get update
```

```
marwen@ubuntu:~$ sudo apt-get install logstash
```

IV.3.4 Installation de Kibana

Kibana peut être installé avec un gestionnaire de paquets en ajoutant la liste des sources de paquets d'elastic .donc on présente la commande suivante qui permet de créer la liste des sources de Kibana :

```
marwen@ubuntu:~$ echo "deb http://packages.elastic.co/kibana/4.5/debian stable m
ain" | sudo tee -a /etc/apt/sources.list.d/kibana-4.5.x.list
```

Par la suite on doit mettre à jour la base de données de paquets apt et installer kibana avec les commandes suivantes :

```
marwen@ubuntu:~$ sudo apt-get update
marwen@ubuntu:~$ sudo apt-get -y install kibana
```

Afin de vérifier le bon fonctionnement des trois composants de la pile ELK-stack. on doit tout d'abord les démarrer puis afficher leurs états de service. Les figures ci-dessous montrent le bon fonctionnement de la triade d'ELK.

```
marwen@ubuntu:~$ service elasticsearch start
marwen@ubuntu:~$ service elasticsearch status
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; disabled; vend
   Active: active (running) since Fri 2018-06-01 14:39:29 PDT; 11s ago
     Docs: http://www.elastic.co
  Process: 25463 ExecStartPre=/usr/share/elasticsearch/bin/elasticsearch-systemd
 Main PID: 25465 (java)
   CGroup: /system.slice/elasticsearch.service
           └─25465 /usr/bin/java -Xms2g -Xmx2g -XX:+UseConcMarkSweepGC -XX:CMSIn
```

Figure IV- 14 : Activation et état de service d'elasticsearch

```
marwen@ubuntu:~$ service logstash start
marwen@ubuntu:~$ service logstash status
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; disabled; vendor preset
   Active: active (running) since Fri 2018-06-01 14:43:43 PDT; 21s ago
 Main PID: 26521 (java)
   CGroup: /system.slice/logstash.service
           └─26521 /usr/bin/java -XX:+UseParNewGC -XX:+UseConcMarkSweepGC -XX:CM
```

Figure IV-15 : Activation et état de service logstash

```
marwen@ubuntu:~$ service kibana start
marwen@ubuntu:~$ service kibana status
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; disabled; vendor preset:
   Active: active (running) since Fri 2018-06-01 14:45:47 PDT; 842ms ago
 Main PID: 27240 (node)
   CGroup: /system.slice/kibana.service
           └─27240 /usr/share/kibana/bin/../node/bin/node --no-warnings /usr/sha
```

Figure IV- 16 : Activation et état de service kibana

Pour offrir une meilleurs flexibilité d'utilisation de la plie ELK-stack d'une façon automatique lors du démarrer du système. Pour ce faire on doit exécuter les commandes suivantes :

```
marwen@ubuntu:~$ sudo update-rc.d elasticsearch defaults 95 10
marwen@ubuntu:~$ sudo update-rc.d logstash defaults 95 10
marwen@ubuntu:~$ sudo update-rc.d kibana defaults 95 10
marwen@ubuntu:~$
```

Figure IV- 17 : Activation automatique des services ELK-stack

IV.4 Configuration de la pile ElK

Après installation des services d'ElK-stack. il faut maintenant les configurer pour qu'ils puissent recevoir et analyser les logs des routeurs de la zone réseau du **NAFTAL**

IV.4.1 Paramétrage d'Elasticserach

La configuration Elasticscsearch utilise un fichier de configuration appelé « elasticsearch.yml » qui nous permet de configurer les paramètres généraux tels que le nom de nœud. et les paramètres généraux tels que le nom de nœud, et les paramètres réseaux

Ce fichier est accessible par la commande suivante :

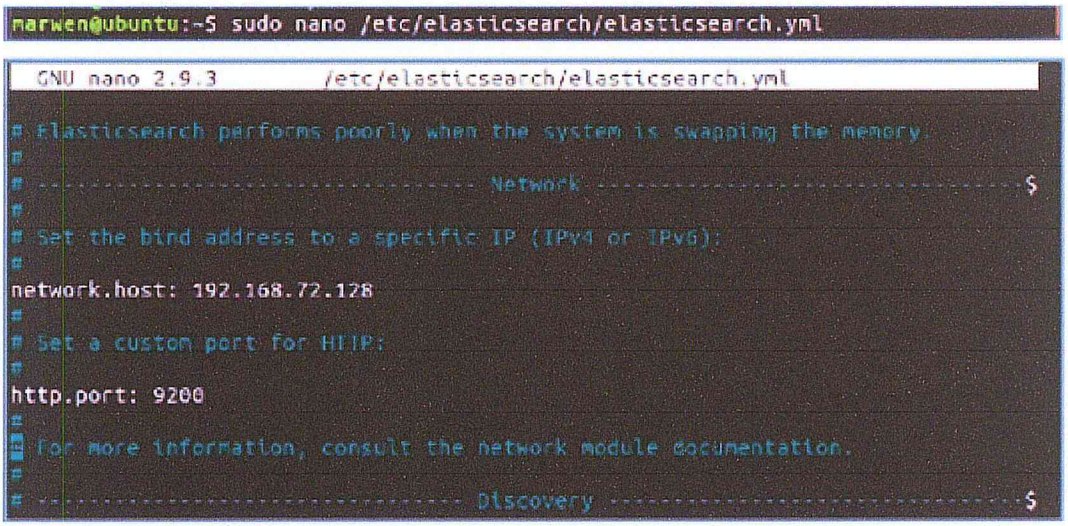

Figure IV-18 : Configuration Ela$ticsearch

Comme il est montré dans la figure ci-dessus.. nous avons associés Elasticsearch â l'adresse IP de notre machine virtuelle hébergent la pie ELK, ainsi que nous avons restreint l'accès extérieur a l'instance elasticsearch par l'affectation du port 9200, de sorte que les utilisateurs externes ne puissent pas lire les données.

IV.4.2 Paramétrage de Logstash

Le fichier de configuration de logstash est au format JSON. Il se trouve dans /etc/logstach/conf.d. la configuration prend, en considération deux paramètre importants, en premier lieu on doit affecter l'adresse IP de notre serveur ELK-stack, ainsi que le numéro de port d'écoute « 5011 » utilisé par moteur d'indexation logstash pour recueillir les logs et les collecter dans la Base de données Elasticsearch. La figure ci-dessous montre la configuration effectuée

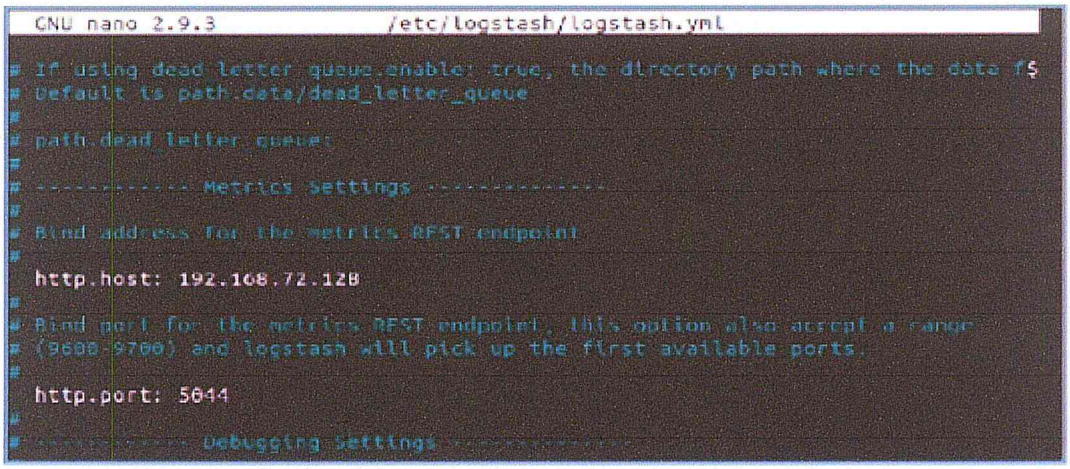

Figure IV- 19 : Configuration Logstash

IV.4.3 Paramétrage de Kibana

Il faut maintenant appliquer les paramètres nécessaires de Kibana en modifiant son fichier de configuration " Kibana.yml " existant sous le répertoire /etc/kibana/kiibana.yml. Comme il est montre dans la figure ci-dessus, les paramètres spécifiques indiquent a kibana a quelle connexion elasticsearch va se connecter et quel port va-t-il utiliser, cette adresse sera utilisée par la suite pour qu'on puisse connecter à l'interface graphique d"ELK stack et visualsEr les Journaux

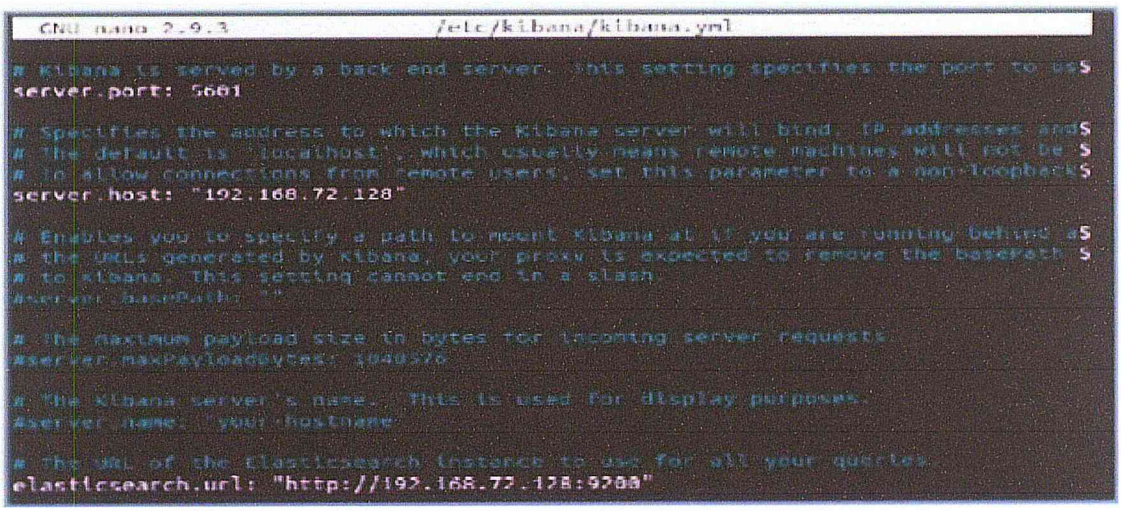

Figure IV- 20 : Configuration Kibana

IV.5 Analyse des journaux

IV.5.1 Configuration des routeurs

A ce stade la tout ce qui reste à faire est de rétablir renvoie des logs de la part des routeurs Vers .le serveur ELK. En premier lieu. Nous avons recours à activer le service logging aux niveaux de tous les routeurs en spécifiant l'adresse source d'envoie et

L'adresse destination du serveur auquel routeur va envoyer ses journaux ainsi que le type et le numéro du protocole.

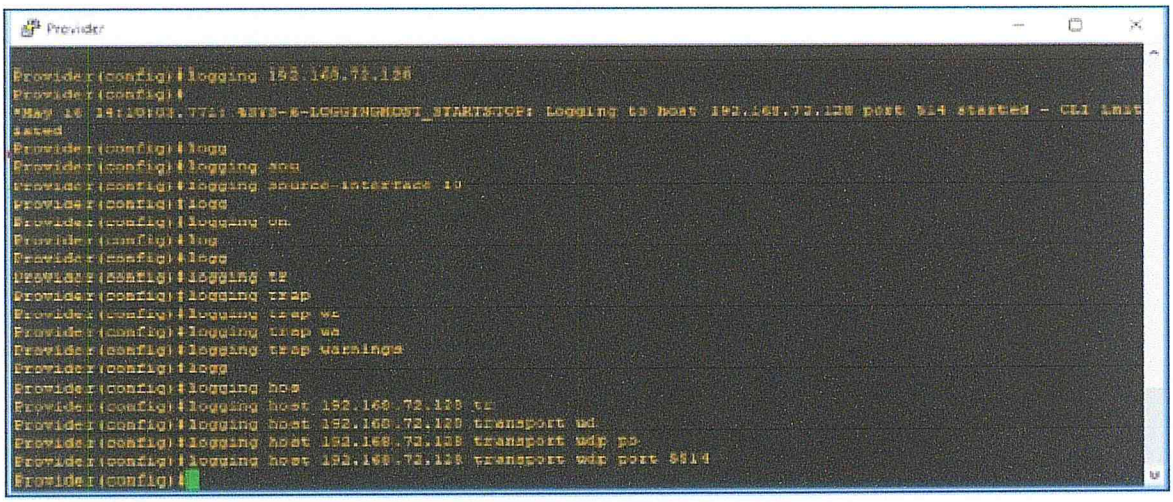

Figure IV-21 : Configuration logging du routeur Provider

Comme il est montré dans la figure, on a activé l'envoie des journaux d'évènement au niveau de routeur provider du réseau, en indiquant son adresse « loopback 0 » comme adresse source' d'envoie des logs, et l'adresse IP « 192.168.72.128 » comme adresse destination de serveur

ELK-,stack ainsi que spécifier type de journaux à envoyer et comme nous le savons, il existe sept niveaux de sécurité d'événements qui peuvent être envoyé. vers le Serveur d'analyse de log partant de 0 à 6 en fonction de degrés d'urgence:

- **Niveaux de sécurité « 0 » -Urgence.**
- **Niveaux de sécurité « 1 » -Alerte.**
- **Niveaux de sécurité « 2 » -Critique.**
- **Niveaux de sécurité « 3 » -Erreur.**
- **Niveaux de sécurité « 4 » -Avertissement (waming)**
- **Niveaux de sécurité « 5 » -Notification**
- **Niveaux de sécurité « 6 » -Information.**

Pour éviter la saturation du serveur par des évènements normaux tel que les notifications les informations, nous avons choisi d'activer l'envoie des logs, seulement pour les cinq premiers type, d'évènement les plus urgents (urgence, alerte', critique, erreur et avertissement) par la commande « logging trap warning ».

Et finalement, on n'a pas oublié bien sûr d'indiquer le protocole UDP et son port 5514, sur lequel connectent les routeurs pour transférer ses journaux.

IV.5.2 Configurations de script de log

Pour cette étape, nous avons créé un fichier script appelé **log2.conf** qui doit être exécute lors du démarrage du serveur ELK-stack, ce fichier contient les paramètres nécessaires pour la réception, l'indexation et la recherche des journaux envoyées par les routeurs du réseau.

- **Input/beats** : le numéro de port d'écoute « 5044 » utilise, par moteur d'indexation logstash pour recueillir les logs et les collecter
- **Protocole** : le type et le numéro de port du protocole auquel les routeurs vont envoyer les journaux
- **Type de log** : « Windows-Event-log », puisque dans notre cas les équipements qui vont envoyer ses journaux sont implémentes dans un environnement Windows 10.
- **Output** : logstash, après qu'il collecte es logs. il faut les indexer dans une Base de donnée et moteur de recherche elasticsarch. La dite tâche est assurée par la section output, ou nous avons indiqué. l'adresse IP et le port du moteur de recherche elasticsearch

La figure ci-dessous montre les paramètres procédés aux niveaux du fichier script **log2.conf**

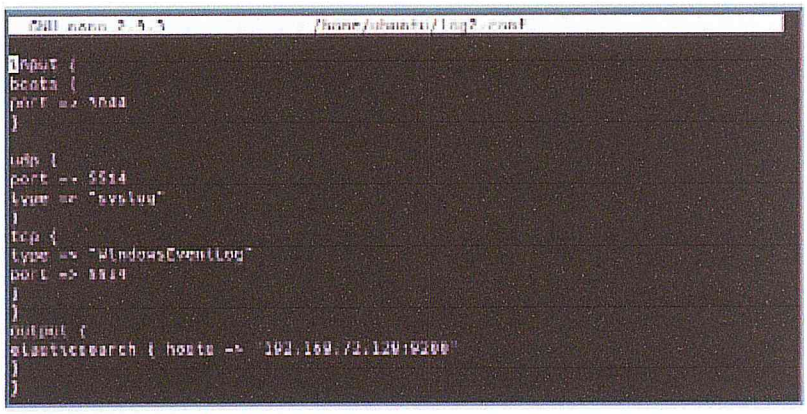

Figure IV- 22 : Configuration de script log2.conf

IV.5.3 Test d'analyse de log

Arrivant à la phase finale de vérification et test d'envoie des journaux des évènements des routeurs du reseau vers le serveur ELK-stack. Pour réaliser cette tâche nous avons recours en première étape d'exécuter le script « log2.conf » qu'on a créé précédemment, par La dite commande suivante:

```
ubuntu@ubuntu:/usr/share/logstash$ sudo bin/logstash -f /home/ubuntu/Log2.conf
```

Par la suite, on va produire une sorte d'incident comme la désactivation d'une interface de n'importe quel moteur de. la zone réseau de **NAFTAL ,** Nous avons pris l'exemple de la désactivation/activation de l'interface Giga-EtheNet 0/0 du routeur PE-1. Le résultat dans l'interface Graphique de Kibana est montré dans la figure ci-dessous.

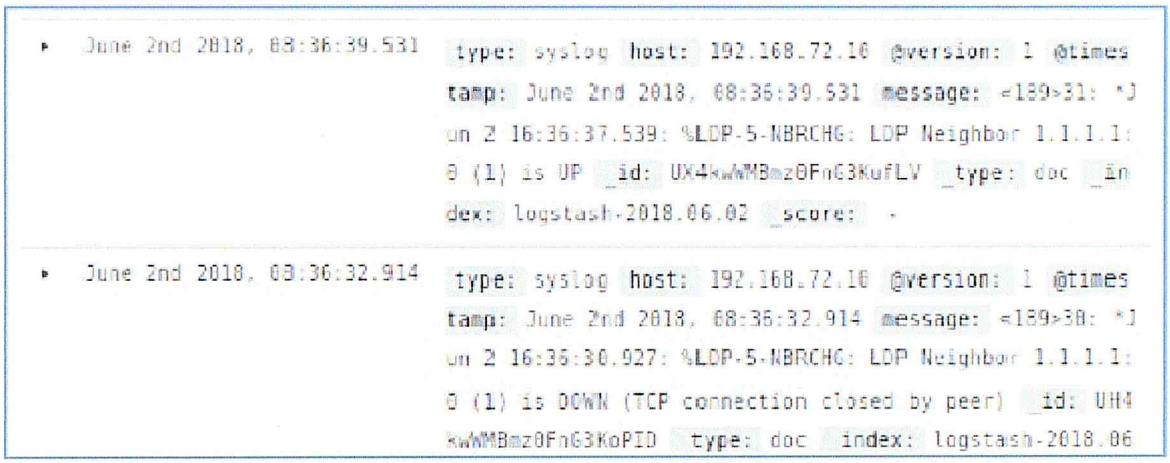

Figure IV- 23: Test d'analyse de log par EIK stack

les messages affichés annoncent a une date précise, que l'interface Giga-Ethemet 0/0 a été désactivée ce qui a provoqué l'arrêt du service de voisinage de routage OSPF (LDP Neighbors) entre le routeur Provider et le Provider Edge 1. Avant qu'il se réactivera de nouveaux ainsi que le service OSPE. Ces informations sont détectables par l'interface loopback 0 « 1.1.1.1 » du provider edge1.

IV.6 Gestion de l'interface Web de Kibana

L'interface de Kibana est composée de plusieurs parties dont les plus importantes:

- **Discover.**
- **Visualize.**
- **Dashboard.**

Après la connexion à Kibana, nous allons être redirigés vers la pace « Discover » où nous trouverons les logs reçus les plus récents.

Kibana offre un tableau de bord Intéressant avec une variété de représentations des différents résultats collectes par les shippers. Dans la figure ci-dessous. Nous

trouverons un histogramme qui illustre la fréquence d'arrivée des messages pendant une durée de temps donnée.

Figure IV- 24: Découvert des logs par Kibana

IV.6.1 Recherche des messages

Kibana nous permet de chercher un type de message donné en tapant dans la barre de recherche le message souhaité avec un Intervalle de temps précis. Nous pouvons aussi chercher par source en donnant une adresse IP.

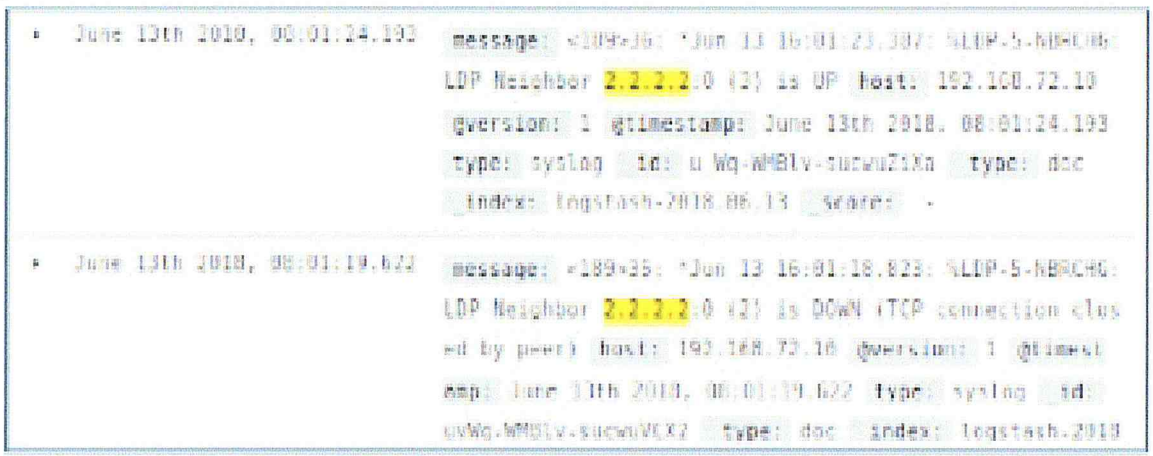

Figure IV- 25 : Recherche des messages sur Kibana

IV.6.2 Tableau de bord et visualisation

Dans la section « visualize » nous pouvons créer , modifier et voir nos propres visualisation, il y a différents types de visualisations comme les histogrammes, les pile charts, les tableaux de données ,etc… les visualisations peuvent etre sauvgardes et partages avec d'autres utilisateurs qui ont l'accès a l'instance kibana.

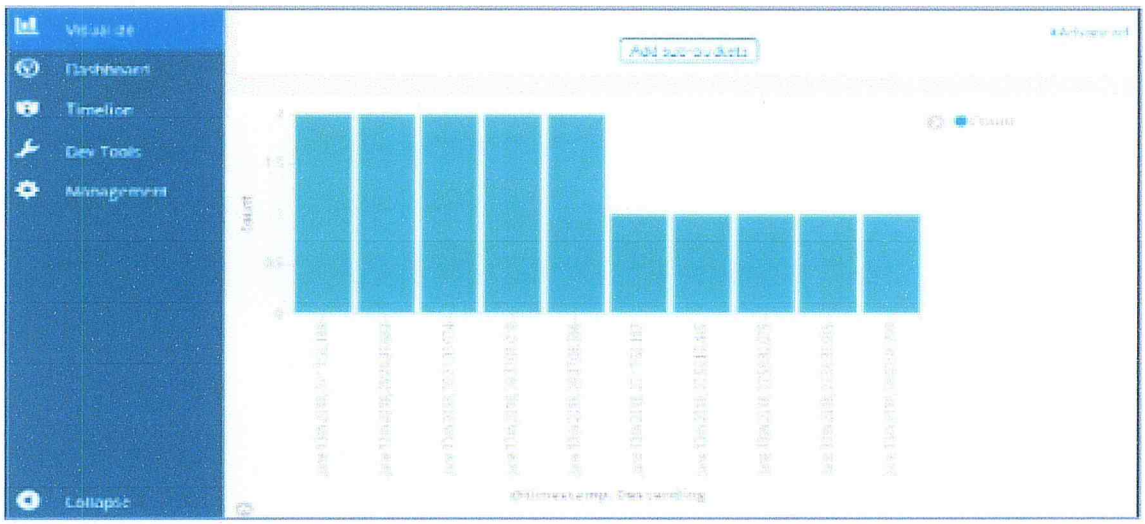

Figure IV-26 : Création de nouvelle visualisation

La troisième section de kibana « dashboard » nous permet de combiner toutes nos visualisations crées en une seule page pour pouvoir les gerer facilement .les tableaux de bord peuvent être filtres selon nos requêtes recherche

Figure IV-27 : Création d'un tableaux de bord

IV.6.3 Génération des rapports

La plateforme ELK nous permet d'élaborer des rapports d'informations concernant les équipements réseaux et système, tout en sauvegardant dans sa base de données les différents logs des utilisateurs de réseau, les rapports peuvent être affiches sous format HTML. Ce qui est très pratique pour l'administrateur s'il a des messages logs importants dont il veut garder une copie pour la disponibilité.

IV.7 Conclusion

Dans cette deuxième partie, nous avons exposé en détail les étapes de l'installation avec les conditions préalables de la pile ELK-STACK comme une deuxième étape, nous avons configure les équipements réseaux de la zone réseau **NAFTAL** simulée sous GNS3, pour qu'ils puissent envoyer ses journaux finissant par le test de la solution d'analyse des logs.

Ce chapitre a également étudie les caractéristiques offertes par le serveur virtuels implémentes dans notre projet, le serveur d'analyse de logs et « ELK-Stack », qui sont très utiles à l'administrateur réseaux pour faciliter son travail en créant des statistiques des analyses à l'aide des journaux d'évènements reçus

Conclusion générale

Ce rapport s'inscrit dans le cadre d'un projet de fin d'études élaboré au sein de la société direction générale **NAFTAL** .durant ce stage , nous étions chargées pour la conception et la mise en place d'un SIEM, comme nous venons de le voir, la mise en place de cette solution n'est pas forcement complexe, mais elle exige tout de même qu'on suive une démarche structurée et rigoureuse.de ce fait, un travail et une analyse de l'environnement dans lequel fonctionne notre solution, ont été faits afin de dégager les besoins et les exigences ciblées.

Le projet s'articulait ainsi autour de deux principaux volets à savoir :

La simulation d'une topologie prototype de réseau **NAFTAL**, par l'émulation de quelques techniques proposées.

La mise en place d'un système de centralisation et d'analyser des journaux des équipements réseaux, dont le but est d'anticiper les pannes qui peuvent se produit

Le travail dans le cadre de ce projet de fin d'étude, était d'une importance considérable dans la mesure où il nous a servi comme portail vers le monde professionnel et la vie en entreprise l'environnement du travail dans ce cadre nous a permis de renforcer nos capacités de communication, de s'intégrer au sein d'une équipe et de faire face aux difficultés inhérentes telles que la gestion du temps et des efforts

En termes de perspectives, plusieurs améliorations restant envisageables dans ce travail ces améliorations touchent essentiellement l'extensibilité de notre solution pour prendre en charge d'autres fonctionnalités a savoir :

- Corrélation des logs entre le serveur supervision et le serveur **SIEM**
- Intégration de la notification par sms dans elk-stack

Références bibliographiques

[B1] SITE OFFICIEL DG NAFTAL URL : HTTPS://WWW.NAFTAL.COM

[B2]Https//ogma-sec.fr/quest-ce-que-la-sccuritc-de-linformationl

[B3]Http://Www.Cn-Cncc.Dz/Images.Lboulahdourpdf

[B4]O.SANTOSetJ.STUPPI,CCNA Security210-260 Official Cen Guide ,USA Cisc

[B5] S.GHERNAOUTI,sécurité informatique et réseaux 4èm édition, Paris :Dunod2013.

[B6]C.LIORENS, L.LEVIER et D.VALOIS, Tableaux de bord de la sécurit éréseau, Paris: Eyrolles,2006

[B7] C.PINET,10cléspourlasécuritédel'informationISO/CE27001,Afuor,2012

[B8] IOS/IEC TR 27000 :2009

[B9] IOS/IEC TR 18044 :2004

[B10]HTTPS://WWW.SSI.GOUV.FR/ENTREPRISE/GLOSSAIRE/I/

[B11] NIST SP 800-82 REV .2 SOUS ATTAQUE (CNSSI 4009)

[B12] GUIDE IOS/IEC 79 :2002

[B13] Nagios open source .URL:[http://www.nagios.org/]

[B14]Article supervision réseaux ZABBIX réalisé par[VincentBENIOIST] publie le [08/10/2016] URL:[https//www.supinfo.com/articles/single/2482-supervision-reseau-zabbix]

[B15] INTRODUCTION CHEK-MK URL:// [HTTPS://WIKI.MONITORING-FR.ORG/NAGIOS/ADDONS/CHEK-MK/START]

[B16]aticlz universite de Toulon[mise en place d'une supervision] relaise par[Jean Phllipe Baruteu] publie 21/04/2016

[B17] https:// www.ssi.gouv.fr/actualite/prevention-detection-et-reponse-aux-incident-au-centre-des-preoccupations-des-gs-day-2016

[B18] article LOG URL://https/// support.ankama.com/hc/fr/articles qu-est-ce-que un log publie 15/01/2014

[B19]article [La gestion des evenements et des incidents] auteur [Lionel GUILLET] Publie le [14/08/2011]

[B20] documentation Graylog 2.4 architecture et composant URL: [Https/// docs.graylog.org/en/2.4/pages/architecture.html]

[B21] blog officiel de fluentd URL:[Https//www.fleuentd.org/blog/]

[B22] déploiement ELK en conditions réelles/ présentation faite lors de l'edition 2016 du breizhcamp à rennes URL :[https://fr.slideshare.net/geoffroyanoud/deploiement –elk-en condition réelles publie le 25/03/2016

[B23] Article Introduction Elk :Publie Par [Olivier Jan]Le 30/04/2014

Configuration des interfaces

Annexe 1 :

```
PE2# conf t
PE2 (config)# interface Loopback 0
PE2 (config-if)#ip address 2.2.2.2 255.255.255.255
PE2 (config-if)#interface g0/0
PE2 (config-if)#ip address 10.1.1.10 255.255.255.252
PE2 (config-if)#no shutdown
PE2 (config-if)#interface g2/0
PE2 (config-if)#ip address 192.168.1.13 255.255.255.252
PE2 (config-if)#no shutdown
PE2 (config-if)#interface g1/0
PE2 (config-if)#ip address 192.168.1.9 255.255.255.252
PE2 (config-if)#no shutdown
```

```
Provider# conf t
Provider (config)# interface Loopback 0
Provider (config-if)#ip address 3.3.3.3  255.255.255.255
Provider (config-if)#interface g0/0
Provider (config-if)#ip address 10.1.1.2  255.255.255.252
Provider (config-if)#no shutdown
Provider (config-if)#interface g1/0
Provider (config-if)#ip address 10.1.1.9 255.255.255.252
Provider (config-if)#no shutdown
Provider (config-if)#interface g2/0
Provider (config-if)#ip address 192.168.85.10 255.255.255.0
Provider (config-if)#no shutdown
Provider (config-if)#interface g3/0
Provider (config-if)#ip address 192.168.72.10 255.255.255.0
Provider (config-if)#no shutdown
```

```
PE1# conf t
PE1(config)# interface Loopback 0
PE1(config-if)#ip address 1.1.1.1 255.255.255.255
PE1(config-it)#interface g0/0
PE1 (config-if)#ip address 10.1.1.1 255.255.255.252
PE1(config-it)#no shutdown
```

```
CPE-21# conf t
CPE-21 (config)# interface Loopback 0
CPE-21 (config-it)#ip address 172.16.21.21 255.255.255.255
CPE-21 (config-if)#interface g0/0
CPE-21 (config-if)#ip address 192.168.1.6 255.255.255.252
CPE-21 (config-if)#no shutdown
```

ANNEXE 2

```
Provider(config)# router ospf 1
Provider(config-router)# network 10.1.1.0 0.0.0.3 area 0
Provider(config-router)# network 10.1.1.8 0.0.0.3 area 0
Provider(config-router)# network 3.3.3.3  0.0.0.0 area 0
```

```
PE2(config)# router ospf 1
PE2(config-router)# network 10.1.1.8 0.0.0.3 area 0
PE2(config-router)# network 2.2.2.2  0.0.0.0 area 0
```