

Rapport de Projet de stage d'été

Ingénierie des Systèmes Informatiques " Computer Engineering"

Spécialité : Ingénierie des Réseaux et Systèmes

Par

Nidhal Ghazouani

*Etude comparative des solutions de gestion de la sécurité des
systèmes d'information NAC (open-sources et payants)*

Encadrante professionnel : Oumayma Ayadi

Réalisé au sein d' Adactim



Sommaire

Introduction Générale	3
Chapitre 1 : Contexte du Projet.....	5
Introduction	5
1. Cadre général	5
2. Organisme d'accueil :	5
3. Problématique	6
4. Solution proposée	7
5. Démarche méthodologique	7
5.1. Démarche suivi	7
Conclusion	7
Chapitre 2 : Notions de bases et étude technique.....	8
Introduction	8
1. Présentation des notions de base	8
1.1. La sécurité informatique	8
1.2. Le contrôle d'accès au réseau	10
Chapitre 3 : Etude Comparative entre Solution NAC	14
Introduction :	14
1. Présentation des solutions de contrôle d'accès au réseau (NAC)	14
1.1. Les solutions de contrôle d'accès commerciales	14
1.2. Les solutions de contrôle d'accès libres	15
2. Etude Comparative entre Solution NAC	16
2.1. Etude comparatives des solutions NAC commerciales et libres	16
3. Problèmes rencontrés	27
Conclusion	27
Conclusion & Perspectives	28

Liste des figures

Figure 1 : Organigramme de la Société Adactim	6
-----------------------------------------------------	---

Liste des tableaux

Tableau 1 :Comparaison de quelques solutions libres	16
Tableau 2 :Comparaison entre les solutions NAC commerciales et libres	17
Tableau 3 :Les Points forts et faibles d'Endian Firewall	23

Introduction Générale

En 2018 de plus en plus l'importance des nouvelles technologies, les habitudes de travail changent, ordinateurs, les smartphones, les tablettes et des quantités énormes de données facilement sauvegardée sur clé USB et les mini cartes mémoire, De ce fait la sécurité réseau des entreprises s'avère être menacée et difficile à être contrôlée.

La sécurité des terminaux ne s'arrête plus sur un pare-feu personnel ou un antivirus. On cherche un concept de protection par une application qui garantit une validation des politiques de sécurité.

La solution de contrôle d'accès au réseau (NAC) est une technologie garantissant un accès sécurisé aux ressources réseau des entreprises en se basant sur l'authentification et l'identification des utilisateurs et des machines en plus la vérification de leurs compatibilités d'avec les stratégies de la sécurité.

Le NAC permet de protéger contre les logiciels malveillants (pirates), et de contrôler l'accès au réseau pour les personnels, les stagiaires, les fournisseurs ou autres personnes n'appartenant pas à l'entreprise pour ce faire la tâche de l'administrateur réseau est réduit, les failles de sécurité seront fermées potentiellement, avec une grande visibilité des activités.

L'entreprise d'accueil Tunisie Telecom permet aux employés, les clients et les invités d'apporter leurs propres appareils, de gérer d'une manière efficace l'accès sur son réseau, donner les privilèges d'accès selon les tâches prédéfinies, s'assurer que les politiques de sécurité sont appliquées, supprimer les logiciels nuisant la sécurité, gérer le réseau d'une manière simple. Pour se faire, une architecture sécurisée est nécessaire. Pour cela, le cœur d'une telle architecture devra être basé sur un firewall. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela représente une sécurité supplémentaire rendant le réseau ouvert sur Internet beaucoup plus sûr. De plus, il peut permettre de restreindre l'accès interne vers l'extérieur c'est le cadre de notre projet de fin d'étude intitulé « Mise en place d'une solution de contrôle d'accès au réseau ».

Ce mémoire est composé de quatre chapitres :

- Le premier chapitre est consacré à une présentation du contexte du projet illustrant notre travail.
- Le deuxième chapitre présente un état de l'art présentant une étude générale sur les

technologies des solutions de contrôle d'accès et une étude technique sur la solution choisie.

- Le troisième chapitre sera réservé à l'analyse des besoins et la conception de la solution
- Le quatrième chapitre sera réservé au déploiement de notre solution de contrôle d'accès au réseau (NAC) et des tests et évaluation des fonctionnalités de la solution réalisée au cours de ce projet de fin d'étude.

Chapitre 1 : Contexte du Projet

Introduction

Ce chapitre sera dédié à l'exposition du contexte général de notre projet de stage d'été

D'abord, nous présentons le cadre général de notre projet, ainsi nous parlerons de l'organisme d'accueil Tunisie Télécom, son organigramme et ses différentes missions et services. Ensuite, nous dégagons la problématique liée à notre projet pour aboutir aux objectifs fixés par l'entreprise. Par la suite, nous présenterons la méthodologie de travail adoptée.

1. Cadre général

Le présent projet intitulé « Etude et mise en place d'une solution de contrôle d'accès au réseau », a été réalisé dans le cadre de la préparation du projet de fin d'études présenté en vue de l'obtention du diplôme de mastère à l'UVT pour l'année universitaire 2017/2018. Il a été réalisé au sein de la société Tunisie Télécom

2. Organisme d'accueil :

Filiale du groupe WEVIOO et PGH,

ADACTIM est un opérateur de services managés ERP et Cloud. Elle accompagne ses clients tout au long des cycles de transformation de l'entreprise (audit, conseil, intégration, infogérance, roll out).

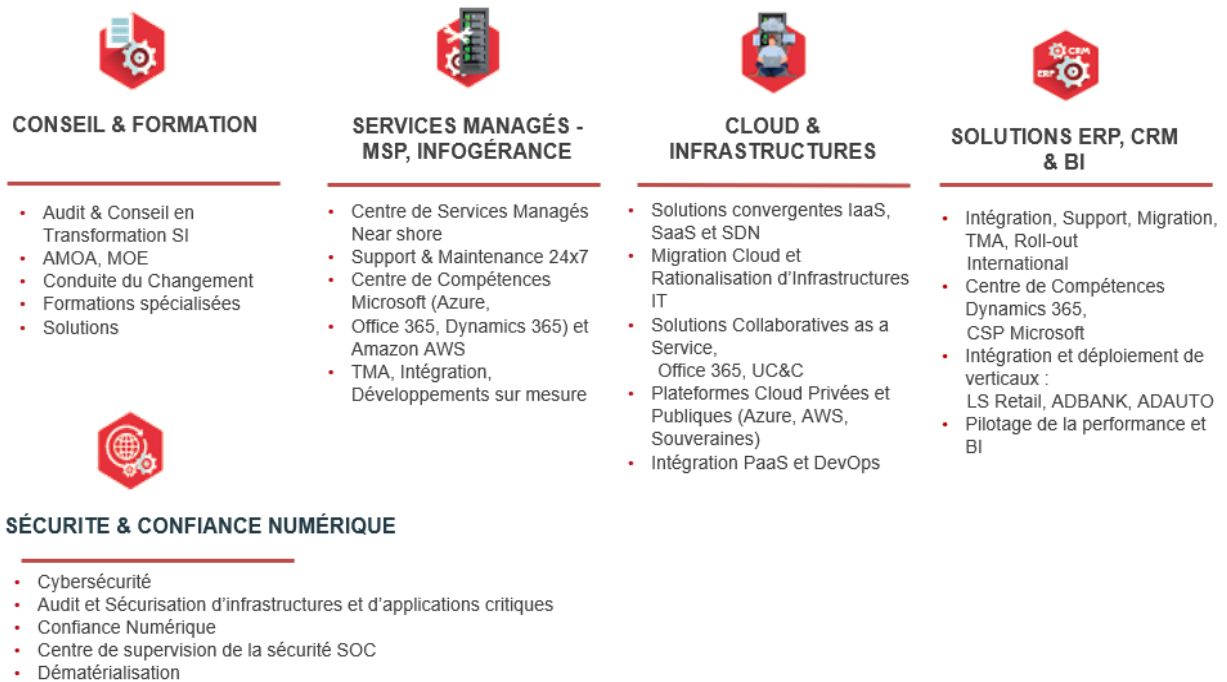
Adactim a ainsi pour mission d'assurer les activités relatives au domaine des services managés ERP et Cloud. Il est notamment chargé de :

- accompagne ses clients dans leurs projets de transformation métier et technologique.
- aide à optimiser et à simplifier leur processus de gestion ainsi que l'exploitation de leur système d'information, ainsi que leur infrastructures et services
- fournit ses solutions et ses services aux entreprises régionales et aux multinationales dans le monde entier.



Notre Expertise :

OPÉRATEUR DE SERVICES MANAGÉS, CLOUD ET ERP



La figure 1 présente l'organigramme de l'entreprise :

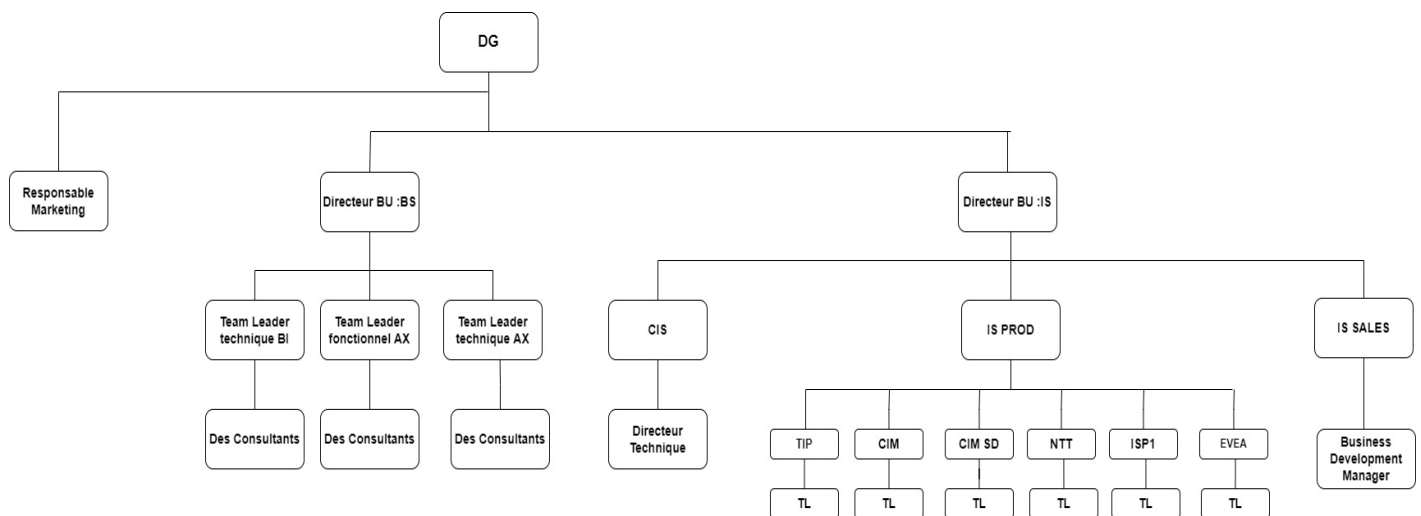


Figure 1 : Organigramme de la Société Adactim

3. Problématique

Le cadre de mon projet est de faire Etude comparative entre Les solutions de Contrôle d'accès réseau qui est dédiée principalement pour le traitement des réclamations DATA et Mobile des clients grand compte (Entreprise et client).

Suite à l'étude des différentes fonctionnalités on a relevé un certain nombre d'inconvénients à savoir :

- Les serveurs et des ordinateurs de bureau et portable qui ne respectent pas la confidentialité des données (accès aux NMS : équipement client et ID client : profile).

- L'accès est permis à tous les sites internet quel que soit l'internaute.
- Pas de scan des terminaux avant l'accès au réseau.
- réseaux locaux ouverts.

Dans ce cadre, les responsables cherchent des solutions de sécurité à haut niveau et moins complexes pour garantir un réseau efficace aux fournisseurs, aux partenaires et aux employés mobiles ou distants.

Pour ce faire je vais faire l'étude comparative entre les solution de sécurité au sein de mon réseau local ce qui permet le contrôle d'accès au réseau.

4. Solution proposée

Afin de réussir l'étude comparative d'une solution NAC, en respectant les exigences matérielles et logicielles de l'entreprise et les besoins réels de l'utilisateur.

Il faut assurer les objectifs suivants :

- Refuser l'accès des utilisateurs au réseau sans authentification.
- le contrôle de conformité.
- la traçabilité et la visibilité.
- Gérer les ressources réseau (exemple la bande passante).
- Contrôler l'accès aux ressources du réseau afin d'empêcher toute attaque.
- Administrer et suivre quotidiennement le journal des alertes.

Cette solution doit permettre d'atteindre ces objectifs par la mise en place d'une topologie réseau en utilisant une solution NAC performante, l'intégration et la configuration des outils assurant la sécurité et le développement d'une interface d'authentification

5. Démarche méthodologique

Lors du développement d'un projet, il est nécessaire de suivre une méthode de conception. Cette méthode doit être composée d'une démarche. La démarche décrit les différentes étapes nécessaires pour traduire les besoins des utilisateurs en un produit logiciel. Cette dernière (démarche) permet d'augmenter la productivité et d'estimer le temps de développement.

5.1. Démarche suivi

Pour le déroulement de notre projet, nous avons choisi de suivre la démarche suivante :

- **Etude technique** : elle consiste à faire des recherches et étude comparative de la solution NAC

Conclusion

Ce premier chapitre a été consacré à la présentation de l'organisme d'accueil et la mise du projet dans son cadre général, en introduisant la problématique et les objectifs du projet. Nous avons aussi annoncé la démarche qui vont être suivis tout au long de ce projet

Chapitre 2 : Notions de bases et étude technique

Introduction

Dans ce chapitre on va initier par la présentation des notions fondamentaux du contrôle d'accès, la présentation des solutions de contrôle d'accès existent sur le marché puis de choisir la solution NAC adéquate.

1. Présentation des notions de base

1.1. La sécurité informatique

1.1.1. Exigence fondamentale à la sécurité

La sécurité du réseau informatique d'une entreprise a pour objectif de faire des actions contre les menaces intentionnelles ou accidentelles. Le système informatique est souvent établi par la totalité des informations et des ressources matérielles et logicielles de la société permettant de les stocker ou de les faire transiter. Il représente un patrimoine important de la société, qu'il est nécessaire de sécuriser.

La sécurité de l'information protège l'information d'une multitude de intimidations afin de garantir la continuité de l'organisme, restreindre les dommages et participer le plus que possible à avoir le degré de protection désiré.

La sécurité de l'information vise la confidentialité, de l'intégrité et de disponibilité de l'information :

- **Confidentialité** : Assure le secret de l'information. Au moment où la confidentialité est convenablement garantie, elle permet l'accessibilité à l'information aux seuls utilisateurs autorisés. Il est ici question d'endiguer toute révélation non admis des dispositifs et information,
- **Intégrité** : Garantit la conformité de l'information. Elle permet aux utilisateurs d'avoir l'assurance que l'information est exacte et qu'elle n'a pas été changée par une personne non autorisé. Il est ici question d'endiguer toute altération non admis des dispositifs et informations,
- **Disponibilité** : Assure que l'information parvienne à être utilisable. Elle permet aux utilisateurs de pouvoir accéder aux applications qui traitent ces

informations. Il est ici question de contrarier toute arrêt de prestation et de productivité.

1.1.2. Attaque et contre-attaque

1.1.2.1. Le virus :

Un virus informatique est un type de code ou programme malveillant qui vise à modifier le fonctionnement d'un ordinateur et à se répandre d'une machine à une autre. Le virus informatique est intégré dans un programme ou joint à un document légitime qui prend en charge les macros afin d'exécuter son code. Il peut ainsi avoir des effets inattendus ou causer des dégâts : il endommagera par exemple un logiciel système en altérant ou détruisant des données.

L'excellente solution est l'emploi d'un logiciel de sécurité à jour et de faire les patches des applications afin de fuir l'utilisation des bugs.

1.1.2.2. L'écoute du réseau (Sniffer) :

Il existe des logiciels qui, à l'image des analyseurs de réseau, permettent d'intercepter certaines informations qui transitent sur un réseau local, en retranscrivant les trames dans un format plus lisible (Network packet sniffing).

La meilleure solution contre cette attaque est l'utilisation d'une carte SIM ou d'une calculatrice à mot de passe.

1.1.2.3. Le cheval de Troie :

Suite l'accès au système cible, les pirates utilisent la crédibilité en installant un logiciel qui permet de transmettre les données par web.

La meilleure solution est de contrôler l'accès des utilisateurs à l'ordinateur et d'installer et mettre à jour des antivirus.

1.1.2.4. Le Déni de service (DDoS) :

Le "Distributed denial-of-service" ou déni de service distribué est un type d'attaque très évolué visant à faire planter ou à rendre muette une machine en la submergeant de trafic inutile (voir fiche DoS). Plusieurs machines à la fois sont à l'origine de cette attaque (c'est une attaque distribuée) qui vise à anéantir des serveurs, des sous-réseaux, etc.

D'autre part, elle reste très difficile à contrer ou à éviter. C'est pour cela que cette attaque représente une menace que beaucoup craignent.

La meilleure solution contre cette attaque est le firewall ou la répartition des machines sur un réseau sécurisé.

1.2. Le contrôle d'accès au réseau

C'est un mécanisme permettant de sécuriser les actifs de la société des intimidations et des faiblesses en bridant l'usage d'une ressource (physique : Serveur, Point d'Accès, Routeur, ou rationnel : Application, Système d'informations, Processus) du si aux seules structures autorisées.

1.2.1. Le principe de fonctionnement

Le principe de fonctionnement du processus de contrôle d'accès au réseau :

- Indiquer quels utilisateurs peuvent avoir accès au système,
- Indiquer les ressources auxquelles ils peuvent avoir accès,
- Indiquer les opérations qu'ils peuvent réaliser,
- Donner la responsabilisation de chacun.

1.2.2. Les différents types

On distingue trois types de contrôle d'accès à savoir :

- **Technique:** ce genre de contrôle d'accès touche l'ensemble des accès logiques aux

ressources du si. Il est intégré avec des règlements logicielles et matérielles se basant sur des technologies,

- **Physique :** Il touche l'ensemble des accès physiques aux bâtiments et ressources matérielles,
- **Administratif :** ce type de contrôle d'accès est opéré via des documents exposant les stratégies, les responsabilités et les fonctions administratives requis pour gérer l'environnement de contrôle.

1.2.3. Les méthodes de contrôle d'accès

Après la présentation des concepts essentiels dans la sécurité informatique et l'obligation de contrôle d'accès pour la protection des actifs de la société, au cours de cette section nous allons dévoiler les dispositions de sécurité qui peuvent ne pas se heurter au les dangers qui menacent la sécurité informatique des réseaux locaux au sein des entreprises

1.2.3.1. La procédure d'identification et d'authentification

- **L'identification** : C'est une phase dans laquelle, l'utilisateur établit son identité unique.

Ainsi, on peut le connaître.

- **L'authentification** : C'est la méthode qui a pour objectif, pour un système informatique, à contrôler l'identité d'une entité (personne, ordinateur,) afin de permettre

l'accessibilité de cette entité à des ressources (systèmes, réseaux, applications,)

- **L'autorisation** : permettre ou non l'accessibilité à la ressource donnée.

1.2.3.2. La fonction de hachage

Une fonction de hachage est aussi appelée fonction de hachage à sens unique ou "one-way hash function" en anglais. Ce type de fonction est très utilisé en cryptographie, principalement dans le but de réduire la taille des données à traiter par la fonction de cryptage. En effet, la caractéristique principale d'une fonction de hachage est de produire un haché des données, c'est-à-dire un condensé de ces données. Ce condensé est de taille fixe, dont la valeur diffère suivant la fonction utilisée : nous verrons plus loin les tailles habituelles et leur importance au niveau de la sécurité.

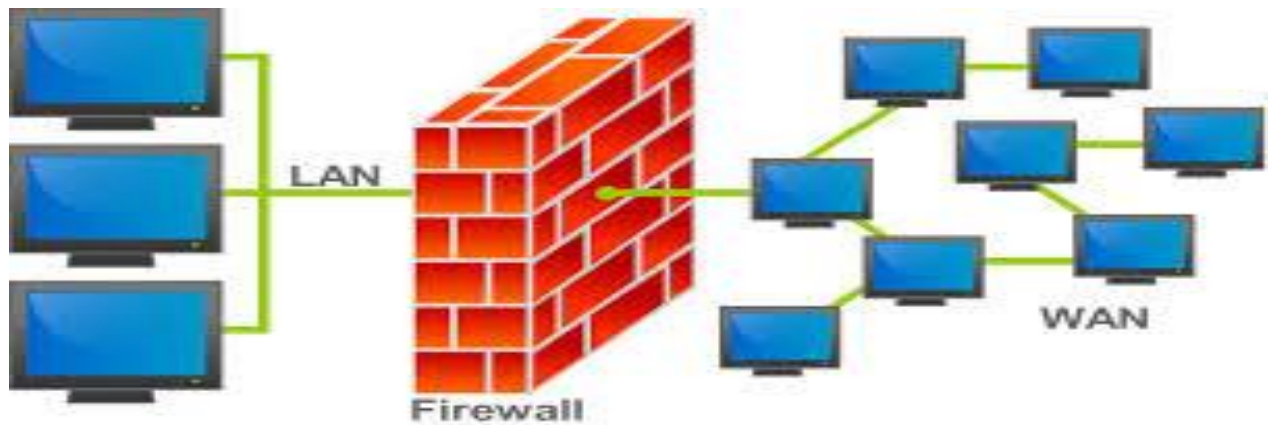
1.2.3.3. Le logiciel de protection (antivirus)

Un antivirus permet de détecter d'éradiquer logiciels malveillants ou les virus et empêcher l'attaque.

Son fonctionnement consiste à analyser régulièrement les fichiers du système pour vérifier qu'ils ne contiennent pas de code malveillant en inspectant les disques durs, la mémoire et les volumes amovibles (CD, disque dur externe, clé USB, DVD...).

1.2.3.4. Le pare-feu

Un pare-feu (ou firewall en anglais), est un système (logiciel / matériel) servant d'interface entre un ou plusieurs réseaux et internet afin de contrôler et éventuellement bloquer la circulation des paquets de données, en analysant les informations.



Ci-dessous, on observe une image présentant un firewall qui filtre les échanges de données entre un ordinateur et Internet. La connexion verte est autorisée, refusées, alors que celles en rouge sont refusées. (8)

1.2.3.5. Les systèmes de détection d'intrusion

Un système de détection d'intrusion IDS est un mécanisme écoutant le trafic du réseau pour localiser les activités inhabituelles et permet d'avoir une action préventive sur les menaces d'intrusion. (9)

1.2.3.6. Les systèmes de prévention d'intrusion

L'IPS (Intrusion Prevention System) est un outil de prévention et protection contre les intrusions en prenant des mesures pour diminuer les impacts d'une attaque.

Il peut bloquer immédiatement les attaques en utilisant la technique de filtrage de paquets et le blocage des ports automatiquement. (10)

1.2.4. Les protocoles

1.2.4.1. Le protocole IEEE 802.1X

IEEE 802.1X est un standard de l'IEEE qui permet de contrôler d'accès au réseau en se basant sur les ports. Il fait partie du groupe de protocoles IEEE 802 (802.1). Il assure l'authentification aux équipements connectés à un port Ethernet. Ce standard peut être utilisé pour quelques points d'accès WiFi, 802.1X est une fonctionnalité disponible sur certains commutateurs réseau.

Les acteurs du 802.1x :

- Suppliquant : C'est le système à authentifier (le client),
- Port Access Entity (PAE) : C'est le point d'accès au réseau,
- Authenticator System : C'est système authenticateur qui contrôle les ressources

disponibles via le PAE. (11)

1.2.4.2. Le protocole Radius

Le protocole RADIUS (Remote Authentication Dial-In User Service) est un protocole de type AAA (Authentication Autorization Accounting) permettant de centraliser l'authentification et l'autorisation des accès distants.

Il repose essentiellement sur un serveur (RADIUS), connecté à une base d'identification (LDAP par exemple) et un client RADIUS, nommé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur. Les échanges entre le client RADIUS et le serveur RADIUS est chiffré et authentifié avec l'appui d'un secret partagé. (12)

1.2.4.3. Le protocole EAP

Le protocole EAP (Extensible Authentication Protocol) assure les connexions à internet à distance et permet l'identification des utilisateurs sur le réseau. Il permet d'utiliser plusieurs choix d'authentification, citons-les parmi lesquelles :

- **EAP-MD5** : Authentification avec un mot de passe,
- **EAP-TLS** : Authentification avec un certificat électronique,
- **EAP-TTLS** : Authentification avec n'importe quelle méthode d'authentification, au sein d'un tunnel TLS,
- **EAP-PEAP** : Authentification avec n'importe quelle méthode d'authentification EAP, au sein d'un tunnel TLS.

Les types de paquets de base :

- **EAP Request** : Envoyé par le contrôleur d'accès au client.
- **EAP Response** : Réponse du client au contrôleur d'accès.
- **EAP Success** : Paquet envoyé au client en fin d'authentification si elle est réussie.
- **EAP Failure** : Paquet envoyé au client en fin d'authentification si elle est ratée. (13)

Chapitre 3 : Etude Comparative entre Solution NAC

Introduction :

Dans le but de choisir une solution de contrôle d'accès au réseau qui répond aux exigences fixées au préalable et satisfait les attentes de la société, ce chapitre est consacré à l'étude Comparative entre Solution NAC (open-sources et payants) qui est une phase cruciale dans notre projet.

1. Présentation des solutions de contrôle d'accès au réseau (NAC)

Dans cette partie, on va étudier quelques solutions de contrôle d'accès au réseau (NAC) libre et commerciales qui existent dans le marché afin de pouvoir étudier les solutions NAC

1.1. Les solutions de contrôle d'accès commerciales

1.1.1 La solution Cisco ASA

La solution Cisco ASA est basée sur le firewall Cisco ASA 5500-X, son objectif est d'assurer l'équilibre entre performance et productivité. De plus, il garantit les services de sécurité réseau

d'une entreprise

1.1.2. La solution Palo Alto

La solution Palo Alto Networks est l'un des acteurs fleurons de la récente époque de la sécurité, et protège maintenant quelques centaines de sociétés, fournisseurs de services et organismes gouvernementaux. A l'inverse aux équipements plus habituels, cette architecture de sécurité permet aux opérations business d'avoir toute sécurité dans le domaine informatiques.

1.1.3. La solution Sonic wall

Les services Sonic Wall sont élaborés pour répondre aux besoins de la société en protégeant la puissance de vente mobile, et assure la sécurité des services web.

1.1.4. La solution Stone soft

La solution StoneGate est l'ensemble des services de la sécurité réseau que sont le firewall (FW), l'infrastructure privé virtuel (VPN), la prévention d'intrusion (IPS), le VPN SSL, la sortie de bout en bout, de même qu'un équilibre

des charges, dans un système dont la gestion est centralisée et unifiée. Elle a un très bon rapport prix/performances

1.2. Les solutions de contrôle d'accès libres

1.2.1. La solution Netfilter

Netfilter est l'intégration au niveau du noyau du firewall Linux, Quand un colis vient sur une

interface, Netfilter regarde à l'en-tête IP pour voir si ce colis fait partie d'une session

connue. Selon le cas, il fixe la situation du colis au sein des cas suivants ;
Nouveau, liée,
invalidé.

1.2.2. La solution Ipcop

IPCOP est un OS minutieux établi sur un kernel sous linux amélioré, qui est voué à garantir la sécurité de notre réseau. Ce firewall est à l'état qui cherche à donner une méthode facile mais performante pour paramétrer un firewall sur une architecture de type PC. IPCOP propose les prestations sympathiques comme l'ordinateur mandataire, un DHCP, un DNS...

1.2.3. La solution Pfsense

PfSense est une distribution gratuite et open source de FreeBSD, hébergé et développé par Rubicon Communications, LLC (Netgate).

Il spécialement conçu pour être utilisée comme pare-feu et routeur, entièrement gérée via une interface Web. En plus d'être une plate-forme de routage et de pare-feu flexible et puissante, elle inclut plusieurs fonctionnalités (La compatibilité multi-plates-formes, La personnalisation complète des pages accessibles aux utilisateurs, La simplicité d'utilisation grâce à une page de connexion)

1.2.4. La solution Endian firewall

La solution Endian Security Gateway est conçue pour faciliter la gestion de réseaux complexes (la difficulté d'utiliser un produit efficacement). Elle a pour objectif de fournir aux administrateurs tous les outils nécessaires pour fournir une protection complète avec le moins d'effort possible.

2. Etude Comparative entre Solution NAC

Dans cette partie nous allons choisir une solution NAC qui est l'objectif de notre projet en se basant sur son fonctionnement et les solutions du marché présentés au-dessus.

2.1. Etude comparatives des solutions NAC commerciales et libres

Ce qui différencie les solutions open source et payantes est le matériel supporté, les fonctionnalités principales, la documentation, la communauté dédiée à chaque solution, l'interface Web ergonomique.

Pour étudier entre les solution de contrôle d'accès réseau, il faut sélectionner les différentes architectures, méthodes et outils. Puisque les solutions NAC disponibles (gratuite ou commerciale) sont diversifiée le choix dépend des critères présentés dans les tableau ci-dessous :

Services	Solutions				
	Smoothwall Express	Vyatta Community	IPCop	PFSense	M0n0wall
Proxy web	X	X	X	Ajouter Squid	—
Proxy IM, POP3, SIP	X	—	—	—	—
DNS	X	X	X	X	X
VPN, WebGUI via HTTP	X	—	X	X	X
Possibilité de détection d'intrusions	X	—	X	X	—

Tableau 1 : Comparaison de quelques solutions libres

Les critères	Solution open source				Solution commerciale			
	Netfilter	Pfsense	Ipcop	Endian firewall	Palo Alto	Cisco ASA	Sonic wall	Stone soft
Stateful	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
NAT	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
DMZ	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
VPN (site to site)	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
VPN (client to site)	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
IPS/IDS	Non	Oui	Oui	Non	Oui	Oui	Oui	Oui
SSH	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Antimalware	Non	Oui	Non	Oui	Oui	Non	Oui	Oui
Anti spam	Non	Oui	Non	Oui	Oui	Oui	Oui	Oui
Proxy	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Haute disponibilité	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Identification des Utilisateurs	Non	Non	Non	Non	Oui	Oui	Non	Non
Identification des applications	Non	Non	Non	Non	Oui	Oui	Non	Non

Tableau 2 : Comparaison entre les solutions NAC commerciales et libres

2.1.1. Les critères de base pour le choix

Le tableau 2 fait une classification des solutions NAC commerciales et libres du marché.

2.1.1.1 pfsense :

❖ Les points forts :

- Son point fort se base, en plus de son fonctionnement irréprochable, sur le fait qu'il est complètement configurable grâce à une interface web simple et intuitive.
- La gestion se fait entièrement via web en pointant directement sur l'IP du serveur Cloud et pour la configuration plus profonde, il n'est pas nécessaire d'intervenir en ligne de commande. Toutefois, pour les utilisateurs les plus expérimentés, l'accès via SSH est également prévu, utile pour accéder au « backstage » de la machine virtuelle

*En plus de la fonction de Firewall, pfSense dispose des différentes fonctionnalités comme :

- Stateful Firewall
 - DHCP (Dynamic Host Configuration Protocol) Server
 - NAT (Network Address Translation)
 - HA (High Availability) – via CARP il est possible de configurer deux firewalls sur deux Cloud Server Firewall identiques de manière à ce qu'ils puissent se répliquer (pfsync) et s'auto-remplacer en cas de panne de l'un des deux
 - Load Balancing (Équilibrage de la charge) pour distribuer la charge de travail sur deux ou plusieurs serveurs Cloud (très utile habituellement pour les systèmes web, systèmes mail, systèmes e-commerce)
 - VPN (Virtual Private Network) – possibilité de créer et de gérer des réseaux VPN de type IPsec, OpenVPN et PPTP
 - Graphiques RRD et informations en temps réel
 - DNS dynamiques
- Très fréquemment rencontré dans les PME et les petites structures, pfSense offre une solution complète de routage, filtrage, VPN et partage de connexion. Il est basé sur pf, et intègre un grand nombre de composants tiers : serveur DHCP/DNS, serveur de temps, proxy web, monitoring... La configuration se fait entièrement via une interface web.
- *lorsque on parle de PfSense, on peut le représenter comme une plateforme riche de sécurité. il est caractérisé par une large bibliothèque de package avec une intégration facile. PfSense est ,à la fois, un firewall, proxy, VPN, Routeur, DNS, DHCP, Snort..... Tout simplement, c'est un redoutable outil.*

*Il offre une Interface d'administration :

- Interface web
- Mode CLI
- Interface ligne de commandes = édition de fichiers de configuration
- Debug / Log / Trace efficace

*Brique Firewall :

- Filtrage sur IPs
- Filtrage sur protocoles
- Réalisation de NAT
- Vision par groupe

*Brique Firewall avancée :

- Gestion simple des mises jour
- Gestion des VPNs : VPN IPSEC + compatibilité avec les VPNs opensource ou wireguard

Aussi Il permet :





- Filtrage par IP source et destination, port du protocole, IP source et destination pour le trafic TCP et UDP
- IPv6
- Capable de limiter les connexions simultanées sur une base de règle
- pfSense utilise p0f, un utilitaire permettant de filtrer le trafic en fonction du système d'exploitation qui initie la connexion.
- Possibilité d'enregistrer ou de ne pas enregistrer le trafic correspondant à chaque règle.
- Politique très souple de routage possible en sélectionnant une passerelle sur une base par règle (pour l'équilibrage de charge, basculement, connexions WAN multiples, etc)
- Utilisation d'alias permettant le regroupement et la désignation des adresses IP, des réseaux et des ports, rendant ainsi votre jeu de règles de pare-feu propre et facile à comprendre, surtout dans des environnements avec plusieurs adresses IP publiques et de nombreux serveurs.
- Filtrage transparent au niveau de la Couche 2, le pare-feu est capable d'agir en pont filtrant.
- La normalisation des paquets est utilisée, il n'y a donc aucune ambiguïté dans l'interprétation de la destination finale du paquet. La directive « scrub » ré-assemble aussi des paquets fragmentés, protège les systèmes d'exploitation de certaines formes d'attaque, et laisse les paquets TCP contenant des combinaisons de Flags invalides.





❖ Les points faibles :

- *pfSense est un des rares à intégrer d'emblée IPv6. Il n'est pas très "sexy" mais l'environnement de gestion est clair et on s'y retrouve assez facilement. J'ai essayé le portail captif : il gagnerait à intégrer des fonctions de "personnalisation", mais c'est probablement lié à une faiblesse de la documentation sur ce point... ”*
- *Très performant et robuste mais avec quelques problèmes avec les mises à jour.*
- *Le produit pourrait offrir plus de plugins intégrés.*
- *L'interface Web pourrait être améliorée et plus conviviale.*

2.1.1.2. Endian Firewall (UFW) :

Les Points forts et faibles sont cités dans le tableau ci-dessous :

General	EFW Community	Virtual Appliance	Software Appliance	Hardware Appliance
				
Open Source License (GPL)	✓	✓	✓	✓
Commerical support options	No	✓	✓	✓
Ticket System Support	No	✓	✓	✓
Direct support from Endian	No	Optional	Optional	Optional
Phone Support	No	Optional	Optional	Optional
Live/Remote Support (hands on)	No	Optional	Optional	Optional
Instant Hardware Replacement	No	N/A	N/A	Optional
Industrial Grade Hardware	No	N/A	N/A	N/A
DynDNS support	✓	✓	✓	✓

General	EFW Community	Virtual Applianc	Software Appliance	Hardware Appliance
				
Network Security	✓	✓	✓	✓
Application Control	No	✓	✓	✓
Advanced Content Security	No	✓	✓	✓
CYREN URL Filter	No	✓	✓	✓
CYREN Anti-spam	No	✓	✓	✓
Bitdefender Anti-malware Engine	No	✓	✓	✓
Web Security	✓	✓	✓	✓
URL Filter	1.8 million URLs	150 million URLs	150 million URLs	150 million URLs
Mail Security	✓	✓	✓	✓

Anti-spam	Single Engine	Dual Engine	Dual Engine	Dual Engine
Quarantine Management	No	✓	✓	✓
Anti-virus	✓	✓	✓	✓
Anti-virus	Single Engine	Dual Engine	Dual Engine	Dual Engine
Virus disinfection	No	✓	✓	✓
User Authentication	✓	✓	✓	✓
Local User Authentication	✓	✓	✓	✓
HTTP Remote User Authentication	✓	✓	✓	✓
VPN Remote User Authentication	No	✓	✓	✓
VPN One-Time Password Support	No	✓	✓	✓
Virtual Private Networking	✓	✓	✓	✓
IPsec	✓	✓	✓	✓

L2TP	No	✓	✓	✓
XAuth	No	✓	✓	✓
OpenVPN	✓	✓	✓	✓
WAN Failover	✓	✓	✓	✓
BYOD and Hotspot	No	✓	✓	✓
Network Address Translation	✓	✓	✓	✓
Routing	✓	✓	✓	✓
Bridging	✓	✓	✓	✓
High Availability	No	✓	✓	✓
Event Management	✓	✓	✓	✓
Email Notifications	✓	✓	✓	✓
SMS Notifications	No	✓	✓	✓
Python Scripting Engine	No	✓	✓	✓
Logging and Reporting	✓	✓	✓	✓
Live Network Monitoring	✓	✓	✓	✓
Event Reporting	No	✓	✓	✓
Management	✓	✓	✓	✓
Management Interface	✓	✓	✓	✓
Full System Access	✓	✓	✓	✓
Updates and Backup	✓	✓	✓	✓
Centralized Management	No	✓	✓	✓

Tableau 3 :Les Points forts et faibles d’Endian Firewall

2.1.1.3. IPCop :

- IPCop est un projet Open Source dont le but est d'obtenir une distribution Linux complètement dédiée à la sécurité et aux services essentiels d'un réseau.
 - IPCop joue le rôle d'intermédiaire entre un réseau non sûr (Internet) et un réseau qu'on souhaite sécuriser (réseau local), tout en offrant des services ajoutés.
 - Les principaux services offerts de base sont les suivants : DHCP, NTP (serveur de temps), PROXY, SSH, IDS(détection d'intrusions), FIREWALL incluant le SHAPING (mise en forme du trafic).
 - Les services de bases concernant le firewall et le shaping sont assez sommaire et n'exploite pas l'intégralité des fonctionnalités offertes par NetFilter.
 - IPCop permet l'ajout de fonctionnalités par l'intermédiaire de plugins sans avoir à redémarrer la machine. On peut par exemple citer les plugins suivants : filtrage de mail contre les virus et les spams, filtrage du protocole HTTP et FTP pour les virus, ...
 - L'installation est simple et rapide car tous les éléments non nécessaires à son objectif de distribution de sécurité ont été omis. Le fait d'omettre un maximum d'éléments est également un gage de sécurité car cela évite au firewall d'être vulnérable aux attaques ciblant des logiciels périphériques (applications bureautique, ...)
 - La configuration se révèle aussi très simple car elle est effectuée par l'intermédiaire d'une interface web épurée
-
- IPCop est un logiciel en mode SAAS (software as a service) : il est donc supporté par tous les systèmes d'exploitation (Windows, Mac, OS Mobiles ...) car il est accessible depuis un navigateur web Internet (comme Chrome ou Firefox) ...
 - Accessibilité 24-7
 - Intégration avec LDAP et Active Directory
 - Intégration de la prévention des intrusions
 - Visibilité et contrôle des applications
 - Prise en charge des environnements physiques et virtuels

- Identifiez et contrôlez les menaces d'applications évasives
Sandbox, ou émulation de menace isolée et basée sur le cloud
- L'interface de ce logiciel est traduite en plusieurs langues, dont :
Anglais ...

2.1.1.4. Palo Alto :

L'inconvénient avec Palo Alto est qu'ils n'ont pas de solution basée sur le cloud qui inclut une passerelle Web sécurisée.

Les capacités d'intégration avec d'autres solutions doivent être abordées.

2.1.1.5. SONICWALL :

Network Security Manager (NSM) de SonicWall vous offre tout ce dont vous avez besoin pour gérer vos pare-feux de bout en bout.

- Intégrez et gérez des dizaines ou des centaines de pare-feux de manière centralisée à partir d'une seule interface
- Déployez et administrez des pare-feux à distance avec un déploiement autonome
- Simplifiez la configuration grâce à des assistants
- Identifiez et corrigez les risques en matière de sécurité grâce à des analyses détaillées et des tableaux de bord intuitifs
- Déployez rapidement et facilement de nouveaux pare-feux avec des modèles de configuration personnalisés
- Fédérez toutes les politiques de sécurité de votre entreprise
- Automatisez le reporting pour les audits
- Bloque plus d'attaques avec RTDMI™ :

Le Real-Time Deep Memory Inspection (RTDMI™) détecte et bloque proactivement les malwares inconnus via une inspection de mémoire profonde en temps réel, une approche révolutionnaire pour la défense contre les attaques zero-day et par canal latéral et d'autres menaces non reconnues.

- Travailleurs distants sécurisés :

Sonicwall NetExtender fournit un client de connexion SSL-VPN intuitif, facile à déployer et à configurer. Permettez à vos employés distants de disposer

aisément d'un accès sécurisé à votre réseau d'entreprise depuis les appareils Linux, Mac et Windows.

➤ **Technologie Secure SD-WAN :**

Oubliez les MPLS et passez à un réseau plus agile, plus sûr et plus rentable, optimisé pour le paysage cloud à haut débit d'aujourd'hui. La technologie Secure SD-WAN est intégrée aux pare-feux NSa, il n'est donc pas nécessaire d'acheter d'autres appliances et licences SD-WAN.

➤ **Contrôleur sans fil intégré :**

Mettez en œuvre la sécurité sans fil haute vitesse en combinant un pare-feu nouvelle génération série NSa avec un point d'accès sans fil Sonicwall SonicWave. Les pare-feux série NSa et les points d'accès SonicWave sont dotés de ports 2,5 Gbe qui permettent un débit sans fil multi-gigabit offert dans la technologie sans fil Wave 2.

➤ **Coût total de possession réduit :**

Commencez à faire des économies d'entreprise avec un pare-feu SonicWall NSa. De la réduction des coûts au déploiement sans intervention, en passant par le déploiement du SD-WAN et la présentation de taux de blocage des menaces NetSecOPEN, le tout aussi bien ou mieux que les concurrents pour une fraction du coût, les pare-feux Sonicwall NSa sont la solution de sécurité incontournable.

➤ **Gestion centralisée basée sur le cloud et sur site :**

Bénéficiez d'une visibilité accrue de votre entreprise, même si elle devient plus complexe, hors-site et sur site. Étroitement intégré à l'écosystème Sonicwall, apportez vos pare-feu dans une gestion, une licence, un reporting et une analyse à point unique

➤ **Hautes performances et densité de ports :**

Déployez des pare-feux de nouvelle génération qui offrent aux moyennes entreprises et aux entreprises distribuées la solution de prévention des menaces dont elles ont besoin, à des vitesses de plusieurs gigabits et une densité de ports élevée, y compris avec des ports 10 GbE, pour des connexions réseau plus flexibles

➤ **Plateforme hautes performances**

➤ **Inspection approfondie des paquets**

- Prévention contre les intrusions
- Veille, contrôle et visualisation des application
- Sécurité, performances et contrôle

2.1.1.6. Cisco ASA :

La solution **Cisco ASA** est située premier leader dans les solutions NAC du marché. Bien qu'elle présente plusieurs avantages pas mal d'inconvénients existent tels que :

- Le cout est très élevé,
- Uniquement les équipements Cisco sont supportés alors qu'une architecture ouverte est exigée dans notre entreprise : Support d'environnements multifournisseur.

3. Problèmes rencontrés

Comme dans tout projet, il a eu des moments difficiles durant plusieurs phases d'avancement.

Nous tenons ici à signaler les majeurs problèmes rencontrés :

- La difficulté de choisir un firewall adéquat à notre solution et efficace à cause du manque de documentation,
- Problème de compatibilité des services et qui nécessitent des certificats.

Conclusion

Dans ce chapitre, nous avons présenté les solutions NAC et l'étude comparative entre eux .

Conclusion & Perspectives

Ce projet de stage d'été consiste à faire l'étude comparative entre Les solutions NAC open-source et payant qui a pour objectif de choisir la solution adéquate puis je souhaite continuer et évoluer ce projet avec la mise en place d'une solution de contrôle d'accès au réseau qui a pour objectif de renforcer la sécurité des entreprises.

Ce travail a consisté en premier lieu à étudier les besoins de sécurité pour une entreprise pour pouvoir trouver une solution pour chaque besoin et pour parer contre toute nouvelle menace.

Après une analyse approfondie des besoins de l'entreprise, nous avons pu faire une étude comparative de différentes solutions possibles

Bien évidemment, nous avons rencontré plusieurs difficultés durant la réalisation du travail essentiellement l'absence quasiment totale de toute documentation technique.

En outre, ce projet était bénéfique sur le plan professionnel et technologique et c'était l'occasion pour améliorer nos connaissances et acquérir de nouveaux concepts dans le domaine de la sécurité informatique.

De point de vue perspectif, le travail est encore à évoluer :

- La Mise en place d'une solution de contrôle d'accès au réseau
- Intégration des autres outils comme WebFilter,
- Suivi en temps réel de l'activité de chaque utilisateur,
- Scanner et désinfecter les machines endommagées afin de les autoriser à accéder au réseau