Sommaire

Liste des figures

Liste des tableaux

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 tache 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 taches 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 fin d'études. D'abord, nous présentons le cadre général de notre projet, ainsi nous parlerons de l'organisme d'accueil Tunisie Télécom, son organigramme et ses déférentes missions et services. Ensuite, nous dégageons 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

Le groupe Tunisie Télécom est un grand opérateur historique de télécommunications en Tunisie.

Cet opérateur livre à ses clients publics et grand compte (les entreprises) plusieurs services et produits à savoir ; Internet, voix fixe et mobile.

Avec presque de 6 millions d'abonnés (un chiffre variable), l'opérateur incarne aujourd'hui les valeurs de proximité, d'accessibilité et d'universalité en visant toujours une meilleure qualité de service et une satisfaction client malgré l'existence de deux opérateurs concurrents

Tunisie Telecom se compose de 24 directions régionales, de 140 Espaces TT et points de vente et de plus de 13 mille points de vente privés (franchises). Elle emploie plus de 6000 agents. (1)

Le Groupe Tunisie Telecom comporte :

- La Société Nationale des Télécommunications (Tunisie Telecom)
- La Société Tunisienne d'Entreprises de Télécommunications (SOTETEL)

- Topnet (FSI)
- La Société d'Investissement DIVA SICAR
- La Société Mauritano-Tunisienne de Télécom (MATTEL)
- L'Agence Tunisienne de l'Internet (ATI).

Tunisie Télécom a ainsi pour mission d'assurer les activités relatives au domaine de télécommunication. Il est notamment chargé de :

- Le développement, l'entretien, l'installation, et l'exploitation des réseaux de téléphone et la transmission des données,
- Le lancement des services de télécommunication nouveaux,
- L'offre de tous les services publics ou privés de télécommunication correspond aux divers besoins à caractère social et économique,
- La participation à l'effort national d'enseignements supérieur au niveau du secteur de télécommunication,
- La promotion de la coopération dans tous les domaines de télécommunications, l'Office National de Télécommunications Tunisie Télécom est placée sous la tutelle du ministère de la communication ; son siège est fixé à Tunis.

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

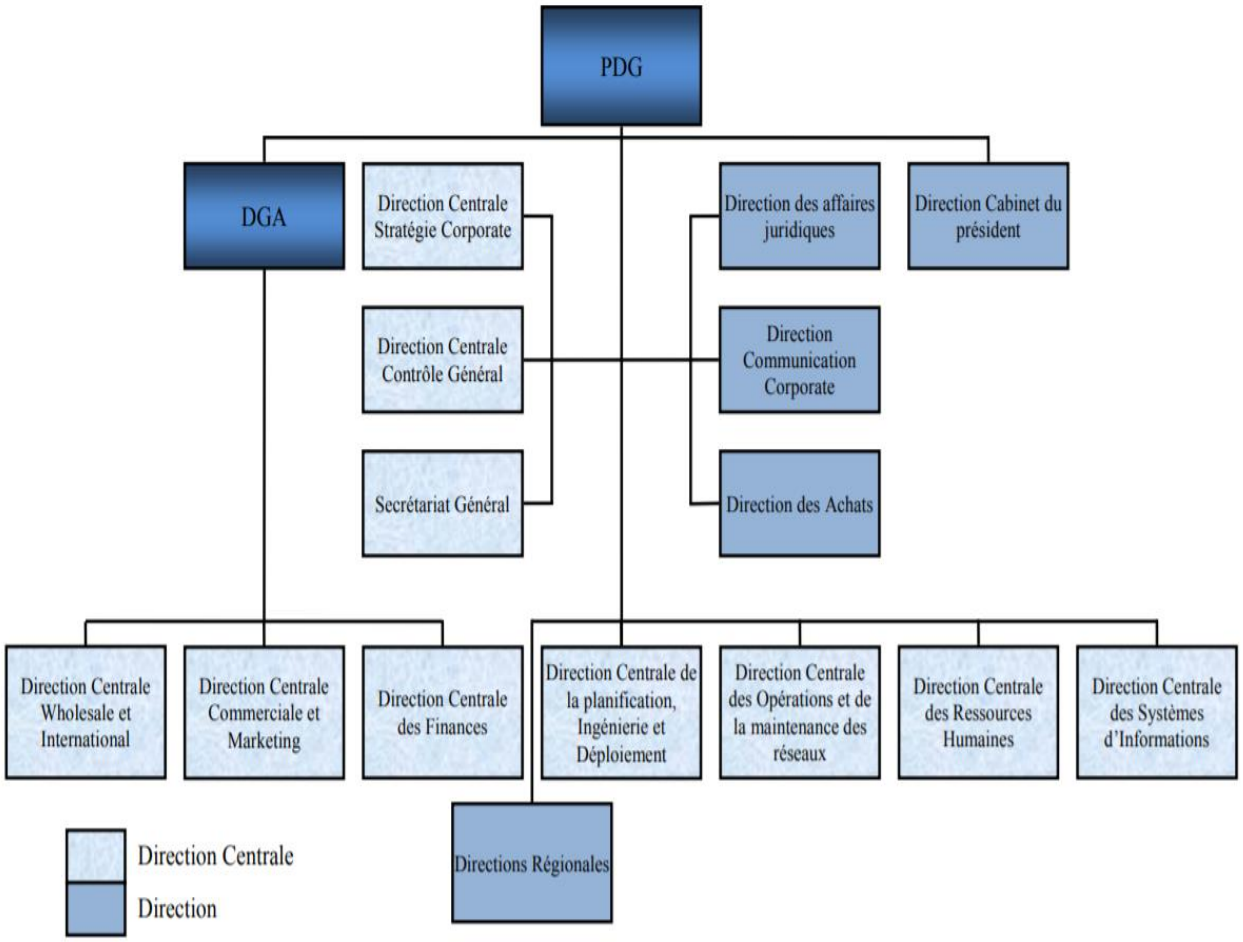


Figure 1: Organigramme de Tunisie Télécom *(2)*

L'organigramme de Tunisie Telecom se compose d'une direction générale, neuf directions centrales et vingt-quatre directions régionales.

Chaque partie prenante de l'organisation rempli un rôle incontestablement important. Cependant, dans le cadre de ce mémoire, nous allons nous intéresser en exclusivité à la Direction Central Technique et plus spécifiquement au CNOC et la politique qu'elle met en œuvre pour accompagner et soutenir la stratégie et la performance de l'entreprise.

3. Problématique

Le cadre de mon projet est le CNOC « Customer Network Operation Center » qui est une direction appartenant au groupe Tunisie Telecom et qui est dédiée principalement pour le traitement des réclamations DATA et Mobile des clients grand compte (Entreprise et client SLA).

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.

Dans ce cadre, les responsables de CNOC 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 CNOC propose l'étude et la mise en place d'une solution de sécurité au sein de son réseau local ce qui permet le contrôle d'accès au réseau.

4. Solution proposée

Afin de réussir la mise en place d'une solution de sécurité intelligente au réseau local du CNOC, 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,
- 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 le firewall Pfsense, 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'un formalisme et d'une démarche. Le formalisme permet de représenter le système d'information de l'entreprise à l'aide d'un ensemble de modèles ou de diagrammes donnant une vision statique, dynamique et organisationnelle de l'entreprise. La démarche décrit les différentes étapes nécessaires pour traduire les besoins des utilisateurs en un produit logiciel. La combinaison de ces deux éléments (formalisme et démarche) permet d'augmenter la productivité et d'estimer le temps de développement.

4.1. Formalisme utilisé

Pour représenter les différentes composantes de notre application, nous avons choisi le langage de modélisation UML.

Cette norme proposée par l'OMG (Object Management Group) est aujourd'hui acceptée par la communauté des informaticiens et supportée par la plupart des outils de conception (AGL1).

4.2. 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 choix de la solution NAC adéquate,
- **Analyse et conception :** il s'agit de recenser les besoins fonctionnels et non fonctionnels et décrire sous forme de diagrammes les solutions proposées pour répondre à ces besoins,
- **Implémentation :** il s'agit de la mise en place de l'application conformément aux diagrammes élaborés lors de l'étape de conception,
- **Evaluation :** il s'agit de tester les différents modules de l'application.

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 le formalisme et la démarche qui vont être suivis tout au long de ce projet.

Chapitre 2 : Notions de bases et Etude 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

4.3. 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. (3)

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 calculette à mot de passe.

1.1.2.3. Le cheval de Troie

Suite l'accès au système cible, les pirates utilisent la cridibilité 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. (4)

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. (5)

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

4.4. 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.

1.1.3. 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.

1.1.4. 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 stratégiques, les responsabilités et les fonctions administratives requis pour gérer l'environnement de contrôle.

1.1.5. 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.

1.1.5.1. 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.

1.1.5.2. 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. (6)

1.1.5.3. 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...). (7)

1.1.5.4. 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.

Figure 2: Principe du fonctionnement d'un firewall

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)

1.1.5.5. 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)

1.1.5.6. 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)

1.1.6. Les protocoles

1.1.6.1. 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 :

- **Supplicant :** 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 authentificateur qui contrôle les ressources disponibles via le PAE. (11)

1.1.6.2. 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)

1.1.6.3. 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)

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

Dans cette partie, on va étudier quelques solutions de contrôle d'accs au réseau (NAC) libre et commerciales qui existent dans le marché afin de pouvoir par la suite choisir une solution adéquate à notre projet.

1.1.7. Les solutions de contrôle d'accès commerciales

1.1.7.1. 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 (14)

1.1.7.2. 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. (15)

1.1.7.3. 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. (16)

1.1.7.4. 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 (17)

1.1.8. Les solutions de contrôle d'accès libres

1.1.8.1. 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, invalide. (18)

1.1.8.2. 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... (19)

1.1.8.3.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,) (20)

1.1.8.4.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. (21)

2. Choix d'une solution de contrôle d'accès au réseau

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 choisir une 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 le tableau ci-dessous :

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 1: Comparaison entre les solutions NAC commerciales et libres

2.2. Synthèse

Après l'étude comparatives des solutions NAC payantes et libres, on va choisir une solution adéquate objectif de notre projet.

2.2.1. Les critères de base pour le choix

Le tableau 1 fait une classification des solutions NAC commerciales et libres du marché.
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.

Nous constatons suite à une étude profonde des solutions de contrôle d'accès libres et professionnelles, plusieurs avantages à savoir la disponibilité du code source et la possibilité de l'étudier et de le modifier selon nos besoins et de le diffuser ainsi la gratuité de téléchargement. De plus, il existe plusieurs utilisateurs et développeurs qui offrent une assistance par le partage des documentations et les participations aux forums, participant par la suite à l'amélioration des logiciels open source.

2.2.2. La solution de contrôle d'accès choisie

Après avoir opté pour une solution libre et gratuite, Les grandes différences entre les solutions open source proviennent de l'ensemble du matériel supporté, les fonctionnalités de base, les actions possibles, la documentation, la communauté propre à chaque solution, ainsi que de l'ergonomie de l'interface Web, la granularité des informations obtenues, et la sûreté générale. En regardant le tableau, nous remarquons que Pfsense est le plus performant par rapport aux autres outils open source disponibles. Ils supportent aussi différents types de matériels.
Après la comparaison des outils NAC disponibles, open source et commerciales, et tandis que le réseau de Tunisie Telecom est homogène et qu'elle opte à la mise en place des outils open source, on a pris la décision, avec notre tuteur de l'entreprise, de choisir une solution open source « PFsense ». C'est une solution complète et supporte différents types de matériels. Elle intègre plus de fonctionnalités que les autres solutions open source et assure tous les objectifs du NAC. De plus, son interface Web est pratique.

3. Choix des outils de contrôle d'accès au réseau

Les systèmes et outils de contrôle d'accès au réseau sont divers, on a choisie certains outils compatibles à notre solution Pfsense et répondent aux besoins de l'entreprise.

3.1. Presentation des outils NAC

3.1.1. Le protocole Free Radius

FreeRADIUS est un protocole client-serveur libre qui permet la centralisation de l'authentification des machines/utilisateurs pour l'accès filaire et sans-fil au réseau local dont les transactions sont chiffrées et authentifiées grâce à un secret partagé.

3.1.2. L’annuaire OpenLDAP

OpenLDAP est un annuaire LDAP open source de type hiérarchique (les données sont structurées en arbre) offrant de très bonnes performances en consultation, modifications et suppression. (22)

3.1.3. Le proxy SQUID

Un serveur proxy est appelé serveur mandataire faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet. Il est utilisé pour le web, il s'agit alors d'un proxy HTTP. Il nous permettra ainsi de gérer l'accès à internet aux utilisateurs de notre réseau local en fonction des heures d'accès, des ports de destination d'un service, d'IP sources, (23)

3.1.4. Le système de détection d’intrusions Snort

Snort est un Système de Détection d'Intrusion basé sur le réseau déjà décrit dans la partie 1 de ce chapitre.

3.1.5. Le portail captif

Le portail captif est un moyen permettant aux utilisateurs de s’authentifier sur un réseau. Il oblige tout utilisateur désirant naviguer sur internet de s'identifier grâce notamment à une redirection vers une page de connexion. (24)

3.1.6. Le langage HTML

Le langage HTML (HyperText Markup Langage) est utilisé pour afficher une page Web et indiquer au navigateur s'il doit charger des ressources supplémentaires (image, contenu multimédia, feuille de style externes, page de script), ainsi que l'adresse (url) de chacune d'entre elles. (25)

3.1.7. Le langage CSS

Le langage CSS (Cascading Style Sheets) a été développé afin d'ajouter des informations graphiques à des documents XML et HTML.

Le principe de base de CSS est donc la séparation du contenu et de la présentation, le document XML ou HTML étant le contenu et le fichier CSS contenant les informations de présentation. (26)

3.2. Synthèse

3.2.1. Description des fonctionnalités des outils

Dans cette section nous allons présenter les principales fonctionnalités de chaque outil dans notre solution de contrôle d'accès comme présenté dans le tableau 3 :

Outil	Fonction
FreeRadius	Centralisation d'authentification des utilisateurs
OpenLDAP	Vérification d'identité d'un user et Validation de demande d'accès au réseau
Captive Portal	Autorisation d'accès au réseau de l'entreprise selon les privilèges Configuration de PFsense via l'interface web
SQUID	Gestion des caches de connexion Autorisation d'accès par filtrage Monitoring Gestion des trafics entrants et sortants Gestion des log
PFsense	Consulter les logs de toutes les sessions établies, échouées Bloquer l'accès en cas de doute Extrait des informations, statistiques sur les équipements accédés au réseau
Snort	Analyse des paquets et détection des alertes
HTML	Création et affichage d'une page web
CSS	Mise en forme des documents HTML

Tableau 2: Fonctionnalitées des outil NAC

3.2.2. Interaction des outils NAC

D'après la figure 10, on résume les différents composants logiciels de notre solution NAC. Voici une description détaillée des différents composants ainsi que les relations existantes entre eux :

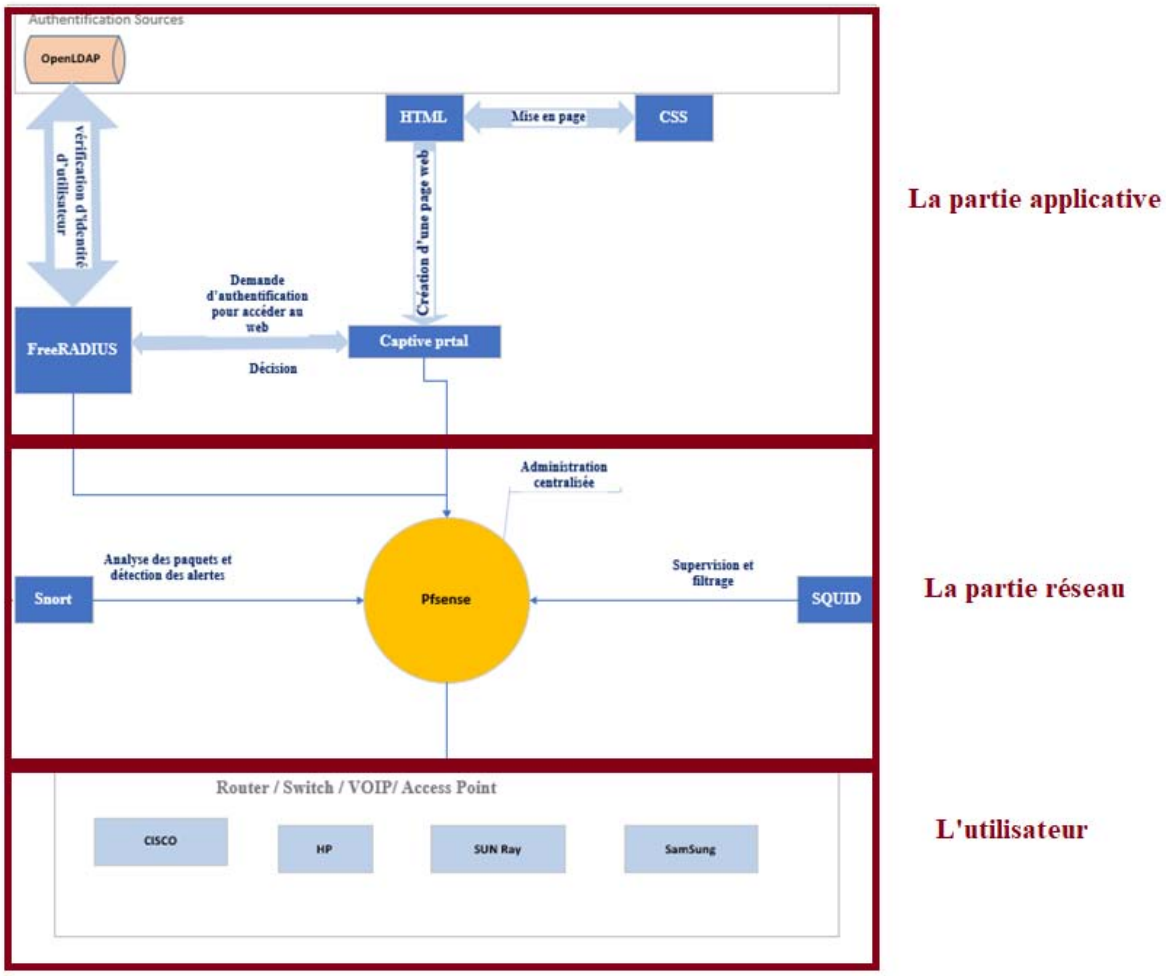


Figure 3: Interaction des outils NAC

Conclusion

Dans ce chapitre on a étudié les notions de base de contrôle d'accès au réseau puis on a pu choisir une solution NAC objectif de notre projet en présentant les outils nécessaires et ses fonctionnalités pour le faire.

Chapitre 3 : Analyse des besoins et Etude Conceptuelle

Introduction

Dans le but de mettre en place 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'analyse des besoins et une étude conceptuelle qui sont une phase cruciale dans le processus de notre solution.

1. Analyse des besoins

Dans cette section nous allons analyser la situation existante dans la direction CNOC de point de vue architecture de réseau, utilisateurs, politique de sécurité.

1.1. Etude de l'existant

1.1.1. Présentation de l'architecture du réseau local (CNOC)

La figure 4 présente la topologie du réseau interne de la direction CNOC :

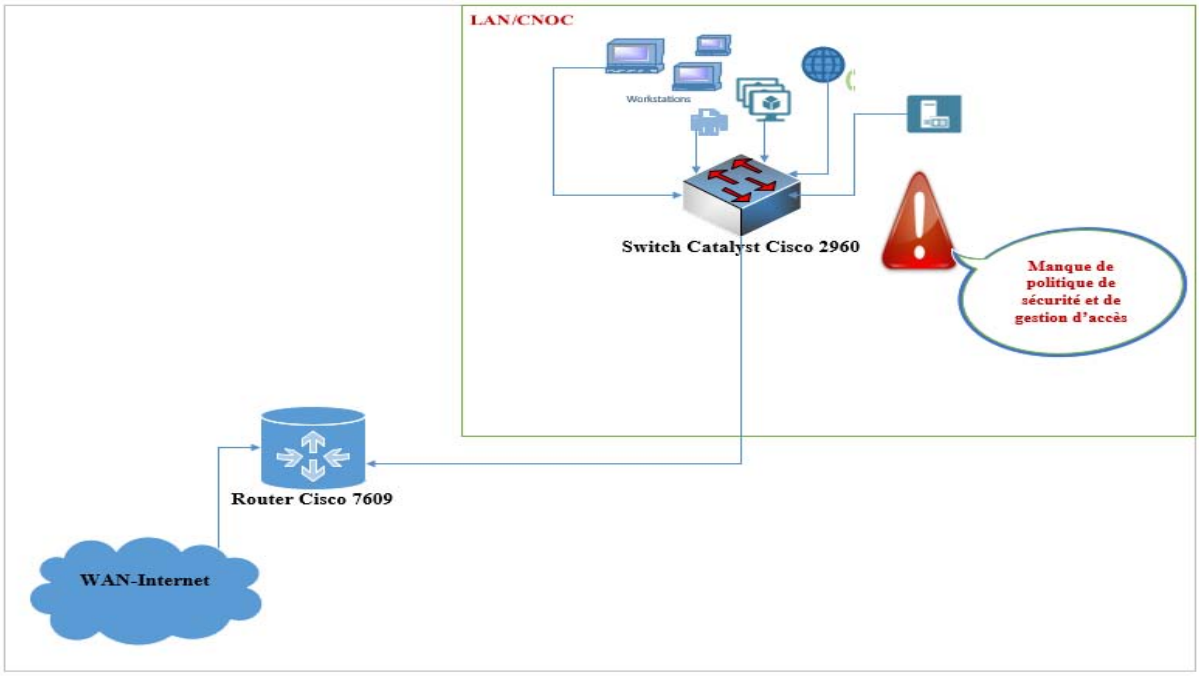


Figure 4: Architecture du réseau du CNOC

1.1.2. Description des équipements existants

Dans cette partie, nous allons décrire les équipements de l'architecture de notre réseau comme suit :

- Un serveur VMware assurant la gestion des VM,
- Des ordinateurs fixes et portatifs de marque HP et Lenovo équipés d'un système d'exploitation Linux,
- Une imprimante de Ecosys,
- 10 téléphones VOIP,
- Un Switch Catalyst Cisco 2960 permettant de lier ces équipements,
- Des VM permettant d'accéder à distance aux systèmes de gestion des réseaux pour traiter les réclamations ou configurer les équipements des clients (routeurs, switch,),
- Un routeur Cisco 7609 jouant le rôle de connecter le réseau local de CNOC au réseau WAN y compris les sites distants et à internet.

1.1.3. Présentation des utilisateurs

Les utilisateurs qui accèdent au réseau local de la direction sont nombreux, on peut les classer en trois types :

- **Les employés :** Ce sont les techniciens (les superviseurs), les ingénieurs, et les responsables (directeur, chef service, chef de bureau, chef projet,) ; ils sont autorisés à accéder au réseau de CNOC (wifi) en utilisant ses ressources,

- **Les invités :** Ce sont les fournisseurs, les sous-traitants, les clients et les stagiaires, ils sont autorisés à accéder seulement à l'internet.

1.1.4. Critique de l'existant

Avant d'entamer une analyse des besoins, on a relevé des failles de sécurité nécessitant une résolution à travers notre solution :

- Pas de politique de sécurité assurant une utilisation juste et légale des ressources partagées,
- Aucun contrôle des activités sur le réseau,

- Mal gestion de la ressource internet : en effet, comme cela était le cas très fréquemment, web était très demandé par les stagiaires. Ceux-ci s'adonnaient à des téléchargements à longueur de journée, ce qui abaissait le débit au niveau des machines administratives. Cela se faisait ressentir pendant l'ouverture des pages web,

- L'absence d'un système de détection d'intrusions,

- Absence d'informations résumant l'état du fonctionnement du parc informatique en temps réel,

- Pour des raisons de contrôle et de sécurité, En cas des besoins d'accès pour les visiteurs (clients, stagiaires, fournisseurs, sous-traitants…), c'est nécessaire de les attribuer un autre réseau selon leurs privilèges.

1.2. Specification des besoins

Cette phase représente l'aspect « fonctionnel » de la solution. Il sera question principalement de définir les acteurs et les différents cas d'utilisation.

1.2.1. Les besoins fonctionnels

L'analyse des besoins effectuée dans l'avant-projet porte uniquement sur les processus majeurs du projet. Dans cette partie, il est nécessaire de faire une étude plus approfondie des besoins, il s'agit de l'étude préalable dans laquelle nous nous assurons que les besoins sont exprimés uniquement de manière fonctionnelle et non pas en termes de solutions.

1.2.1.1.La gestion d'authentification

- Renforcer la gestion de l'authentification des utilisateurs en utilisant serveur d'authentification FreeRadius.
- Gérer l'authentification des utilisateurs selon à la stratégie de sécurité de CNOC.

1.2.1.2. La gestion d'accès

- Contrôler l'accès en isolant toute machine pouvant nuire le réseau de l'entreprise par exemple une machine n'ayant pas une mise à jour des antivirus récents,

1.2.1.3. La supervision

- Consulter l'historique des accès au réseau, l'état de conformité des machines, des flux réseaux.
- Être capable de visualiser les différentes phases d'accès pour n'importe quelle machine et consulter les machines bloquées.

1.2.1.4. L'administration

- Permettre de configurer le système en ajoutant des autres services ou protocoles,
- Créer des interfaces réseau au niveau firewall et fixer ses règles de routage et ses politiques de sécurité,
- Ajouter des comptes utilisateurs.

1.2.1.5. La gestion des ressources internet

- Filtrer quelques domaines ou sites internet,
- Visualiser les sites visités,
- Fixer la bande passante de chaque utilisateur.

1.2.2. Les besoins non fonctionnels

L'application à développer doit assurer les besoins non fonctionnels suivants :

- **La simplicité**

Notre application doit être simple et facile à utiliser les interfaces graphiques en supportant n'importe quel type de système ou équipements.

- **La rapidité du temps de réponse**

Le temps des décideurs est précieux. Les réponses doivent être par conséquent fournies dans un délai très réduit.

- **La sécurité**

L’accès à l’application ne doit être possible que pour les personnes autorisées. L’accès aux différentes pages doit être contrôlé. Ceci doit être fait en utilisant le protocole « https ».

- **La flexibilité**

Notre solution peut être évolué sans touchant la topologie réseau et gratuitement.

- **La virtualisation**

On va implémenter notre solution en mode virtuel en utilisant VMware Workstation.

1.2.3. Modélisation des besoins fonctionnels

Les diagrammes de cas d’utilisation décrivent les services les plus importants rendus par un système, Partant des acteurs, participants externes qui interagissent avec le système

Pour que notre solution NAC soit performante on a ajouté une interface web accessible par les utilisateurs.

1.2.3.1.Identification des acteurs

Un acteur est une personne ou un système extérieur qui interagit avec le système à réaliser afin de réaliser une valeur ajoutée.

Dans notre cas l’utilisateur principale du système est l’administrateur ; via l’interface web, il peut effectuer plusieurs taches présentées par le diagramme de cas d’utilisation.

1.2.3.2. Diagramme de cas d'utilisation global

La figure 5 présente le diagramme de cas d'utilisation global qui traduit les besoins fonctionnels cités ci-dessus.

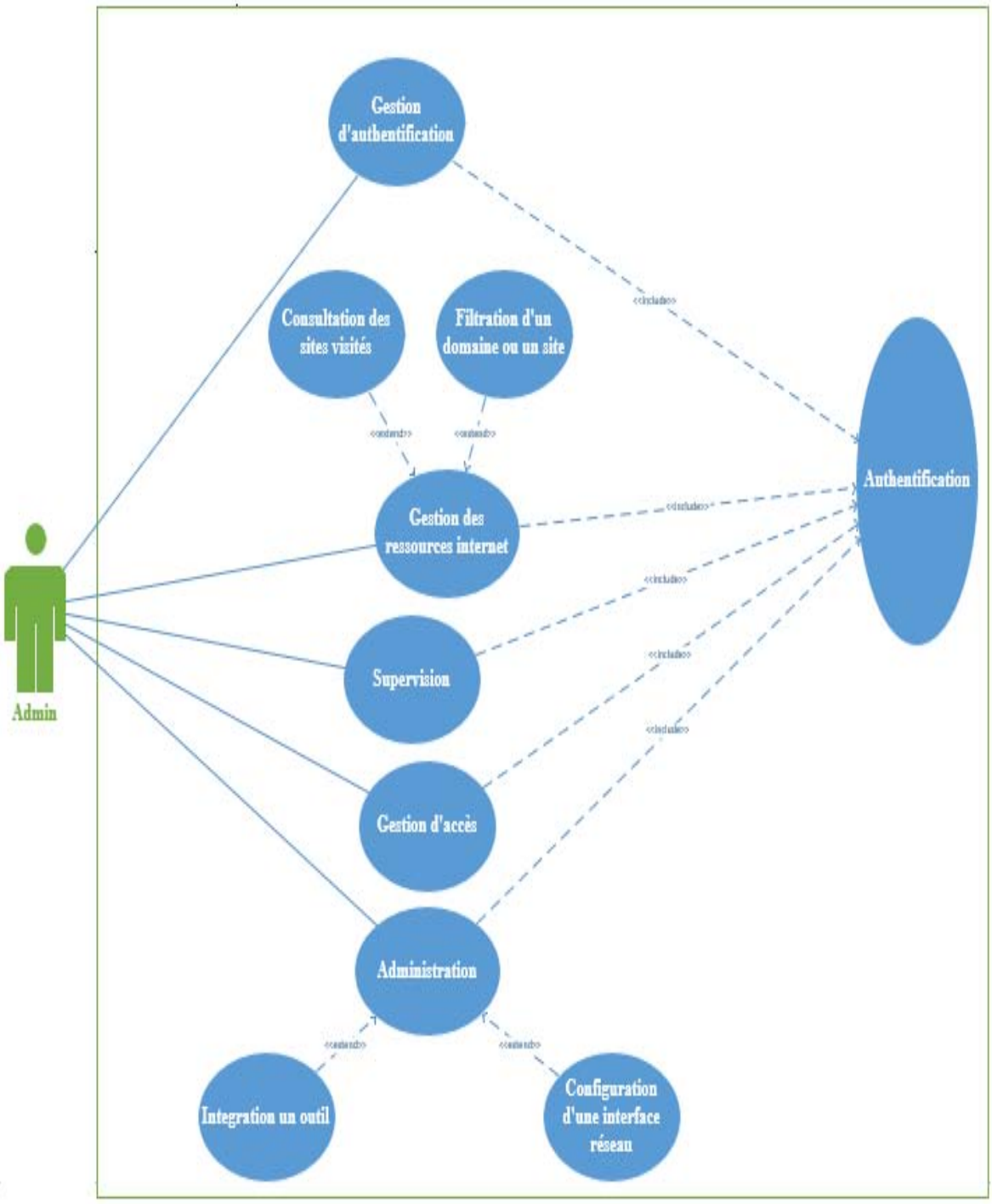


Figure 5: Diagramme de cas d'utilisation global

4. Conception

Cette partie va s'occuper de la conception en 2 étapes : la conception préliminaire (ou générale) décrivant le schéma physique des données et la conception détaillée qui va mapper quelques diagrammes de séquence objets.

4.1. Architecture physique de la solution proposée

La figure La figure suivante illustre l'architecture 3-tiers de notre solution (NAC) qui se compose de :

- Le client (les utilisateurs)
- Le serveur firewall
- Le serveur base de données (Active Directory)

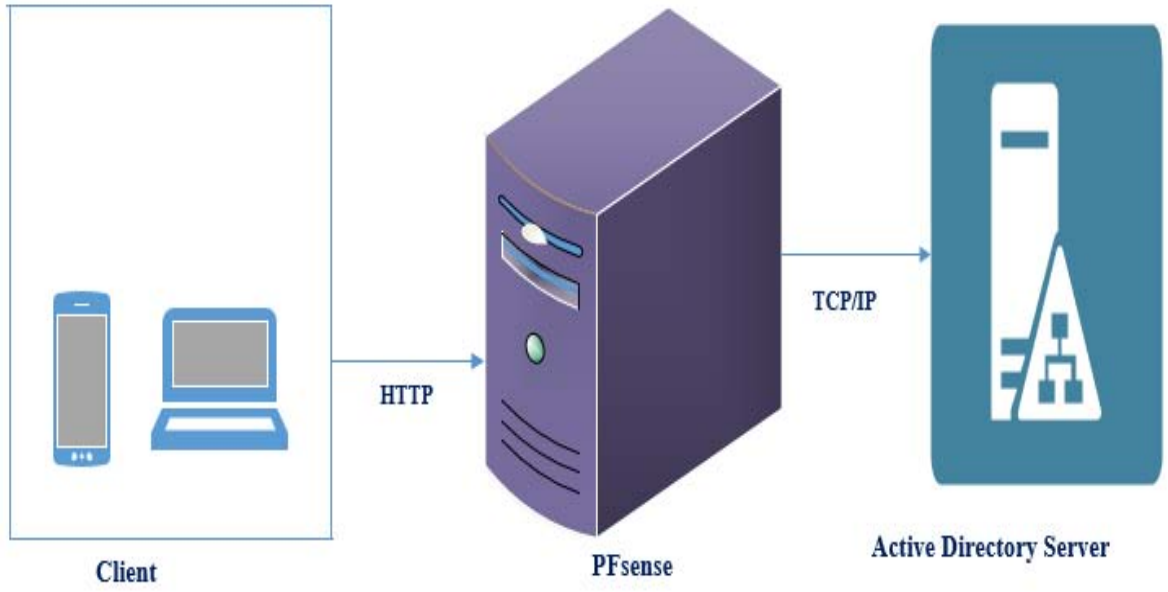


Figure 6: Architecture physique

4.2.Architecture de déploiement

L'architecture de déploiement utilisée est l'architecture 3 tiers composée des trois couches suivantes :

- **Client :** en utilisant un navigateur, le client affiche les différentes pages de l'application,

- **Serveur d'application :** il permet la gestion des requêtes envoyées par le client et vérifie avec le serveur de données,
- **Serveur de données :** il exécute les requêtes envoyées par le serveur d'application et envoie les résultats correspondants.

La figure 7 présente le diagramme de déploiement de notre application composé de trois nœuds

- Un nœud « Client » qui contient un navigateur web,
- Un nœud « Serveur d'applications » qui contient la solution NAC (Pfsense),
- Un nœud « Serveur de données » qui contient la base de données Active Directory.

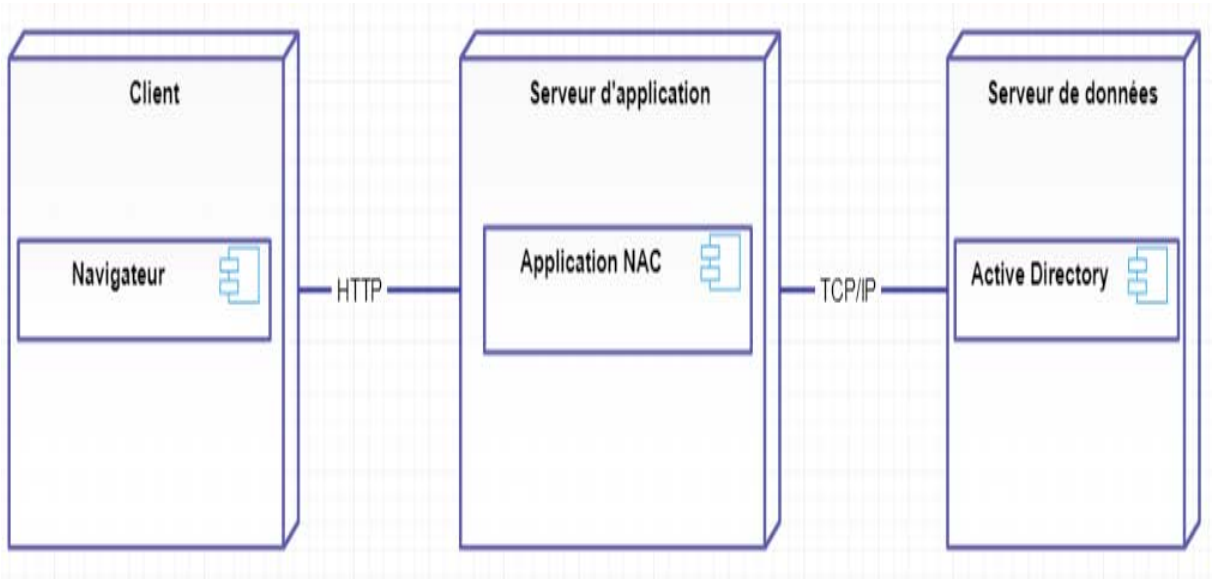


Figure 7: Diagramme de déploiement

4.3. Les diagrammes de séquences

Un diagramme de séquences et un outil permettant de présenter la coopération entre les différents objets sous forme des messages.

On va présenter quelques diagrammes de séquences pour les cas d'utilisation de la figure 5.

4.3.1. Le Diagramme de séquence « Bloquer un site ou un domaine »

Le diagramme de séquence dans le cas de filtrage d'un site ou d'un domaine est présenté par la figure ci-dessus, elle nous présente les coopérations faites entre l'admin et le système (Pfsense) ; Apres l'authentification, il demande de bloquer un site ou un domaine, le système affiche la fenêtre de filtrage, ensuite, l'administrateur saisi les domaines ou Urls à filtrer.

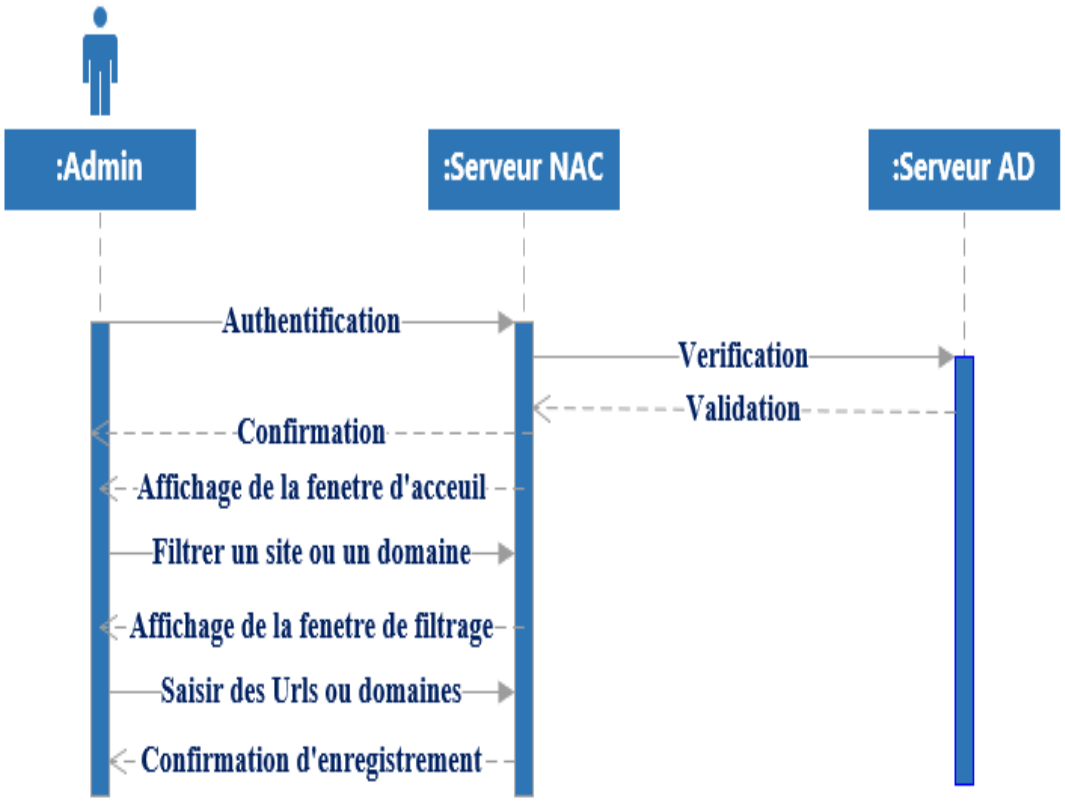


Figure 8: Diagramme de séquence « Bloquer un site ou un domaine »

4.3.2. Le diagramme de séquence « configurer une interface réseau »

Le diagramme ci-dessous représente le cas de configuration d'une interface réseau, elle nous montre les coopérations faites entre l'administrateur et Pfsense, âpres s'être identifié, l'administrateur demande de Configurer une interface réseau (WAN, LAN ou DMZ, le système lui affiche la fenêtre de configuration, et enfin l'administrateur affecte l'adressage, règle le routage ou fixe la politique de sécurité (Rules)

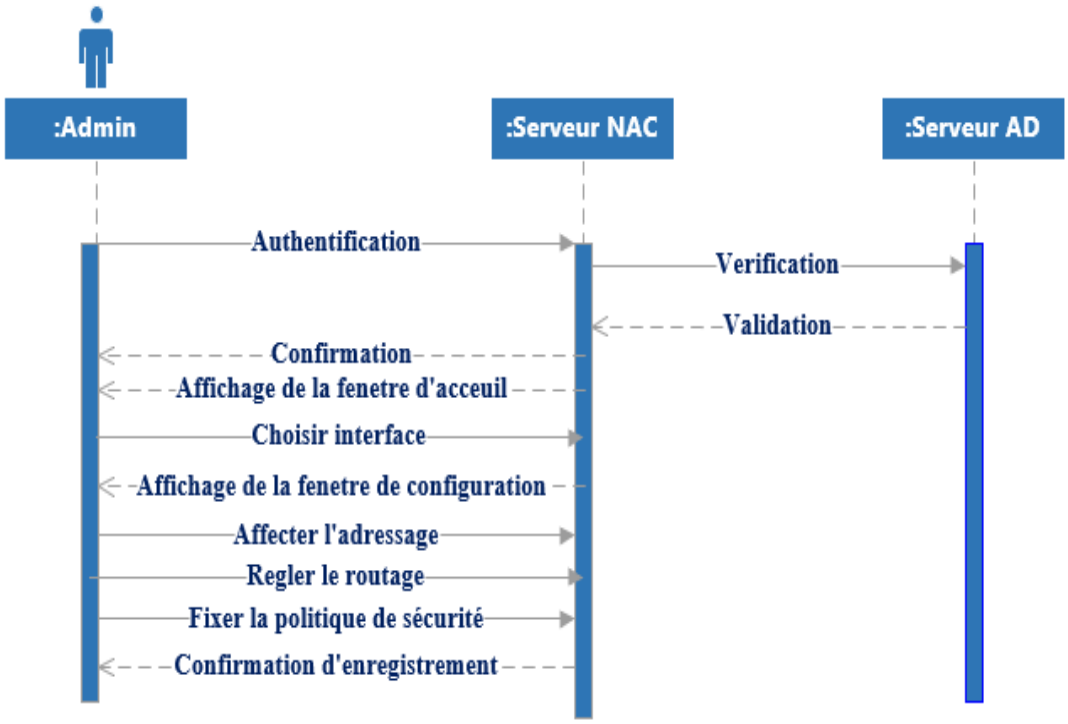


Figure 9:Diagramme de séquence « configurer une interface réseau »

Conclusion

Dans ce chapitre on a présenté l'étude de l'existant, les besoins fonctionnels ainsi que les besoins non fonctionnels qui seront offerts par notre future application. Finalement nous avons présenté ces besoins sous forme de diagramme de cas d'utilisation global.

Chapitre 4 : Mise en place de la solution et Evaluation

Introduction

Dans ce chapitre on va mettre en place notre solution de contrôle d'accès NAC puis on va faire des tests et évaluation.

1. Environnement du travail

Dans cette on introduira l'environnement matériel et logiciel utilisé pour la réalisation de ce projet.

4.6. Environnement materiel

On a installé la machine virtuelle « Vmware Workstation » dans un PC portable HP ayant les caractéristiques suivantes :

Processeur	Intel ® Core™ i7 CPU 2,5 GHz
RAM	8 Go
Type du système	Système d'exploitation 64bits

Tableau 3: les caractéristiques du PC

4.7. Environnement logiciel

Le tableau 5 montre les versions des divers services et outils démarrages nécessaires pour la mise en place de la solution Network Acess Control :

Nom de l'outil	La version
VMWARE WORKSTATION	VMware-workstation-full-12.exe
CentOS 7	CentOS 7-s001.vmdk
Free RADIUS	freeradius2 1.7.9
SNORT	snort-2.9.9.0_3
Pfsense	pfs-s001.vmdk
Windows Server /Active Directory	Windows Server 2012 R2.vmdk.lck
Squid Proxy Server	Lightsquid 3.0.6_4
Squid Reserve Server	squid 0.4.42
SquidGuard Proxy Server	squidguard-1.4_15

Tableau 4: Les version des outils NAC

2. Mise en place de la solution NAC

2.1. Infrastructure de déploiement

La figure 10 présente l'infrastructure de déploiement et les adressages nécessaires :

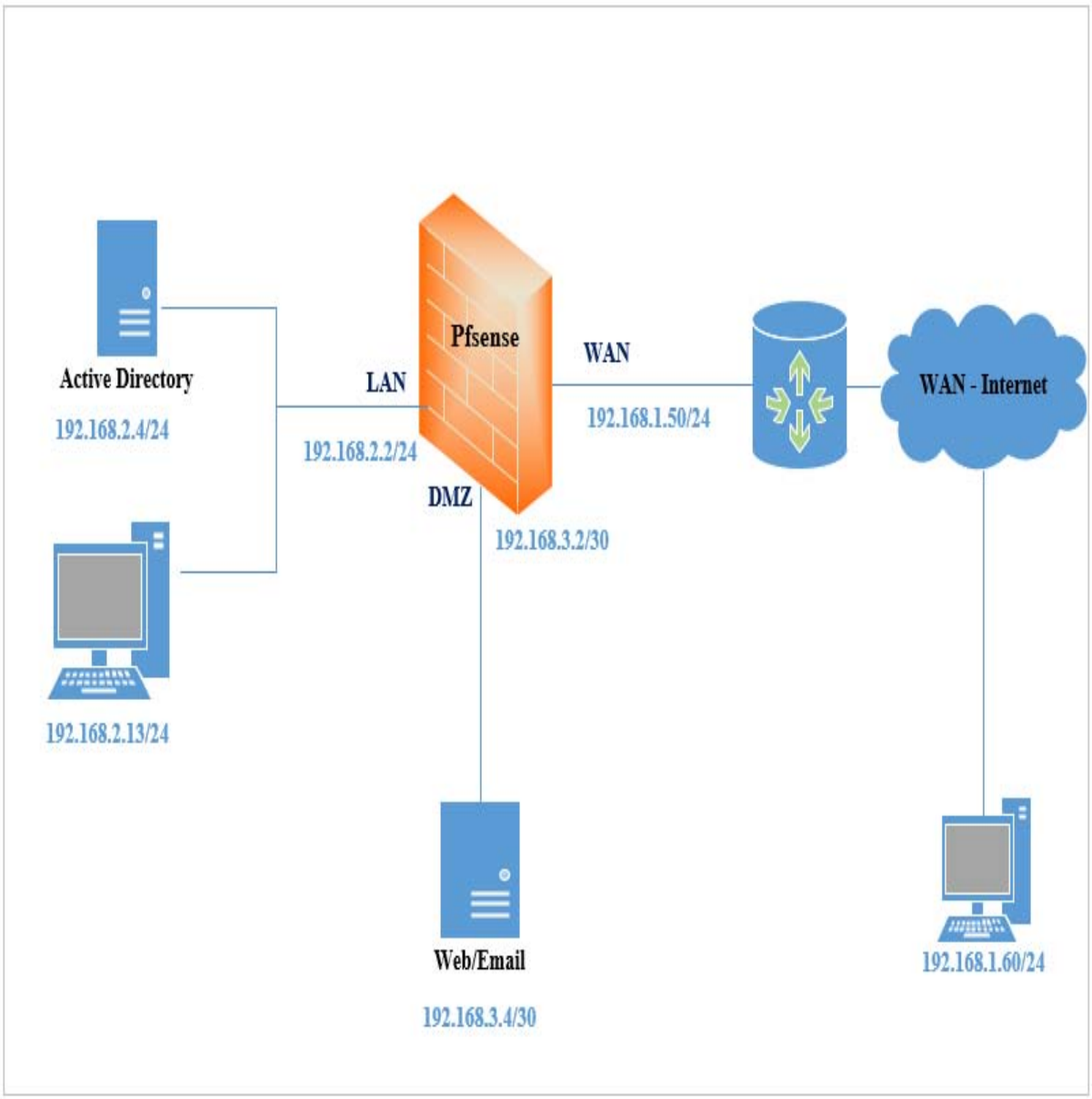


Figure 10: La topologie réseau de notre solution

2.2. Etapes de déploiement

On trouve comme suit les grandes étapes de déploiement de notre solution, par la suite on va décrire chaque étape.

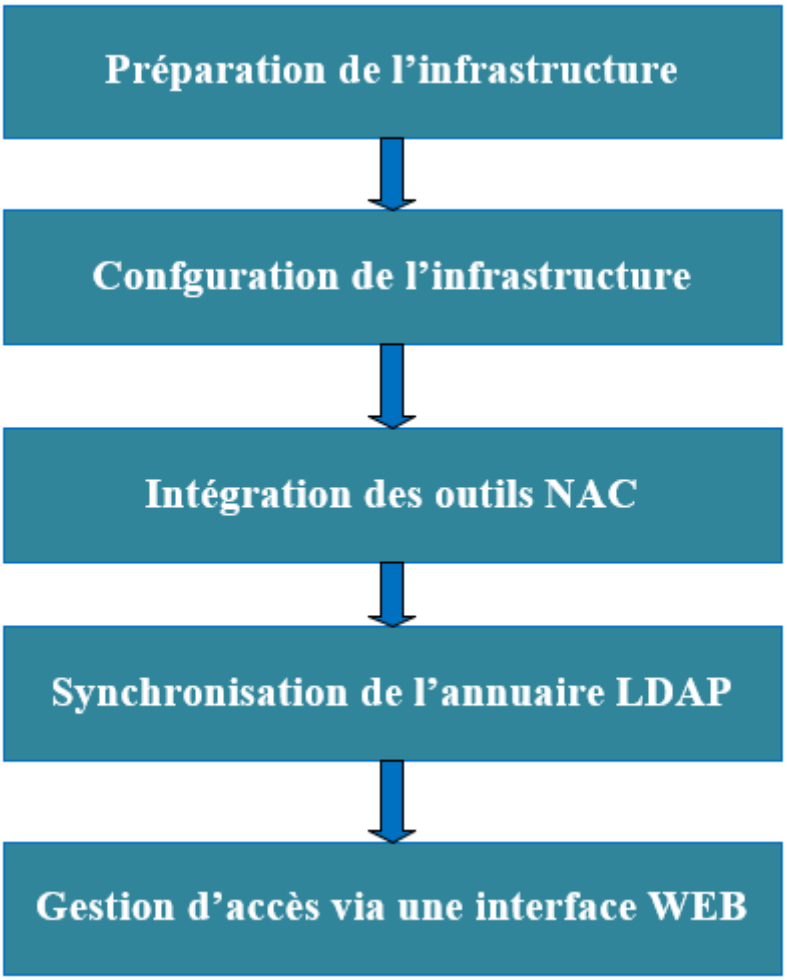


Figure 11: Etapes de déploiement

2.2.1. Préparation de l'infrastructure

2.2.1.1. La création des machines virtuelles

Via Workstation, on a créé une machine virtuelle PFsense et autre Linux Mint pour qu'on puisse accéder à l'interface LAN de Pfsense.

PFsense possède trois cartes réseaux (VMnet8 : interface WAN, VMnet1 : interface LAN, VMnet8 : interface DMZ).

2.2.1.2. La connexion entre PFsense et les machines du LAN et WAN

On a configuré les cartes réseaux virtuelles ; @IP et mode (**briged**, **NAT**, **Host Only**).

On a braché PFsense et Linux Mint à travers la carte VMnet1 en mode Host only, VMnet8 en mode NAT, et VMnet0 en mode Briged.

Ensuite, on a assigné l'adressage des interfaces LAN, DMZ et WAN du firewall :

```
*** Welcome to pfSense 2.3.4-RELEASE (i386 full-install) on pf ***

 WAN (wan)       -> le3        -> v4: 192.168.1.50/24
 LAN (lan)       -> le2        -> v4: 192.168.2.2/24
 DMZ (opt1)      -> le1        -> v4: 192.168.3.2/24
```

Figure 12: Les interfaces réseaux du Pfsense

2.2.2. Configuration de l'infrastructure

2.2.2.1. Paramétrage de base

Pour configurer PFsense, on a accédé à son interface graphique Web via la machine Linux Mint ;

Passons maintenant à la configuration de base de notre système y compris le nom (pf), le domaine (tunisietelecom.tn), le serveur NTP (time zone), le DNS (8.8.8.8 /8.8.4.4), DHCP (192.168.2.10 - 192.168.2.200), et la passerelle par défaut (192.168.1.1) pour qu'on puisse accéder à internet via l'interface WAN (notre point d'accès c'est un clé USB).

2.2.2.2.Réglage de routage

Au niveau menu **Routing**, **Gateway**, on a fixé la passerelle par défaut de l'interface LAN, WAN et DMZ pour préciser les chemins des paquets entre ces réseaux :

IPv4 Routes

Destination	Gateway	Flags	Use	Mtu	Netif	Expire
default	192.168.1.1	UGS	3617	1500	le3	
127.0.0.1	link#8	UH	3873	16384	lo0	
192.168.1.0/24	link#4	U	25290	1500	le3	
192.168.1.50	link#4	UHS	0	16384	lo0	
192.168.2.0/24	link#3	U	34168	1500	le2	
192.168.2.2	link#3	UHS	75	16384	lo0	
192.168.3.0/24	link#2	U	0	1500	le1	
192.168.3.2	link#2	UHS	1	16384	lo0	

Figure 13: la table de routage

Maintenant on va tester la connectivité entre les interfaces réseaux ; exemple **LAN=>WAN**

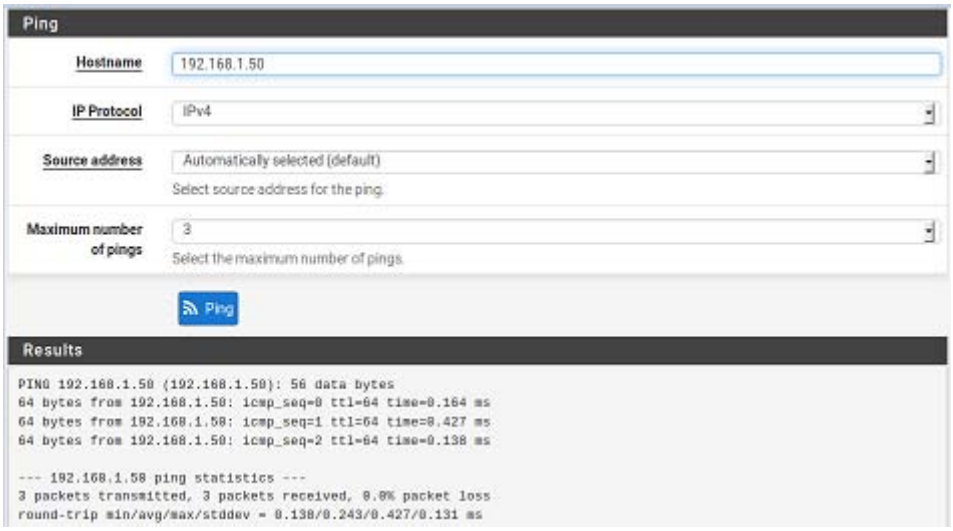


Figure 14: Test de connectivité entre Lan et WAN

2.2.2.3. Fixation de la politique de sécurité

On a fixé les règles de filtrage des paquets au niveau de chaque interface du Pfsense :

- **L'interface réseau DMZ :**

La figure 15 présente les droits d'accès des utilisateurs redirigés au réseau DMZ.

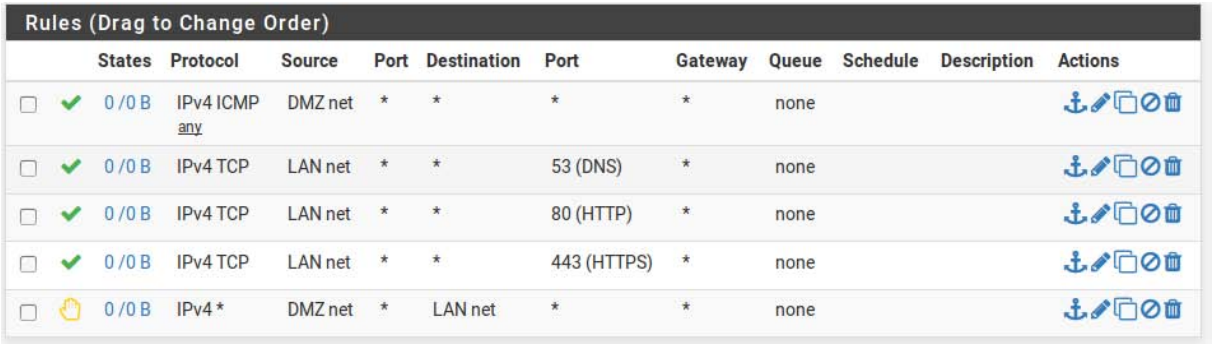
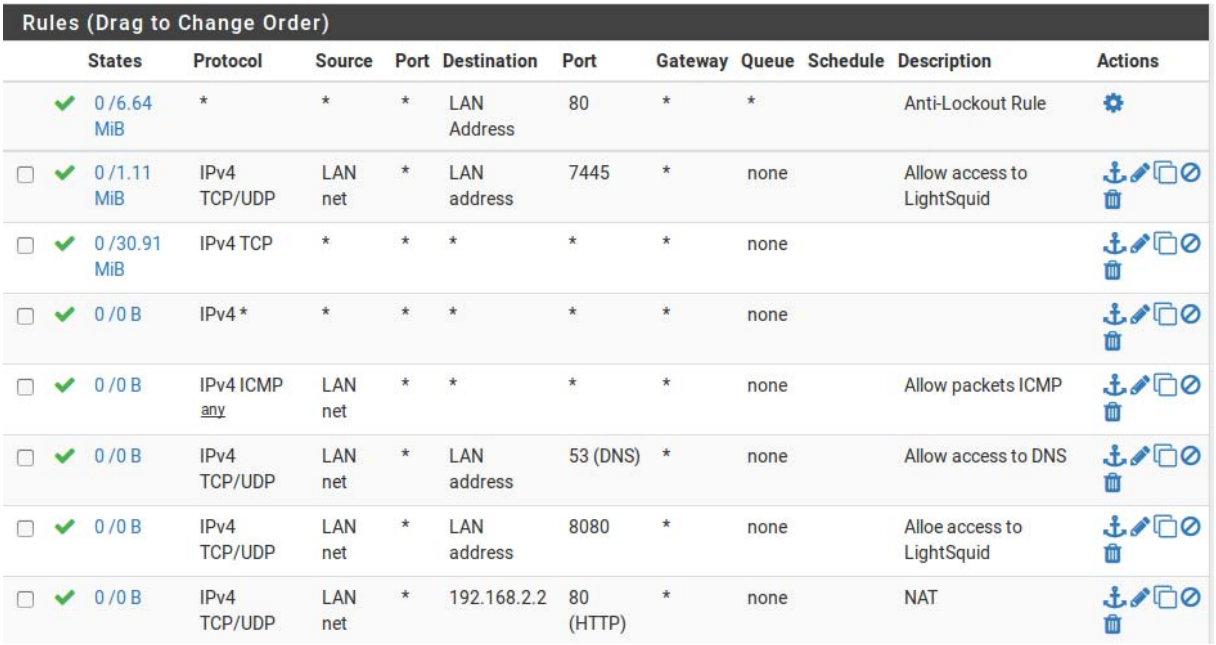


Figure 15: Les règles de filtrage au noveau DMZ

- **L'interface réseau LAN :**

A travers cette interface on a permis aux utilisateurs du réseau local de CNOC d'accéder à internet via le réseau WAN.



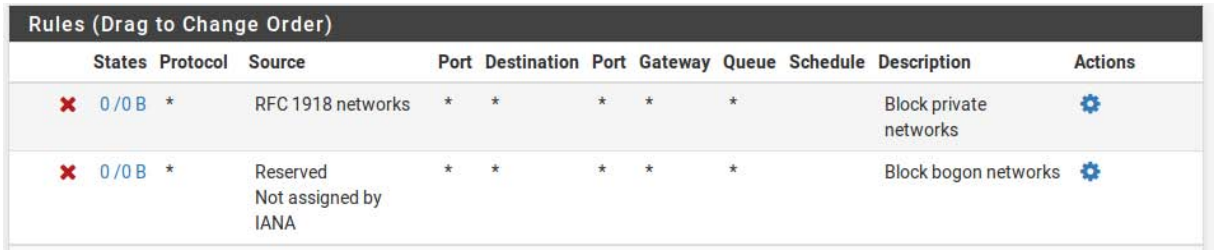
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✔	0 /6.64 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
☐ ✔	0 /1.11 MiB	IPv4 TCP/UDP	LAN net	*	LAN address	7445	*	none		Allow access to LightSquid	⚓✎⧉⊘🗑
☐ ✔	0 /30.91 MiB	IPv4 TCP	*	*	*	*	*	none			⚓✎⧉⊘🗑
☐ ✔	0 /0 B	IPv4 *	*	*	*	*	*	none			⚓✎⧉⊘🗑
☐ ✔	0 /0 B	IPv4 ICMP any	LAN net	*	*	*	*	none		Allow packets ICMP	⚓✎⧉⊘🗑
☐ ✔	0 /0 B	IPv4 TCP/UDP	LAN net	*	LAN address	53 (DNS)	*	none		Allow access to DNS	⚓✎⧉⊘🗑
☐ ✔	0 /0 B	IPv4 TCP/UDP	LAN net	*	LAN address	8080	*	none		Alloe access to LightSquid	⚓✎⧉⊘🗑
☐ ✔	0 /0 B	IPv4 TCP/UDP	LAN net	*	192.168.2.2	80 (HTTP)	*	none		NAT	⚓✎⧉⊘🗑

Figure 16: Les regles de fltrage au niveau LAN

- **L'interface réseau WAN :**

Dans cette interface, on a bloqué tout réseau privé ou réseau présentant une menace.



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✖	0 /0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
✖	0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙

Figure 17: Les regles de fltrage au niveau WAN

2.2.3. Intégration des outils NAC

Afin de développer notre firewall, on a lui intégré les outils suivants :

2.2.3.1. Installation et configuration de FreeRadius

Apres l'installation du serveur d'authentification FreeRadius au niveau Pfsense, on a activé l'interface LDAP assurant sa connexion avec l'annuaire Active directory.

La figure 18 présente les interfaces de FreeRadius :

Interface IP Address	Port	Interface Type	IP Version	Description
*	1812	auth	ipaddr	FreeRadius Auth
*	1813	acct	ipaddr	FreeRadius Acc
*	1816	status	ipaddr	FreeRadius Status

Figure 18 Interfaces de Free Radius

2.2.3.2.Installation et configuration de Snort

Suite l'installation de paquet du protocole de détection des intrusions Snort, on l'a activé au niveau l'interface WNA, on a configuré son interface et lancer les mises à jour nécessaires.

Alors démarre son fonctionnement comme présenté dans la figure suivante :

Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions
☐	WAN		AC-BNFA	DISABLED	DISABLED	WAN	

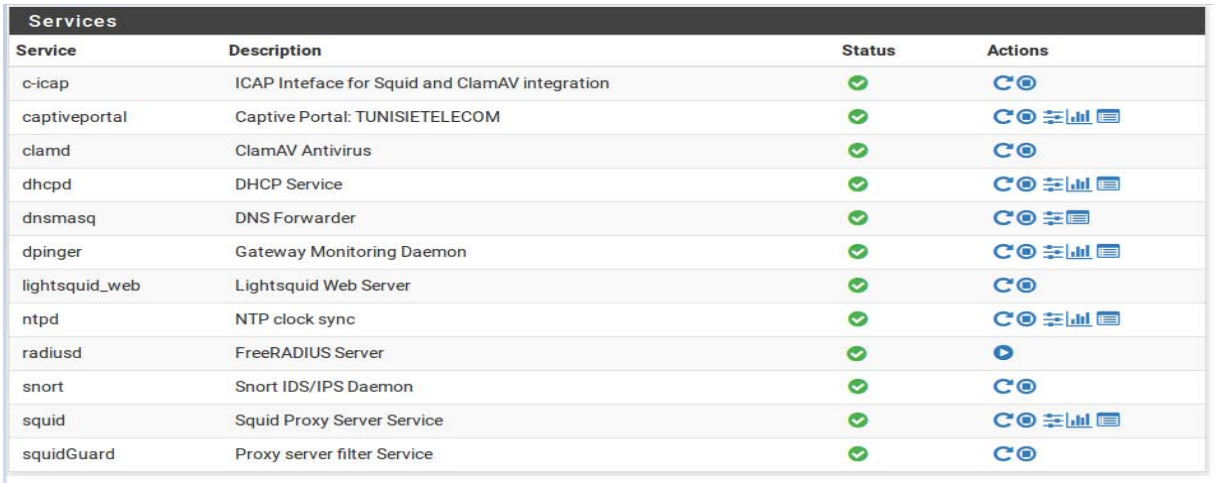
Figure 19: Interface de Snort

2.2.3.3.Installation et configuration Squid Proxy

Pour assurer le filtrage des domaines et le monitoring, on a installé et configuré au niveua de l'interface LAN trois serveur proxy :

- Squid Proxy Server, port 8080 en téléchargeant l'antivirus ClamAV,
- Squid Reserve Server,
- SquidGuard Proxy Server, port 7445 en téléchargeant la liste des mauvais sites (blacklist)pour les bloquer automatiquement.

Alors tous les outils et services installés fonctionnent correctement comme mentionné dans la figure suivante :



Services

Service	Description	Status	Actions
c-icap	ICAP Inteface for Squid and ClamAV integration		
captiveportal	Captive Portal: TUNISIETELECOM		
clamd	ClamAV Antivirus		
dhcpd	DHCP Service		
dnsmasq	DNS Forwarder		
dpinger	Gateway Monitoring Daemon		
lightsquid_web	Lightsquid Web Server		
ntpd	NTP clock sync		
radiusd	FreeRADIUS Server		
snort	Snort IDS/IPS Daemon		
squid	Squid Proxy Server Service		
squidGuard	Proxy server filter Service		

Figure 20: La liste de services et outils intégrés à pfsense

2.2.4. Synchronisation de l'annuaire LDAP

La synchronisation de LDAP nécessite la connexion entre le serveur FreeRadius et la base de données Active Directory :

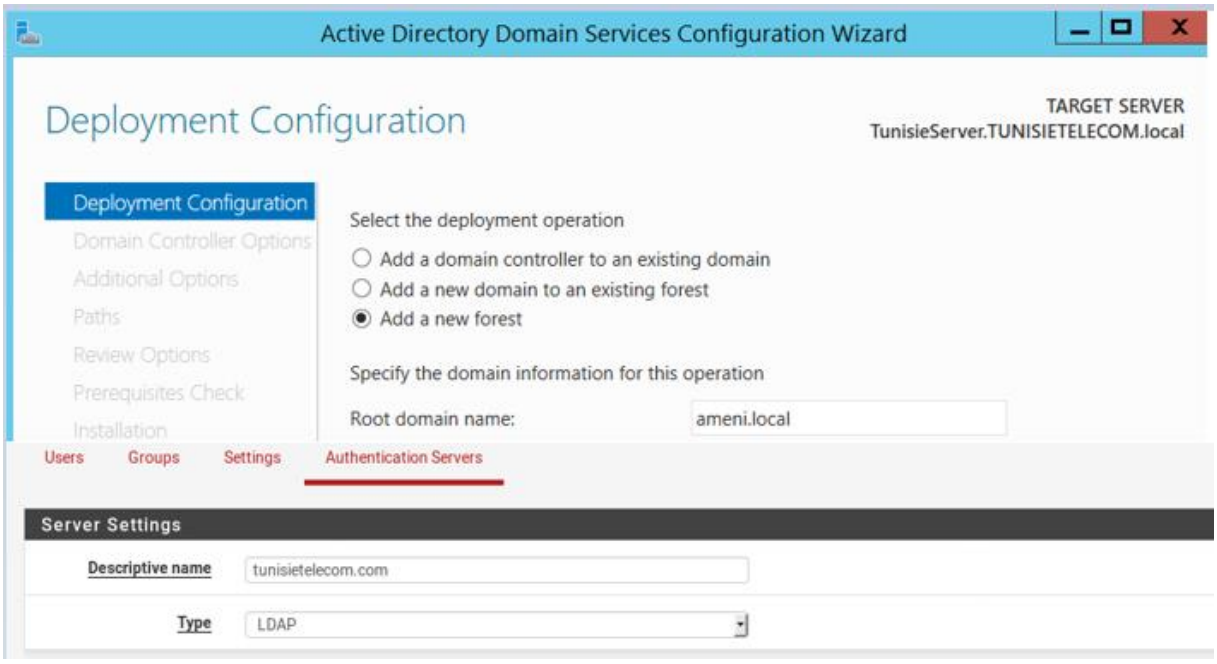


Figure 21: Connexion de Free Radius et AD

Puis la création des comptes utilisateurs :

Figure 22: Interface compte utilisateur

2.2.5. Gestion du contrôle d'accès à travers une interface Web

Afin d'effectuer ses taches, on a développé une interface web accessible par l'administrateur principalement et les autres utilisateurs selon leurs privilèges.

1. Evaluation

Cette partie sera consacré aux tests et évaluation des interfaces réalisées suite la mise en place de notre solution de contrôle d'accès au réseau.

1.1.Interface d'authentification

La figure 24 présente une interface d'authentification permettant aux utilisateurs de l'entreprise s'authentifier avant de connecter au navigateur.

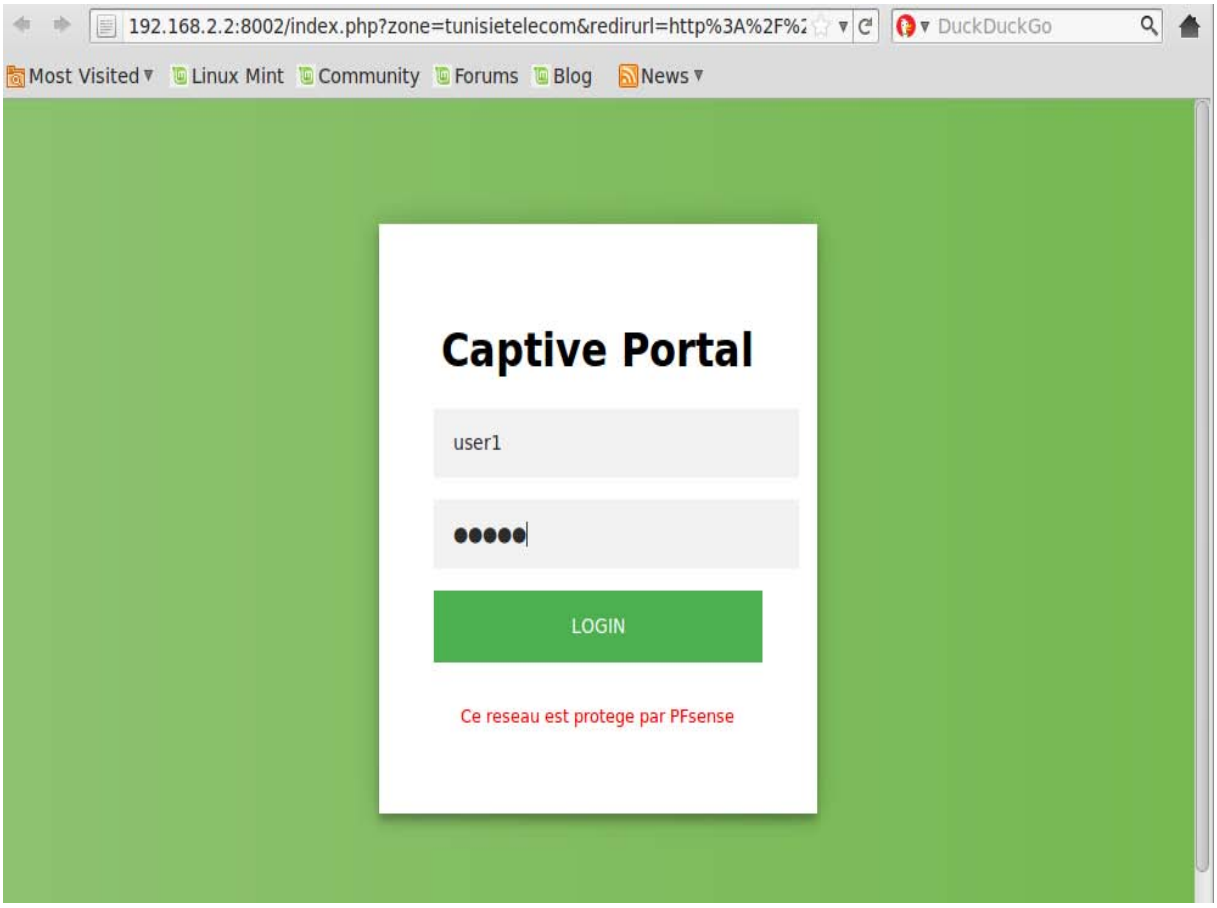


Figure 23: Interface d'authentification (mot de passe correcte)

- **Blocage d'un compte utilisateur**

La figure 25 présente un compte bloqué de l'utilisateur Ahmed.

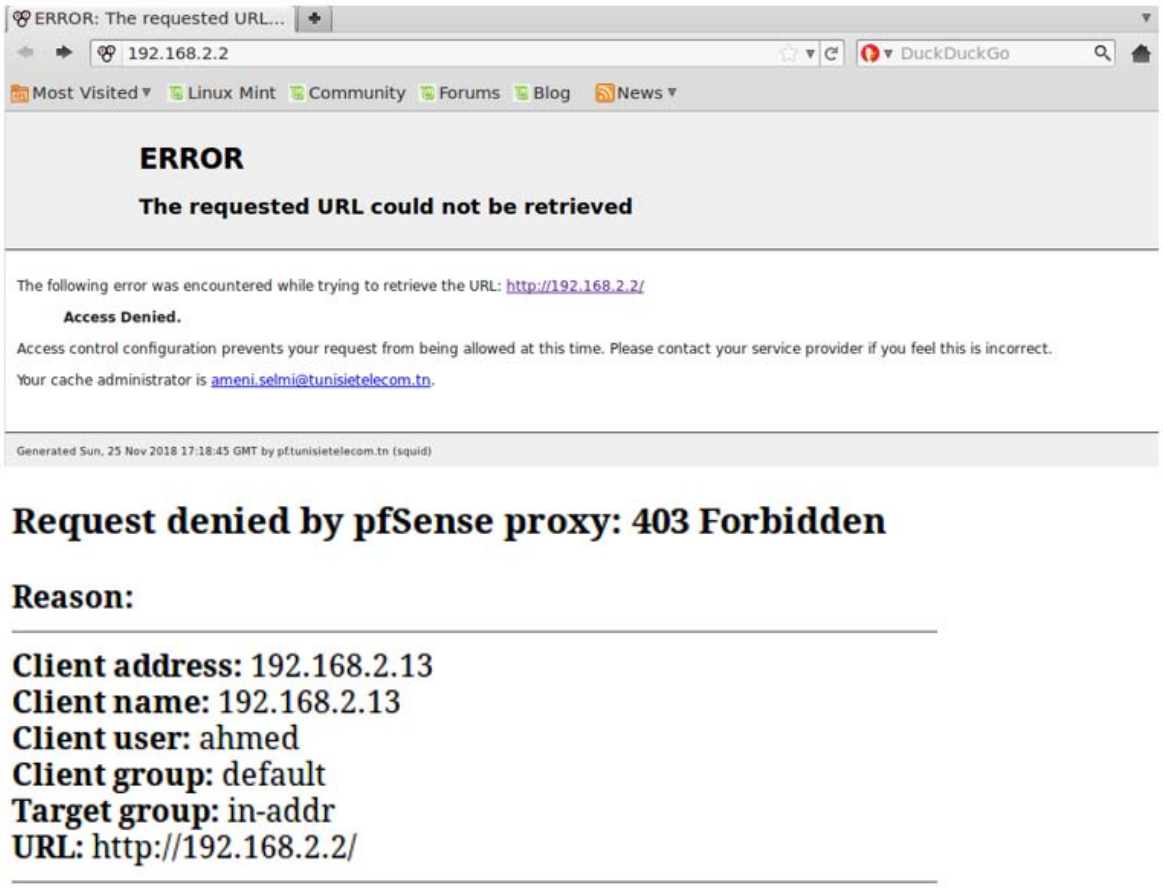


Figure 24: Compte utilisateur bloqué

Dans ce cas, il doit contacter l'administrateur pour faire le nécessaire et résoudre le problème comme affiché dans la figure suivante :

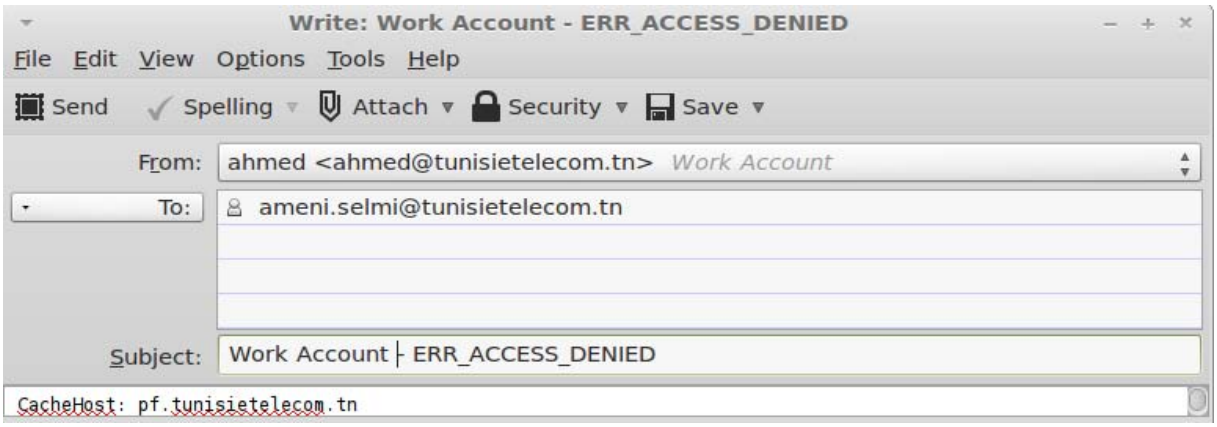


Figure 25: Réclamation d'un utilisateur

1.2.Interface de supervision

- **Supervision du trafic réseau**

A travers cette interface on peut consulter le trafic des réseaux WAN, LAN et DMZ ce qui induit que notre architecture physique est bien fonctionnelle.

Figure 26: Interface de supervision du trafic

- **Consultation des utilisateurs**

La figure 28 nous affiche les utilisateurs de réseau de l'entreprise en les classant selon la bande passante et le nombre d'accès :

Work Period: **Nov 2018**

#	Time	Graph	MONTH	User	Real Name	Connect	Bytes	%	Cumulative
1			[M]	ahmed	?	50	611 137	38.5%	611 137
2			[M]	houssem	?	23	594 268	37.5%	1.1 M
3			[M]	amira	?	26	368 490	23.2%	1.5 M

Figure 27: La liste des utilisateurs

- **Consultation des sites visités par utilisateur**

La figure suivante présente les sites visités avec le nombre d'accès et le débit consommé pour chaque site le 25 Novembre 2018 pour l'utilisateur Ahmed.

Squid user access report

User: ahmed (?)
Group: ?
Date: 25 Nov 2018

#	Accessed site	Connect	Bytes	Cumulative	%
Total			611 137		
1	safebrowsing-cache.google.com	4	533 121	533 121	87.2%
2	pf.tunisietelecom.tn	2	26 092	559 213	4.2%
3	ocsp.msocsp.com	9	19 373	578 586	3.1%
4	ocsp.pki.goog	14	10 704	589 290	1.7%
5	ocsp.digicert.com	9	8 154	597 444	1.3%
6	http://google/	1	4 330	601 774	0.7%
7	192.168.2.2	5	3 309	605 083	0.5%
8	safebrowsing.clients.google.com	1	2 987	608 070	0.4%
9	www.cisco.com	2	1 604	609 674	0.2%
10	www.google.com	1	715	610 389	0.1%
11	www.linuxmint.com	1	492	610 881	0.0%
12	www.microsoft.com	1	256	611 137	0.0%
Total			611 137		

Figure 28: La liste des site visités par l'utilisateur Ahmed

Via l'interface présenté par la figure 30, on peut visualiser le débit consommé par 'utilisateur Ahmed (596 kbits) pendant la journée 25 Novembre 2018.

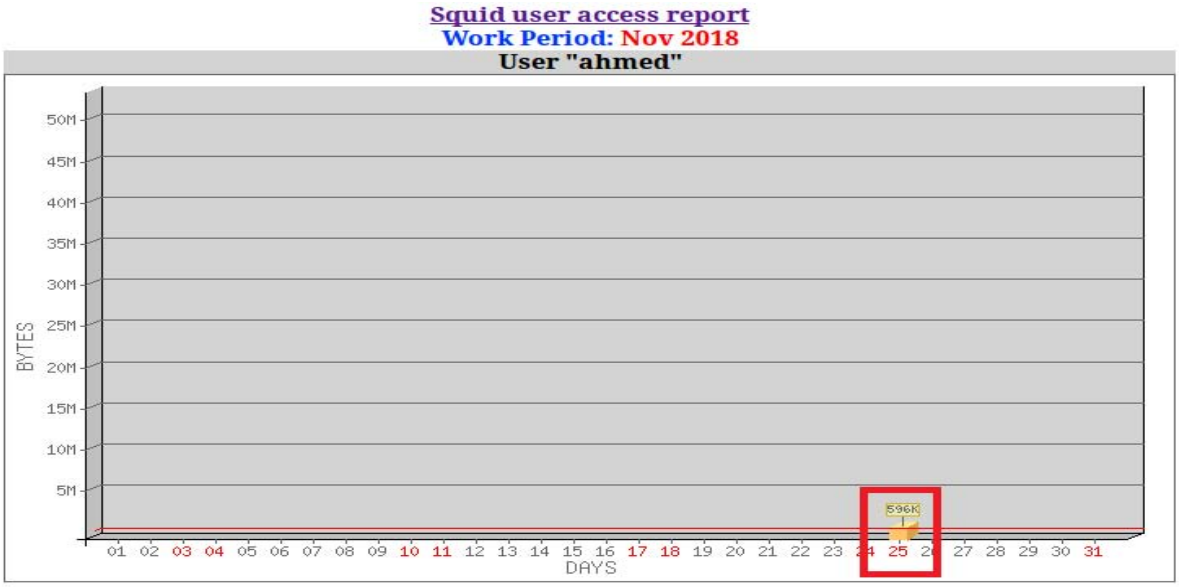


Figure 29: Le débit consommé par l'utilisateur Ahmed

1.3.Interface d'administration

Après authentification, l'administrateur a le droit de :

- Consultation du tableau de bord du firewall,
- Configuration des interfaces réseau (LAN, WAN, DMZ) au niveau menu « **Interfaces** »,
- Supervision de l'état du réseau via le menu « **Status** » et « **Diagnostics** ».

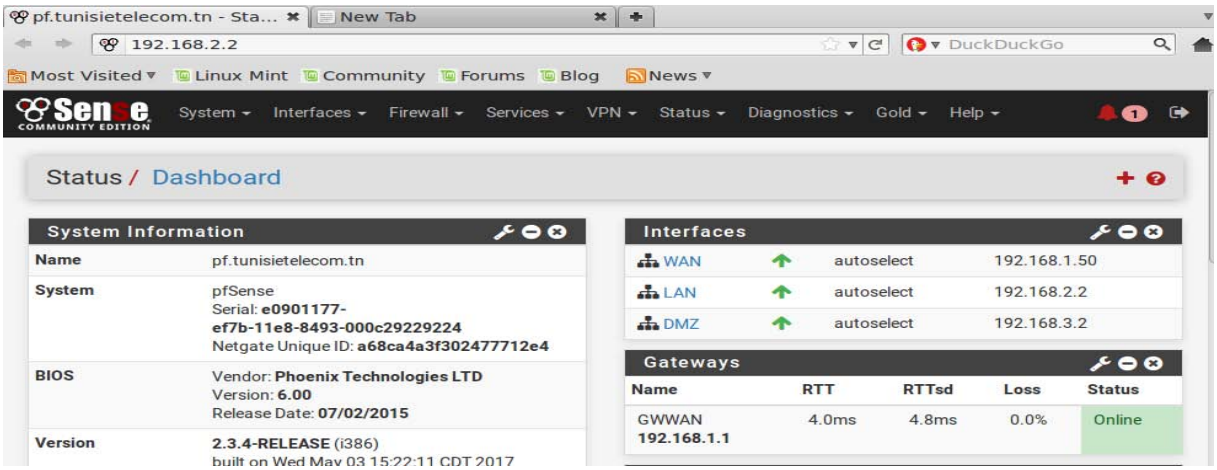


Figure 30: Tableau de bort de pfsense

- **Gestion des utilisateurs**

A travers cette interface l'administrateur peut crier, supprimer ou modifier un compte utilisateur.

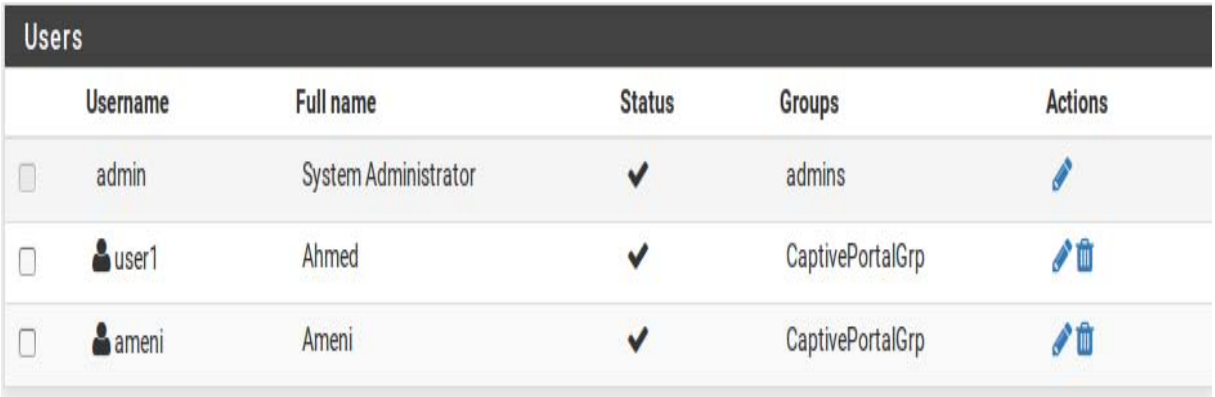
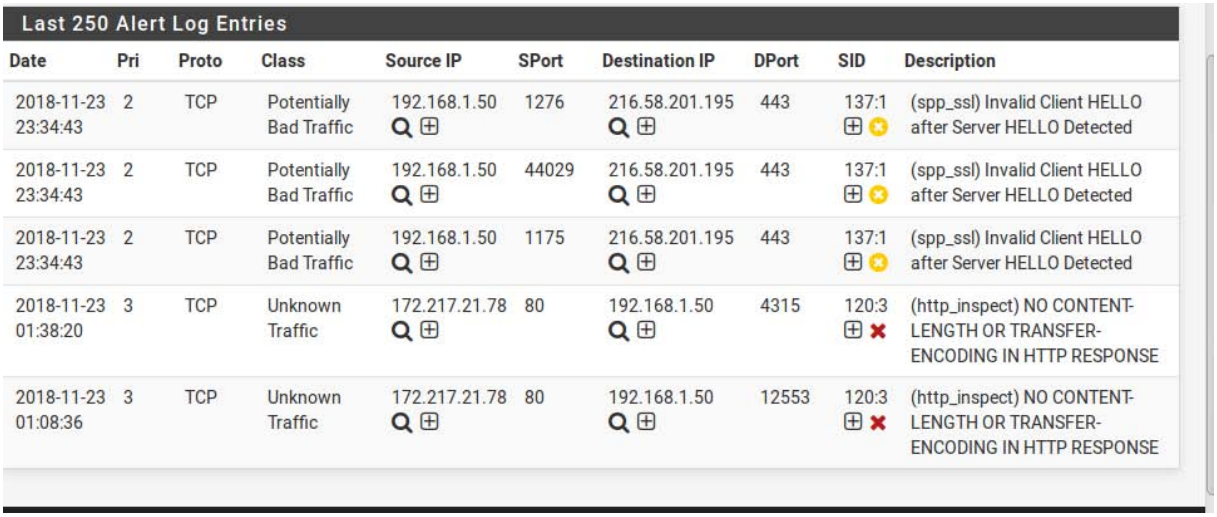


Figure 31: Interface de gestion des utilisateurs

1.4.Interface de gestion d'accès

- **Consultation des alertes**

La figure 28 présente les alertes avec les détails de la machine possédant une menace (@IP de la machine, le port cible, la nature du trafic, et le temps de tentative,) en la bloquant d'accéder au réseau de l'entreprise.



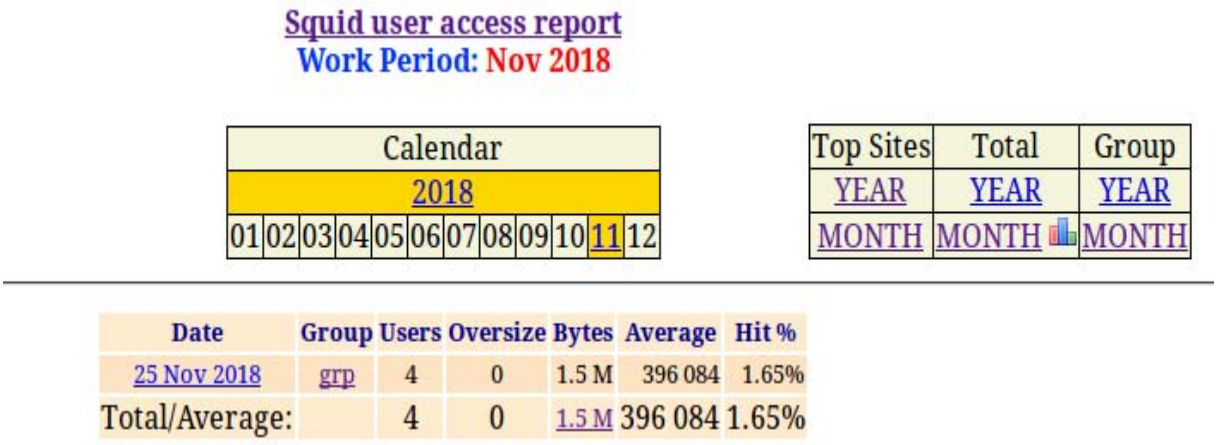
Last 250 Alert Log Entries

Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2018-11-23 23:34:43	2	TCP	Potentially Bad Traffic	192.168.1.50	1276	216.58.201.195	443	137:1	(spp_ssl) Invalid Client HELLO after Server HELLO Detected
2018-11-23 23:34:43	2	TCP	Potentially Bad Traffic	192.168.1.50	44029	216.58.201.195	443	137:1	(spp_ssl) Invalid Client HELLO after Server HELLO Detected
2018-11-23 23:34:43	2	TCP	Potentially Bad Traffic	192.168.1.50	1175	216.58.201.195	443	137:1	(spp_ssl) Invalid Client HELLO after Server HELLO Detected
2018-11-23 01:38:20	3	TCP	Unknown Traffic	172.217.21.78	80	192.168.1.50	4315	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2018-11-23 01:08:36	3	TCP	Unknown Traffic	172.217.21.78	80	192.168.1.50	12553	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE

Figure 32: Interface des alertes

- **Consultation l'historique d'utilisation du réseau**

Cette interface affiche un rapport détaillé d'accès du 25 Novembre 2018 ; le groupe des utilisateurs, les Top sites visités, la bande passante consommée et le nombre d'accès.



Squid user access report
Work Period: Nov 2018

Calendar											
2018											
01	02	03	04	05	06	07	08	09	10	11	12

Top Sites	Total	Group
YEAR	YEAR	YEAR
MONTH	MONTH	MONTH

Date	Group	Users	Oversize	Bytes	Average	Hit %
25 Nov 2018	grp	4	0	1.5 M	396 084	1.65%
Total/Average:		4	0	1.5 M	396 084	1.65%

Figure 33: Rapport d'accès d'utilisateurs au réseau

1.5.Interface de gestion des ressources internet

- **Filtrage du site Facebook**

L'utilisateur a le droit d'accéder au site www.micrososft.com mais il est interdit d'accéder au www.facebook.com en affichant un message d'erreur « Problem loading page » comme montre la figure 34.

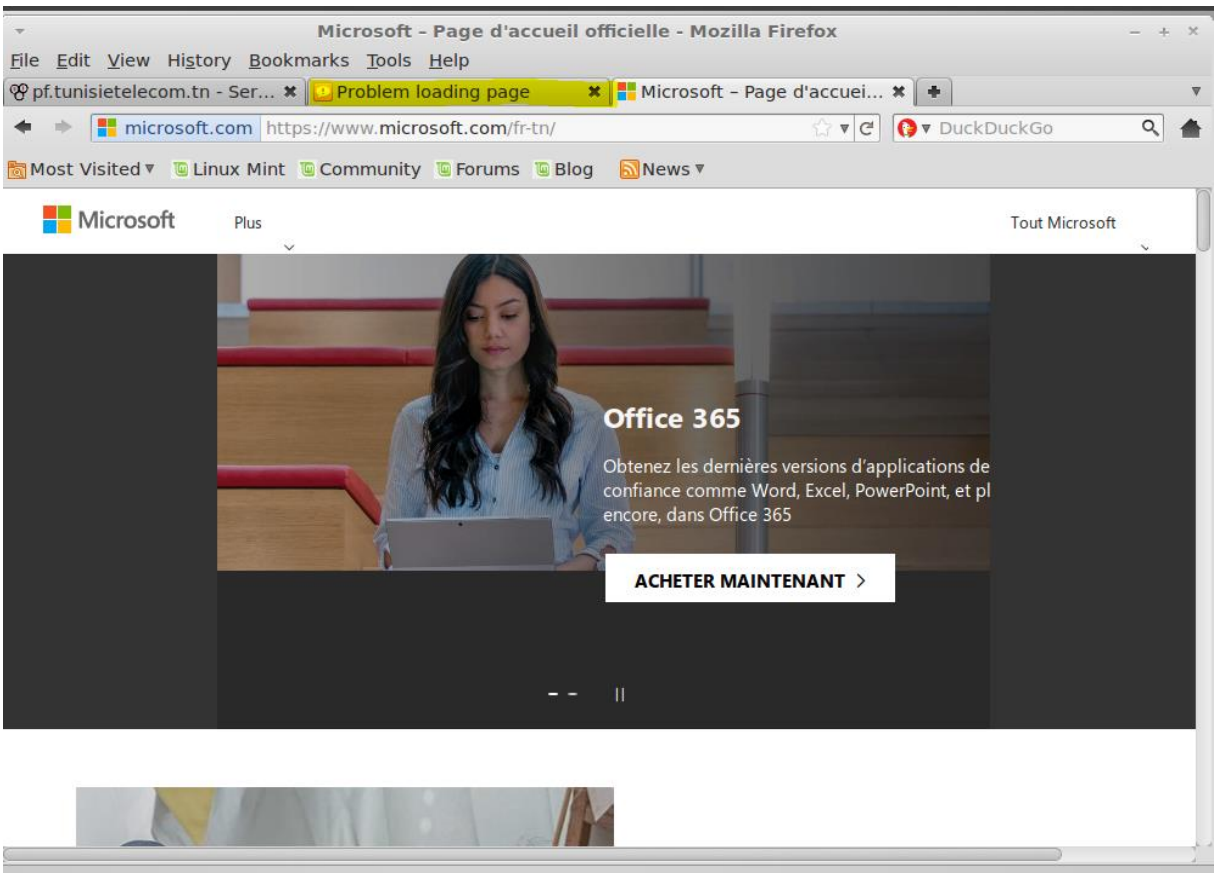


Figure 34: Site facebook bloqué

- **Visualisation des sites visités**

Les Top sites visités le 25 Novembre 2018 par tous les utilisateurs sont classés comme présenté par la figure 35.

Top Sites

Work Period: 25 Nov 2018

	Accessed site	Connect	Bytes	%
1	who ocsp.pki.goog	22	17 303	1.0%
2	who ocsp.msocsp.com	20	43 417	2.7%
3	who ocsp.digicert.com	17	15 402	0.9%
4	who cache_object://localhost/active_requests	14	10 442	0.6%
5	who safebrowsing-cache.google.com	12	1.4 M	89.6%
6	who 192.168.2.2	8	5 273	0.3%
7	who ocsp.comodoca.com	4	4 336	0.2%
8	who safebrowsing.clients.google.com	3	11 748	0.7%
9	who pf.tunisietelecom.tn	3	39 138	2.4%
10	who www.cisco.com	2	1 604	0.1%
11	who http://google/	2	8 660	0.5%
12	who ocsp.usertrust.com	2	1 912	0.1%
13	who www.google.com	2	1 430	0.0%
14	who www.linuxmint.com	1	492	0.0%
15	who ocsp2.globalsign.com	1	2 243	0.1%
16	who www.tunisietelecom.tn	1	377	0.0%
17	who www.microsoft.com	1	256	0.0%
18	who ocsp.entrust.net	1	2 599	0.1%
Total			**1.5 M**	

Figure 35: Top sites visités

2. 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,
- La complexité concernant le déploiement de l'architecture réseau sous un environnement virtuel en se connectant au point d'accès physique,
- Problème de compatibilité des services et qui nécessitent des certificats.

Conclusion

Dans ce chapitre, nous avons présenté l'environnement de travail que nous avons vécu. Nous avons aussi abordé les test et validation de sécurité offerte par les outils utilisés et les problèmes rencontrés tout au long de la phase de réalisation de ce projet.

Conclusion & Perspectives

Ce mémoire consiste à mettre en place une plateforme de contrôle d'accès 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 qui nous a conduits à orchestrer plusieurs outils open sources remplissant les exigences d'un firewall nouvelle génération et la valider sur un environnement de test. En effet si un client veut se connecter au réseau de l'entreprise, il doit s'authentifier en premier lieu, ensuite il traverse l'OpenAppID pour identifier l'application, s'il a le droit d'utiliser cette application ou non, enfin le trafic traverse le PFSence pour détecter s'il y'a des menaces dans le contenu du trafic.

Bien évidemment, nous avons rencontré plusieurs difficultés durant la réalisation du travail essentiellement lors de la configuration du firewall proxy squid guard avec l'absence quasi-totale de toute documentation technique. De plus la plupart des versions souffraient de plusieurs anomalies (bugs) et de dépendances avec des versions spécifiques de librairies.

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 :

- 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.

Bibliographie et Netographie

1. Tunisie Telecom. Presentation de Tunisie Telecom. [En ligne] https://www.tunisietelecom.tn/Fr/Particulier/A-Propos. S0.

2. —. Présentation de Tunisie Telecom. [En ligne] https://www.tunisietelecom.tn/Fr/Particulier/A-Propos. S1.

3. Symantec. Présentation d'un virus. [En ligne] https://fr.norton.com/internetsecurity-malware-whatis-a-computer-virus.html.

4. Bouzid, Mohamed Ben. *« Mise en place d'une solution de détection des pirates et de malwares dans les sites tunisiens ».* s.l. : rapport du projet fin d'étude d'ingénieur en Informatique. S37.

5. SecuriteInfo.com. Le Déni de Service Distribué. [En ligne] https://www.securiteinfo.com/attaques/hacking/ddos.shtml. S30.

6. —. Les Fonctions de Hachage. [En ligne] https://www.securiteinfo.com/cryptographie/hash.shtml. S6.

7. Vulgarisation-informatique.com. Présentation d'un antivirus. [En ligne] https://www.vulgarisation-informatique.com/fonctionnement-antivirus.php. S7.

8. FUTURA TECH. Présentation d'un firewall. [En ligne] https://www.futura-sciences.com/tech/definitions/internet-firewall-474/. S8.

9. CommentCaMarche.com. Présentation d'un systeme de detection d'intrusion. [En ligne] https://www.commentcamarche.com/contents/237-systemes-de-detection-d-intrusion-ids. S9.

10. CommentCamarche.Com. Présentation d'un systeme d'intrusion et de prévention. [En ligne] https://www.commentcamarche.com/contents/238-systemes-de-prevention-d-intrusion-ips. S10.

11. Duvallet, Claude. Architectures et Protocoles des Réseaux. [En ligne] http://litis.univ-lehavre.fr/~duvallet/enseignements/Cours/M1INFO/Reseau/MI-Cours-Reseau-Cours8-4p.pdf. S12.

12. —. Le protocole RADIUS. [En ligne] http://litis.univ-lehavre.fr/~duvallet/enseignements/Cours/CNAM/CNAM-Cours-ServeurRadius.pdf. S13.

13. PODMILSAK, Audric. Extended Authentication Protocol. [En ligne] http://igm.univ-mlv.fr/~dr/XPOSE2008/802.1x/EAP.html. S14.

14. Cisco. Présentation de la solution Cisco ASA. [En ligne] https://www.cisco.com/c/fr_fr/products/security/asa-5500-series-next-generation-firewalls/index.html. S29.

15. Paloaltonetworks. Présentationd e la solution Palo Alto. [En ligne] https://www.paloaltonetworks.com/company/press/2014/cyber-defense-palo-alto-networks-la-premiere-solution-de-securite-reseau-certifiee-par-lanssi-en-france. S31.

16. Sonicwall. Présentation de la solution Sonic wall. [En ligne] https://www.sonicwall.com/fr-fr/solutions. S32.

17. Stonesoft. Présentation de la solution Stone soft. [En ligne] https://brain-networks.fr/stonesoft.html. S33.

18. CONNECT. Présentationd e la solution Netfilter. [En ligne] https://connect.ed-diamond.com/GNU-Linux-Magazine/GLMFHS-041/Introduction-a-Netfilter-et-iptables. S35.

19. PIERRE, Romain. Présentation de la solution IPCOP. [En ligne] http://it4all.wpweb.fr/wp-content/uploads/sites/12051/2015/06/rapport_ipcop_romain_pierre.pdf . S34.

20. pfsense. pfSense Overview. [En ligne] https://www.pfsense.org/about-pfsense/. S19.

21. Endian. Présentation de la solution Endian. [En ligne] https://www.endian.com/community/overview/. S36.

22. Thiaw, Djiby. Mise en place d'un proxy Squid sécurisé avec authentification LDAP. [En ligne] 2002. https://www.memoireonline.com/07/11/4611/m_Mise-en-place-dun-proxy-Squid-securise-avec-authentification-LDAP3.html. S20.

23. —. Mise en place d'un proxy Squid sécurisé avec authentification LDAP. [En ligne] 2002. https://www.memoireonline.com/07/11/4611/m_Mise-en-place-dun-proxy-Squid-securise-avec-authentification-LDAP3.html. S21.

24. Sylvain, Thiboult. Portail captif. [En ligne] 19 12 2016. http://www.ac-nantes.fr/medias/fichier/dt-portail-captif-installation-https_1482134888607-pdf. S23.

25. Scientillula. HTML et CSS. [En ligne] http://www.scientillula.net/ISN/HTML_CSS/presentation.html. S24.

26. Igm.univ-mlv. CSS : Cascading Style Sheets. [En ligne] http://www-igm.univ-mlv.fr/~dr/XPOSE2004/css/presentation.php. S25.

27. GRALON. Présentation des spywares. [En ligne] https://www.gralon.net/articles/internet-et-webmaster/logiciel/article-qu-est-ce-qu-un-spyware--1230.htm. S2.

28. Symantec. *Présentation d'un virus.* [En ligne] https://fr.norton.com/internetsecurity-malware-what-is-a-computer-virus.html. S1.

29. KASPERSKY. Présentation d'un vers informatique. [En ligne] https://www.kaspersky.fr/resource-center/threats/viruses-worms. S3.

30. CommentCaMarche. Presentation d'un cheval de troie. [En ligne] https://www.commentcamarche.com/contents/1234-chevaux-de-troie-informatique. S4.

31. SecuriteInfo.com. Le Déni de Service Distribué. [En ligne] https://www.securiteinfo.com/attaques/hacking/ddos.shtml. S5.

32. CHARLOT, Cécilien. Solutions NAC de contrôle d'accès au réseau. 10 oct. 2008.

33. CISCO. Description de la gamme Cisco N. [En ligne] https://www.cisco.com/web/FR/documents/pdfs/datasheet/vpn_security/Cisco_NAC_Presentation_synoptique.pdf. S15.

34. Microsoft. About NAP. [En ligne] 31 5 2018. https://docs.microsoft.com/en-us/windows/desktop/nap/about-nap. S16.

35. JUNIPER NETWORKS. UNIFIED ACCESS CONTROL. [En ligne] 3 2012. https://www.juniper.net/us/en/local/pdf/brochures/1500051-en.pdf. S17.

36. JafSec.com. Open Source Network Access Control Solutions. [En ligne] http://jafsec.com/Network-Access-Control/free-nac.html. S18.

37. QUACK1☠BLOG. Snort : Présentation rapide de l'IDS. [En ligne] 13 03 2013. http://quack1.me/snort_overview.html. S22.

38. www.cisco.com. Présentation de la solution Cisco ASA. [En ligne] https://www.cisco.com/c/fr_fr/products/security/asa-5500-series-next-generation-firewalls/index.html. S28.

Liste des Abréviations

A

AAA: Authentication **A**utorisation **A**ccounting

ACL: Access **C**ontrol **L**ist

AD: Active **D**irectory

AP: Access **P**oint

C

CA: Certification **A**uthority

CPU: Central **P**rocessing **U**nit

D

DDOS: Distributed **D**enial **O**f **S**ervice

DHCP : Dynamic **H**ost **C**onfiguration **P**rotocol

DMZ : Zone **D**émilitarisée

DNS: Domain **N**ame **S**ystem

DoS: Denial **O**f **S**ervice

E

EAP: Extensible **A**uthentication **P**rotocol

F

FTP: File **T**ransfer **P**rotocol

H

HTTP: Hypertext **T**ransfer **P**rotocol

HTTPS: Hypertext **T**ransfer **P**rotocol **S**ecured

I

ICMP: Internet **C**ontrol **M**essage **P**rotocol

IDS: Intrusion **D**etection **S**ystem

IEEE: Institute **of E**lectrical **and E**lectronics **E**ngineers

IP: Internet **P**rotocol

IPS: Intrusion **P**revention **S**ystem

L

LAN: Local **A**rea **N**etwork

LDAP: Lightweight **D**irectory **A**ccess **P**rotocol

M

MAC: Media **A**ccess **C**ontrol

MD5: Message **D**igest 5

N

NAC: Network **A**ccess **C**ontrol

NAS: Network **A**ccess **S**erver

NAT: Network **A**ddress **T**ranslation

O

OS: Operating **S**ystem

P

PC: Personal **C**omputer

R

Radius: Remote **A**uthentication **D**ial-**I**n **U**ser **S**ervice

S

SSH: Secure **Sh**ell

SSL: Secure **S**ockets **L**ayer

T

TCP: Transmission **C**ontrol **P**rotocol

TLS: Transport **L**ayer **S**ecurity

U

UML: Unified **M**odeling **L**anguage

URL: Uniform **R**esource **L**ocator

V

VoIP: Voice **o**ver **IP**

VPN: Virtual **P**rivate **N**etwork

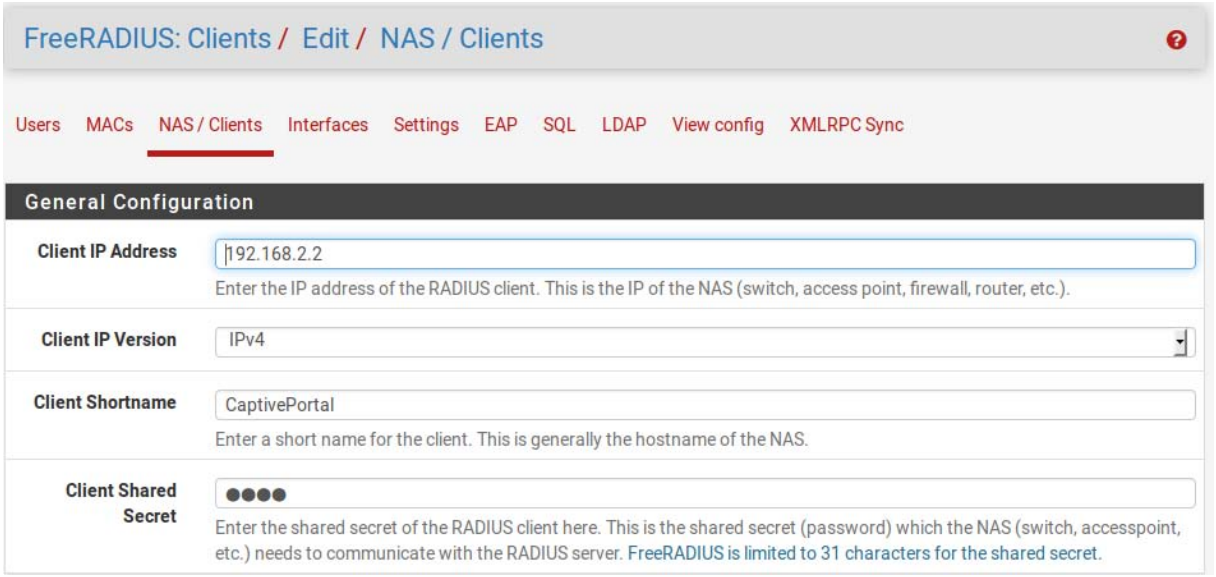
W

WAN: Wide **A**rea **N**etwork

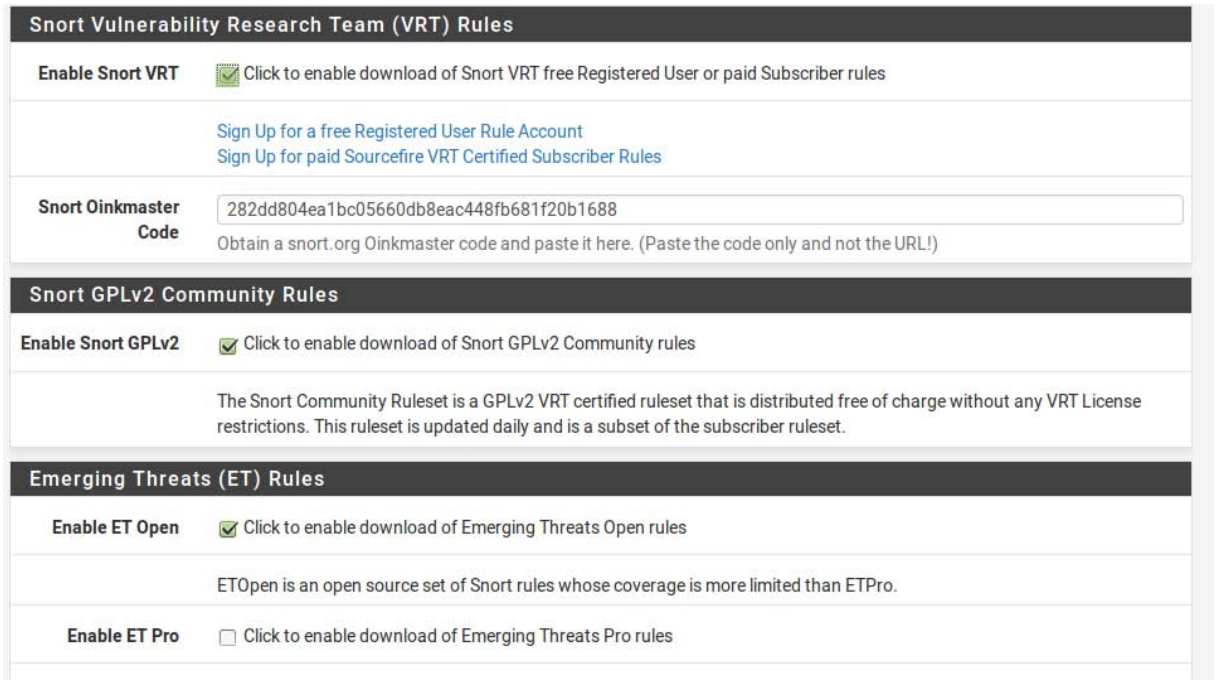
WiFi: Wireless **Fi**delity

Annexe 1 : Configuration des outils de pfsense

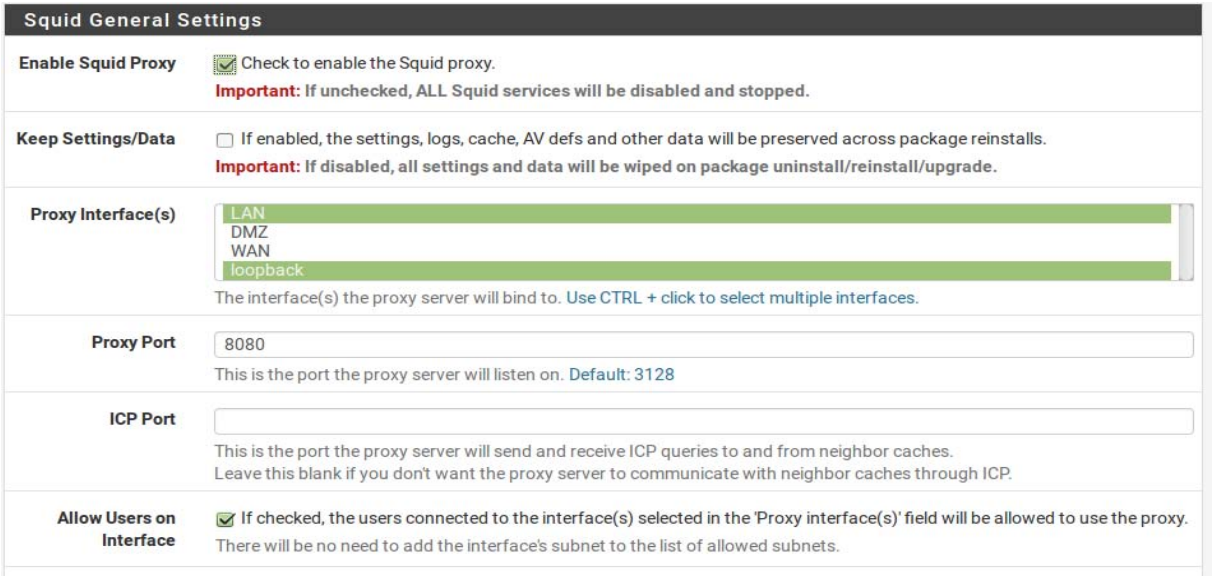
Configuration du serveur FreeRadius



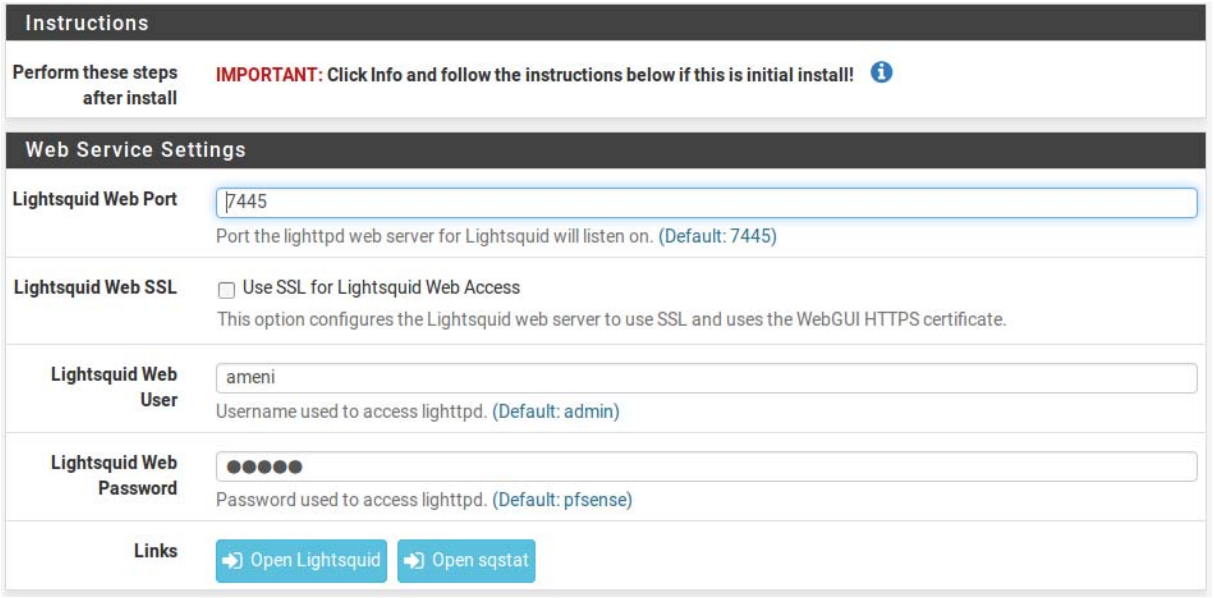
Configuration du Snort



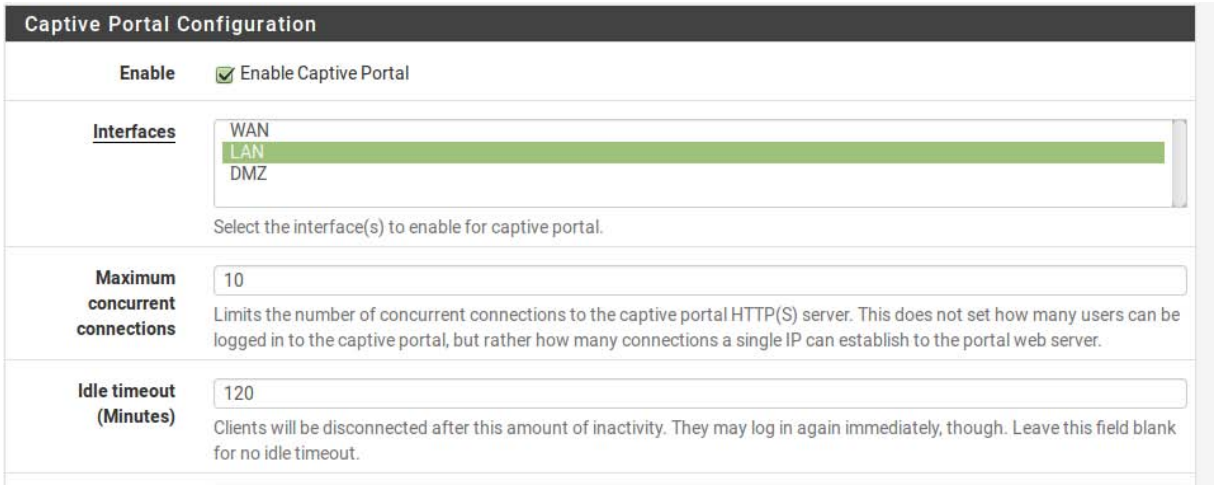
Configuration du squid proxy server



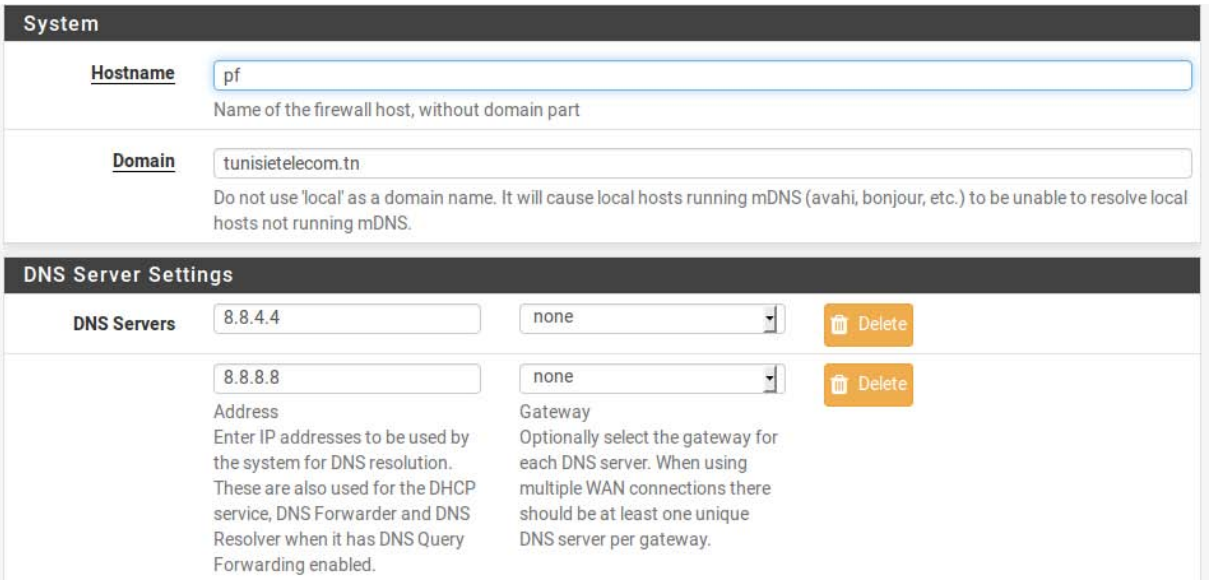
Configuration du Server Reporter



Configuration du portail captif

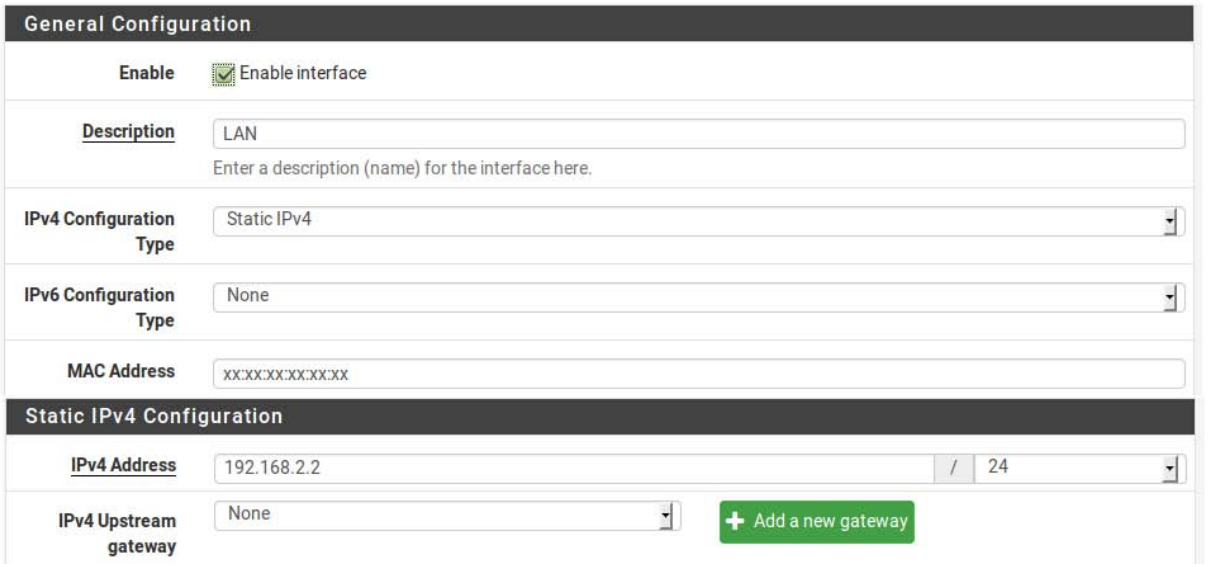


Configuration de Pfsense

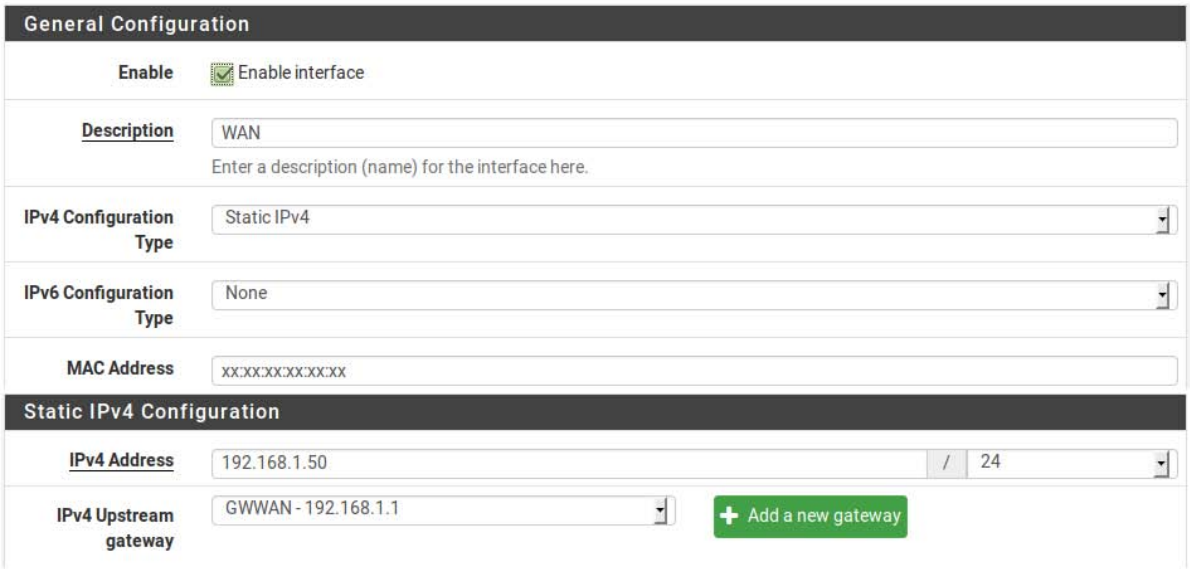


Annexe 2 : Configuration des interfaces réseau

Configuration de LAN

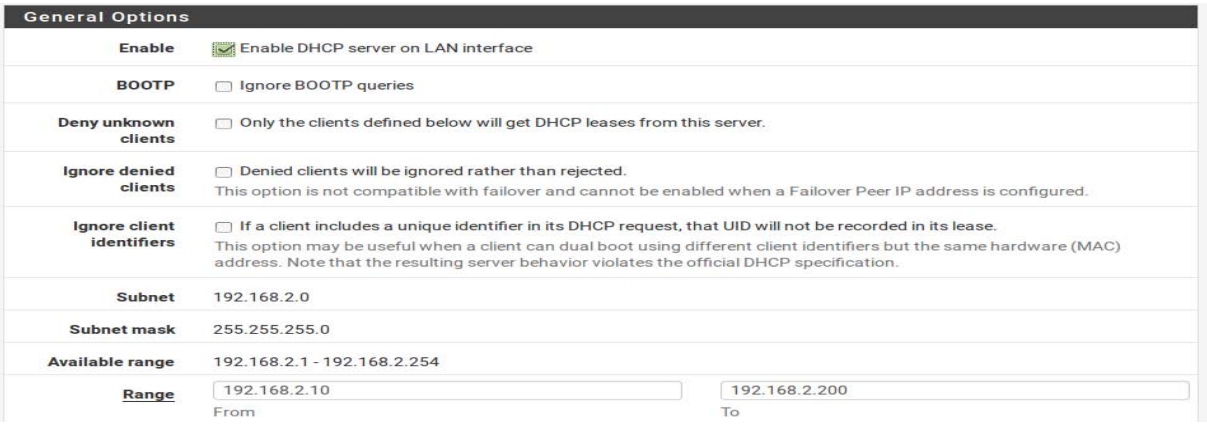


Configuration du WAN



Configuration de DMZ

Activation du serveur DHCP



Filtrage des sites indisérables

Target Categories		
Horaire du travail [Bloquagefacebook]	access	deny
[blk_BL_adv]	access	deny
[blk_BL_aggressive]	access	deny
[blk_BL_alcohol]	access	deny
[blk_BL_anonvpn]	access	----
[blk_BL_automobile_bikes]	access	----
[blk_BL_automobile_boats]	access	----
[blk_BL_automobile_cars]	access	----
[blk_BL_automobile_planes]	access	----
[blk_BL_chat]	access	deny
[blk_BL_costtraps]	access	----
[blk_BL_dating]	access	----
[blk_BL_downloads]	access	----
[blk_BL_drugs]	access	deny
[blk_BL_dynamic]	access	----
[blk_BL_education_schools]	access	----
[blk_BL_finance_banking]	access	----
[blk_BL_finance_insurance]	access	----
[blk_BL_finance_moneylending]	access	----
[blk_BL_finance_other]	access	----
[blk_BL_finance_realestate]	access	----