République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle

En vue d'obtention du diplôme de Master professionnel
Option : Administration et Sécurité des Réseaux

Thème

Amélioration de la sécurité du réseau local. Cas d'étude : Entreprise Portuaire de Béjaïa.

Réalisé par:

M^{lle} AZZI Meriem

M^{lle} MAHINDAD Asma

Président :	*M.*	**OMAR M.**	**Maître Assistant A**	**U. A/Mira Béjaïa.**
Examinateur :	*M.*	**ABBACHE B.**	**Maître Assistant A**	**U. A/Mira Béjaïa.**
Examinatrice :	M^{me}	**BOUTRID S.**	**Maître Assistant A**	**U. A/Mira Béjaïa.**
Promoteur :	*M.*	**BOUKERRAM A.**	**Professeur**	**U. A/Mira Béjaïa.**
Encadreur :	*M.*	**BETACHE I.**	**Directeur du CI**	**EPBéjaïa.**
Encadreur :	*M.*	**MEKHOUKH F.**	**Administrateur Réseaux**	**EPBéjaïa.**

Année universitaire 2015 / 2016

Remerciements

***N**ous rendons grâce à Dieu le tout puissant et miséricordieux de nous avoir donné le courage et la patience de mener à bout ce modeste travail.*

***N**ous tenons à exprimer notre profonde gratitude et nos sincères remerciements à notre tuteur de stage à l'Entreprise Portuaire de Béjaïa M. MEKHOUKH F. pour tout le temps qu'il a consacré, ses directives précieuses, et pour la qualité de son suivi durant toute la période de notre stage.*

***N**ous tenons également à remercier vivement le directeur du centre Informatique de l'EPB, M. BETACHE I. qui a accepté de nous accueillir en stage au sein de son organisation.*

***N**ous voudrions adresser un sincère respect à tout le personnel de l'EPB pour sa gentillesse et son soutien.*

***N**os vifs et profonds remerciements vont à nos encadrants Dr. OMAR Mawloud et Pr. BOUKERRAM A.*

***U**n merci pudique s'adresse aux membres du jury d'avoir accepté d'évaluer notre travail et pour l'intérêt qu'ils y portent.*

***U**n grand merci à nos familles, pour leur soutient permanent, leur patience et leurs encouragements qui nous ont permis de trouver la force et la volonté cachées au plus profond de nous mêmes.*

***N**os remerciements vont enfin à toute personne ayant contribué de près ou de loin à l'élaboration de ce travail.*

Dédicaces

__N__ous dédions ce modeste travail

***À** nos très chers parents qui ont légué un sens à notre existence, pour leur confiance et leur énorme soutien*

***À** nos merveilleux frères et sœurs pour leur présence et leur appui*

***À** nos familles*

***À** nos précieux amis qui ont toujours cru en nous*

Asma et Meriem

Table des Matières

Liste des figures

Liste des tableaux

INTRODUCTION GÉNÉRALE

1 Contexte

Les exigences de la sécurité de l'information au sein des organisations ont conduit à deux changements majeurs au cours des dernières décennies. Avant l'usage généralisé d'équipements informatiques, la sécurité de l'information était assurée par des moyens physiques (classeurs fermés par un cadenas) ou administratifs (examen systématique des candidats au cours de leur recrutement). Avec l'introduction de l'ordinateur, le besoin d'outils automatisés pour protéger fichiers et autres informations stockées est devenu évident.

Le second changement majeur qui affecte la sécurité est l'introduction de systèmes distribués et l'utilisation de réseaux et dispositifs de communication pour transporter des données entre un terminal utilisateur et un ordinateur, et entre ordinateurs. Les mesures de sécurité des réseaux sont nécessaires pour protéger les données durant leur transmission. On parle alors de sécurité des réseaux.

Le développement d'utilisation d'Internet a permis à beaucoup d'entreprises d'ouvrir leurs systèmes d'information à leurs partenaires ou leurs fournisseurs, sur ce, il s'avère donc essentiel de connaître les ressources de l'entreprise à protéger et ainsi maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.

Une des manières d'assurer la sécurité d'un réseau informatique d'une grande entreprise serait de protéger l'accès à Internet. C'est très délicat dès que le réseau est physiquement étendu.

2 Problématique

L'architecture initiale du réseau local de l'entreprise portuaire de Béjaïa était une architecture très simple, plate, où tout le monde se trouve dans le même domaine de diffusion, sur la même plage d'adresse IP. Bien qu'adaptée au début du temps où le nombre des machines n'était pas aussi important, les limites de cette architecture commencent désormais à se faire sentir et il est absolument nécessaire d'y remédier avant qu'elles ne soient atteintes. En termes de performance, cette architecture était loin d'être optimale à cause du nombre très important de broadcast transmis, des plateformes devenues obsolètes avec l'arrivée de nouvelles versions, des nouvelles technologies, par conséquent de nouvelles méthodes d'approches.

Des améliorations ont été apportées et une nouvelle architecture a été mise en place. La mise à niveau des contrôleurs de domaines sous Active Directory Windows Server 2012, l'augmentation de la capacité totale et la réduction des risques de panne ont été quelques-unes. Bien que ces

changements aient amenés des abonnissements, le facteur de sécurité n'a pas été pris en considération et cette seconde architecture présente de potentielles failles au niveau des barrières de sécurité.

La sécurité des réseaux informatiques est un sujet essentiel pour favoriser le développement des échanges dans tous les domaines. Vu l'expansion et l'importance grandissante des réseaux informatiques, lesquels réseaux ont engendré le problème de sécurité des réseaux locaux ; Il s'avère indispensable de renforcer les mesures de sécurité, dans le but de maintenir la confidentialité, l'intégrité et le contrôle d'accès au réseau pour réduire les risques d'attaques.

3 Motivation

Les réseaux ont vu un essor rapide accompagné par la découverte de nouvelles technologies, les entreprises entrevoyant les possibilités offertes par ces nouveaux apports sont amenées à les assimiler très vite, aux divers niveaux de l'architecture d'interconnexion des systèmes ouverts (OSI : Open System Interconnexion), aussi bien au niveau des protocoles que des infrastructures physiques supportant ces réseaux.

L'administration des réseaux informatiques évolue sans cesse et elle s'affirme aujourd'hui comme une activité clé de toute entreprise, en plus d'être constamment en fonction, ces outils d'échange de données et de partage d'information en temps réel doivent être en mesure d'offrir une confidentialité maximale et une sécurité à toute épreuve. L'administrateur d'aujourd'hui doit arriver à déjouer des envahisseurs virtuels qui disposent de nouvelles armes de plus en plus sophistiquées, autre difficulté : l'arrivée de nouveaux employés qui n'ont pas toujours conscience de l'importance à accorder à la sécurité informatique.

En jouant un rôle de tout premier plan dans la gestion, l'échange et la transmission de l'information, l'administration des réseaux informatiques prend une importance capitale pour un nombre croissant d'entreprises, bien au fait des produits et des services offerts dans le domaine et constamment à l'affût des innovations.

4 Objectifs et méthodologie

La recherche sur les technologies réseaux a été très active ces dernières années et de nombreuses approches ont été proposées. L'objectif de ce travail est double, dans un premier temps, nous allons faire une synthèse de l'état de l'art sur les différents outils et techniques d'administration d'un réseau informatique. Par la suite, nous allons tenter d'apporter des solutions aux problèmes et lacunes recensées d'abord sur le plan théorique puis nous passerons à la mise en œuvre de ces solutions en environnement réel. Plusieurs configurations peuvent répondre aux besoins escomptés de l'entreprise et dans ce cas la configuration choisie devrait être celle qui offre les meilleures qualités de services, tout en tenant compte des ressources disponibles, ainsi, nous adoptons la méthodologie suivante :

- Étudier en profondeur l'infrastructure informatique et le réseau actuel de l'EPB en partic-

ulier afin de prendre conscience des lacunes et des problèmes rencontrés lors de l'exécution des tâches journalières et en faire une synthèse.

- Étudier les différentes techniques et outils visant à sécuriser les réseaux informatiques et en faire une synthèse.
- Modéliser l'architecture réseau existante et proposer une architecture meilleure qui répond aux exigences de l'entreprise.
- Mettre en œuvre les solutions proposées pour pouvoir gérer les fonctions suivantes :
  - La politique de sécurité régissant tous les types d'accès au réseau (accès interne, accès à distance, gestion de réseau, détection des intrusions...) ;
  - La surveillance et l'assurance de la fiabilité générale du réseau ;
  - Modernisation des équipements ;
  - Mise à niveau des plateformes obsolètes.

5 Organisation du manuscrit

Dans le premier chapitre, nous nous contentons dans un premier temps de la présentation de l'entreprise portuaire de Béjaïa, de l'organisation humaine ainsi que la place du centre informatique au sein de l'entreprise. Dans un second temps nous passons à l'étude des principaux aspects du réseau local intervenant dans le routage et l'acheminement des flux en provenance des utilisateurs où nous décrivons l'architecture réseau mise en place au départ ainsi que celle proposée récemment et qui devait remplir les lacunes rencontrées auparavant. Les besoins et faiblesses du réseau de l'entreprise, des solutions d'amélioration du réseau en plus d'une nouvelle architecture retenue sont également recensés.

Le second chapitre traite de la partie pratique de notre travail, nous abordons la configuration et la mise en œuvre des solutions proposées pas à pas, en commençant par la mise en place et paramétrage du premier pare-feu pfSense, la configuration de la sécurisation du réseau local et pour finir un deuxième pare-feu pfSense sera mis en place servant comme miroir au premier pare-feu.

Le troisième et dernier chapitre est dédié à la mise en place d'une liaison virtuelle consacrée à l'interconnexion de l'entreprise au site distant par la mise en place d'un tunnel VPN, en exploitant les technologies pfSense grâce à l'Appliance OpenVPN.

1

Étude de l'existant

Introduction

Une sécurité bien comprise passe par la connaissance de l'entreprise, des éléments constituant le réseau informatique de celle-ci, de son périmètre de sécurité en plus de son organisation afin d'en déduire les différents risques et menaces auxquels elle y est exposée. Pour y remédier une nouvelle vision du réseau sera proposée dans le présent chapitre afin de pallier aux problèmes mis en évidence tout en passant par le volet modernisation afin d'aboutir à un réseau qui accompagne la croissance de l'entreprise : un réseau évolutif et sécurisé à forte disponibilité.

1.1 Présentation de l'Entreprise Portuaire de Béjaïa

Le port de Béjaïa joue un rôle très important dans les transactions internationales vu sa place et sa position géographique. Aujourd'hui, il est classé premier port d'Algérie en marchandises générales et troisième port pétrolier. Il est également le premier port du bassin méditerranéen certifié ISO 9001/2000 pour l'ensemble de ses prestations et à avoir ainsi installé un système de management de qualité. Cela constitue une étape dans le processus d'amélioration continue de ses prestations au grand bénéfice de ses clients. L'Entreprise Portuaire a connu d'autres succès depuis, elle est notamment certifiée à la Norme ISO 14001/2004 et au référentiel OHSAS 18001/2007, respectivement pour l'environnement et l'hygiène et sécurité au travail [1].

1.1.1 Missions de l'EPB

La gestion, l'exploitation et le développement du domaine portuaire sont les charges essentielles de l'Entreprise Portuaire de Béjaïa, dans le but de promouvoir les échanges extérieurs du pays. Les missions de l'EPB consiste en [1] :

- Le traitement, dans les meilleures conditions de délais, de coût et de sécurité, l'ensemble des passagers, des marchandises et des navires.
- La gestion et l'exploitation des infrastructures et des superstructures portuaires.
- La manutention et l'aconage des marchandises en transit par le port de Béjaïa.
- Le transit des passagers et leurs véhicules par la gare maritime du port de Béjaïa.
- La mise à disposition d'infrastructures nécessaires aux activités relatives aux hydrocarbures (exportation pétrole et de cabotage national des produits raffinés et gaz de pétrole liquéfié).
- Le pilotage, le remorquage et le lamanage des navires dans les limites de la zone de pilotage dans le port de Béjaïa.

1.1.2 Organisation de l'entreprise

Les différentes structures de l'EPB sont présentées dans l'organigramme ci-dessus :

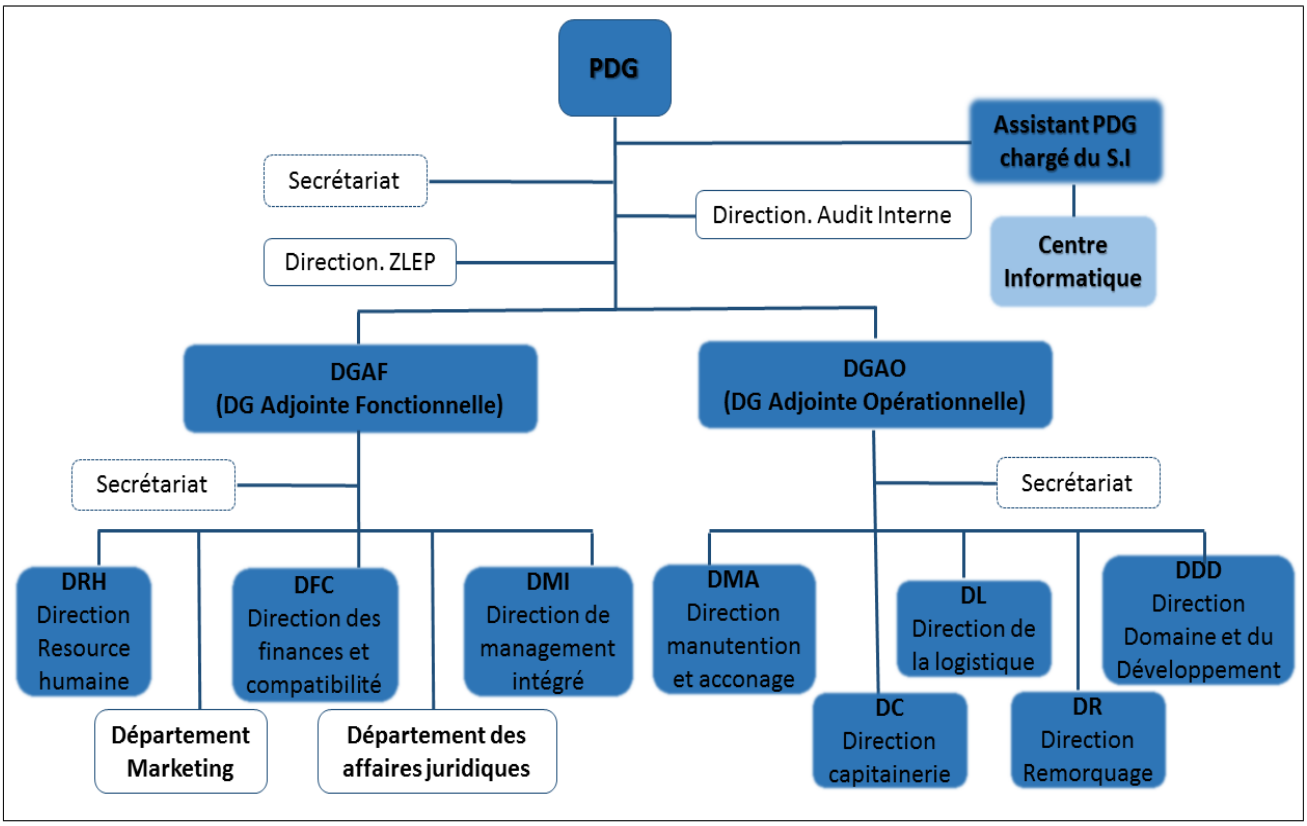

Figure 1.1: Organigramme général de l'EPB.

1.2 Le centre informatique

1.2.1 Présentation du centre informatique

Le centre informatique est une structure de l'EPB rattachée directement à la direction générale, elle a pour mission l'automatisation des métiers de l'Entreprise Portuaire de Béjaïa, et cela en mettant en place les logiciels et l'infrastructure nécessaires pour la gestion du système d'information [1].

L'EPB déploie des systèmes d'informations pour accroitre la productivité, automatiser les processus métiers et fournir un meilleur service aux clients. Ces systèmes intègrent de plus en plus des fonctionnalités réseau pour relier tous les utilisateurs à l'entreprise ou établir des liens avec la clientèle et les fournisseurs. Le réseau local de l'entreprise apporte aujourd'hui une réelle valeur ajoutée en permettant d'intégrer de nouveaux partenaires, fournisseurs et clients.

1.2.2 L'organisation humaine

Le centre informatique se compose de trois départements sous la coupe de l'assistant du PDG chargé du SI, chaque département est structuré en services comme le montre l'organigramme suivant [1] :

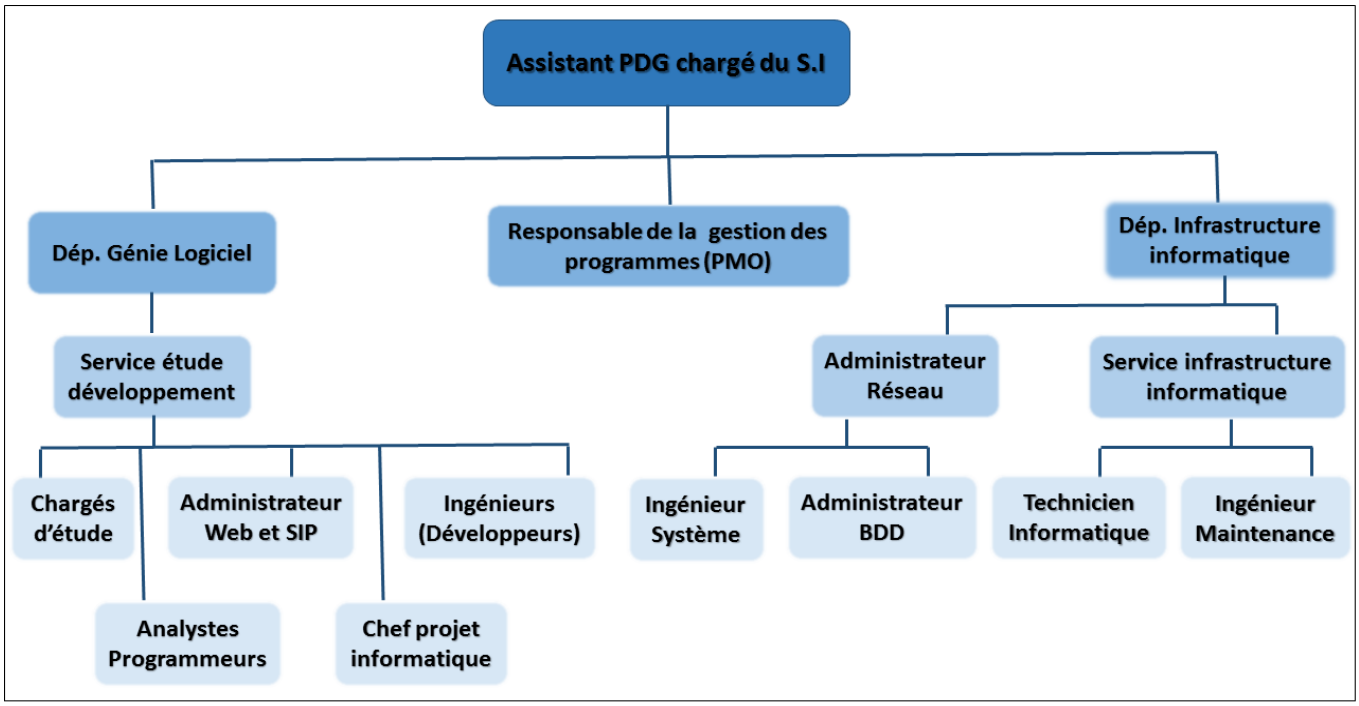

Figure 1.2: Organigramme de la structure informatique.

1.3 Le réseau local de l'EPB

Le réseau local de l'EPB permet aux différents postes de travail de s'échanger des informations, de se connecter vers l'extérieur et d'utiliser les applications hébergées en internes nécessaires à l'exécution des tâches quotidiennes des employées. Le réseau du port de Béjaïa s'étend du port pétrolier (N16) aux ports 13 et 18 (port à bois) [1].

1.3.1 Architecture du réseau local initiale

L'architecture du réseau local initiale de l'EPB est représentée comme suit :

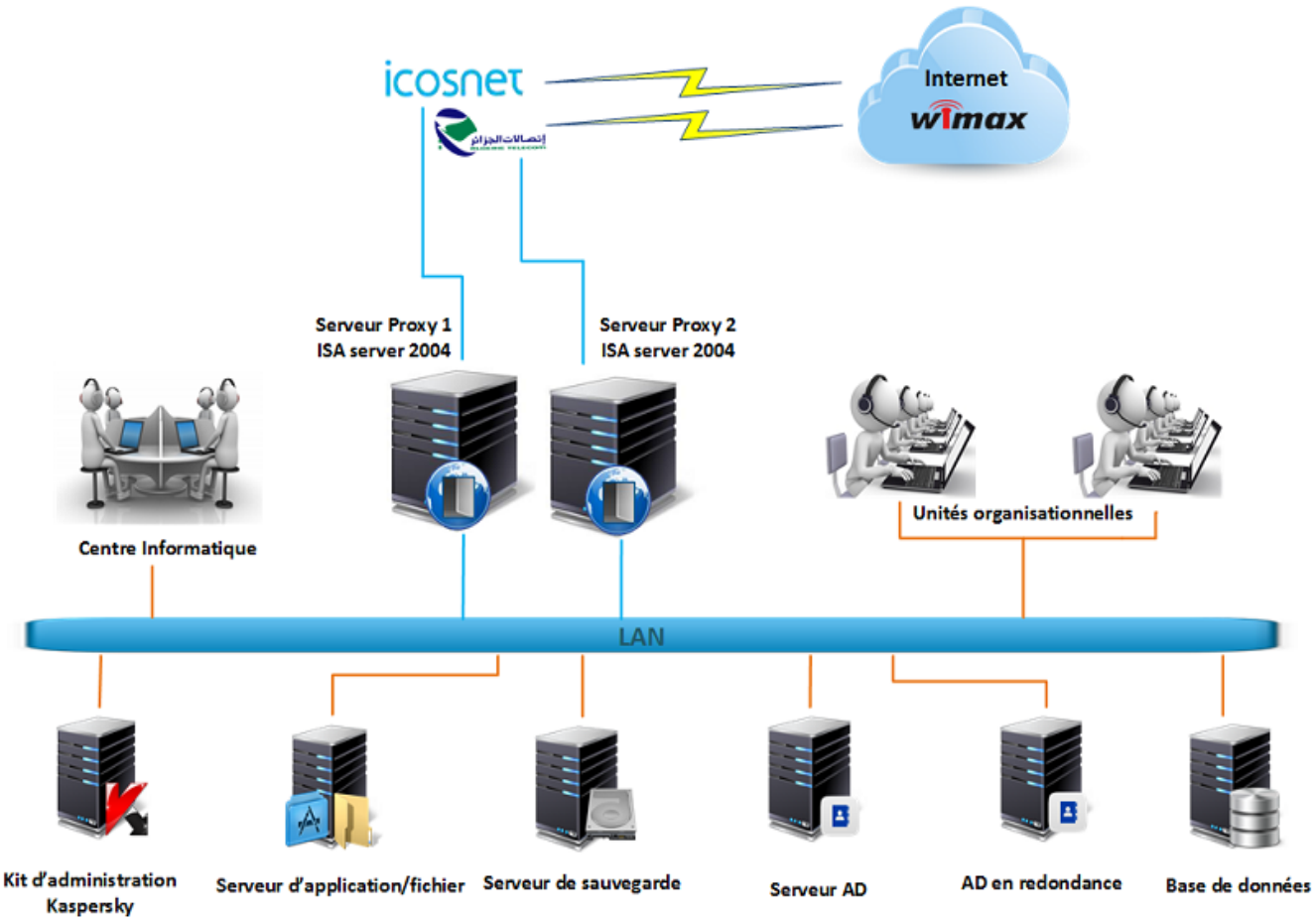

Figure 1.3: Architecture actuelle du réseau local de l'EPB.

L'architecture du réseau de l'entreprise portuaire de Béjaïa est une architecture client/serveur plate. L'armoire de brassage constitue l'essence même du réseau de l'EPB elle contient les équipements réseau permettant aux employés de l'entreprise d'accéder à Internet et de faire de l'Intranet. On y distingue plusieurs switchs et platines où arrivent les câbles qui sont connectés aux différentes armoires de brassage de petite taille placées dans chaque étage du bâtiment, reliées aux prises murales où les employés connectent leurs ordinateurs. Les différents serveurs offrent des services aux différents postes clients.

- **Sécurité** : assurée par deux pare-feu logiciels ISA server 2004 (Internet Security Acceleration server) qui jouent le rôle de proxy définissant les règles d'accès à un réseau comme Internet et interdisant selon une liste noire, les sites considérés comme malveillants et/ou inutiles au contexte de travail de l'entreprise, d'une part et de filtre agissant sur les flux entrants et sortants du réseau afin de permettre d'appliquer une politique d'accès aux ressources réseau de l'entreprise d'autre part.

- **Connexion internet** : l'Entreprise Portuaire de Béjaïa s'est dotée de deux connections Wimax à savoir *Icosnet* et *Algérie Telecom*. Ce type de connexion, permet de se connecter à Internet haut-débit grâce à une antenne Outdoor qui communique par ondes hertziennes via une station de base située au mont Gouraya respectivement, d'une trés grande fiabilité permettant ainsi d'éviter l'usage du câble et le risque d'une panne physique par conséquent.

- **Salle machine** : qui regroupe les ressources nécessaires au bon fonctionnement du LAN de l'entreprise, est considérée comme le cœur du réseau où reposent toutes les activités du port et comporte les switchs et les différentes machines serveurs :

    1. Serveur de base de données (SQL server 2005 et MySQL) : pour le stockage, l'extraction, la gestion et mises à jour des données dans une base de données. Ce serveur offre un accés simultané à la base à plusieurs serveurs Web et utilisateurs.
    2. Serveur de contrôleur de domaine DC1 (sous Active Directory Windows sever2003) : Les contrôleurs de domaine servent à stocker les données de l'annuaire et à gérer les interactions entre l'utilisateur et le domaine, en plus des processus d'ouverture de session, l'authentification et les recherches dans l'annuaire.
    3. Serveur de contrôleur de domaine en redondance (DC2) : permet au service d'annuaire Active Directory de conserver des réplicas des données de l'annuaire sur un autre contrôleur de domaine, et ce afin de garantir la disponibilité et l'efficacité de l'annuaire pour tous les utilisateurs.

4. Serveur Intranet (applications/fichiers) : qui met à disposition des ressources applicatives à distance, sans prendre en considération l'environnement du poste utilisateur : c'est le serveur d'application qui fait tourner les applications qui sont accessibles simplement via un navigateur internet.
5. Serveur de sauvegarde : Le serveur, en collaboration avec la baie de stockage, ont pour rôle de sauvegarder en continu les données générées par l'entreprise. Si un employé efface par erreur un document, ou qu'il y ait un dysfonctionnement d'un ordinateur, le serveur est en mesure de rétablir le fichier perdu.

Il est à noter que l'entreprise s'appuie notamment sur l'utilisation de produits Microsoft sous licence particulièrement pour les systémes d'exploitation. On y retrouve Windows Seven et XP pour les postes clients et Windows server 2003 (mis à niveau en Windows Server 2012) pour les serveurs, elle favorise aussi l'exploitation de logiciels Open source.

1.3.2 Diagnostic du réseau de l'entreprise

1.3.2.1 Infrastructure informatique déclinante

Bien que l'entreprise se soit agrandit et est aménagé dans des locaux plus vastes, développé et diversifié ses services, l'équipement système et réseau initiale déployée depuis quelques années a évolué sans grande concertation et n'a jamais fait l'objet d'une remise en cause globale, l'état des lieux nous a permis de diagnostiquer les faits suivants :

- **Plateformes anachroniques et serveurs obsolètes**
  - Le processeur de ces serveurs est d'une architecture 32 bits, ce qui pose un réel problème pour la mise à niveau vers une nouvelle plateforme car la plus part d'entre elles sont des architectures 64 bits ;
  - Fin du support Windows Server 2003 et mises à jour annoncées le 14 juillet 2015 donc plus de garantie sur le support des applications utilisées sur ces serveurs ;
  - Arrêt des patchs de sécurité : le réseau est exposé aux failles de sécurité (37 mises à jour critiques sur Windows Server 2003 en 2013) ;
  - Des risques potentiellement importants liés à la non-conformité avec les standards et les réglementations ;
  - Explosion des coûts de maintenance de serveurs obsolètes à long-terme.

- **Pare-feu logiciels défaillants : ISA Server 2004**
  - Protection obsolète contre les nouvelles menaces, ceci dit plus de déclenchement des alertes en fonction des configurations, que peut utiliser l'entreprise pour suivre et atténuer les nouvelles attaques.

- Fin du support en juillet 2009 donc ne permet plus de réduire la propagation des virus et la submersion consécutive des connexions qui représentent un enjeu récurrent pour le réseau de l'entreprise, mises à jour et alertes de sécurité.
- Absence de politique de gestion des connexion internet : pas d'équilibrage de charge des liaisons WAN ni de basculement WAN (haute disponibilité).
- Fonctionnalités de filtrage limitées et basiques par rapport à des pare-feu faisant meilleur filtrage.

- **Technologie de stockage dépassée (DAS)**
  - Indépendance de gestion des périphériques de stockages complique l'administration et la gestion du parc.
  - Partage de ressources peut impliquer une charge supplémentaire sur le réseau en place.
  - Opérations de sauvegardes planifiées de façon centralisée engorgent le réseau en accédant aux différents périphériques çà et là.
  - Opérations de sauvegardes faites indépendamment sur chacun des serveurs alourdissent l'administration de l'infrastructure.

1.3.2.2 Mise en évidence des vulnérabilités

Nous prétendons qu'aucun mécanisme ou approche ne peut garantir un réseau inviolable. Le réseau actuel de l'EPB dispose d'un certain nombre de mécanismes de sécurité qui lui permettent de se protéger des attaques et menaces externes, cependant l'étude que nous avons menée, nous a permis de relever certaines vulnérabilités :

- Le réseau se présente sous une architecture plate. Il n'y a pas de segmentation physique ni de cloisonnement du réseau. En cas d'intrusion, l'intrus aura accès à l'ensemble des communications, des stations du réseau, y compris dans les zones les plus sensibles.
- Absence d'outil de supervision systèmes et réseaux : difficulté de la supervision manuelle des systèmes en réseau du nombres consésequent d'équipements à superviser (infrastructure réseau et système conséquente).
- Absence de système de détection et de prévention d'intrusions (IDS/IPS) nuit à la détection rapide des tentatives de compromission et d'éventuelles violations et activités malveillantes.

- Politique de contrôle d'accès est à revoir, les utilisateurs se connectent avec des sessions locales donc ont des droits d'administrateur sur leur machines, augmentant les risques de compromission du SI.
- Absence d'une zone démilitarisée DMZ a comme conséquences le non filtrage réseau entre les différents réseaux ainsi inter connectés et la non sécurisation du serveur web.

1.3.2.3 Mises en évidence des faiblesses

- Surcharge du réseau : absence de segmentation, donc un seul et unique domaine de diffusion ce qui implique une surcharge énorme du réseau ; des machines surchargées mais non sollicitées.
- Gaspillage d'adresses : les adresses sont de classe A avec un masque sous réseau de 8 bits ce qui n'est pas un choix judicieux compte tenu de la structure de l'entreprise.
- Adressage statique : absence de serveur DHCP, une mauvaise gestion et attribution d'adresses IP, ce système qui parait simple présente beaucoup d'inconvénients. La saisie de ces chiffres est une importante source d'erreurs. Le maintien de l'information des attributions d'adresses et des attributions de noms doit être effectué manuellement par l'administrateur du réseau. Très vite la liste des adresses devient lacunaire voir erronée. Le changement de ces paramètres doit, quant à lui, passer par une opération manuelle sur tous les postes du réseau (que ce soit une migration de classe d'adresses IP ou le remplacement du serveur de nom par exemple).
- Les ressources de la salle machine ne sont pas exploitées à leur meilleur niveau, compte tenu de la présence de deux armoires de brassages.

1.4 Description des besoins

1.4.1 Actions de mise à niveau de l'infrastructure informatique

Ce tableau présente les nouveaux besoins de mise à niveau [2] :

Projets d'amélioration	**Observations**
Mise à niveau des contrôleurs de domaines	• Migration vers une nouvelle plateforme Active Directory (systéme et paramétrages réseaux) sur les deux contrôleurs; • Création de nouveaux rôles sur le premier contrôleur; • Création de sessions contrôlables organisées selon les organigrammes des structures de l'entreprise; • Mise en place de régles de contrôle d'accés; • Mise en place de stratégies de groupe; • Gestion des partages; • Paramétrage du deuxiéme contrôleur pour la tolérance aux pannes.
Mise en place d'un nouveau serveur de BDD en redondance	• Systéme et paramétrage réseaux; • Allocation des espaces disque et installation de l'ensemble des BDD de l'entreprise; • Gestion des contrôles d'accés.
Mise à niveau des différents serveurs	• Serveur d'application; • Serveur de fichier; • Serveur de sauvegarde.
Mise à niveau du systéme d'adressage	• Revoir le systéme d'adressage IP du réseau.

Table 1.1: Les actions de mise à niveau de l'infrastructure informatique.

1.4.2 Les nouveaux besoins de l'infrastructure informatique

Le tableau suivant présente les nouveaux besoins de l'infrastructure informatique [2] :

Nouveaux Projet	**Observations**
Mise en place d'un serveur pour la supervision et surveillance du réseau informatique	• Dans l'objectif de renforcer la sécurité du réseau informatique.
Mise en place d'une autorité de certification	• Dans l'objectif de renforcer la sécurité du réseau informatique .
Mise en place de deux pare-feu matériels	• Prévue dans le cahier des charges d'acquisition des équipements informatique, dans l'objectif de renforcer la sécurité du réseau informatique et d'éliminer les serveurs Internet.
Mise en place d'un systéme de détection d'intrusions IDS et de supervision d'intrusions IPS	• Dans l'objectif de renforcer la sécurité du réseau informatique et des données.

Table 1.2: Les nouveaux besoins de l'infrastructure informatique.

1.5 Projets d'amélioration réalisés

1.5.1 Présentation des améliorations

Le diagnostic soulève en particulier des questions relatives à l'architecture du réseau de l'EPB proposée précédemment. L'architecture ci-dessous présente les différentes améliorations apportées résidente dans la consolidation des serveurs avec une solution de virtualisation Vmware Esxi à travers l'acquisition de nouveaux serveurs dernière génération visant :

1. ***La mise à niveau des contrôleurs de domaines sous Active Directory Windows Server 2012 en mettant en place :***
    - Des nouveaux rôles sur le premier contrôleur ;
    - Un paramétrage du deuxième contrôleur pour la tolérance aux pannes ;
    - Des sessions contrôlables organisées selon les organigrammes des structures de l'entreprise ;
    - Un serveur DHCP pour l'adressage dynamique dans le but d'avoir une configuration sure et fiable des paramètres de connexion et d'assurer la réduction des gestions de configuration ;

- Un serveur DNS permettant de faire la relation entre le nom de l'ordinateur et l'adresse IP.

2. ***L'amélioration de la politique de stockage :***
   - Configuration des RAID pour une Meilleure gestion du stockage ;
   - Garantir la disponibilité des données.
3. ***La mise en place d'un serveur redondant pour chaque serveur afin de :***
   - Augmenter la capacité totale ou les performances du système ;
   - Réduire le risque de panne ;
   - Combinaison des deux effets.
4. ***Optimisation des ressources :***
   - Meilleur gestion de l'espace ;
   - Réduction de la consommation d'énergie.
5. ***La facilité de déploiement de nouvelles machines incluant :***
   - L'optimisation de la consommation des ressources matérielles ;
   - La facilité de maintenance et d'accès aux données.
6. ***Les possibilités de test, de retour en arrière lors des configurations grâce aux snapshots visant à :***
   - Ouvrir des méthodes souples et avancées de protection des données pour accélérer leur sauvegarde et leur récupération ;
   - Gardez la consommation d'espace disque au minimum.

1.5.2 Architecture intermédiaire

Les projets d'amélioration effectués ont opté pour l'architecture suivante :

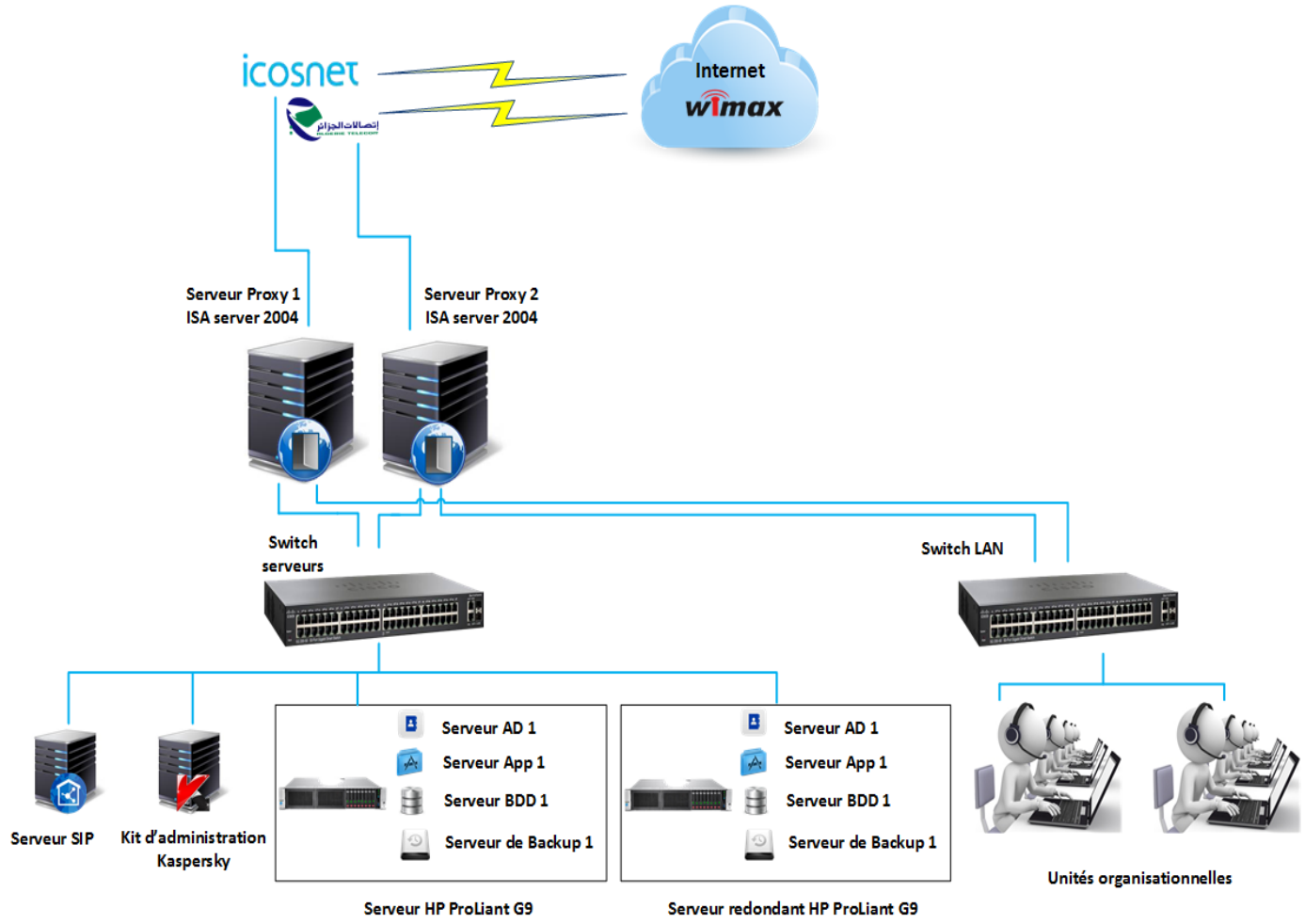

Figure 1.4: Architecture intermédiaire du réseau local de l'EPB.

1.6 Solutions proposées

1.6.1 Renforcement de la sécurité

Comme mentionné précédemment, l'objectif majeur de notre travail est de renforcer la sécurité du réseau informatique de l'Entreprise Portuaire de Béjaïa, tous les mécanismes de sécurité sont centralisés au niveau des pare-feu, donc notre projet consiste en la :

- **Substitution des anciens pare-feu logiciels ISA server 2004 par deux pare-feu Open source *pfSense* :**
  - High Availability (haute disponibilité) : configurer les pare-feu en mode actif-passif pour assurer la continuité en cas de défaillance de l'un d'entre eux ;
  - Loadbalancing (équilibrage de charge) du trafic entrant et sortant pour arriver à des débits stables à chaque extrémité du réseau ;
  - Contrôle parental : limiter l'accés aux sites Web, à la fois définis manuellement dans les listes noire/blanche, mais aussi définis dynamiquement selon le contenu du site, limiter l'accés au web aux utilisateurs désignés et à l'heure définie de la journée ;
  - Contrôle total des flux entrants et sortants ;

- Solution de protection complète et approuvée ;
- Fonctionnalités proxy avancées et optimisation de la bande passante ;
- Meilleure gestion de l'utilisation d'Internet.

En mettant en place ces deux pare-feu logiciels pfSense, on aura une centralisation de la gestion de sécurité qui regroupera les fonctionnaliés suivantes :

- **Système de filtrage d'URL :**
  - Limiter l'accès à certains sites normalement accessibles sur le réseau Internet ;
  - Restrictions d'un accès d'entreprise à un usage professionnel ;
- **Systéme de détection d'intrusions IDS et prévention d'intrusions IPS :**
  - Détection d'activité malveillante : analyser l'activité (trafic) du réseau ainsi que le système afin de détecter les patrons d'attaques enregistrés dans le journal interne ;
  - Anticipation des attaques : empêcher une attaque de débuter et ce en examinant en théorie tous les paquets entrants ou sortants et en visualisant chaque transaction dans le contexte des conversations réseau qui précédent ou qui suivent.
- **Zone démilitarisée DMZ :** consiste en un réseau " tampon " tel que l'ensemble des échanges entre un réseau interne et un réseau externe transite par ce tampon.
  L'objectif recherché est que tous les échanges passent par cette zone et qu'aucun échange direct ne se fasse entre le réseau interne et le réseau externe. Les services de sécurité offerts sont les suivants :
  - Un filtrage réseau entre les différents réseaux ainsi inter connectés ;
  - Des serveurs relais dans la DMZ pour gérer le trafic interne/ externe ;
  - Des antivirus/ analyseurs de contenus pour journalier les échanges et décontaminer les données entrantes ou sortantes conformément à une politique de sécurité ;
  - Des services publics et des serveurs relais permettant de masquer les services et la topologie du réseau interne ;
  - Sécurisation du serveur web.
- **Liaisons sécurisées VPN :** pour répondre au besoin d'interconnexion de l'Entreprise Portuaire de Béjaïa aux différents sites distants, en exploitant pleinement les fonctionnalités des pare-feu *pfSense* qui fournissent des liaisons VPN qui offrant la possibilité de :
  - Créer des tunnels entre l'entreprise et les sites distants permettant ainsi de connecter les ordinateurs sur le même réseau local (virtuel) ;
  - Utiliser des mécanismes de chiffrement et de signature électronique afin que seul le destinataire puisse consulter les données échangées (confidentialité) et que ces données ne puissent être modifiées pendant leur transfert (intégrié) ;
  - Faire que l'accès aux ressources de l'entreprise doir être géré en fonction des droits de chaque utilisateur grâce à la mise en place d'un proxy (Squid/Squidguard sous pfSense).

1.6.2 Nouvelle architecture LAN proposée

Bien que des changements ont été effectués sur la première architecture (Figue 1.3), la seconde (Figue 1.4) demande encore que des améliorations soient apportées afin de s'assurer du caractère complet des barrières de sécurité, et qui n'a pas du tout été pris en concidération lors des amélirations faites dernièrement mais qui sera traité et étudié par nos soins et cela en reliant deux modems diffusant les deux connexions internet à deux pare-feu Open source *pfSense* configurés en actif-passif afin de garantir la haute disponibilité des dispositifs de sécurité et d'assurer une meilleure gestion de l'utilisation d'Internet.

Les pare-feu à leur tour, sont connectés à six autres équipements par des liaisons, ceci dit six interfaces réseau exploitées sur chaque pare-feu :

- Une interface liée à la première connexion WAN (Algérie Telecom) ;
- Une interface liée à la deuxième connexion WAN_1 (Icosnet) ;
- Une troisième interface met en rapport les deux pare-feu l'un à l'autre pour la synchronisation entre les deux, ce qui permet une redondance totale entre eux ;
- Une autre interface relie ces pare-feu avec une zone démilitarisée DMZ (Serveur web, relais SMTP) ;
- La cinqième et avant dernière réuni le premier pare-feu au switch serveurs qui est à son tour lié au serveur SIP, au Kit d'administration *Kaspersky*, au serveur de virtualisation ainsi que son serveur redondant ;
- La dernière liée avec le switch LAN destiné aux unités organisationnelles de l'entreprise.

La connexion aux sites distants grâce au VPN est assurée par la paire pare-feu *pfSense*. Toutes ces fonctionnalités ont pour but de fournir aux employés de l'entreprise les services et ressources nécessaires à l'exécution des tâches quotidiennes, regroupés en unités organisationnelles selon les privilèges.

L'architecture du réseau locale que nous proposons est représentée dans la figure suivante :

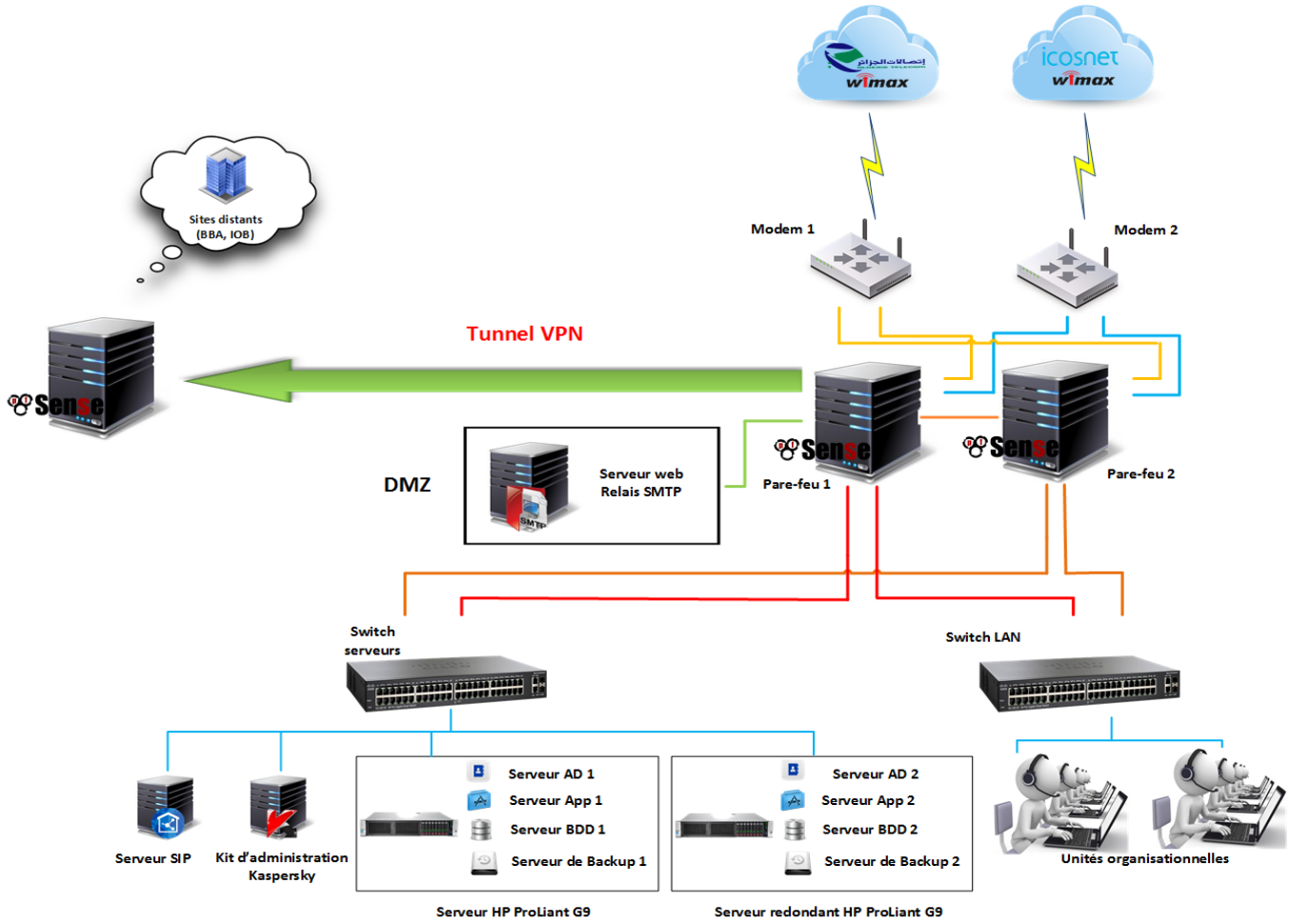

Figure 1.5: Nouvelle architecture du réseau local de l'EPB.

Conclusion

L'étude du réseau de l'entreprise portuaire de Béjaïa a relevé que cette dernière est dotée d'un réseau assez conséquent mais nous a également permit de constater que l'architecture de celui-ci présentait des failles de sécurité. Pour y remédier, nous avons proposé une solution qui consiste à substituer les anciens pare-feu logiciels par deux nouveaux pare-feu Open source pfSense comprenant des fonctionnalités à servir l'entreprise.

Cette solution sera détaillée plus loin, mais auparavant il serait utile de conclure ce chapitre et dire que ces changements au niveau de la sécurité feront preuve sur le réseau l'entreprise.

2

Réalisation et mise en œuvre des solutions

Introduction

Différents problèmes de sécurité sont rencontrés par le réseau de l'entreprise, chacun ayant son contexte propre et ses solutions. Sécuriser un environnement informatique revient à considérer chacun de ces cas. Ces problèmes peuvent être logiciels, matériels ou carrément du piratage.

Après avoir évoqué les caractéristiques principales du réseau local de l'EPB, nous décrivons dans ce chapitre le processus à suivre pour la réalisation des solutions proposées dans le chapitre précédent en passant par la description des différents outils utilisés et qui fournissent une aide précieuse pour effectuer les changements prévus.

2.1 Présentation de pfSense

Les exigences et les besoins requis par l'entreprise nous ont poussé à porter notre choix de pare-feu sur pfSense dans sa version 2.2.6 sortie en 2015. PfSense comporte l'équivalent libre des outils et services utilisés habituellement sur des pare-feu professionnels et convient pour la sécurisation d'un réseau domestique ou de petite voir grande entreprise.

2.1.1 Qu'est-ce que pfSense ?

PfSense, ou " Packet Filter Sense " est un pare-feu / routeur basé sur un système d'exploitation BSD, réputé pour sa stabilité.

PfSense est une distribution Open Source basé sur le système d'exploitation FreeBSD. Il intégre une interface graphique pour la gestion des interfaces WAN, LAN et l'installation de fonctionnalités supplémentaires. Un gestionnaire de paquets est également présent et permet

d'installer de façon élémentaire des modules additionnels afin de profiter d'une expérience encore plus enrichissante. Il est important de comprendre que de cette façon, l'administrateur réseau aura une vision plus juste de l'activité des utilisateurs sur le réseau et pourra mettre en place les solutions adaptées aux besoins de l'entreprise [3].

2.1.2 PfSense en tant que logiciel Open source

Comme toute solution de routeur/pare-feu, pfSense possède son lot d'avantages. Sa polyvalence et le nombre conséquent de fonctionnalités font de cet outil une solution fiable pour les entreprises, et ce, quelles que soient la taille et l'activité de ces dernières. Le coût est un élément à prendre en compte, car comme bien su, les PME[1] pour qui les systèmes d'informations ne sont pas le cœur de métier n'ont pas des budgets importants pour ce genre de solutions. Il existe plusieurs façons de mettre en place pfSense, en passant par une plateforme virtuelle (ESXi par exemple) ou en faisant l'acquisition d'un routeur sur lequel la distribution est déjà installée. Enfin, il est important de souligner que pfSense est très peu gourmand en termes de ressources [3].

2.1.3 Fonctionnalités de pfSense

PfSense est réputé pour fournir de nombreuses fonctionnalités qui ne sont par ailleurs disponibles sur les pare-feu commerciaux coûteux. En outre, avec la sortie des nouvelles versions de pfSense, plusieurs nouvelles fonctionnalités ont été ajoutées au logiciel. Voici quelques caractéristiques qui fournissent des raisons impérieuses de déployer pfSense sur notre réseau [3] :

(1) Équilibrage de la charge : à l'aide de plusieurs composants avec équilibrage de charge, une méthode pour répartir les charges de travail sur plusieurs ordinateurs ou d'autres ressources, peut accroître la fiabilité. Il n'est généralement nécessaire au sein des systèmes grands ou sensibles (par exemple, les sites web populaires, serveurs DNS[2]), et pas tous les produits pare-feu et routeur prennent en charge l'équilibrage de charge. PfSense, cependant, peut être configuré pour équilibrer ou basculer des interfaces WAN. L'équilibrage divise tout le trafic entre les interfaces tandis que basculement utilise une interface unique, mais sur le basculement il commutera automatiquement à l'autre interface.

(2) Basculement : pfSense peut être configuré pour passer à un serveur, système, composant matériel ou réseau à un échec ou à un arrêt anormal de l'application active, serveur, système, composant matériel ou réseau.

(3) Règles personnalisables : tous les pare-feu ont des règles, mais pfSense a des règles hautement personnalisables. Par exemple, une règle peut être mises en place à accepter uniquement le trafic depuis un certain OS (Windows, MacOS et Linux sont pris en charge). En outre, il y a une option de planification, donc les règles seront invoquées seulement durant certaines heures et certains jours.

[1] Petite et Moyenne Entreprise
[2] Domain Name Server : serveur de domaines

(4) VPN : la plupart des pare-feu et routeurs soutiennent les réseaux privés virtuels (VPN), mais peu ont la flexibilité de pfSense. Par exemple, m0n0wall[3] prend en charge les réseaux privés virtuels et a de nombreuses options, mais prend uniquement en charge les protocoles IPSec et PPTP. PfSense, en revanche, prend en charge les protocoles IPSec comme OpenVPN et PPTP, L2TP, et a beaucoup d'options, telles que NAT traversal.

Cette liste de fonctionnalités n'est pas, par tous les moyens exhaustive, ces quelques raisons font de pfSense le plus flexible et le plus puissant des produits concurrents.

2.2 Présentation de FreeBSD

PfSense est un système d'exploitation orienté routeur et pare-feu dérivé de m0n0wall et basé sur FreeBSD " Berkeley Software Distribution ", abrégé en BSD, désigne en informatique une famille de systèmes d'exploitation Unix, développés à l'Université de Californie (Berkeley).

L'objectif du projet FreeBSD est de fournir un système qui puisse servir à tout, avec le moins de restrictions possibles. Il offre des possibilités avancées en termes de réseau, de performance, de sécurité et de compatibilité [4].

2.3 Installation et configuration de pfSense

2.3.1 Au préalable de l'installation

Avant de se lancer dans l'installation, certains éléments du projet doivent être bien préparés, comme la configuration matérielle nécessaire et les services à mettre en œuvre par l'application. La connaissance de l'architecture cible est elle aussi primordiale [5].

2.3.2 Ressources matérielles requises

Afin de mettre en œuvre les deux pare-feu, l'entreprise a dû mettre en place des ressources matérielles qu'elle combine :

- Deux machines de marque (serveurs pare-feu), ayant chacune les particularités suivantes :
  - Processeur : Intel Core i3 minimum ;
  - RAM : de 4 Go ;
  - Disque dur interne (HDD pour Hard Disk Drive) de 500 Go minimum.
- Système de refroidissement performant et fiable : les deux machines seront en marche d'une manière permanente.
- Deux modems : liés chacun à une connexion (Algérie Telecom/Icosnet) et mis en rapport avec les deux pare-feu : chaque modem diffuse grâce à deux liaisons la connexion en sa possession à chacun des pare-feu.

[3]Distribution FreeBSD faisant office de pare-feu.

- 08 interfaces réseau sur chaque serveur pare-feu réparties de la manière suivante :

    1. WAN : première connexion internet Algérie Telecom ;
    2. WAN_1 : deuxième connexion internet Icosnet ;
    3. LAN_USERS : connexion au réseau interne ;
    4. DMZ : interface dédiée à la zone démilitarisée ;
    5. PfSYNC : liaison de synchronisation entre les deux pare-feu ;
    6. SRV : connexion au switch des serveurs ;
    7. OPT1 : interface optionnelle 1 additionnelle (de secours) ;
    8. OPT2 : interface optionnelle 2 additionnelle (de secours).

Il est à noter que pfSense n'est pas gourmand en ressources ce qui est d'ailleurs l'un de ses nombreux avantages, cependant il est préférable de ne pas lésiner sur les ressources afin de pallier à toute mauvaise surprise en termes de performances.

2.3.3 Installation de pfSense

Afin d'installer ce pare-feu, il se trouve nécessaire de passer par quelques étapes. Au début de l'installation la fenêtre qui suit s'affiche à l'écran.

Figure 2.1: Début de l'installation.

2.3.4 Noyau du système d'exploitation

Un noyau de système d'exploitation (abrégé noyau, ou kernel en anglais), est la partie fondamentale de certains systèmes d'exploitation également pfSense. Il gère les ressources de l'ordinateur et permet aux différents composants - matériels et logiciels - de communiquer entre eux [6].

La version du noyau fournie avec la verison 2.2.6 de pfsense est la 4.1.

2.3.4.1 Chargement du noyau

Le Quick / Easy Install est une option, comme son nom l'indique, à la fois rapide et facile. La méthode sera démontrée ci-dessous. Les étapes sont numérotées de 1 à 7.

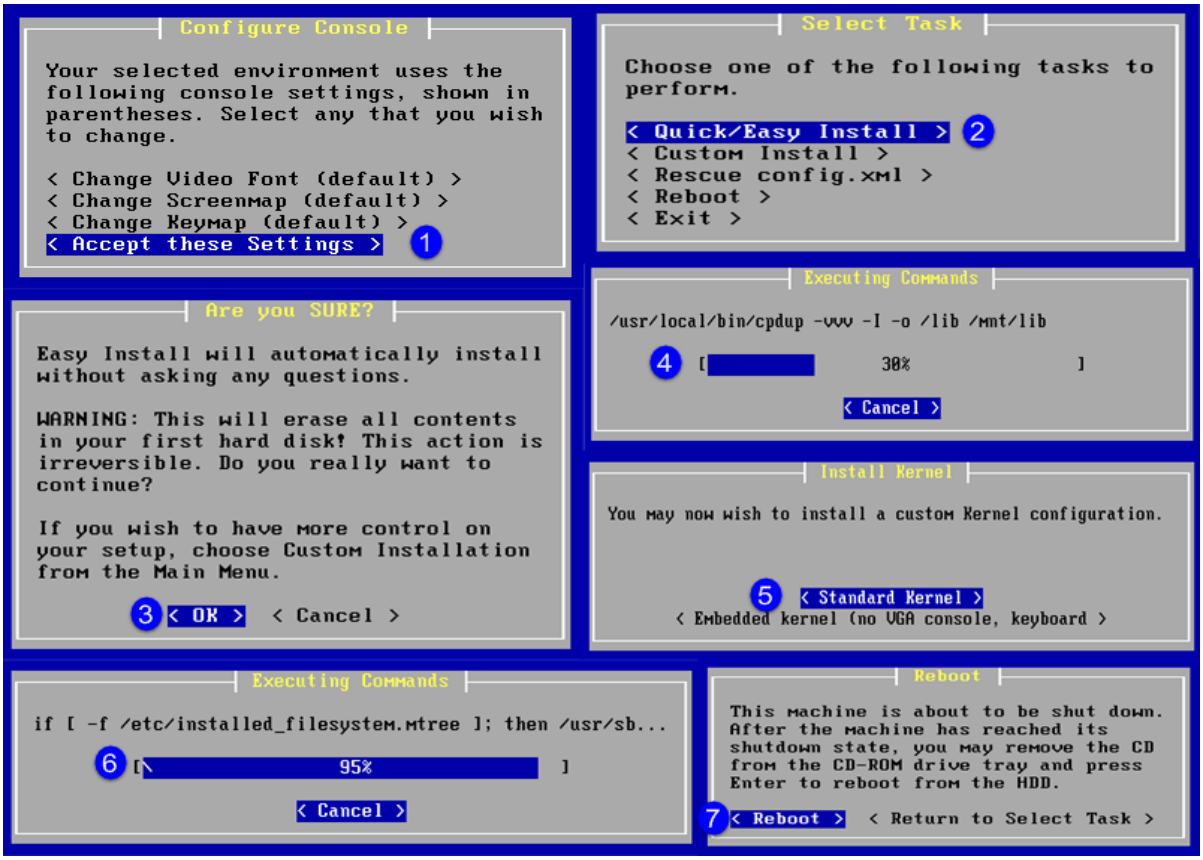

Figure 2.2: Installation du noyau.

Ensuite vient la configuration des interfaces réseau et choisir quelle interface sera le LAN, WAN et WAN_1 à la question " enter the LAN interface name or "a" for auto-detection: ", dans notre cas bge0 sera la WAN (Algèrie Telecom), bge3 la LAN (réseau local de l'entreprise) bge1 la WAN_1 (Icosnet) et les interfaces bge2, bge4 et bge5 feront objet des cartes réseaux qui seront assignées au reste des interfaces ultérieurement. Des adresses IP statiques seront affectées à chacune des interfaces.

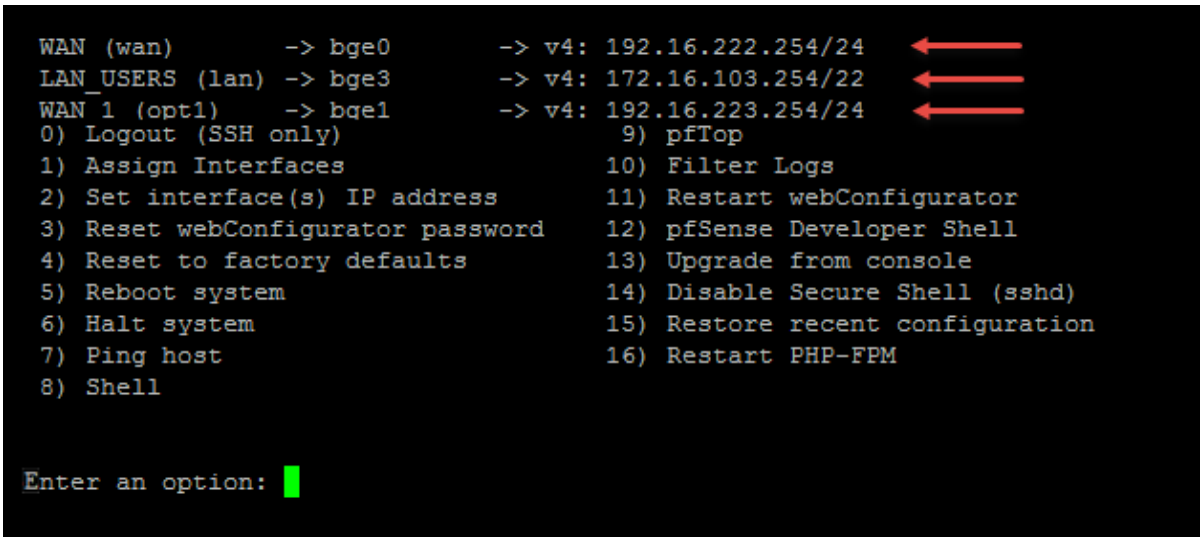

Figure 2.3: Configuration des interfaces.

Il se trouve capital de signaler que pfSense est configuré et géré à partir d'une interface web **WebGUI** ou encore **webConfigurator**.

En introduisant **l'adresse WEB** du serveur LAN dans le navigateur WEB : **https://172.16.103.254**, la page de connexion à l'administration du serveur s'affiche.

Saisir les identifiants par défaut :
- Username : **admin**
- Password : **pfsense**

Figure 2.4: Page de connexion à l'administration du serveur.

2.3.5 Configuration basique de pfSense

À ce stade, nous devons configurer les informations générales notre serveur. Il nous suffit ensuite de spécifier le nom du pare-feu, le domaine ainsi que les adresses du serveur DNS primaire et secondaire (internes).

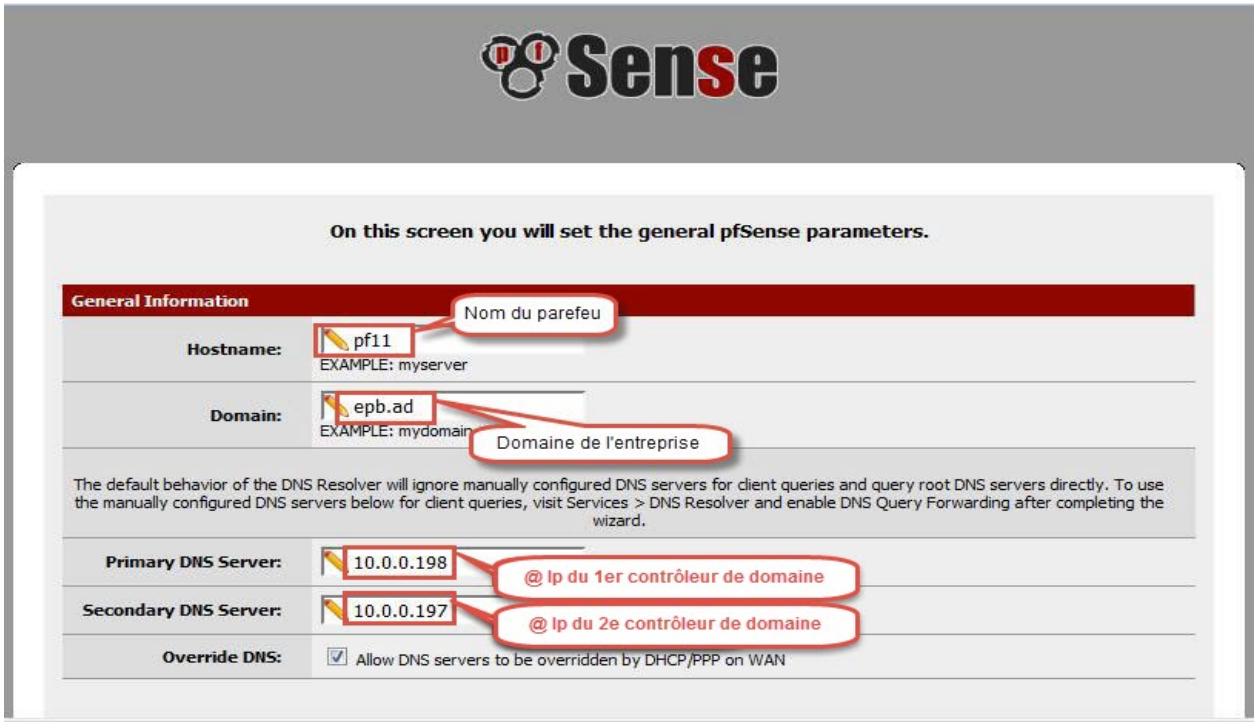

Figure 2.5: Configuration de pfSense.

2.4 Passerelles (Gateway)

Une gateway (passerelle) est un système par lequel pfSense peut accéder à Internet ou à un autre rèseau, donc si plusieurs WANs sont en cours d'utilisation, ou il existe plusieurs chemins d'accès à l'Internet via diffèrentes passerelles, les passerelles associées doivent être définies. Les gateway doivent également être définies pour les réseaux accessibles via des routes statiques [7].

Lors de la création d'une passerelle nous remplissons les champs d'informations nécessaires telles que le nom et l'adresse de la passerelle en spécifiant l'interface à laquelle elle est associée ainsi que l'adresse IP du serveur DNS externe (dans ce cas 8.8.8.8 qui est l'adresse du serveur DNS de google).

Dans le cas démontré ci-dessous, la passerelle créée est considérée comme la principale et donc doit être configurée comme passerelle par défaut.

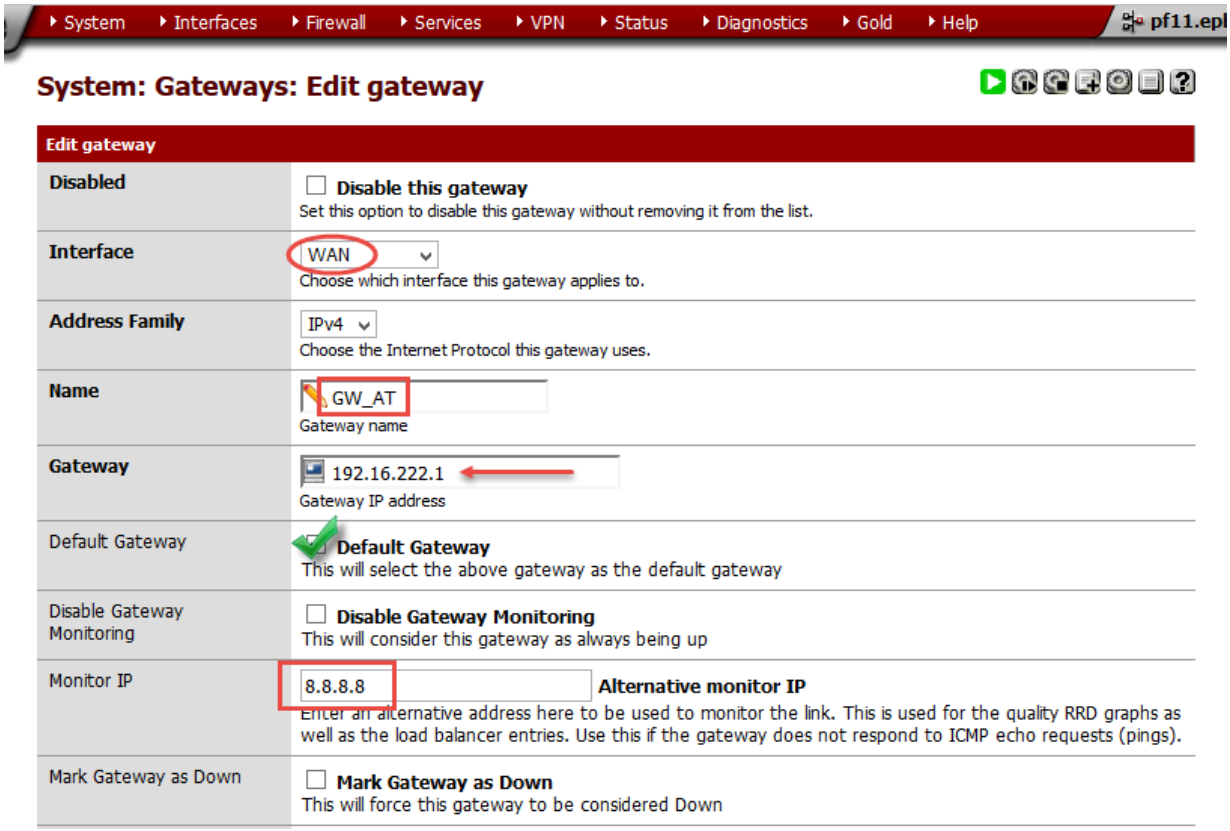

Figure 2.6: Création d'une passerelle.

À l'achèvement de la création de ces passerelles, nous pouvons voir la liste de celles-ci.

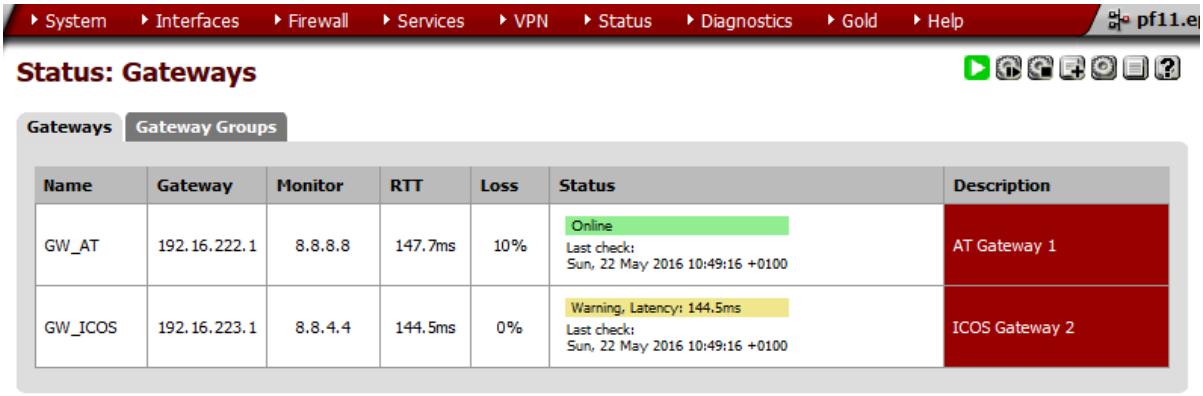

Figure 2.7: Liste des passerelles.

2.4.1 Groupes de passerelles (Gateway groups)

Les groupes de passerelles sont un ensemble de passerelles qui sont traités comme une seule entité dans les domaines de la WebGUI de la passerelle [8].

Lors de la création d'un groupe de passerelle, un nom de groupe et une sélection de niveau de priorité sont requis pour chaque passerelle.

2.4.1.1 Basculement (Failover)

Lorsque deux passerelles sont sur différents niveaux, la (les) passerelle(s) de palier inférieur sont favorisées. Si une passerelle de niveau inférieur baisse, elle est défavorisée de l'utilisation et la passerelle du niveau le plus élevé suivant est utilisée [9].

Lors de la création d'un groupe de passerelle on nomme à volonté notre groupe d'abord, par la suite on détermine le niveau de chaque passerelle.

Dans le cas qui suit on peut voir que la passerelle du réseau d'Algérie Telecom (alimentée d'un débit de 5 MO) est placée au niveau inférieur (tier 2) et donc prend le relais dans le cas où la passerelle du réseau d'Icosnet (alimentée d'un débit de 2 MO) placée à son tour au niveau supérieur (tier1) rencontre un problème de panne.

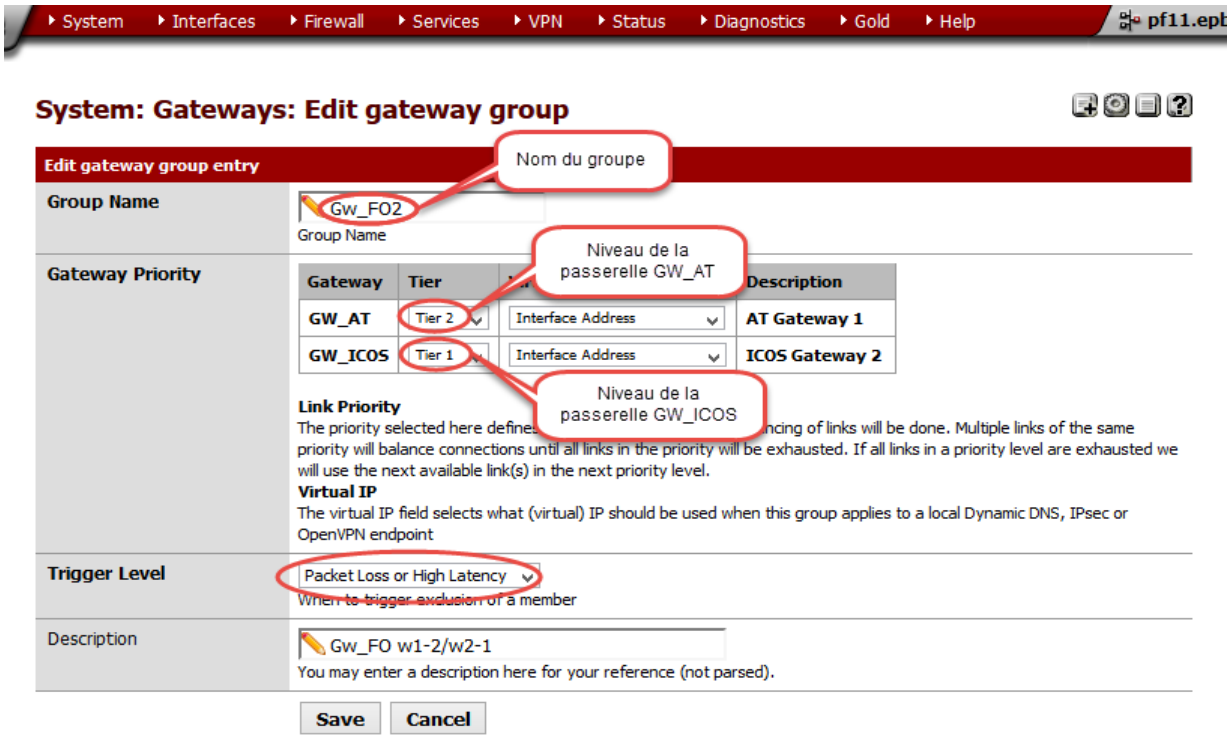

Figure 2.8: Création d'un groupe de passerelles en cas de basculement.

L'option " niveau de déclenchement ou **Trigger Level** " permet de déterminer à quel niveau doit se déclencher le groupe concerné, *Packet Loss or High Latency* pour notre part c'est-à-dire que le groupe de passerelle *GW_FO2* (pareil pour le reste des groupes) se déclenche dans les deux cas :

- Perte de paquets
- Temps de latence considérable (retard).

2.4.1.2 Équilibrage de charge (Load Balancing)

Lorsque deux passerelles sont sur le même niveau, elles peuvent équilibrer la charge. Cela signifie que sur une base par connexion, les connexions sont acheminées sur chaque WAN d'une manière ronde. Si une passerelle sur le même niveau baisse, elle est retirée de l'utilisation et les autres passerelles sur le niveau continuent à fonctionner normalement [9].

Le gateway group créé dans la figure suivante et nommé *GW_LB* s'agit de celui de l'équilibrage de charge. La passerelle du réseau d'Algérie Telecom est au même niveau que celle d'Icosnet (Tier 1), ce qui en résulte un équilibrage de charge entre les deux passerelles au cas de perte de paquet ou latence élevée.

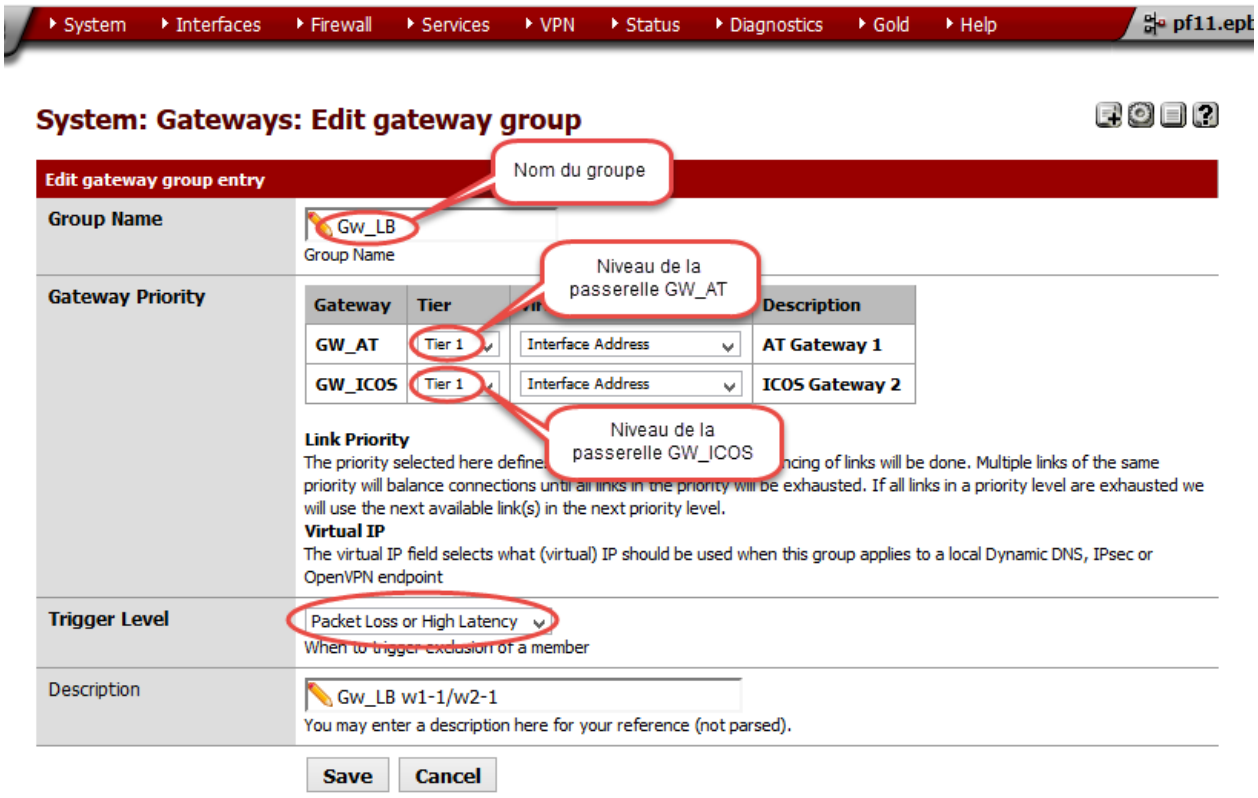

Figure 2.9: Création d'un groupe de passerelles en cas d'équilibrage de charge.

À la fin de la création de ces groupes de passerelles, la liste de ces derniers apparait dans le menu **System** > **Gateway** > **Gateway Groups**.

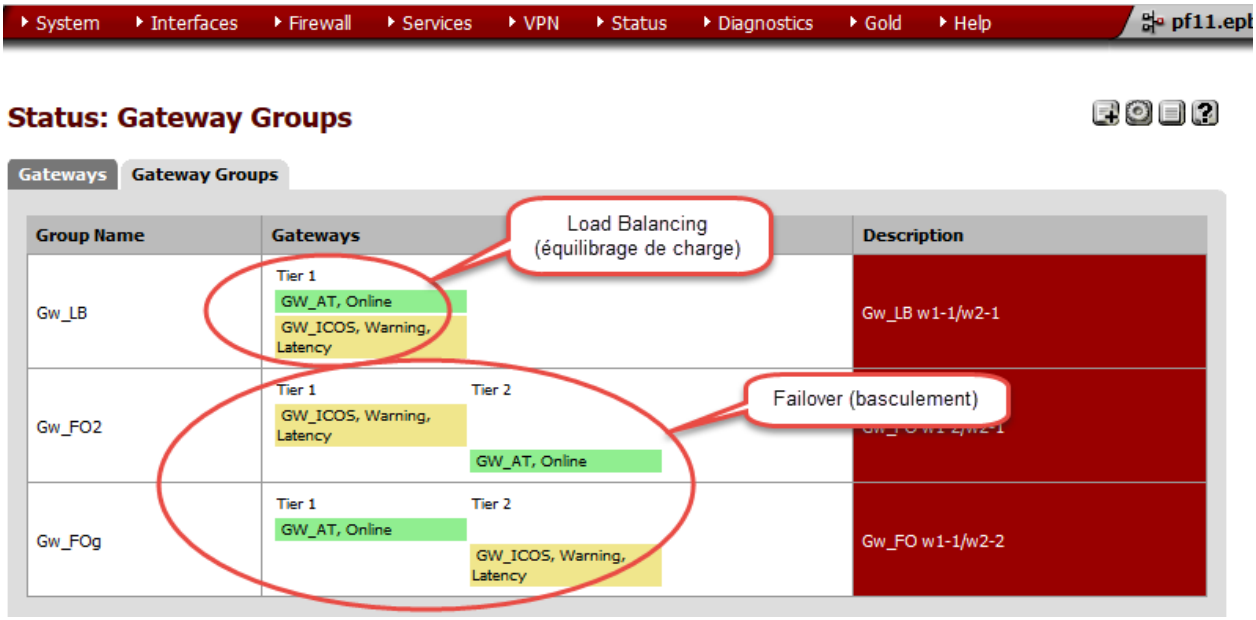

Figure 2.10: Liste des groupes de passerelles.

2.5 Les règles de pare-feu

Les règles de pare-feu contrôlent quel trafic est autorisé à entrer dans une interface sur le pare-feu. Une fois que le trafic est transmis sur l'interface il inscrit une entrée dans la table d'état. Une entrée de table d'état permet la traversée des paquets suivants qui font partie de cette connexion.

Les règles de pare-feu sur le trafic Interface-Groupe procèdent dans le sens entrant et sont traitées de haut en bas, arrêtant au premier correspondant. En l'absence de règles de pare-feu configurées par l'utilisateur, le trafic est refusé.

Les règles sur l'interface LAN permettant le trafic du sous-réseau LAN vers toute destination. Seul ce qui est explicitement autorisé par les règles de pare-feu sera transmis [10].

2.5.1 Création d'une règle

Ces règles de pare-feu sont gérées à partir de **Firewall** > **Rules**. Plusieurs règles peuvent être sélectionnées pour certaines actions.

La règle créée ci-dessous permet aux utilisateurs ayant les adresses IP appartenant à l'alias nommé *Fw_U0810* d'accéder à internet uniquement durant la période de 8h à 10h par le biais de la passerelle du réseau d'Icosnet *GW_ICOS*.

On comprend rapidement par là qu'il faut d'abord créer les alias ainsi que les calendriers horaires (schedules).

2.5.1.1 Alias

Les alias agissent comme des espaces réservés pour les hôtes réels, les réseaux ou les ports. Ils peuvent être utilisés pour minimiser le nombre de changements qui doivent être faits si un hôte, un réseau ou un port change. Le nom d'un alias peut être entré à la place de l'adresse du réseau IP ou du port dans tous les domaines qui ont un fond rouge. L'alias sera résolu conformément à la liste (sur la page Alias du WebGUI) [11].

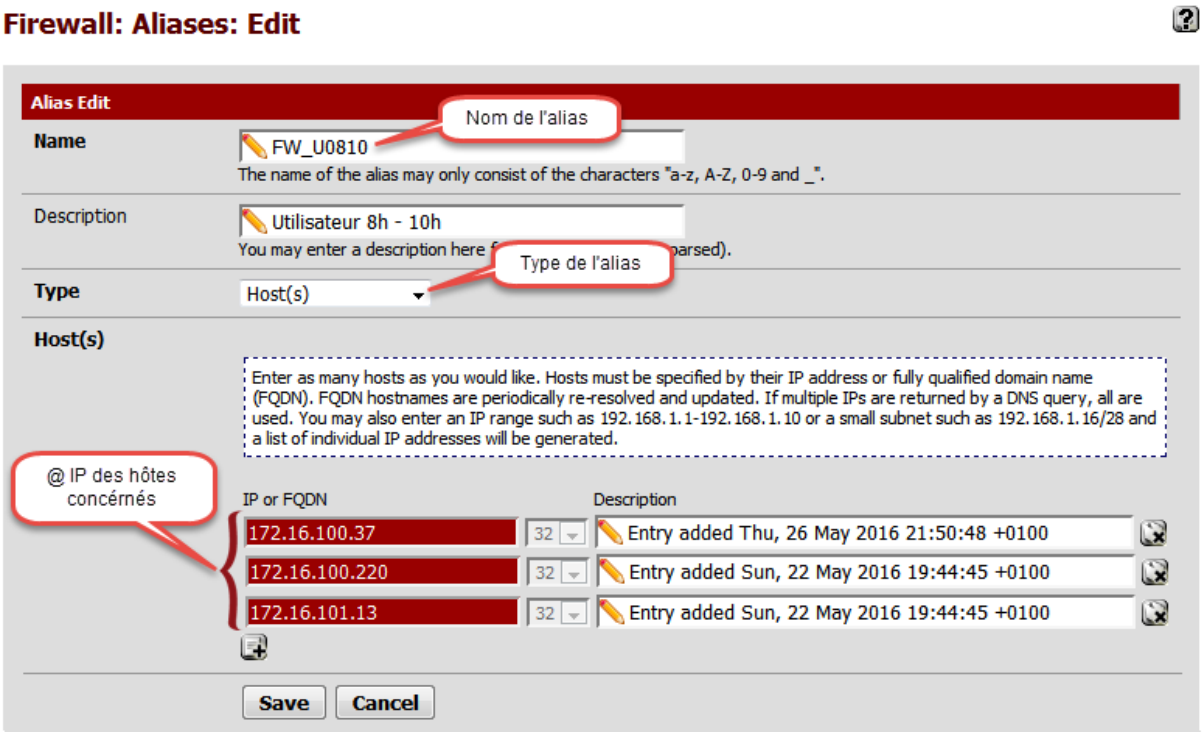

Figure 2.11: Création d'un alias.

2.5.1.2 Calendriers horaires (schedules)

Les règles de pare-feu peuvent être programmées de sorte qu'ils ne sont actifs qu'à certains moments de la journée ou certains jours ou des jours de semaine spécifiques.

Les règles planifiées vont agir comme si elles n'existent pas lorsque le temps programmé n'est pas actif [12].

Avant qu'un calendrier ne soit appliqué à une règle , il doit être créé en vertu du **Firewall > Schedules**. Puis, lors de la création d'une règle, l'utilisateur peut choisir le calendrier défini dans la liste.

Dans le cas du schedule créé ci-après *Fw_ s0810*, l'accès à internet est permit pendant la période de 8h à 10h du matin et ce durant tout le mois de mai.

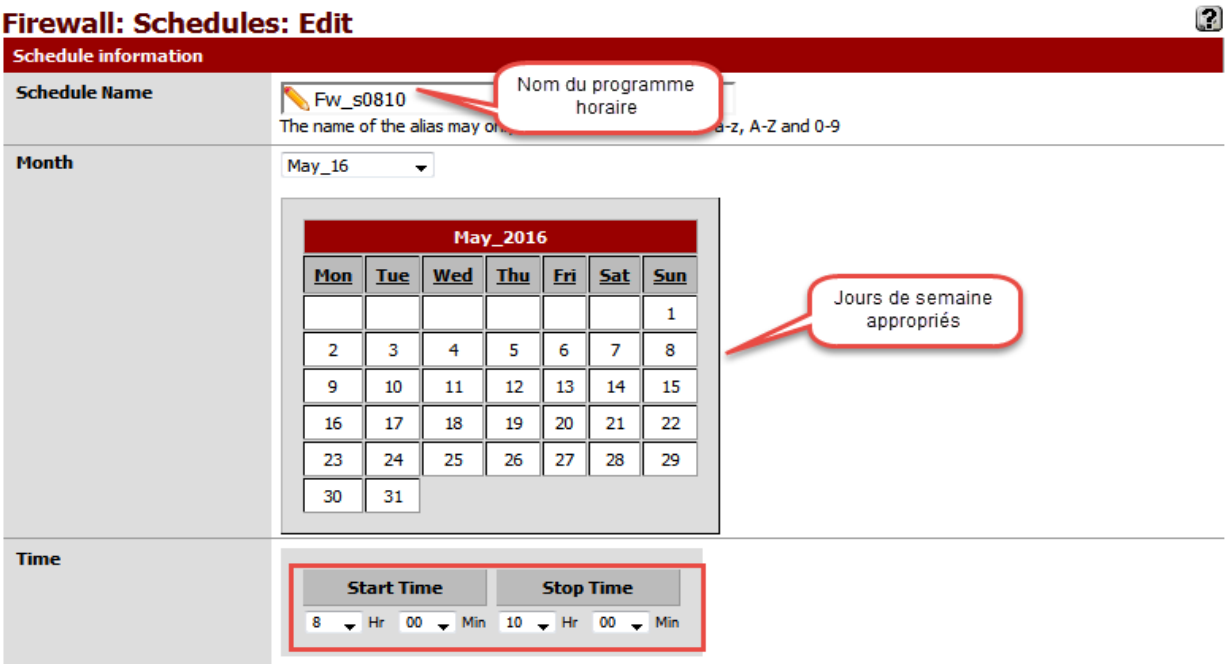

Figure 2.12: Création d'un calendrier horaire (schedule).

Maintenant nous pouvons commencer à créer les règles de pare-feu de chaque interface. Nous avons désigné l'interface LAN_USERS pour démontrer ces étapes.

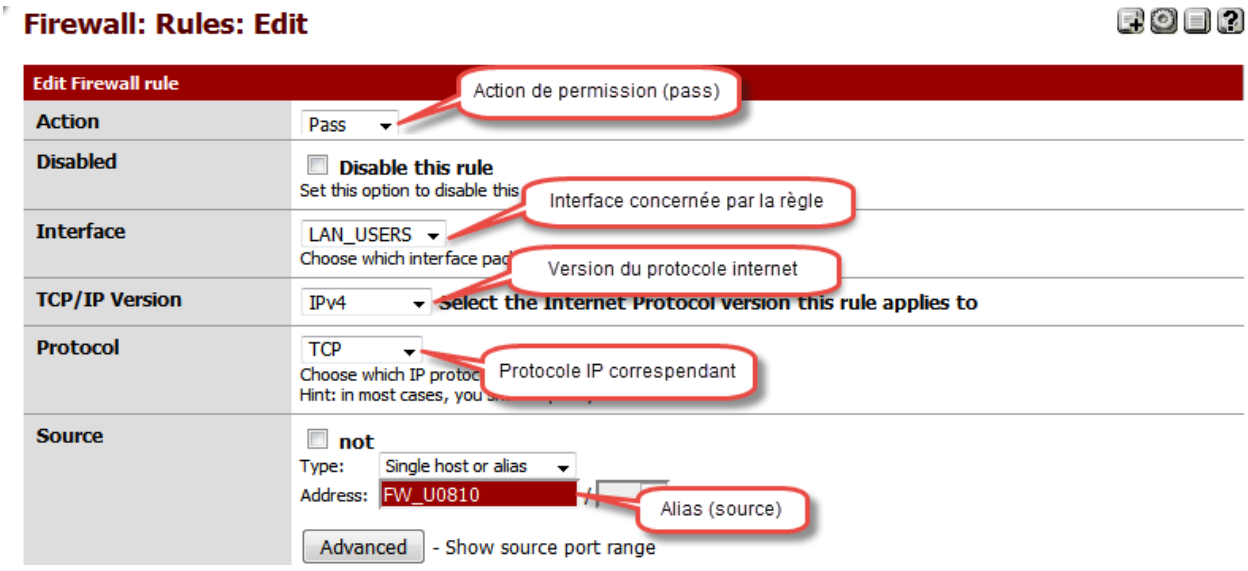

Figure 2.13: Création d'une règle.

Et c'est au niveau des fonctionnalités avancées que nous pouvons spécifier le *schedule* (calendrier horaire) dans lequel s'applique la règle créée ainsi que la passerelle dédiée.

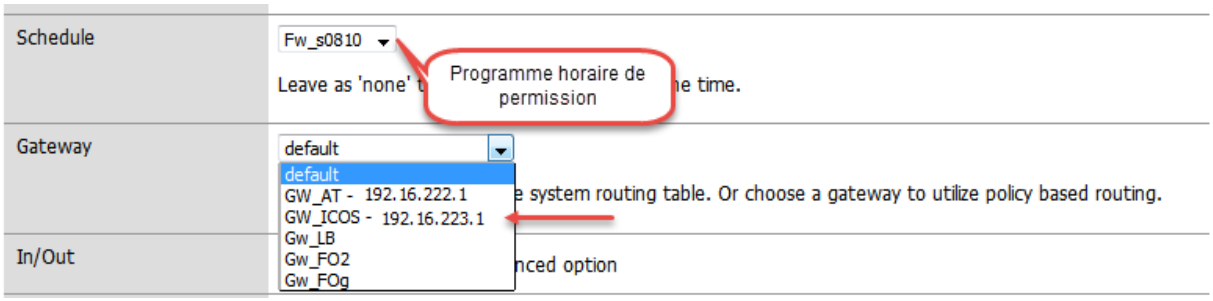

Figure 2.14: Suite de la création de la règle.

Les quelques règles crées au niveau l'interface LAN_USERS :

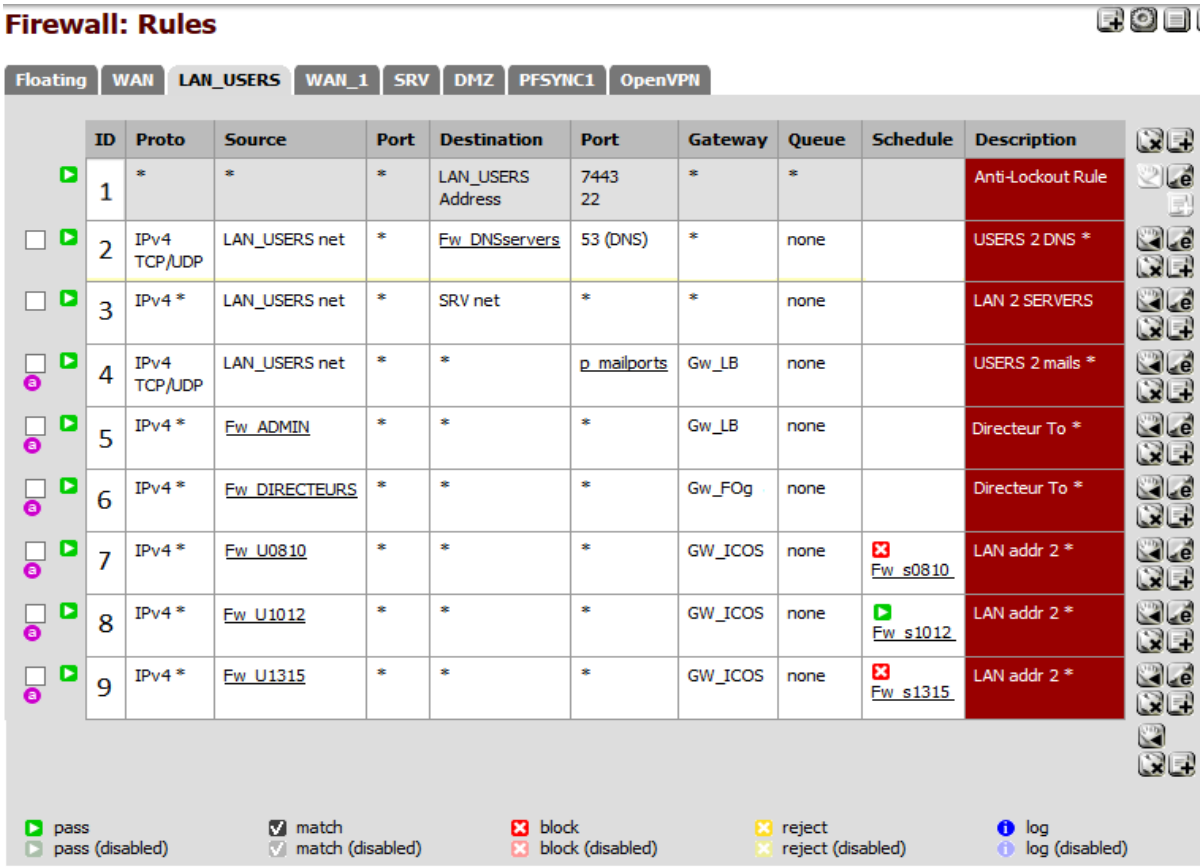

Figure 2.15: Liste des règles de pare-feu.

Le tableau qui suit décrit en bref les règles de pare-feu créées au niveau de l'interface *LAN_ USERS*. Cette liste de règles représente une partie des règles créées.

ID règle	Description
1	Autorise l'accès à tous les utilisateurs vers le réseau interne LAN par les ports HTTPS (7443) et SSH (22) et ce quelque soit le protocole, la source, le port source/destination et la passerelle.
2	Autorise aux utilisateurs du réseau local l'accès aux serveurs DNS par le port 53 en utilisant le protocole TCP/UDP.
3	Permet aux utilisateurs du LAN par le biais de tous les ports en se servant de tout protocole d'accéder aux réseau des serveurs et en utilisant toute passerelle.
4	Autorise l'accès aux utilisateurs du réseau interne par les ports figurant dans l'alias *p_ mailsports* en se servant du groupe de passerelle *Gw_ LB*.
5	Les administrateurs ont la possiblité d'accéder à toute destination et sans réstriction par la passerelle offrant l'équilibrage de charge *Gw_ LB*
6	Les directeurs ont le privilège d'accéder par n'importe quel port et vers n'importe quelle destination à tout moment et ce par le biais du basculement (failover *Gw_ FOg*).
De 7 à 9	Détermine aux utilisateurs ayant les adresses IP inscrites dans les alias de source d'accéder à internet à des périodes précises dans le schedule et par la passerelle du réseau Icosnet seulement.

Table 2.1: Règles de pare-feu créées au niveau de l'interface *LAN_ USERS*.

2.6 Le filtrage d'URL

2.6.1 Présentation d'un proxy

Le serveur Proxy (appelé aussi serveur mandataire) est un serveur recevant des requêtes qui ne lui sont pas destinées et qui les transmet aux autres serveurs. Quand il reçoit une requête, le serveur proxy stocke le résultat. Si la même requête lui est à nouveau envoyée, il vérifie que le résultat n'a pas été modifié et renvoie le résultat qu'il a " déjà à la main " à celui qui a effectué la requête (fonctionnant aussi comme un cache), c'est la mise en cache des URLs[4] et des objets résultants du surf. Le but est d'améliorer (point de vue vitesse) le surf.

La plupart des proxy permettant également de faire du filtrage de contenu (blacklist[5]), c'est-à-dire d'autoriser ou d'interdire l'accès à certains sites qui peuvent contenir des informations non désirées pour certains publics[13].

[4]Uniform Resource Locator
[5]Liste noire

2.6.1.1 Exemple sans proxy

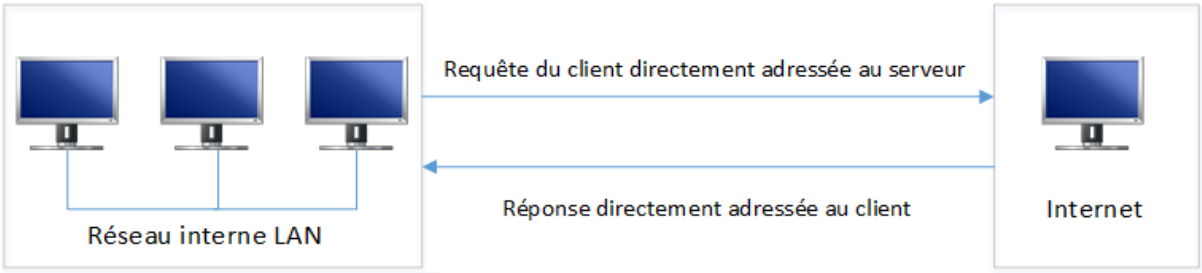

Figure 2.16: Exemple de réseau en l'absence d'un proxy.

2.6.1.2 Exemple avec proxy

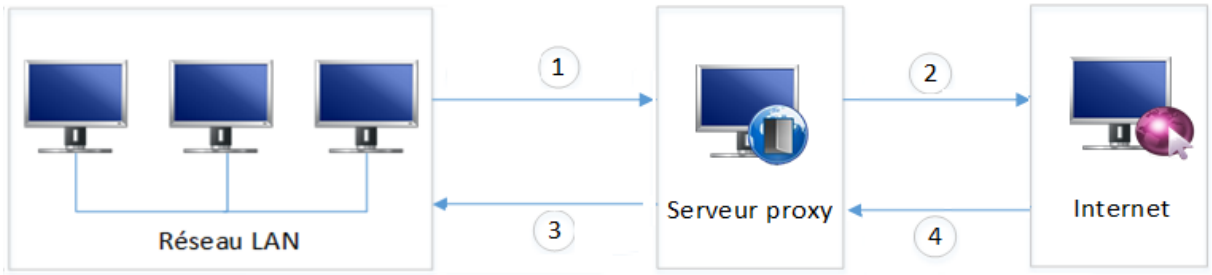

Figure 2.17: Exemple de réseau en l'existence d'un proxy.

1. Un client lance une requête vers internet. C'est le serveur proxy qui l'intercepte et la traite ;
2. **Si** le serveur proxy ne peut pas répondre à la demande du client alors il redirige la requête vers internet **Sinon** aller à 4 ;
3. Le résultat de la requête est retourné vers le serveur proxy qui le stocke dans son cache ;
4. Le serveur proxy retourne la réponse à la requête au client.

2.6.2 Présentation de Squid

Squid est un proxy de mise en cache pour le Web supportant HTTP, HTTPS, FTP, et plus encore. Il optimise le flux de données entre le client et le serveur pour améliorer les performances et les caches fréquemment utilisés pour économiser la bande passante et améliore les temps de réponse par la mise en cache et la réutilisation des pages Web fréquemment demandés. Squid dispose de vastes contrôles d'accès et fait un grand accélérateur de serveur. Il fonctionne sur la plupart des systèmes d'exploitation disponibles, y compris Windows [15].

2.6.2.1 Installation de Squid et de SquidGuard

Pour pouvoir utiliser les fonctionnalités du proxy, il faut ajouter les packages " Squid " et " Squidguard " puis configurer les " **blacklists** ", les différentes restrictions et éventuellement des règles d'accès supplémentaires (ACL), la figure suivante montre le téléchargement et l'installation des packages Squid et Squidguard :

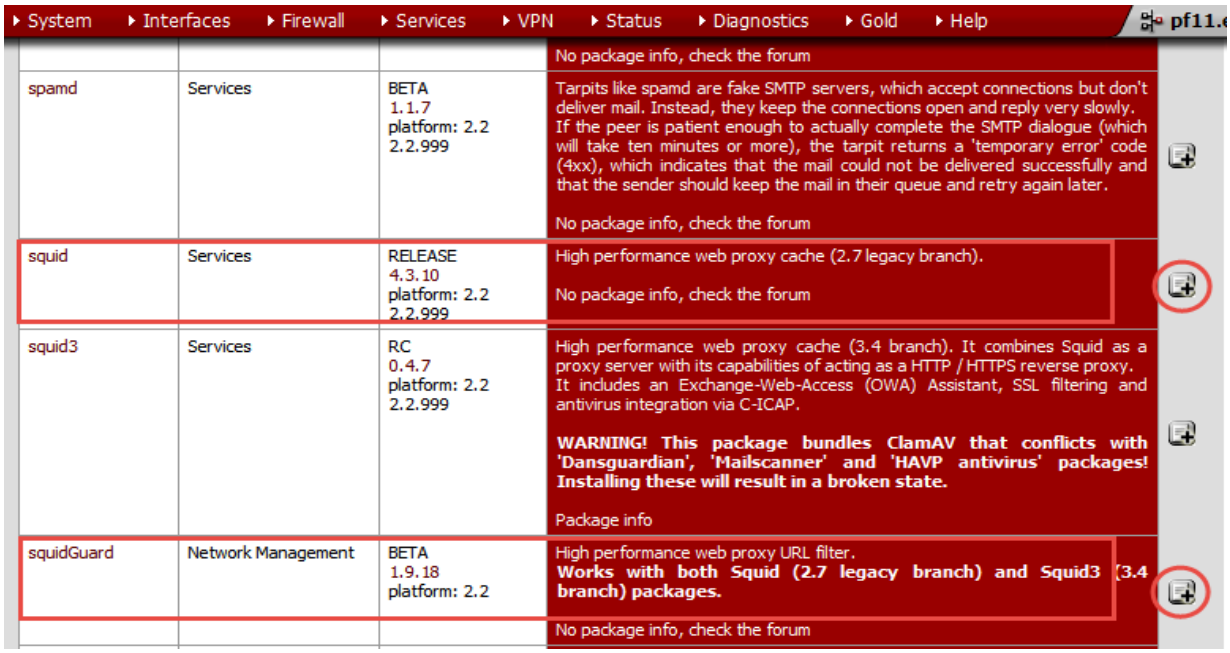

Figure 2.18: Téléchargement et installation de Squid et Squidguard.

2.6.3 Configuration de Squid

Par défaut Squid est configuré et fonctionnel. Cependant, on peut apporter quelques modifications afin de l'optimiser ou mieux l'adapter à certains environnements. Les figures suivantes illustrent les modifications apportées au proxy squid dans notre cas :

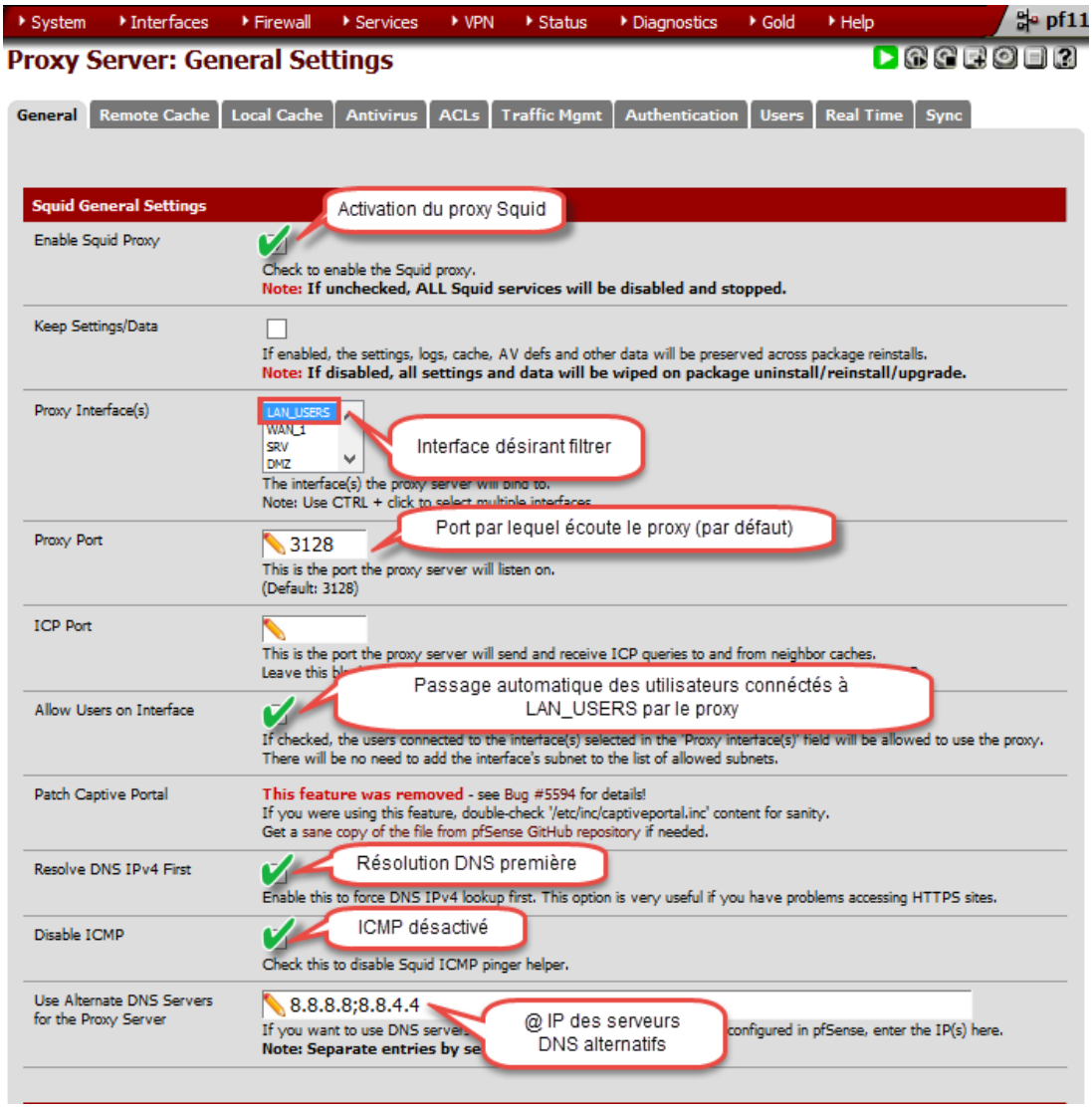

Figure 2.19: Configuration générale de squid.

Les figures qui suivent montrent les configurations effectuées pour rendre le proxy le plus transparent possible, c'est à dire que lorsqu'un client effectue une requête il croit qu'elle a été directement transmise au serveur hors que le proxy l'ait interceptée, analysée puis requêtée vers le serveur, ce dernier répond au proxy qui à son tour achemine la réponse au client.

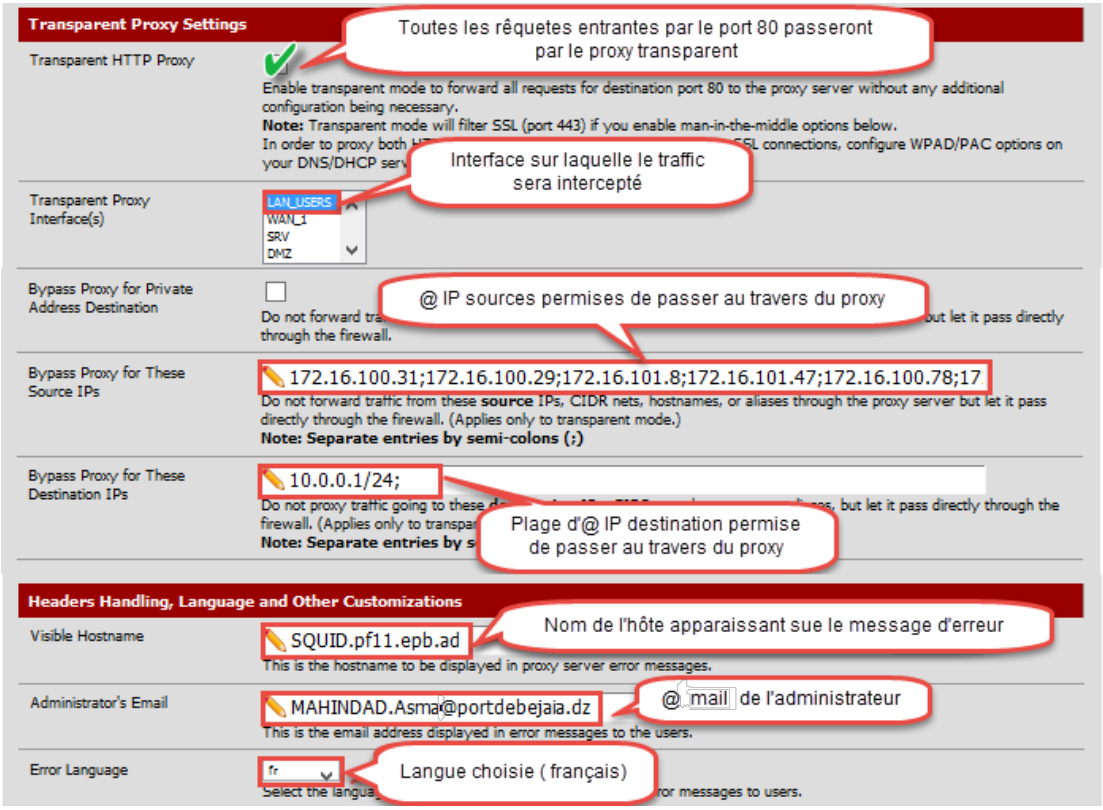

Figure 2.20: Configuration du serveur proxy transparent.

L'attribution de 2 Go de RAM et 5 Go de disque dur au proxy devrait suffire pour couvrir tous les postes du réseau de l'EPB.

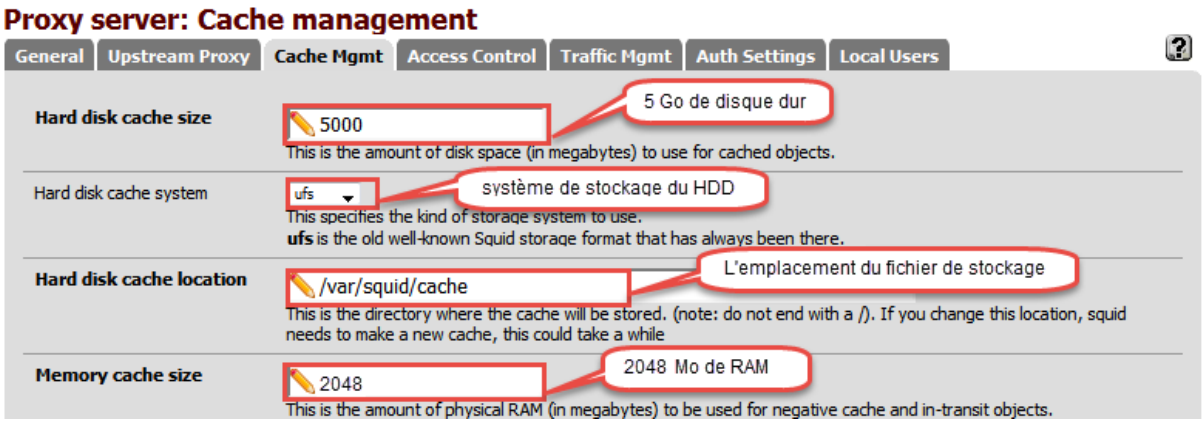

Figure 2.21: Configuration de squid (suite).

Une autre étape importante est de spécifier la plage d'adresses autorisée à passer par le proxy dans notre cas, c'est celle du LAN de l'entreprise qui est: 172.16.100.254/22.

Figure 2.22: Plage d'adresses passant par le proxy.

2.6.4 Présentation de SquidGuard

Squidguard est un redirecteur d'URL et contrôleur d'accès collaborant avec le proxy logiciel Squid. Il a deux grands avantages: rapide et libre [16].

2.6.4.1 Principe de fonctionnement de SquidGuard

SquidGuard peut être utilisé pour [16] :

- Limiter l'accès à internet, à une liste de serveurs acceptés, serveurs web bien connus et/ou aux URL seulement pour certains utilisateurs.
- Bloquer l'accès à certains serveurs et/ou des URL Web sur la liste noire pour certains utilisateurs.
- Bloquer l'accès aux URL correspondant à une liste d'expressions régulières ou des mots pour certains utilisateurs.
- Imposer l'utilisation de noms de domaine/interdire l'utilisation de l'adresse IP dans les URL.
- Rediriger les URL bloqués à une page d'information " intelligente ".
- Rediriger l'utilisateur non enregistré à un formulaire d'inscription.
- Rediriger les téléchargements populaires à des copies locales.
- Avoir des règles d'accès basées sur l'heure du jour, jour de la semaine, date, etc.
- Avoir des règles différentes pour les différents groupes d'utilisateurs.

2.6.4.2 Configuration de SquidGuard

1. **Configuration du système de filtrage d'URL :**

   Cette configuration dépend essentiellement de " l'alimentation " en listes noires d'URL ou de noms de domaines. L'URL de la blacklist prédéfinie est renseigner sur internet, afin de la télécharger et créer les catégories de cette liste.

   La blacklist utilsée est **shallalist**, cette liste est une collection de listes d'url regroupées en catégories à l'intention de l'usage au filtrage d'url, elle regroupe plus d'1.7 millions d'urls, ce qui offre un vaste choix de filtrage.

Figure 2.23: Téléchargement de la blacklist.

À l'issue de ce téléchargement et de la décompression du fichier d'archive, le répertoire blacklist contient les répertoires qui correspondent aux différentes " catégories " de listes noires. Le choix entre les différentes catégories se fait selon nos besoins. L'exemple ci-dessous a visé la catégorie des réseaux sociaux:

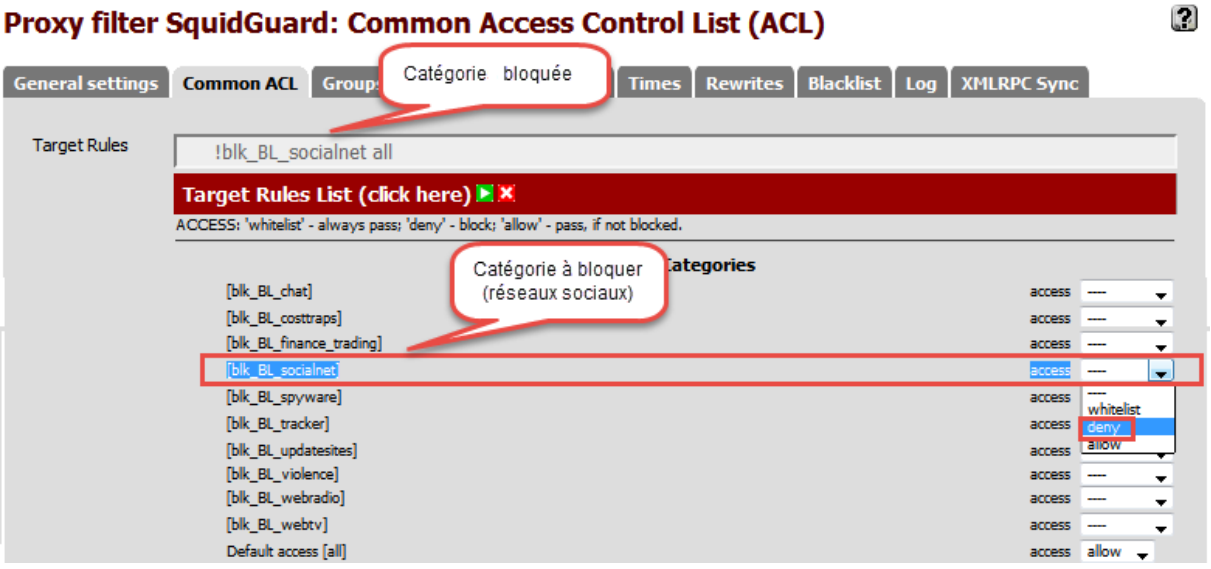

Figure 2.24: Blocage de la catégorie des réseaux sociaux.

Il est à noter que la catégorie “ Réseaux sociaux ” n'est pas la seule catégorie bloquée dans notre cas, tout ce qui n'est pas en relation directe avec le domaine de travail a été bloqué.

2. **Création des catégories de filtrage :**

   Il est possible que la blacklist ne permette pas de bloquer un domaine ou un site que l'on souhaite interdire, il faut alors le bloquer par nous même via une nouvelle catégorie. Il est aussi possible d'autoriser un domaine qui est déjà bloqué dans une des catégories de la blacklist. Cela en manipulant l'onglet **Target Categories** qui a pour but d'ajouter une blacklist ou une whitelist personnelle.

Les droits d'accès dans l'EPB différe d'un utilisateur à un autre. Le tableau suivant montre quelques groupes d'utilisateurs de l'EPB et leurs droits d'accès :

Identifiant du groupe	**Priviléges**
SG_ADMIN, SG_DIRECTEURS	Aucune règle de filtrage n'est appliquée, ont accès à tout sans restriction.
SG_Users_PERM	Ont accès à tout sauf les réseaux sociaux, les téléchargements et les podcasts.
SG_IT	A accès à tout sauf les réseaux sociaux.

Table 2.2: Utilisateurs et leurs droits d'accès.

Dans le cas ci-dessous nous prenons un exemple de filtrage URL plus avancé, en effet dans certains cas les blacklists peuvent présenter certaines limites quant au filtrages URL comme **facebook** par exemple, pour y remédier nous allons personnaliser le filtrage en créant nos propres règles (Target Categories) pour bloquer **facebook**, les téléchargement, les torrents et bien d'autres mais avant ça il nous faudra créer les groupes ACL.

Ces derniers regroupent en une seule entité les utilisateurs concernés par un filtrage spécifique, dans ce cas le groupe ciblé est celui du centre informatique et donc contiendra la liste des adresses IP de tous les utilisateurs du centre informatique et comme démontré dans la figue qui suit :

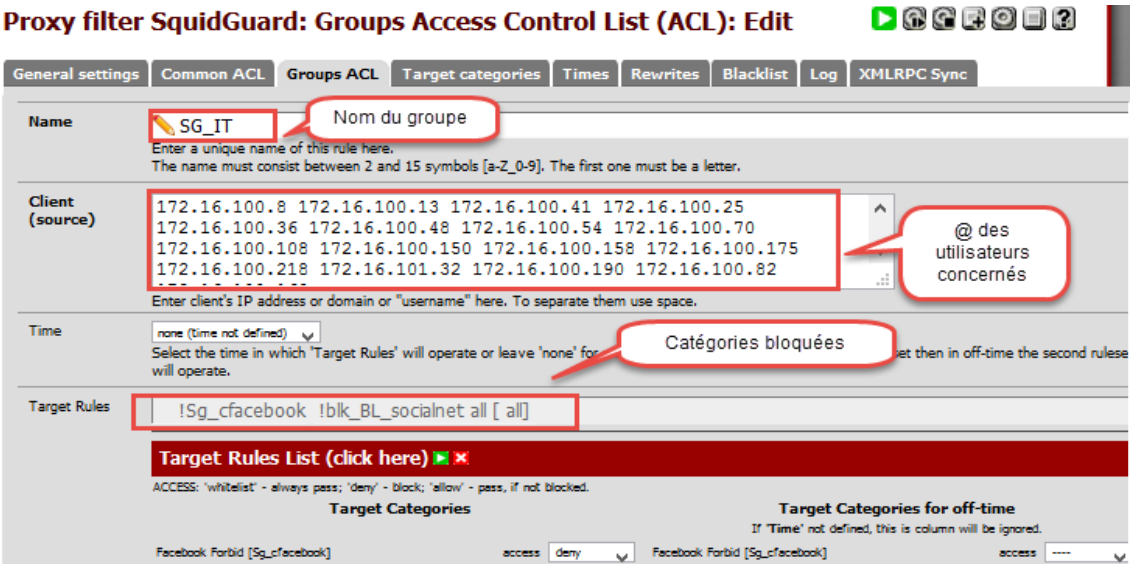

Figure 2.25: Création du groupe ACL des utilisateurs du centre informatique.

À présent nous pouvons passer à la création de notre Target Categorie personnalisée, l'élément clé de cette règle est l'expression régulière (regular expression), en effet chaque URL demandé sera comparé aux éléments en entrée dans l'expression régulière et s'il correspond, l'accès à l'URL demandé est refusé et l'utilisateur se verra redirigé vers une page d'erreur que nous avons pris soin de personnaliser sachant que celle fournie par squidguard est très basique. Il est recommandé de n'utiliser les expressions régulières qu'en cas de nécessité car elles sont très gourmandes en performances CPU.

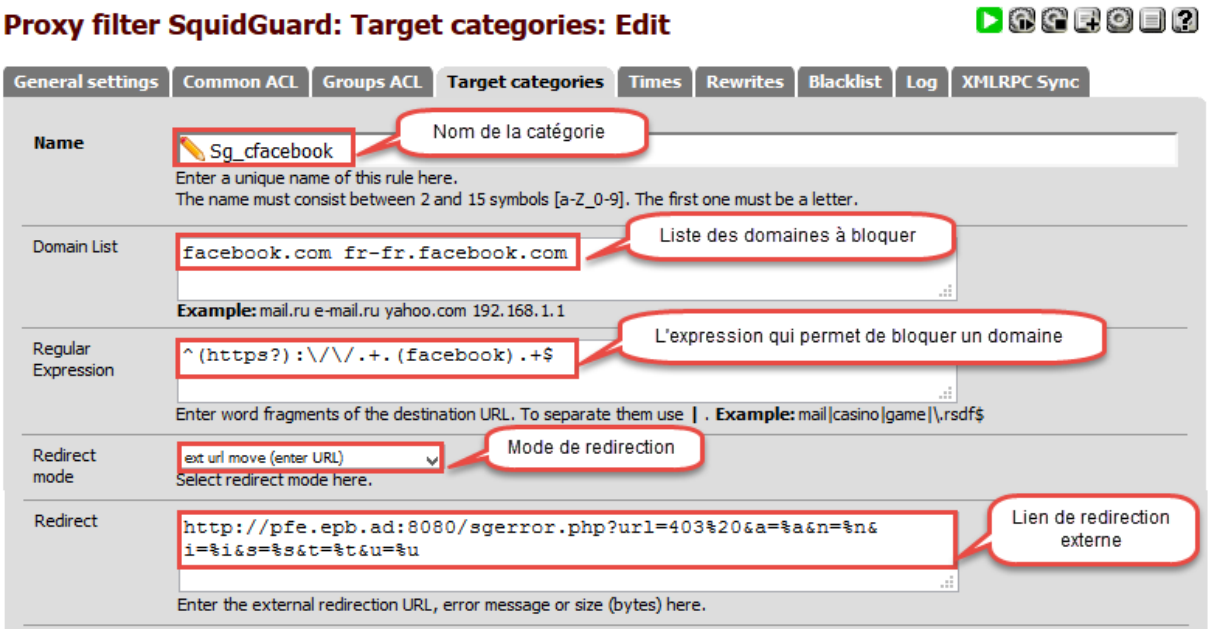

Figure 2.26: Filtrage d'un domaine.

Le service mandataire avec filtrage d'URL est un outil fiable et indispensable dans la panoplie de sécurisation du trafic Web, malgré cela, il existe des moyens qui arrivent à franchir le pare-feu et ses règles, afin d'y remédier nous avons défini l'expression suivante :

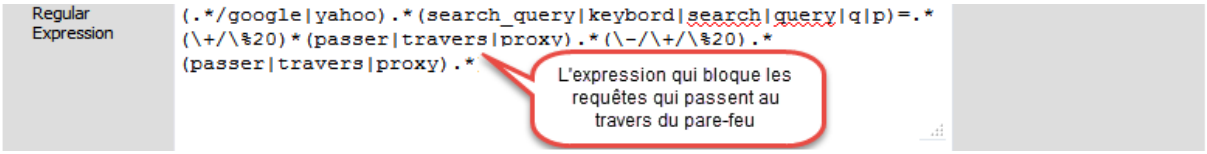

Figure 2.27: Renforcement de la sécurité.

La redirection de page Web pour le trafic bloqué est montrée dans la figure suivante :

Figure 2.28: Page de redirection.

2.7 Supervision de la bande passante NTOPng

2.7.1 Présentation de NTOPng

Ntopng pour ntop new generation est une sonde d'analyse du trafic réseau et nous permet ainsi d'avoir un œil sur l'utilisation qui est faite en temps réel de notre réseau. Nous pouvons également le qualifier de superviseur de bande passante, puisque nous pourrons afficher de manière détaillée un ensemble d'éléments tels que la bande passante moyenne utilisée par un hôte ou un

réseau, les différents flux, leur type et leur sens, et beaucoup plus encore [17].

2.7.2 Architecture NTOPng

Typiquement, Ntopng sera raccordé au cœur du réseau via un port miroir qui effectue une réplication de l'ensemble du trafic transitant via l'élément actif sur lequel il est configuré (généralement un commutateur). Ainsi, l'ensemble des paquets entrants et sortants sera redirigé vers notre pfSense avec Ntopng en écoute.

Un port miroir se contente uniquement de dupliquer les paquets, ils ne sont en aucun cas remaniés, ce qui nous permet de conserver les adresses, ports, etc... d'origine. Ainsi la maquette déployée pour traiter cette partie :

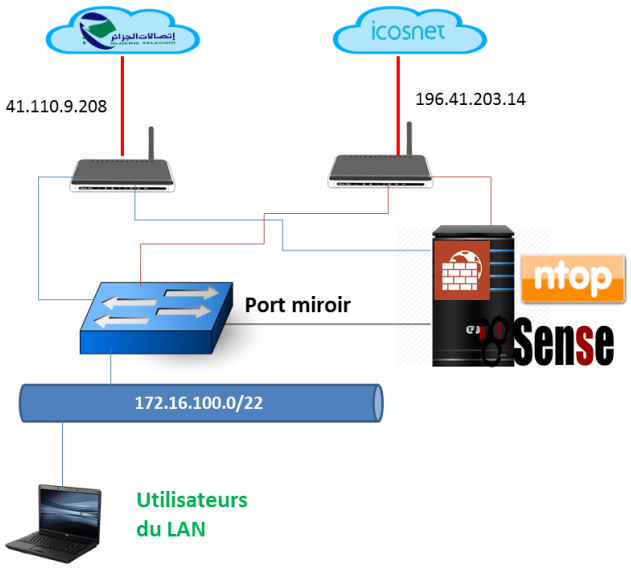

Figure 2.29: Maquette de test de ntopng.

2.7.3 Configuration de NTOPng

Les paramètres disponibles sur la page d'acceuil de NTOPng sont maigres, et permettent seulement de configurer le mot de passe admin pour accéder à la configuration avancée de ntopng.

En se connectant à cette adresse, on aura accès aux statistiques générales de notre réseau, affichant ainsi :

- De brèves informations concernant Ntopng (interface d'écoute, uptime, etc...) ;
- Un rapport concernant le trafic sur l'interface d'écoute (paquets, trafic, ou la charge) ;
- Un diagramme détaillé du trafic par service ;
- Ou encore la répartition totale du trafic par port :

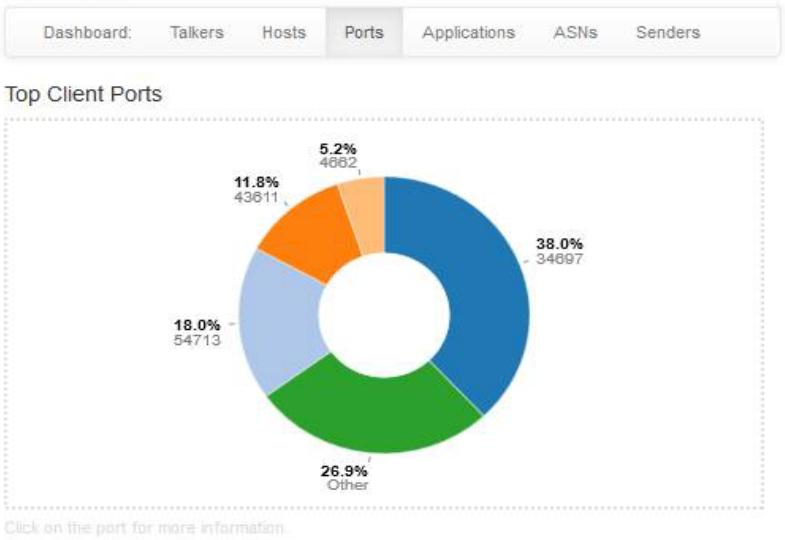

Figure 2.30: La répartition du trafic par ports de clients.

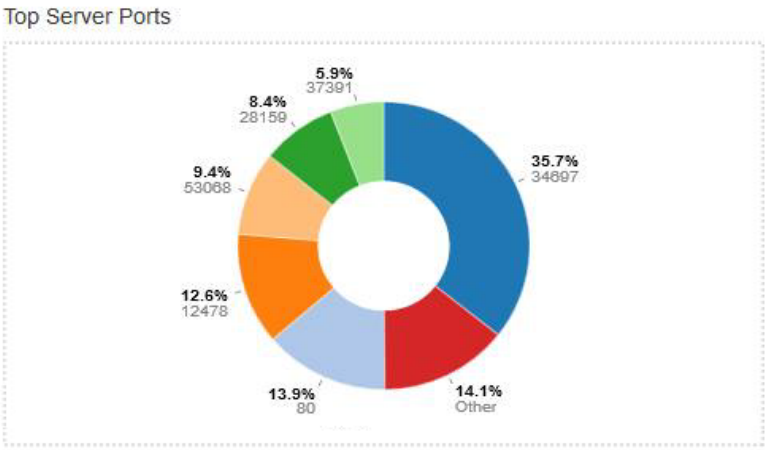

Figure 2.31: La répartition du trafic par ports de serveurs.

2.7.4 Scénarios d'utilisation de NTOPng

Comme dit plus haut, NTOPng est très fournit en termes de menus et de données affichables. Nous allons donc imaginer les scénarios classiques auxquels nous faisons face lorsque nous supervisons notre réseau/bande passante.

2.7.4.1 Quels hôtes consomment le plus de bande passante Internet?

Des lenteurs ont été constatées pour tout accès à Internet, que ce soit pour la téléchargement ou la mise à jour donc nous désirons contrôler l'utilisation que fait chaque hôte de notre connexion Internet, comme nous le montre la figure suivante qui dévoile des rapports à long terme sur les différents paramétres du réseau tels que le serveur, les protocoles d'application...

ntop

Active Flows

Info	Application	L4 Proto	Client	Server
Info	SMB	TCP	172.16.100.18:1279	pfe.epb.ad:445
Info	TDS	TCP	172.16.101.17:49182	10.0.0.196:49266
Info	? Unknown	TCP	ddd-appro-zahir.epb....:1132	serveurbdd.epb.ad:49844
Info	? Unknown	TCP	172.16.100.158:63675	AOrleans-653-1-71-12... :51413
Info	BitTorrent	UDP	172.16.100.158:33681	bas3-quebec09-112859... :56436
Info	Yahoo	TCP	172.16.100.171:57256	r1.ycpi.vip.loa.yaho... :443
Info	VRRP	VRRP	172.16.103.254	224.0.0.18
Info	HTTP	TCP	172.16.100.166:49995	ib.adnxs.com :80
Info	YouTube	TCP	172.16.100.82:55340	r6.sn-hgn7zn7l.googl... :443
Info	TDS	TCP	drh-paie1.epb.ad:4568	serveurbdd.epb.ad:49844

Showing 1 to 10 of 1710 rows

Figure 2.32: Top 10 des hôtes les plus gourmands.

Home | Flows | Hosts | Interfaces | Search Host

10 | Applications

Duration	Breakdown	Actual Thpt	Total Bytes
26 min, 54 sec	Server	15.89 Mbit ↑	234.28 MB
2 h, 42 min, 31 sec	Client Server	0 bps —	86.81 MB
4 days, 22 h, 46 min, 17 sec	Server	0 bps —	75.02 MB
1 h, 43 min, 15 sec	Client	0 bps ↓	49.43 MB
3 h, 11 min, 40 sec	Client	137.49 Kbit ↑	29.85 MB
42 min, 45 sec	Client	78.08 Kbit ↑	18.67 MB
4 days, 22 h, 46 min, 25 sec	Client	279.5 bps ↓	14.68 MB
18 min, 59 sec	Server	52.81 Kbit ↑	9.79 MB
1 min, 40 sec	Server	1.87 Kbit ↑	7 MB
2 h, 6 min, 13 sec	Client Server	0 bps —	6.51 MB

« < 1 2 3 4 5 > »

Figure 2.33: Consommation de la bande passante du top 10 d'utilisateurs.

Nous affichons ainsi l'ensemble des hôtes et nous nous assurant que nos consommateurs de bande passante l'utilise bien à des fins professionnelles, mais aussi les quantités de données reçues et/ou envoyées par notre top 10 des consommateurs et tout cela bien sure en temps réel.

2.7.4.2 Quels hôtes s'échangent le plus de données ?

Nous avons également la possibilité d'afficher les flux locaux, idéal afin de constater les interactions entre différents hôtes.

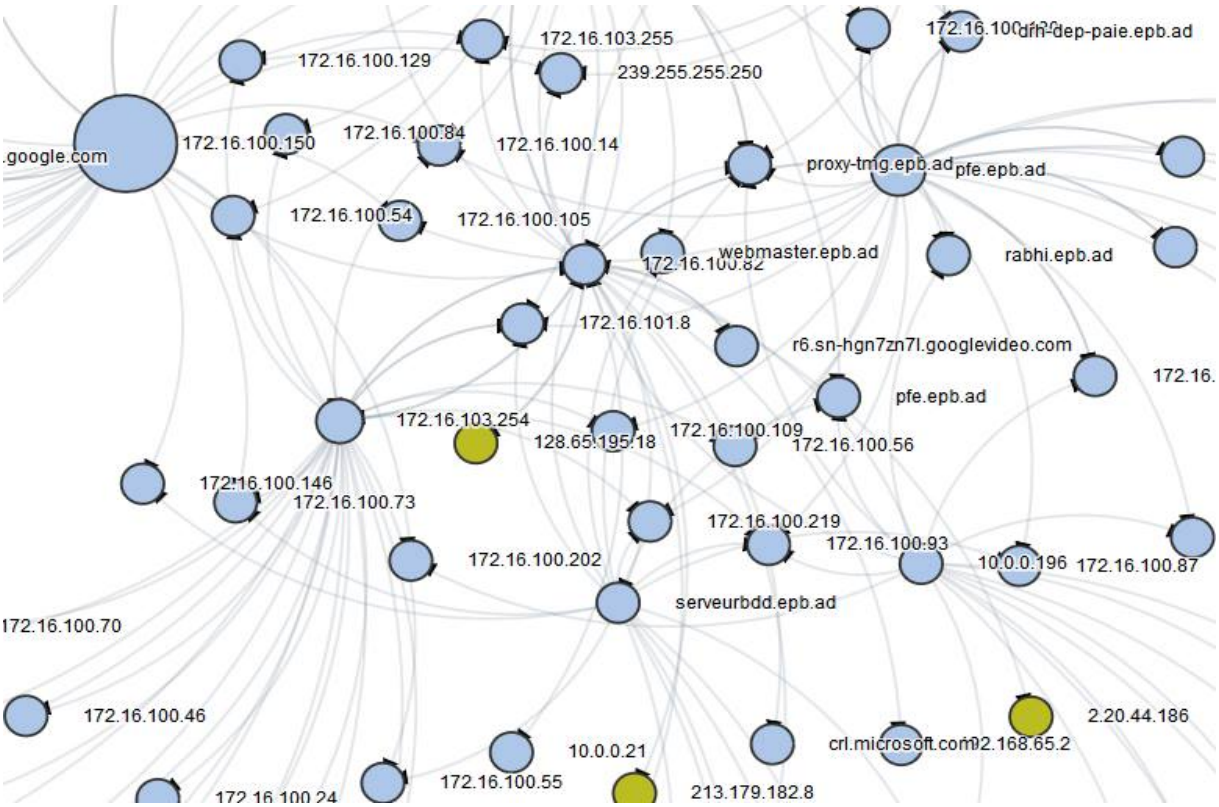

Figure 2.34: Les flux de donnée échangées entre les hôtes.

2.8 Détection et prévention d'intrusions SNORT

2.8.1 Présentation de SNORT

SNORT est un outil open source de détection d'intrusions réseaux (IDS). SNORT est capable d'écouter sur une interface afin d'effectuer une analyse du trafic en temps réel, de logger les paquets IP, de rechercher des correspondances de contenu ; le but étant de détecter une grande variété d'attaques connues. SNORT peut fonctionner en quatre modes différents :

- SNIFFER : capture et affichage des paquets, (pas de log) ;
- PACKET LOGGER : capture et log des paquets ;
- IDS : analyse le trafic, le compare à des régles, et affiche des alertes.
- IPS (détection d'attaques et prévention de celles-ci).

Nous nous concentrerons ici sur les modes IDS et IPS, qui nous rendrons deux services bien différents :

- IDS : Détecter des tentatives d'intrusions réseaux d'après des règles.
- IPS : Empêcher les intrusions réseaux détectées, toujours d'aprés les mêmes règles.

2.8.2 Schéma de réalisation

Le schéma suivant nous permet de tester SNORT afin de mettre en avant ses fonctions d'IDS et d'IPS :

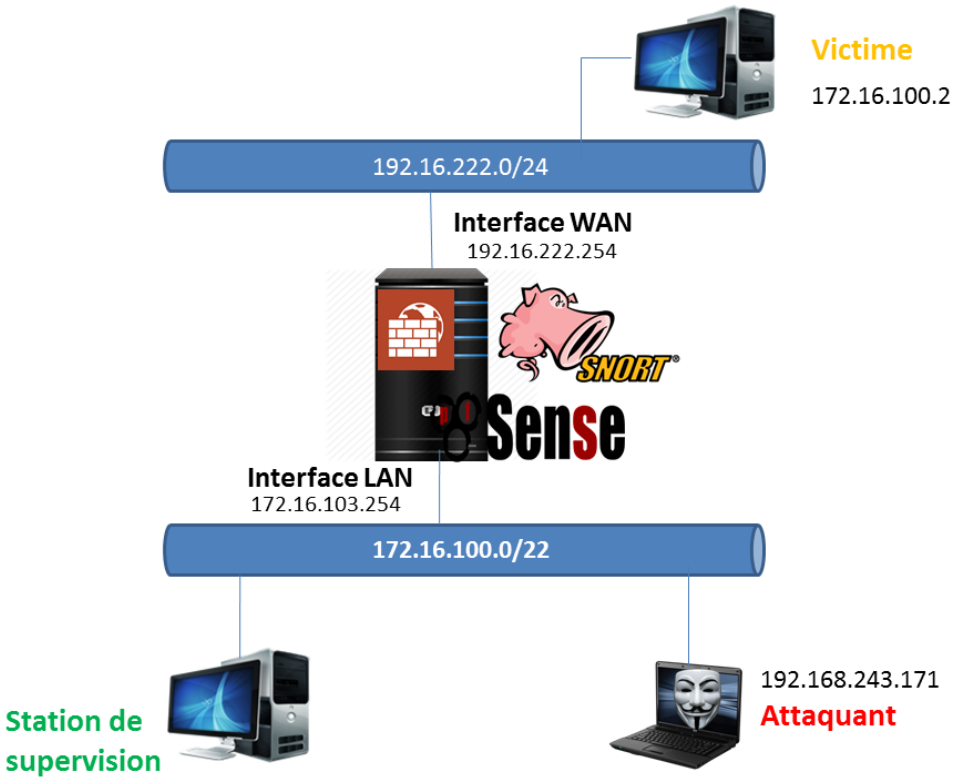

Figure 2.35: Maquette de test de SNORT.

2.8.3 Installation de SNORT

L'installation de SNORT est une installation standard, il suffit de télécharger le package SNORT et de l'installer de la même maniére que les packages installés précédement.

2.8.4 Configuration de SNORT

2.8.4.1 Activation des règles dans SNORT

SNORT fonctionne en utilisant des signatures de détection appelées règles. Les règles de SNORT peuvent être créées sur mesure par l'utilisateur, ces règles sont montrées dans la figure suivante :

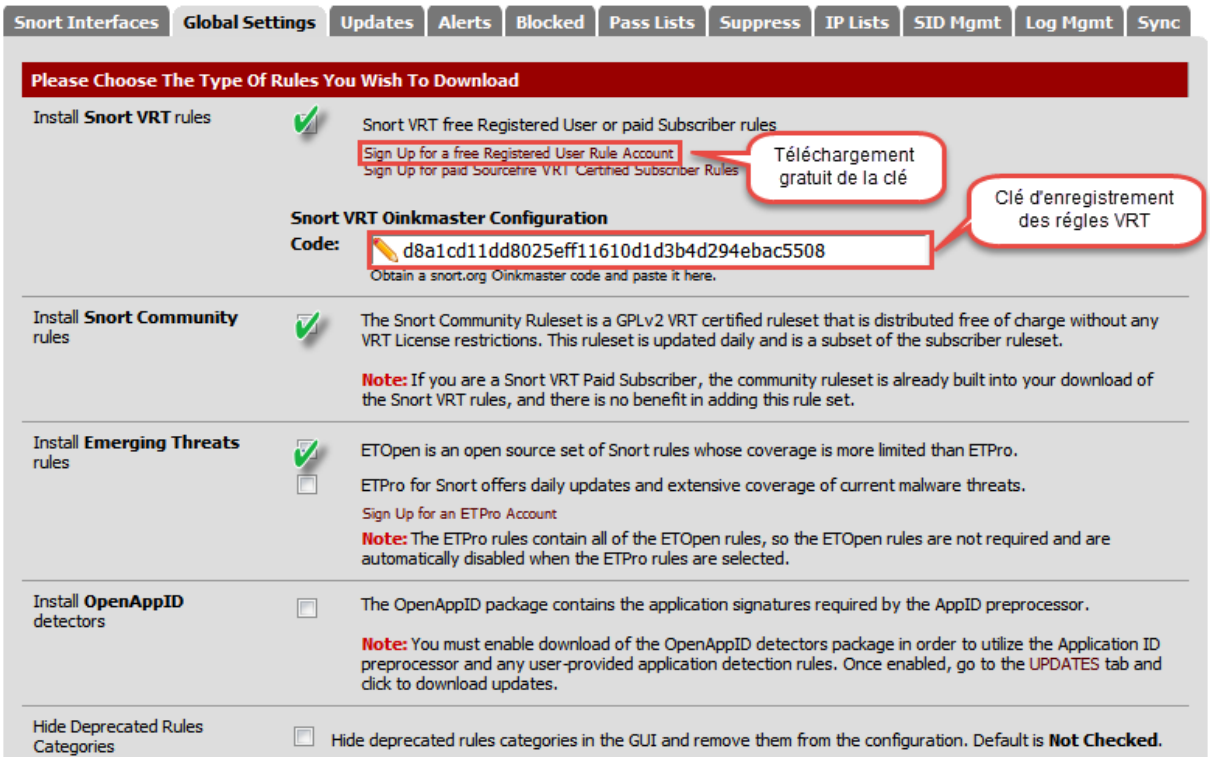

Figure 2.36: Règles SNORT installées.

Dans la figure ci-dessous, les règles ont été téléchargées avec succès. Le hachage MD5 calculé et la date et l'heure du téléchargement sont affichées. A noter également la dernière fois que la mise à jour et le résultat sont indiqués dans le centre de la page.

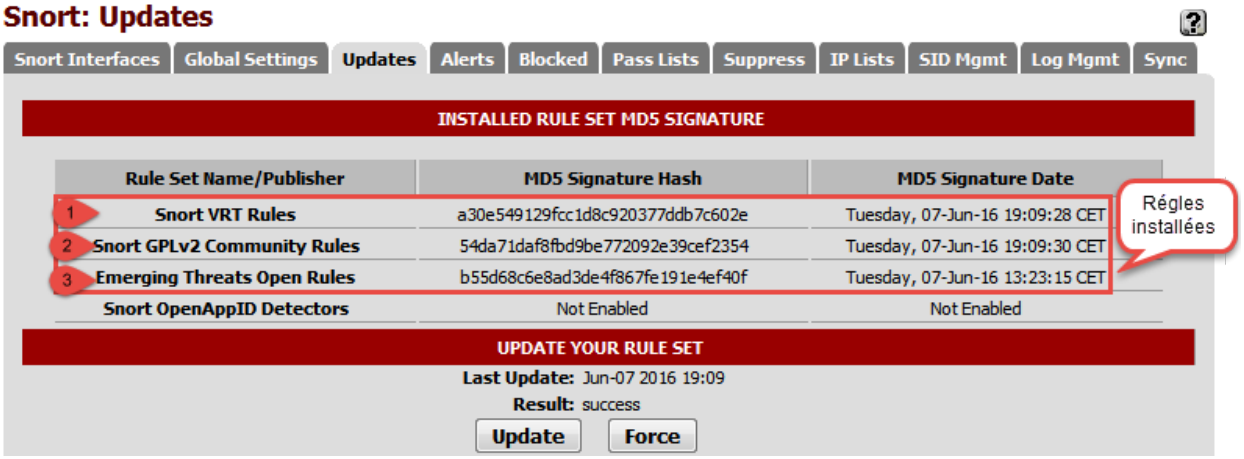

Figure 2.37: Mise à jour des règles installées.

2.8.4.2 Ajouter SNORT à une interface

La sélection de l'interface peut être modifiée en choisissant l'interface désirée, dans notre cas (Figure 2.38), l'interface WAN a été choisie pour appliquer les fonctionnalités de SNORT sur notre première connexion internet (Algérie Telecom), les mêmes configurations

ont été appliquées à l'interface WAN_1 la deuxième connexion internet (ICOSNET).

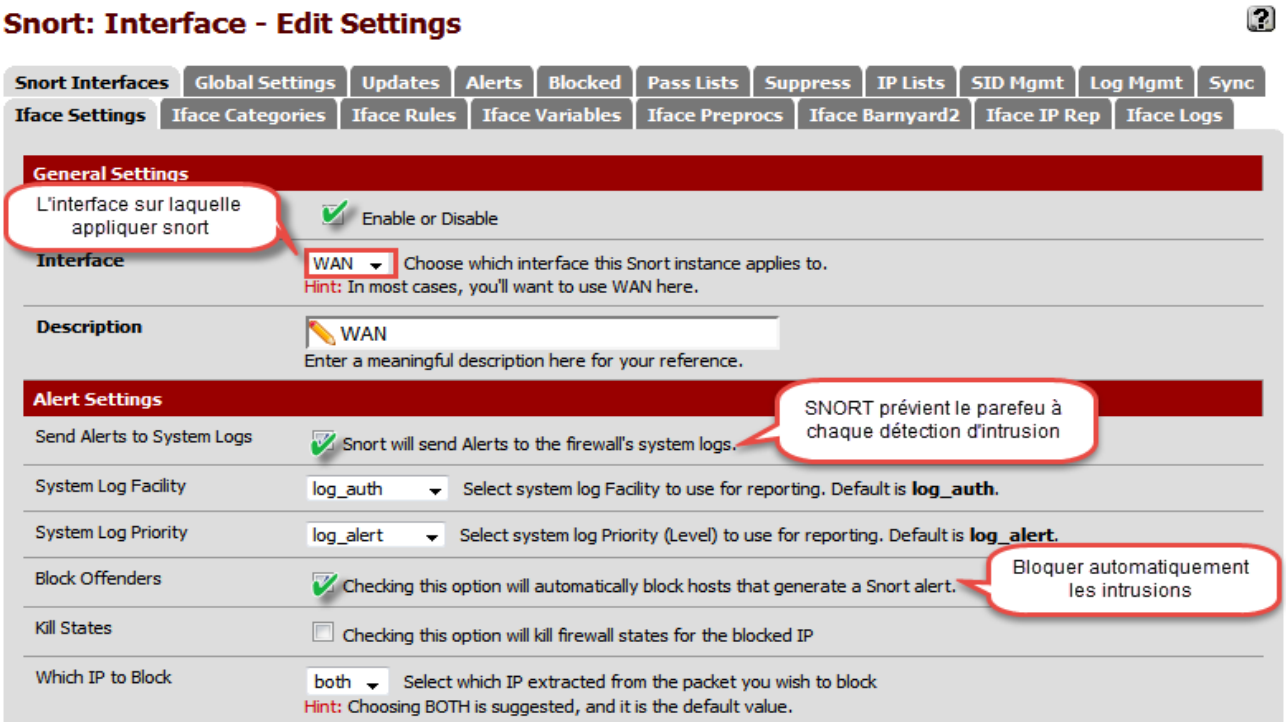

Figure 2.38: Ajout de SNORT à l'interface WAN.

2.8.4.3 Sélectionner les types de règles pour protéger le réseau

L'installation des régles Snort VRT à utiliser lors de l'inspection du trafic simplifient grandement le processus de choix des régles d'exécution pour SNORT. Les politiques IPS ne sont disponibles que lorsque les régles SNORT VRT sont activées. Les trois politiques SNORT VRT IPS sont : connectivité, équilibrage et sécurité.

Celles-ci sont classés par ordre d'accroître la sécurité. Si SNORT est inconnu, l'utilisation de la politique de sécurité la moins restrictive en mode non-bloquant est recommandée. Une fois l'expérience avec SNORT a été acquise dans cet environnement réseau, le mode de blocage peut être activé et ensuite passer à des politiques d'IPS plus restrictives.

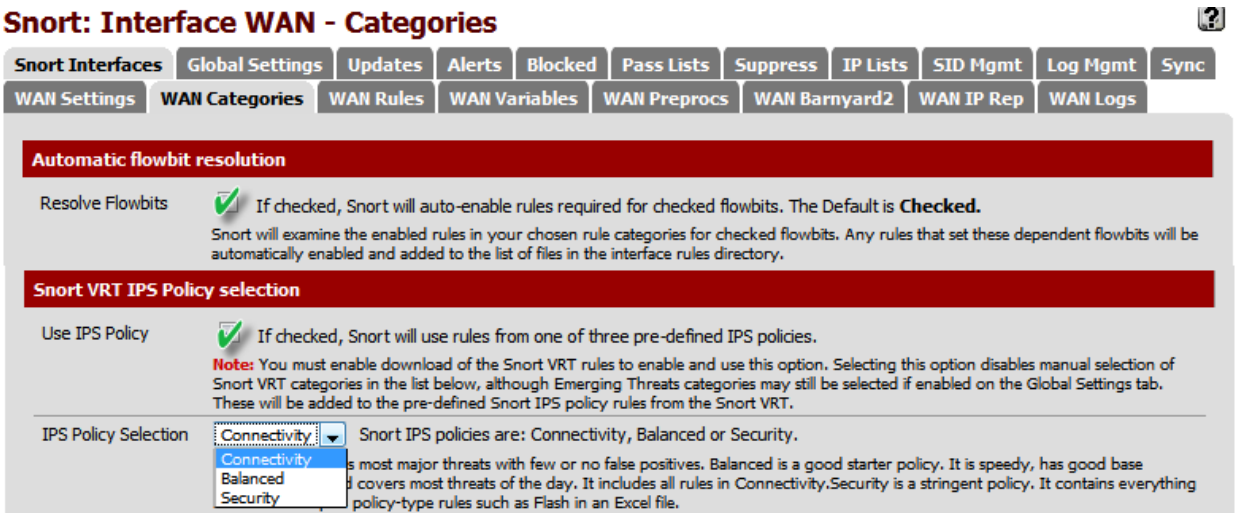

Figure 2.39: Choix des règles VRT.

Si les régles SNORT VRT ne sont pas activées, ou si l'un des autres paquets de régles doit être utilisé, alors il faut faire la sélection de catégorie de règles en cochant les cases en regard des catégories de règles à utiliser (Figure 2.40).

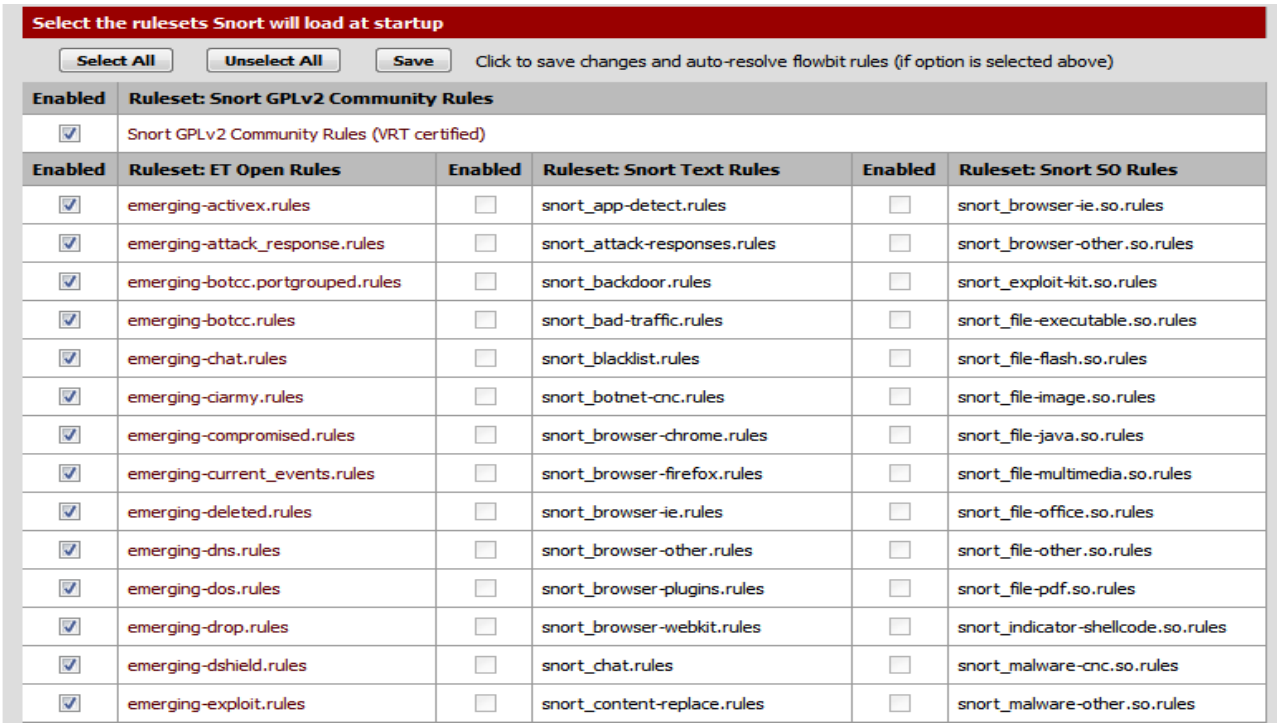

Figure 2.40: Catégories des règles Snort.

Pour effectuer ses analyses SNORT se fonde sur ces règles. Celles-ci vont permettre à SNORT d'écouter, d'analyser et de capturer certains paquets. SNORT va ensuite stocker ses règles et ses résultats dans une base de données. Afin de détecter les intrusions de tout type, il est préférable de cocher toutes les catégories et toutes les règles. Mais cela peut causer un conflit qui est de générer plus de fausses alertes c'est-à-dire de bloquer certaines requêtes non malveillantes.

À présent on peut démarrer Snort sur une interface, dans la figure (Figure 2.42) SNORT est démarré sur l'interface WAN (Algérie Telecom) :

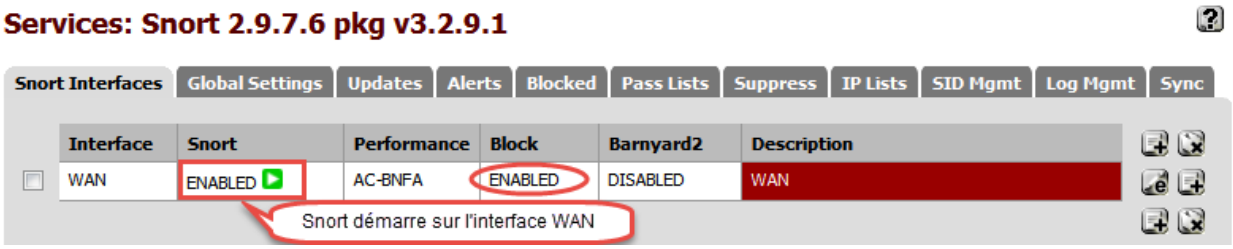

Figure 2.41: Démarrage de SNORT sur une interface.

2.8.5 Test de fonctionnement de la solution

Le test repose sur le schéma présenté dans la figure (Figure 2.35). Un attaquant va effectuer des attaques de type scan de port[6] Nmap[7] sur un hôte distant. Pendant toute la durée du test, l'attaquant effectue en parallèle des attaques vers la victime, afin de vérifier en permanence la connectivité vers l'hôte et mettre en avant le moment où il sera bloqué par SNORT.

La figure suivante montre une attaque simulée avec Nmap :

[6]Technique servant à rechercher les ports ouverts sur un serveur de réseau.
[7]Network Mapper

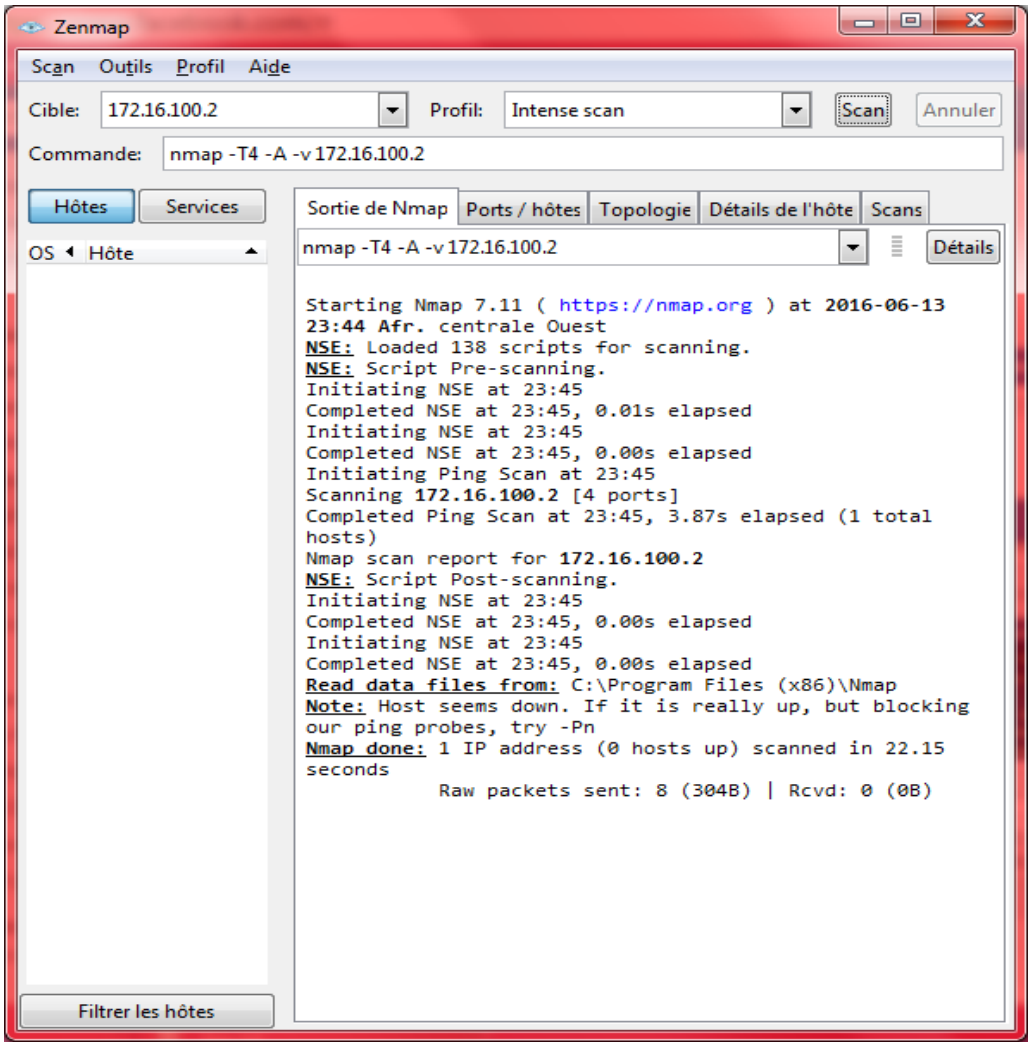

Figure 2.42: Simulation d'une attaque.

Une fois le scan de port lancé, la station de supervision peut très rapidement constater des alertes ainsi que l'adresse IP de notre attaquant bloquée :

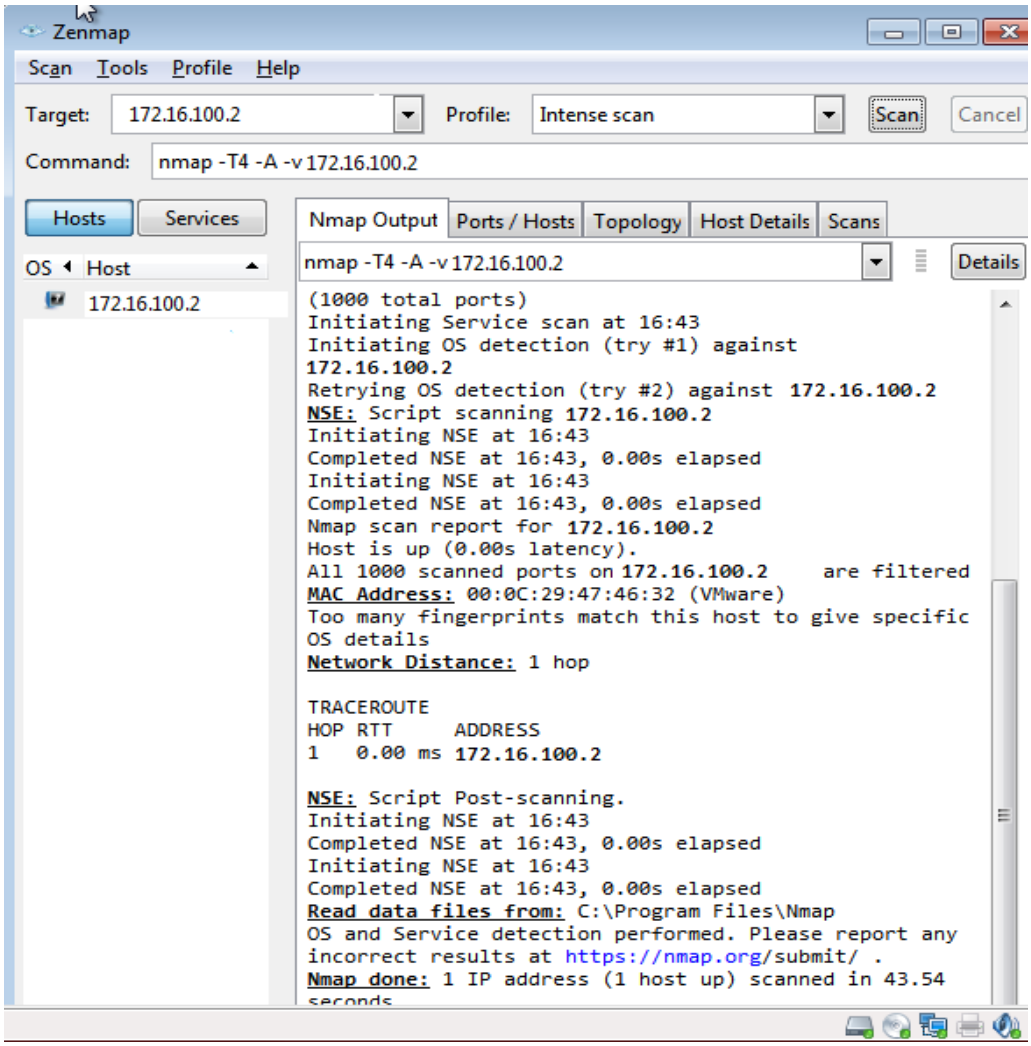

Figure 2.43: Gestion de l'hôte bloqué.

1. **Gestion des hôtes bloqués avec IPS**

   Une fois les attaques lancées, la station de supervision peut trés rapidement constater des alertes ainsi que leurs adresse IP. La figure suivante montre les hôtes actuellement bloqués par SNORT. Les hôtes bloqués peuvent être automatiquement effacés par SNORT. Les options de blocage d'une interface sont configurées dans les paramètres de l'interface SNORT.

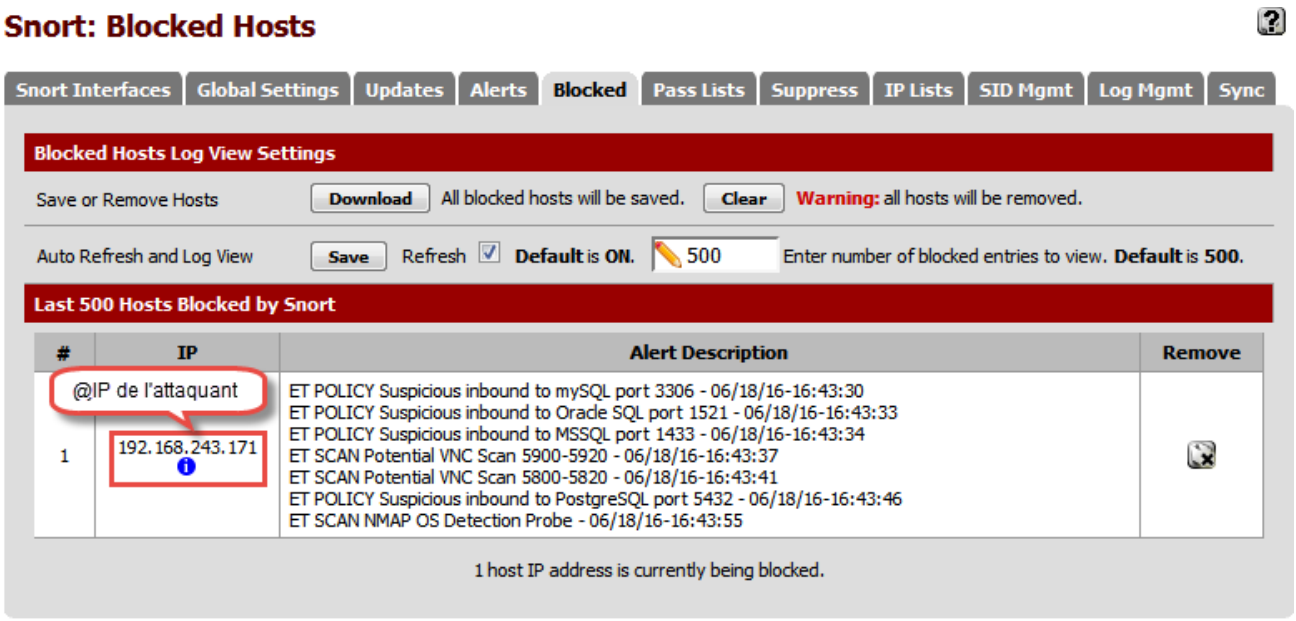

Figure 2.44: Gestion des hôtes bloqués.

2. **Gestion des alertes avec IDS**

La détection d'intrusion est un ensemble de techniques et de méthodes qui sont utilisées pour détecter toute activité suspecte à la fois au niveau du réseau et d'hôte. Les systèmes de détection d'intrusion tombent dans deux catégories de base: des systèmes de détection à base de règles et des systèmes de détection d'anomalies. Les intrus ont des signatures, comme les virus informatiques, qui peuvent être détectés en utilisant un antivirus.

Sur la base d'un ensemble de signatures et des règles, IDS est capable de trouver et de se connecter à une activité suspecte et de générer des alertes. La figure (Figure 2.45) montre quelques alertes détectées lors de la connexion au réseau en indiquant leurs adresses IP, adresses de destination, le protocole ainsi que le port.

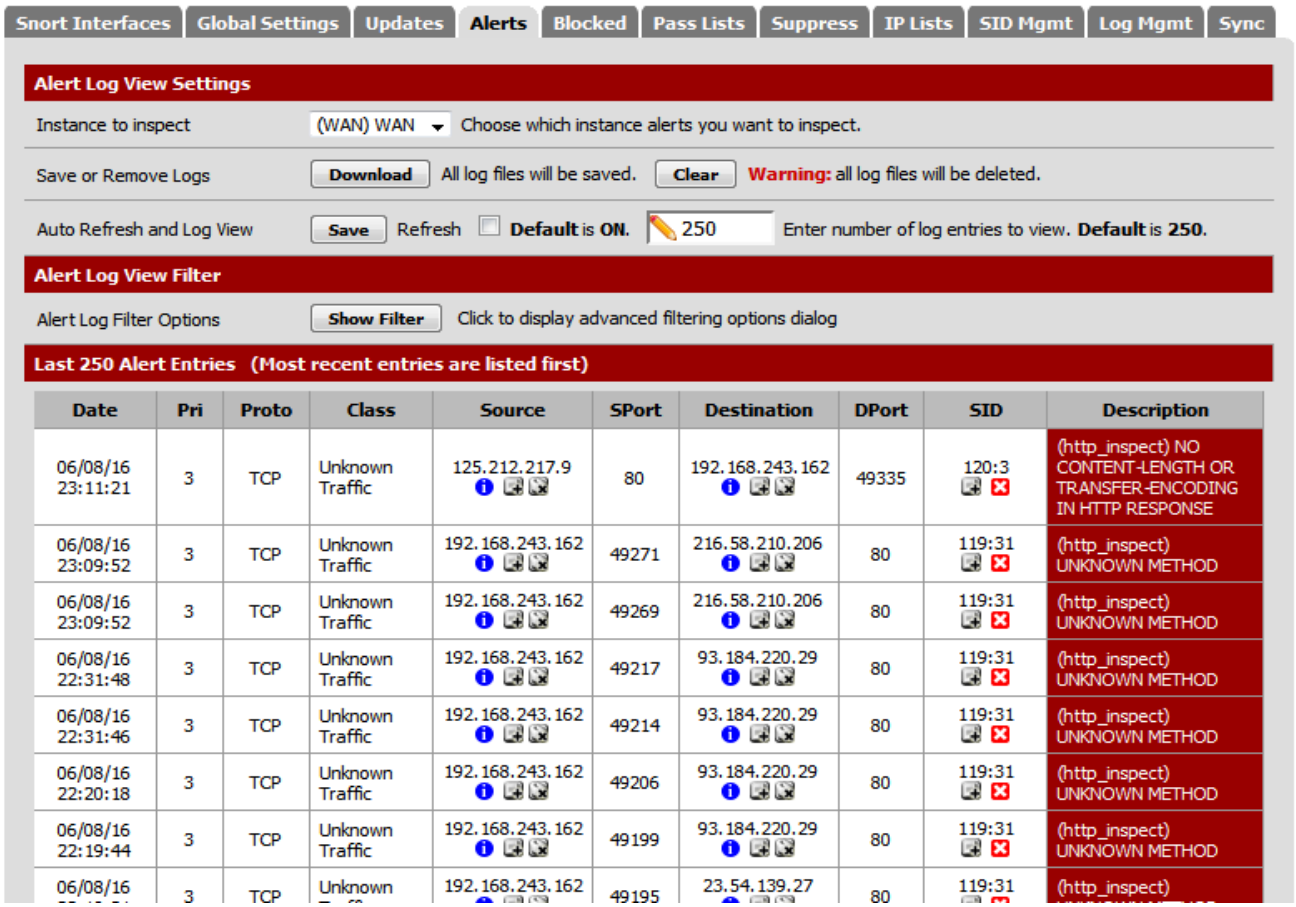

Figure 2.45: Gestion des alertes.

Habituellement un système de détection d'intrusion capte les données du réseau et applique ses règles sur ces données et détecte des anomalies en elles.

2.8.5.1 Gestion des passlists

Les Passlist sont des listes d'adresses IP que Snort ne doit jamais bloquer . Celle-ci peuvent être créées et gérées sur la Passlist. Lorsqu'une adresse IP est répertoriée sur une Passlist, Snort ne pourra jamais appliquer une règle sur cette adresse, même si le trafic malveillant est détecté. La figure 2.46 illustre la création et la configuration d'une passlist.

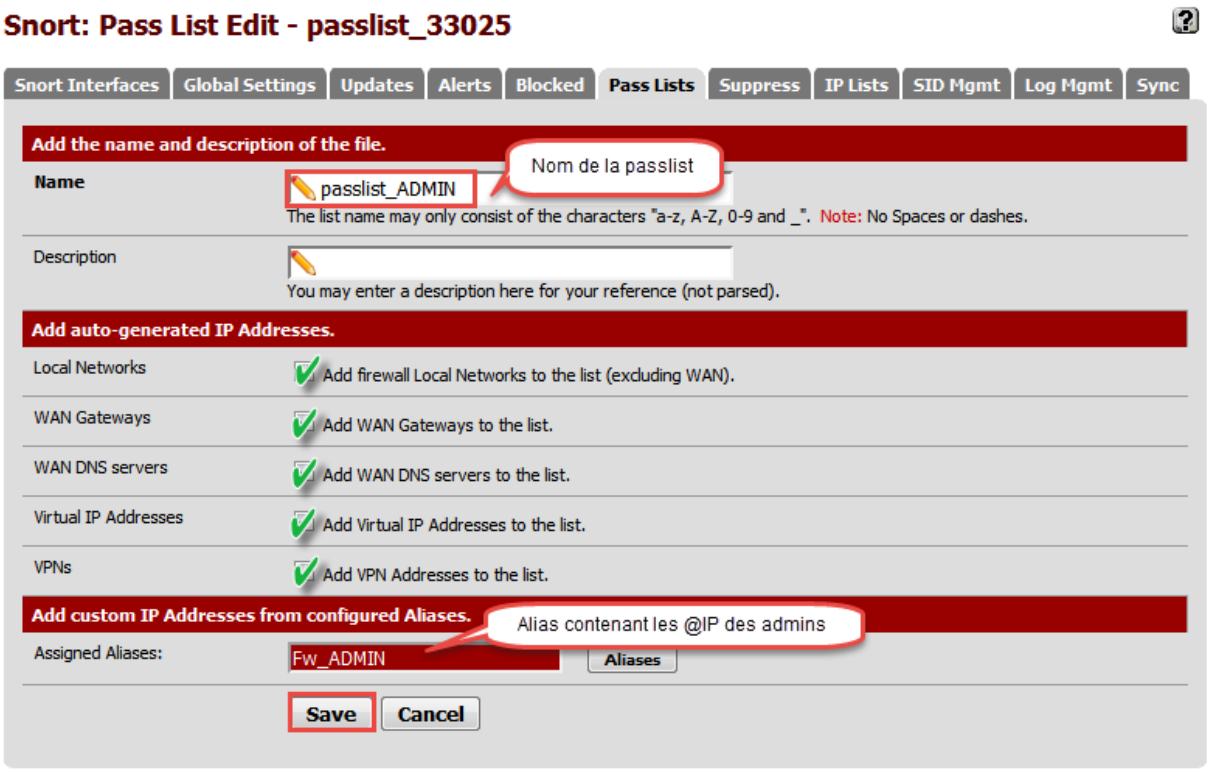

Figure 2.46: Gestion d'une passlist.

Une passlist personnalisée peut être créée et affectée à une interface. Cela peut être fait lorsque les hôtes externes fiables existantes ne sont pas directement connectées aux réseaux sur lequel le pare-feu est appliqué. Pour ajouter des hôtes externes, il faut d'abord créer un alias dans les règles de Pare-feu. Dans l'exemple illustré dans la figure 2.46, l'alias " Fw_ADMIN " a été attribué à cette Passlist. Cet alias contient les adresses IP des hôtes externes de confiance (Les administrateurs du réseau de l'EPB).

2.9 DMZ (zone démilitarisée)

Une DMZ est une interface située entre un réseau connu (réseau interne) et un réseau externe (internet). Une série de règles de connexion congrès sur le pare-feu font de cette interface une zone physiquement isolée entre les deux réseaux. Cette séparation physique permet d'autoriser les accès internet à destination des serveurs placés dans la DMZ et non à ceux destinés au réseau privé (interne) [18].

Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité. Et les services susceptibles d'être accédés depuis Internet seront situés en DMZ.

2.9.1 Assignation de l'interface DMZ

Afin d'assigner une interface pour la zone démilitarisée, nous devons créer celle-ci dans le menu **Interfaces > (Assign)**. Une description et une adresse IP y sont recommandées.

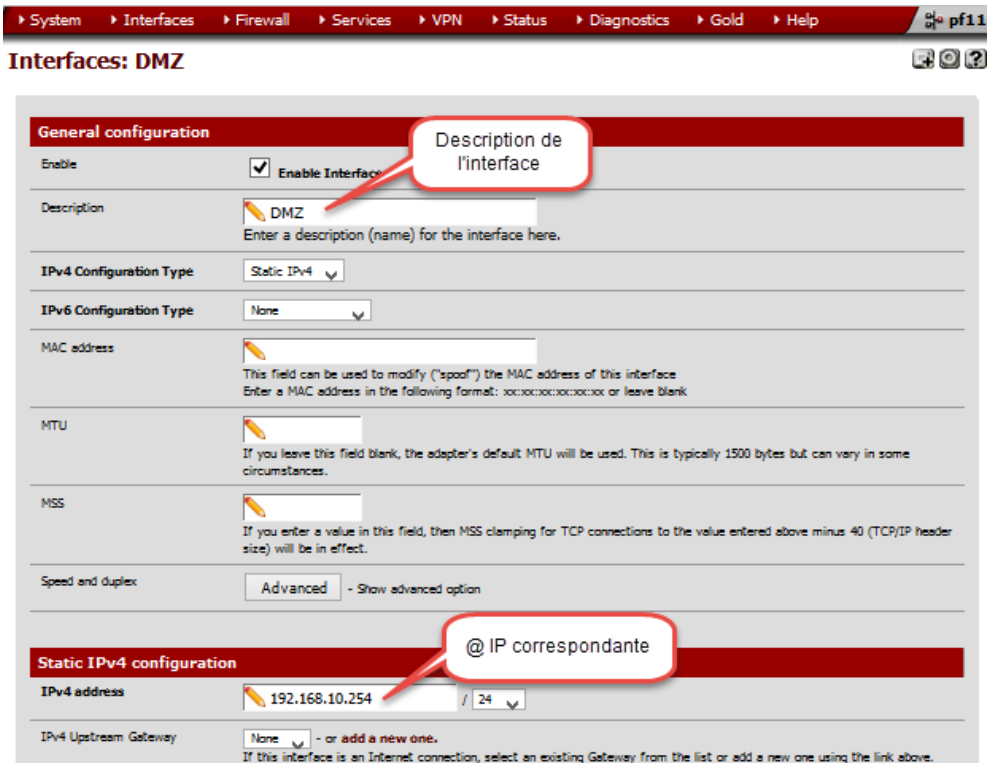

Figure 2.47: Création d'une interface correspondante à la DMZ.

L'interface de la DMZ est à présent prête pour être connectée aux serveurs désirés par l'entreprise.

2.10 Haute disponibilité (High avalability)

2.10.1 La basculement (failover)

2.10.1.1 Présentation

Le basculement (en anglais, failover qui se traduit par passer outre à la panne) est la capacité d'un équipement à basculer automatiquement vers un chemin réseau alternatif ou en veille. Cette capacité existe pour tout type d'équipements réseau : du serveur au routeur en passant par les pare-feu et les commutateurs réseau (switch). Le basculement intervient généralement sans action humaine et même bien souvent sans aucun message d'alerte. Le basculement est conçu pour être totalement transparent [3].

2.10.1.2 Modes de basculement

Il existe deux modes principaux de basculement [3] :

- Actif/actif qui s'apparente plus à de l'équilibrage de charge (load-balancing).
- Actif/passif qui est le mode classique couramment répandu, où l'équipement secondaire (passif) est en mode veille tant que l'équipement primaire (actif) ne rencontre aucun problème.

Le basculement (Actif-Passif) est rendu possible grâce au protocole CARP (Common Address Redundancy Protocol).

2.10.2 Protocole CARP

Common Address Redundancy Protocol (CARP) est utilisé par plusieurs nœuds à " partager " une adresse IP virtuelle entre plusieurs nœuds d'une manière telle que si le nœud préféré échoue, un autre prendra la relève de façon transparente. CARP a été lancée par OpenBSD[8] comme une alternative Open Source à la VRRP[9] [14].

Une utilisation commune de CARP est la création d'un groupe de pare-feu redondants. L'adresse IP virtuelle attribuée au groupe de redondance est désignée comme l'adresse du routeur par défaut sur les machines clientes. Dans le cas où le pare-feu maître rencontre une panne ou est déconnecté du réseau (mise à jour par exemple), l'adresse IP virtuelle sera prise par un des pare-feu esclaves et le service continuera à être rendu sans interruption. C'est justement de type de configuration avec deux pare-feu PfSense version 2.2.6 que nous allons déployer et expliquer dans ce qui suit.

Schéma général

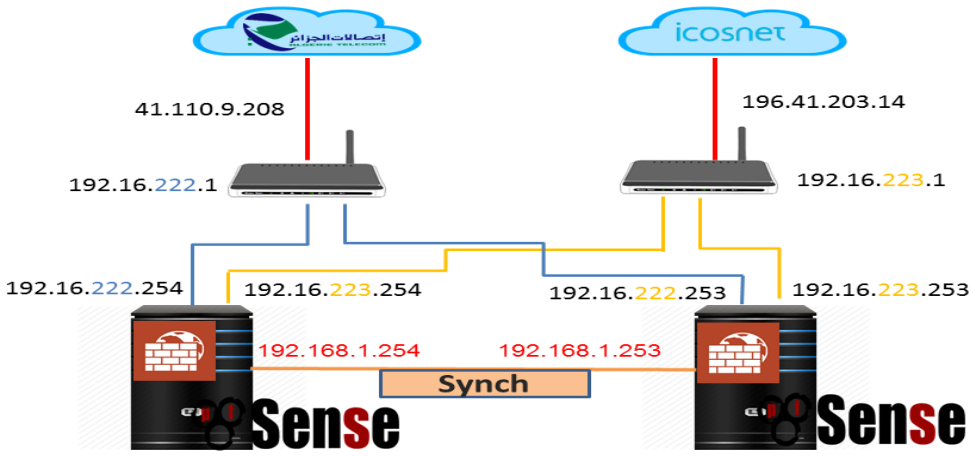

Figure 2.48: Schéma général du basculement.

Description du schéma

À priori l'utilisation de deux modems a comme objectif de disposer de deux adresses routables pour chaque connexion internet (WAN) qui est à la base non routable, ceci a pour objectif de garantir que les deux connexions WAN passent par chaque pare-feu en permanent en d'autres

[8]Système d'exploitation libre de type Unix.
[9]Virtual Router Redundancy Protocol (protocole de redondance de routeur virtuel).

termes chaque pare-feu dispose de toutes les ressources nécessaires à son fonctionnement indépendamment de l'autre pour une tolérance aux pannes en temps réel.

Bien évidement l'installation d'un deuxième pare-feu pfSense qui sera désigné par la suite sous le nom Slave-Pfsense (pare-feu esclave), par conséquent c'est le premier pare-feu qui sera notre Master-PfSense (pare-feu maître), ce dernier utilise le mécanisme pfsync " XMLRPC sync[10] " pouvant synchroniser automatiquement sa configuration sur Slave-PfSense (NAT, Rules, etc.) et paramétrer " nodes (informations de status), advskew (hiérarchie dans le cluster) et vhid (groupe de cluster) ".

Le cluster partage des adresses IP virtuelles suivantes :

- 172.16.103.252 : comme adresse LAN du cluster, cette adresse sera renseignée comme passerelle par défaut sur toutes les machines client.
- 192.16.222.252, 192.16.223.252 : ces adresses désignent les passerelles internet par défaut pour chaque connexion WAN et WAN_1 respectivement.
- 192.168.1.252 : pour la synchronisation des interfaces pfsynch entre les deux pare-feu, ce principe est appliqué au reste des interfaces à savoir DMZ, SRV...

2.10.3 Configuration du basculement Maître-Esclave

Nous avons vu d'un peu plus près le protocole qui allait permettre au deuxième pare-feu de prendre relais dans le cas d'un crash d'une panne au niveau du premier. On entend par là que l'étape de l'installation d'un deuxième pare-feu esclave ne puisse être négligeable c'est-à-dire que nous devons nous munir d'une deuxième machine pfSense.

2.10.3.1 Installation et configuration d'un deuxième pare-feu pfSense

L'installation du deuxième pare-feu se fait identiquement de la même manière que le premier. À l'étape de la configuration un nom de machine, de domaine et une adresse IP LAN sont recommandés.

[10]Extensible Markup Language Remote Procedure Call : permet d'appeler une fonction sur un serveur distant à partir de n'importe quel système.

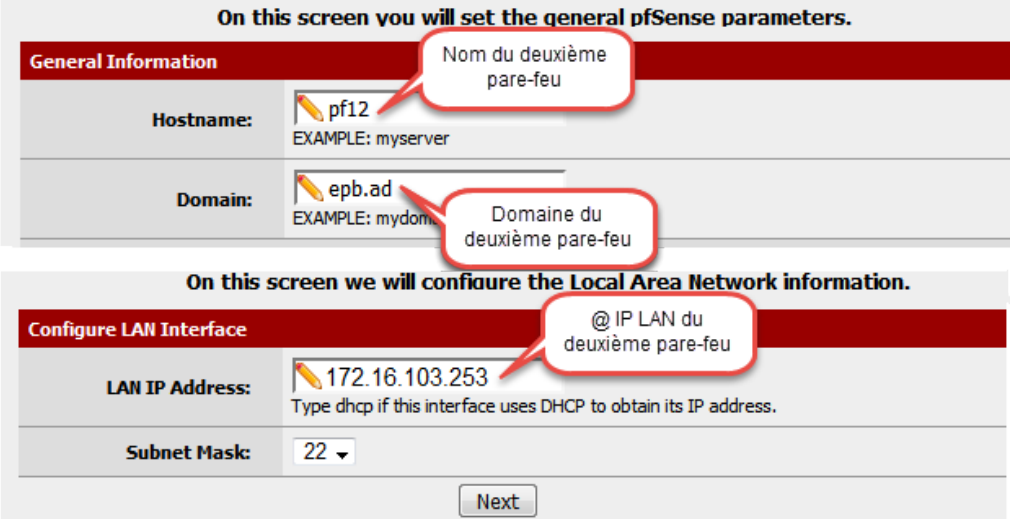

Figure 2.49: Installation et configuration du deuxi`me pare-feu pfSense.

Désormais les deux machines sont prêtes à être inter-connectées.

Il est nécessaire d'assigner les mêmes interfaces existantes sur la première machine au niveau de la deuxième machine (WAN, LAN, WAN_1, DMZ, SRV et PFSYNC).

Afin de configurer le protocole CARP, plusieurs étapes peuvent demeurer indispensables. Telle est l'étape de l'assignation d'une interface dédiée à lier les deux machines.

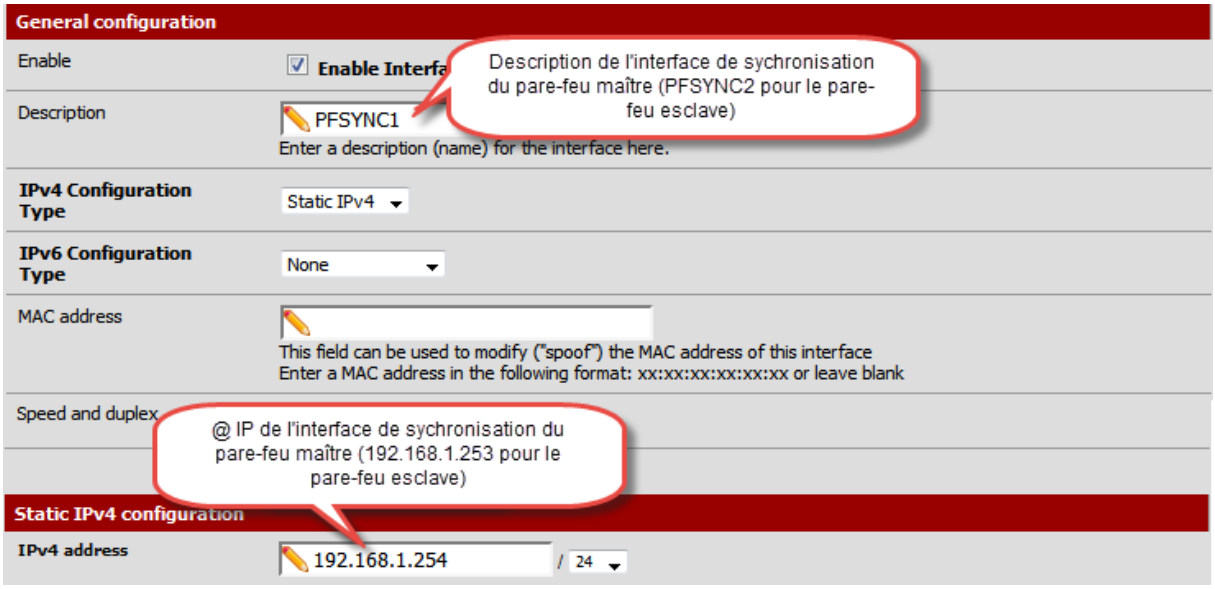

Figure 2.50: Assignation de l'interface dédiée à la liaison des deux pare-feu.

Sur les deux pare-feu et plus précisément au niveau des interfaces PFSYNC1 et PFSYNC2, une seule et unique règle de pare-feu doit être créée sur les deux interfaces. Cette règle permet tout le trafic sur PFSYNC1 et PFSYNC2.

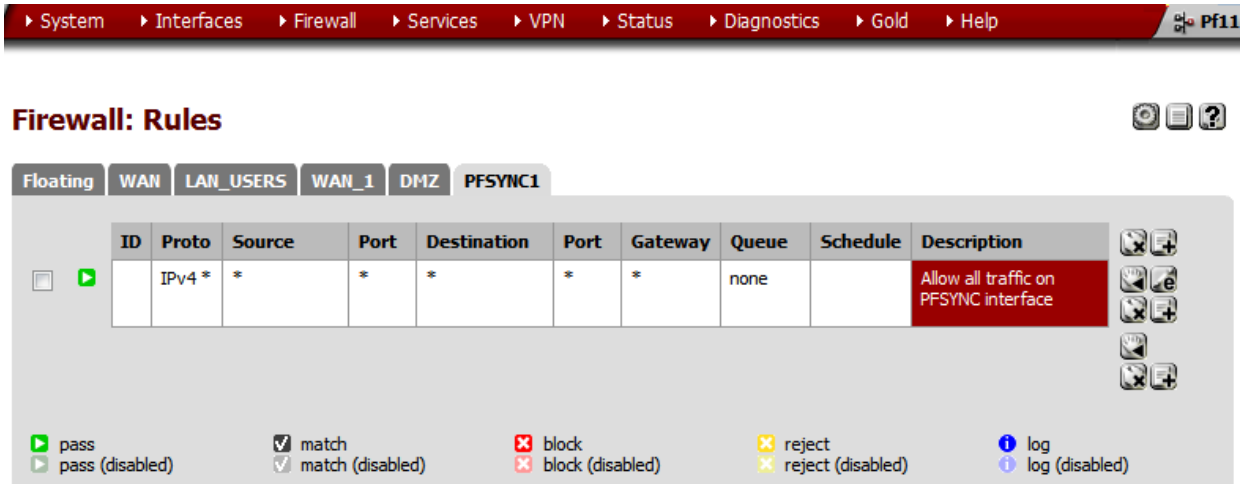

Figure 2.51: Règle autorisant le trafic entre les deux pare-feu.

2.10.3.2 Création des Virtual IPs

Sur le menu **Firewall > Virtual IPs | CARP Settings** et sur les deux pare-feu nous pouvons établir les paramètres qui consistent en l'activation de la synchronisation, désignation de l'interface de synchronisation.

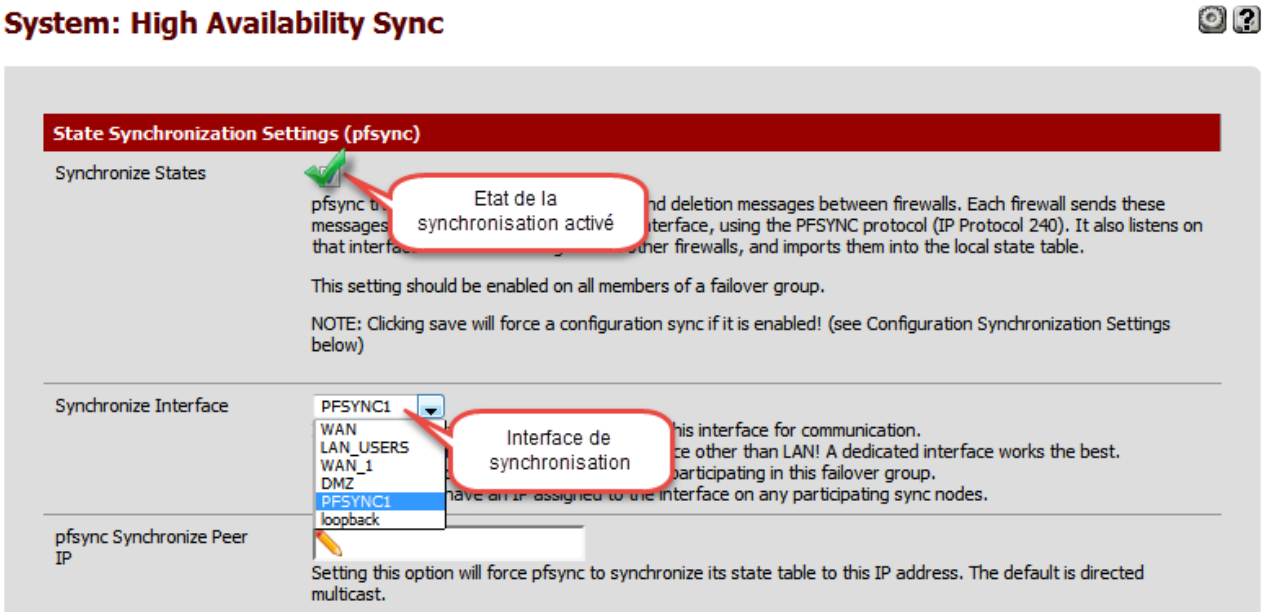

Figure 2.52: Paramètrage de la synchronisation.

Il faut définir l'adresse IP de l'interface de synchronisation du deuxième pare-feu ainsi que toute option voulant être synchronisée sur la seconde machine telle que les règles de pare-feu, utilisateurs et groupes et pleine d'autres options. Un nom d'utilisateur système et un mot de passe y sont indispensables.

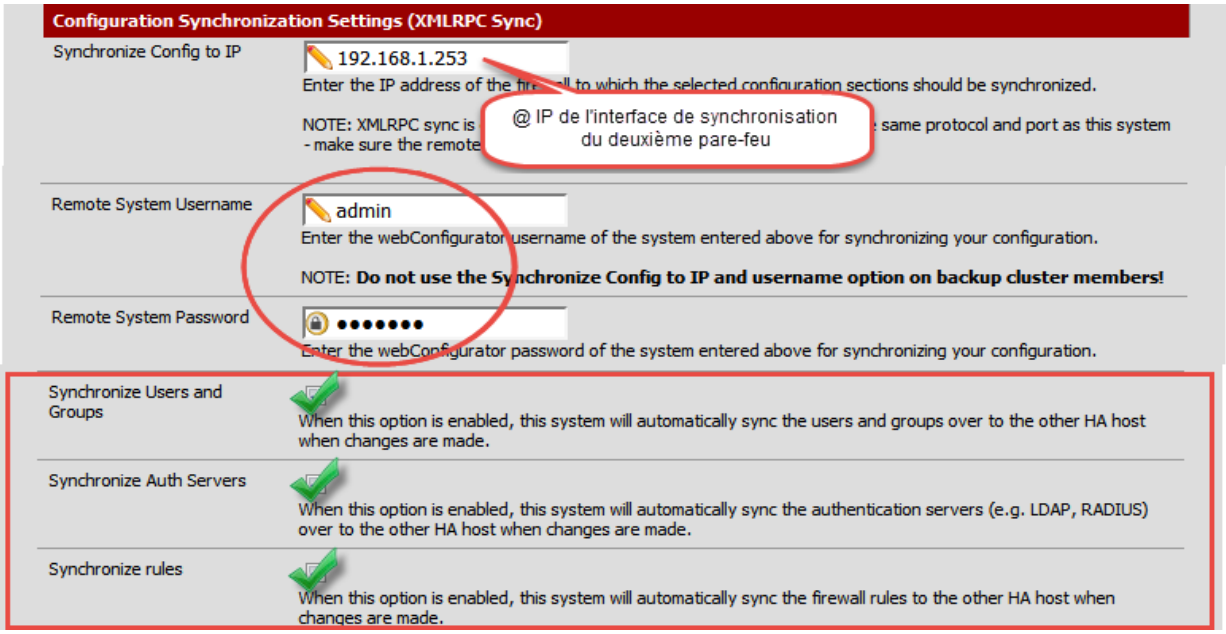

Figure 2.53: Configuration des paramètres de la synchronisation.

La configuration de la synchronisation se fait bien évidemment sur le pare-feu maître et c'est dans l'onglet **Firewall** > **Virtual IPs** | **Virtual IPs** qu'on effectue ces paramètres.

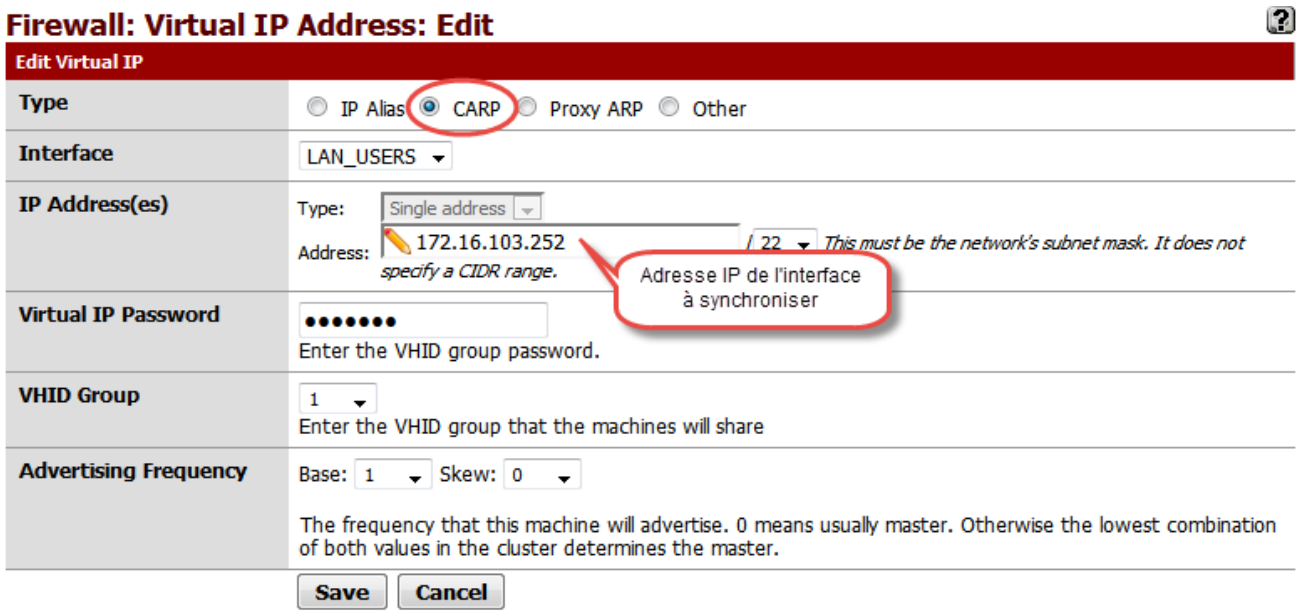

Figure 2.54: Configuration de la synchronisation sur l'interface *LAN_ USERS*.

À ce niveau, il faut définir le type, l'interface à synchroniser, le numéro de groupe VHID partagé par les pare-feu et la fréquence de réclamation (0 généralement pour maître).
Cette opération est à configurer pour toutes les interfaces existantes sur le pare-feu.

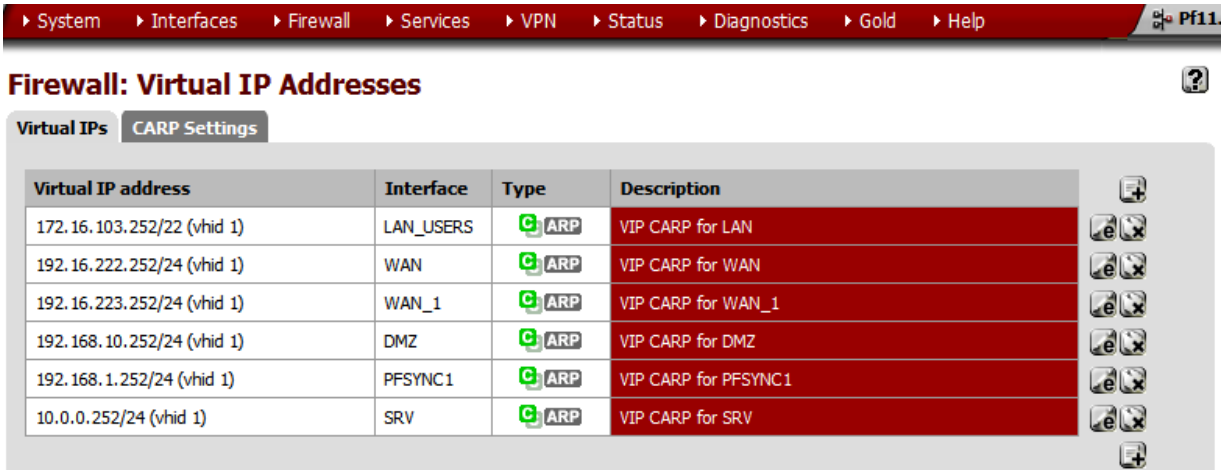

Figure 2.55: Liste des Virtual IPs créée sur le pare-feu maître.

2.10.3.3 Vérification du fonctionnement de CARP

Nous pouvons bien voir que la synchronisation est bien réussie :

- Sur le pare-feu maître : **Status | Failover**, les interfaces font partie du pare-feu maître.

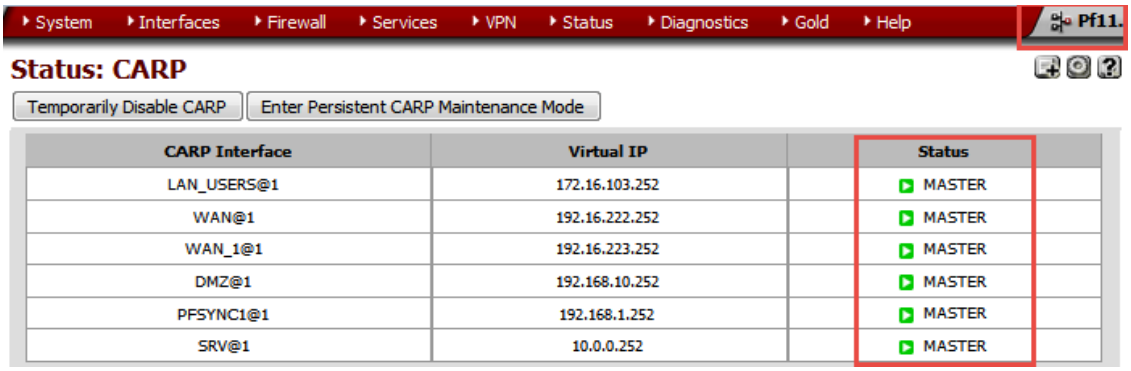

Figure 2.56: Vérification du fonctionnement de CARP au niveau du pare-feu maître.

- Sur le Slave (Slave-PfSense) : **Status | Failover**, les interfaces font partie du pare-feu esclave.

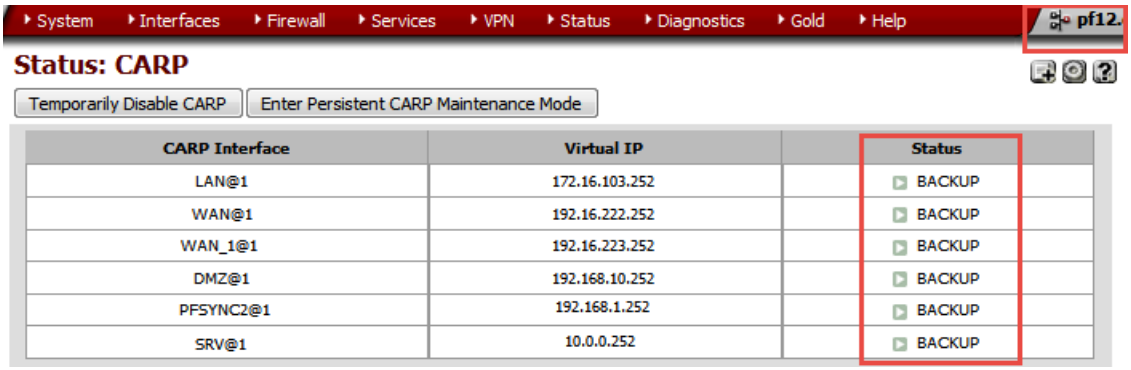

Figure 2.57: Vérification du fonctionnement de CARP au niveau du le pare-feu esclave.

Toujours sur Slave-PfSense, dans l'onglet **Firewall > Virtual IPs | Virtual IPs** nous voyons bien l'apparition automatique des IP virtuelles grâce à pfsync.

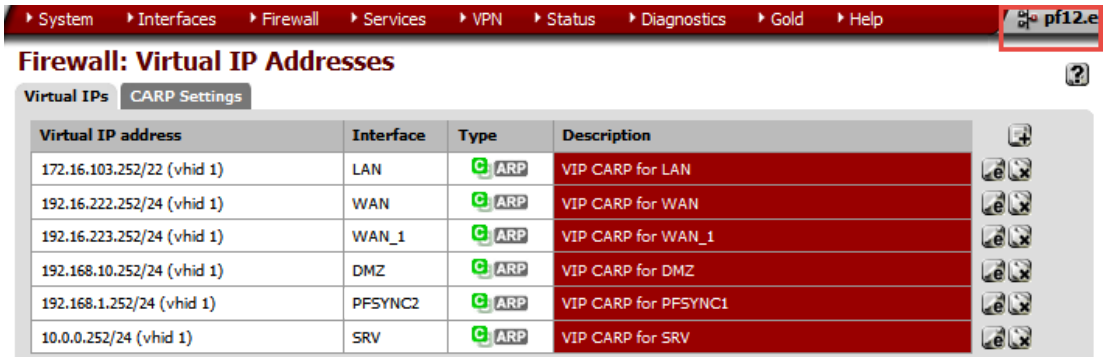

Figure 2.58: Liste des Virtual IPs créée sur le pare-feu esclave.

La synchronisation est désormais achevée. Nous pouvons le constater grâce à un test de fonctionnement.

Explication : le pare-feu pfSense maître transite l'information au départ, c'est lui la passerelle par défaut LAN. Au débranchement du LAN ou du WAN le basculement s'effectue (5 secondes Max) et l'information re-transite au travers du pare-feu pfSense esclave en attendant que le pare-feu maître soit reconnecté et opérationnel.

Ce test est illustré dans la figure suivante :

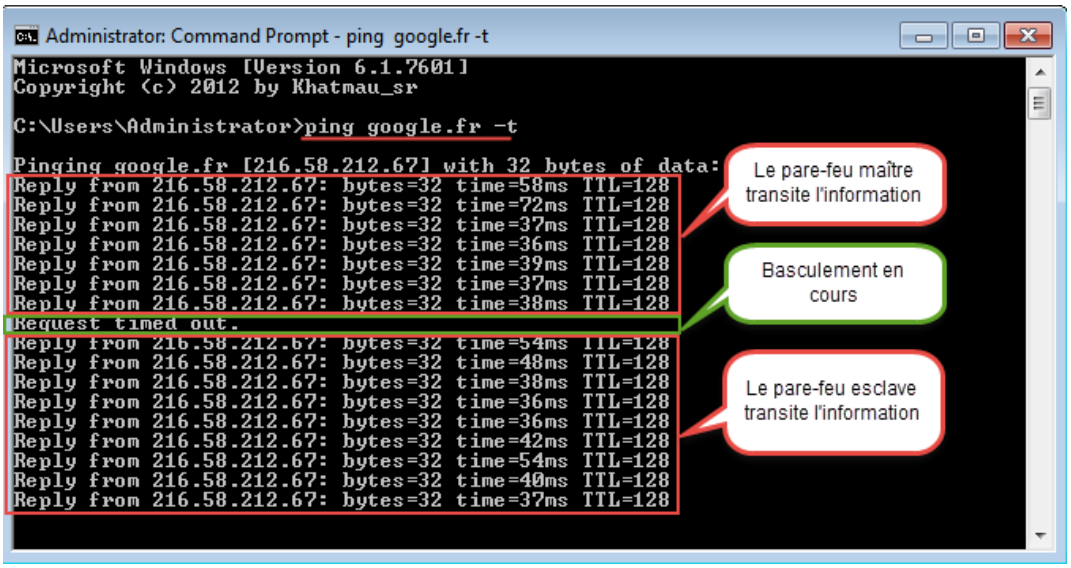

Figure 2.59: Éteinte du pare-feu maître et prise de relais par le pare-feu esclave.

conclusion

Ce chapitre nous a permis de découvrir l'environnement de pfSense et de se familiariser avec ses différents composants et services. Ceci nous a également permis de voir la puissance de cet environnement et de constater qu'il s'agit d'une solution puissante, performante et évolutive qui répond aux critères de sécurité au sein d'une entreprise.

Nous avons mis en place et testé certains services de PfSense, imposer des règles à notre pare-feu d'une part, mis en place un proxy squid et filtrer des URLs d'autres part. Tous ces avantages cohabitent parfaitement ensemble à sécuriser parfaitement le réseau d'une entreprise.

3

Liaison virtuelle VPN

Introduction

Indéniablement, internet est rentré dans les mœurs des entreprises. Les informations traversent ainsi les réseaux en clair, et là où transitent des informations de plus en plus critiques sur le réseau, la sécurité, elle, a peu évolué.

Au cours de ce chapitre, nous allons mettre en place et configurer un VPN de façon à ce que les utilisateurs du site principal de l'EPB puissent accéder aux données situées au niveau des différents sites distants de l'entreprise d'une manière transparente et vice versa.

3.1 Présentation de VPN

Un réseau privé virtuel (VPN, Virtual Private Network) connecte les composants d'un réseau sur un autre réseau. Les VPN obtiennent ce résultat en permettant à l'utilisateur de se connecter par tunnel à travers Internet ou un autre réseau public avec la sécurité et les fonctionnalités disponibles jusqu'à présent uniquement sur les réseaux privés. Il existe deux modes de fonctionnement d'un service VPN, soit en Host-to-LAN soit en LAN-to-LAN.

Un VPN Site-to-Site (ou LAN-to-LAN) permet de joindre deux réseaux de type LAN distants de manière à faire en sorte qu'ils puissent communiquer comme s'ils étaient sur le même réseau. On établit alors un VPN à travers Internet afin de joindre les deux réseaux mais également de manière à sécuriser ces flux au travers un chiffrement [19].

Un VPN est donc considéré comme un tunnel sécurisé permettant la communication entre deux entités y compris au travers de réseaux peu sûrs comme peut l'être le réseau Internet [20].

3.2 Principe de fonctionnement

Un réseau VPN repose sur un protocole appelé "protocole de tunneling". Ce protocole permet de faire circuler les informations de l'entreprise généralement de façon cryptée, d'un bout à l'autre du tunnel; ainsi les utilisateurs ont l'impression de se connecter directement sur le réseau de l'entreprise. Le principe du tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire.

Par la suite, la source chiffre les données au moyen d'algorithmes de cryptographie négociés entre le client et le serveur et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets et extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé alors qu'ils utilisent en réalité une infrastructure d'accès partagée telle que l'Internet. Les données à transmettre peuvent être prise en charge par un protocole différent d'IP, mais dans ce cas le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation [21].

3.3 Présentation d'OpenVPN

OpenVPN est un logiciel libre permettant de créer un réseau privé virtuel (VPN). Il permet à des pairs de s'authentifier entre eux à l'aide d'une clé privée partagée à l'avance, de certificats électroniques ou de couples de noms d'utilisateur/mot de passe. OpenVPN n'est pas compatible avec IPsec ou d'autres logiciels VPN. Le logiciel contient un exécutable pour les connexions du client et du serveur, un fichier de configuration optionnel et une ou plusieurs clés suivant la méthode d'authentification choisie. Ce fichier voit le jour à la fin de la configuration du canal VPN, c'est ce qui va être présenté dans ce qui suit [19].

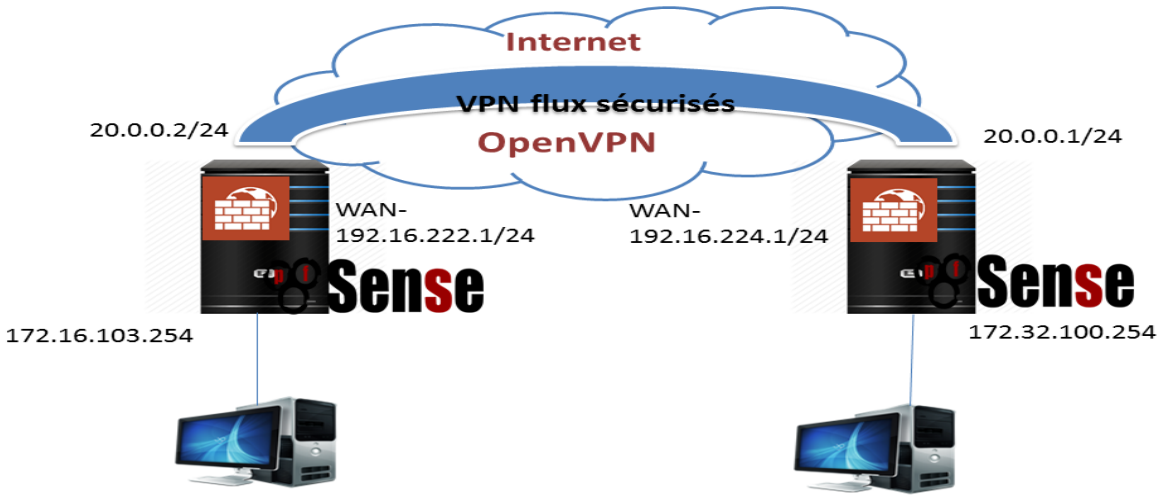

Figure 3.1: Schéma de tunneling.

3.3.1 Installation d'OpenVPN

L'installation d'OpenVPN commence par le téléchargement du package OpenVPN Client Export Utility de la même manière que les packages installés dans le chapitre précédent (Squid-Squidguard-NTOPng-SNORT).

3.3.2 Configuration d'OpenVPN

3.3.2.1 Configuration du premier serveur

Nous entamons les configurations par le pare-feu de l'EPB où nous devons ajouter un serveur depuis un poste client. Nous remplissons les champs d'informations nécessaires.

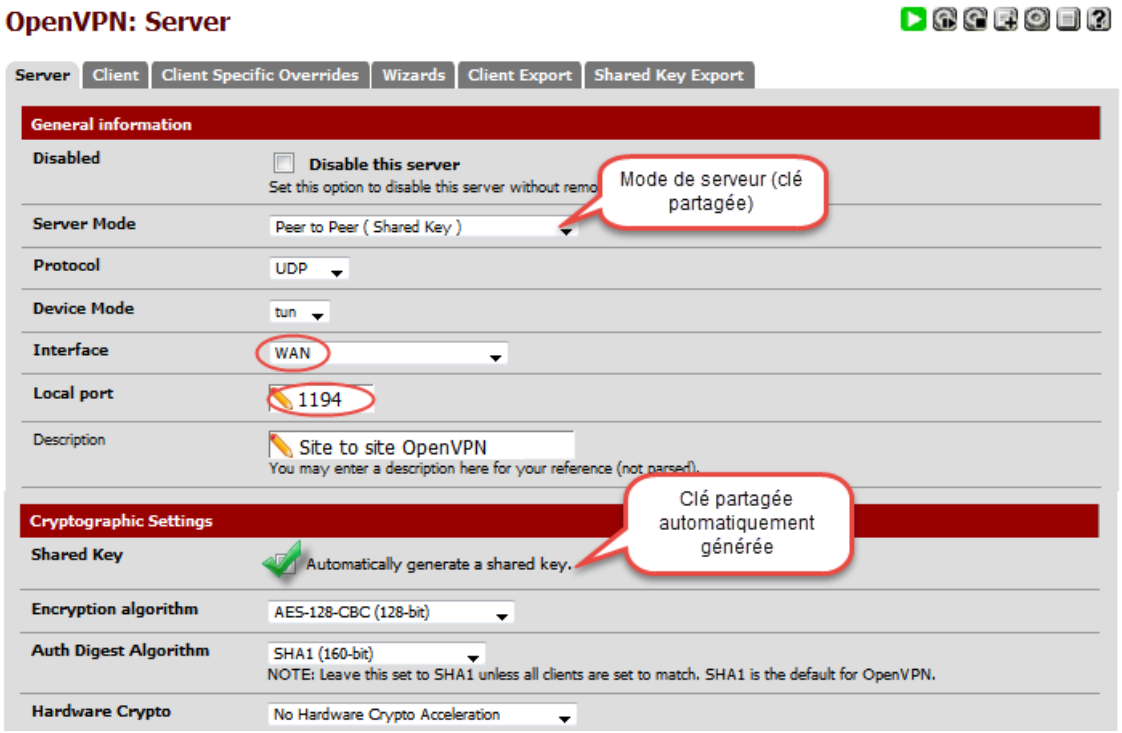

Figure 3.2: Configuration du premier serveur.

Nous devons par la suite configurer les paramètres relatives au tunnel, tels que l'adresse IP du tunnel, les plages d'adresses locales ainsi que l'adresse IP du réseau local distant.

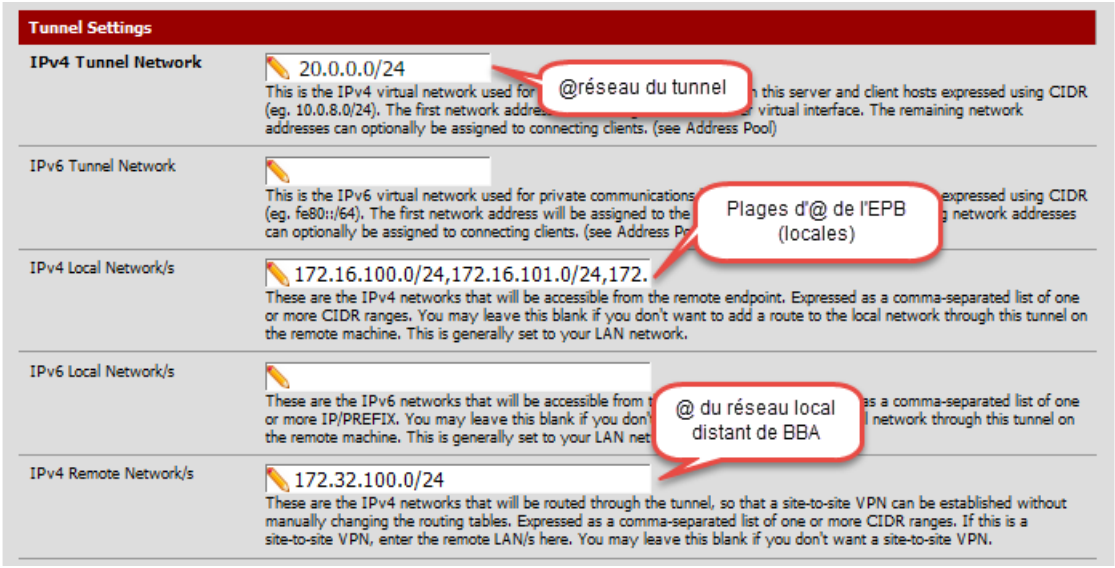

Figure 3.3: Configuration des paramètres du tunnel.

Nous remarquons que le secret (la clé partagée) a directement était généré après avoir sauvegardé ces paramètres. Nous garderons une copie de côté pour le client.

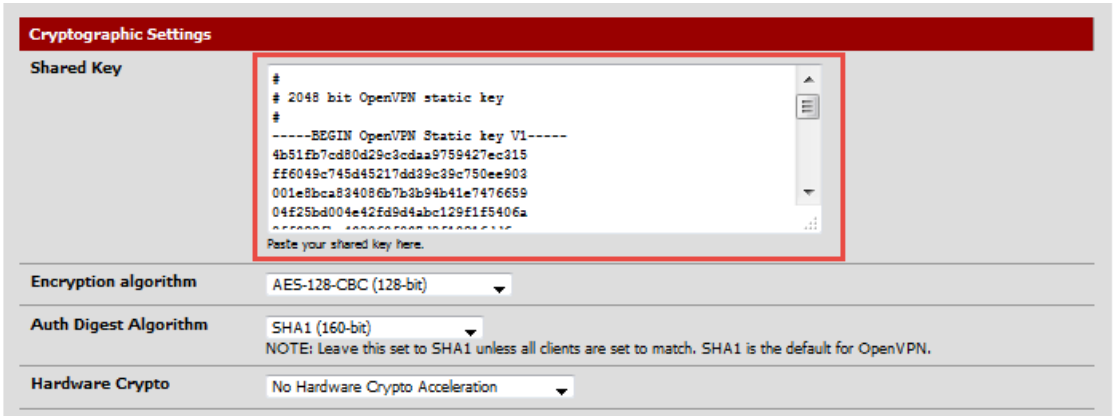

Figure 3.4: Clé générée par le serveur.

Une étape primordiale qui est la création de deux règles de pare-feu, la première sur l'interface WAN et la seconde sur OpenVPN.

La règle créée sur l'interface WAN autorise tout le trafic entre les deux sites et ce grâce à internet. Les ports source et destination sont ceux dédiés à OpenVPN (1194) et le protocole IP utilisé est TCP/UDP.

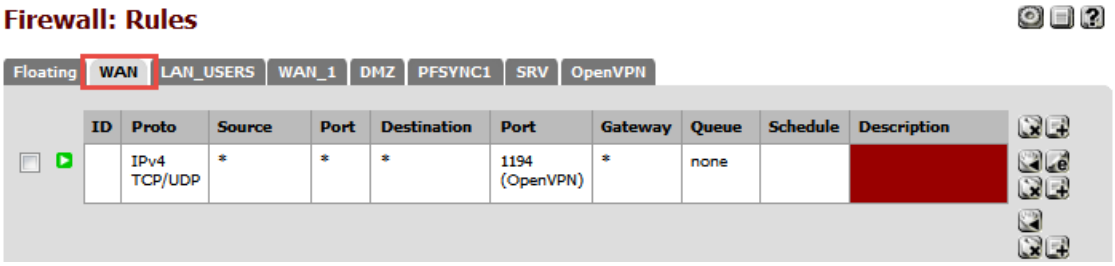

Figure 3.5: Règle de pare-feu créée sur l'interface WAN.

Cette seconde règle ajoutée sur l'interface OpenVPN permet tout le trafic sur le tunnel quelque soit la source, la destination ou le protocole.

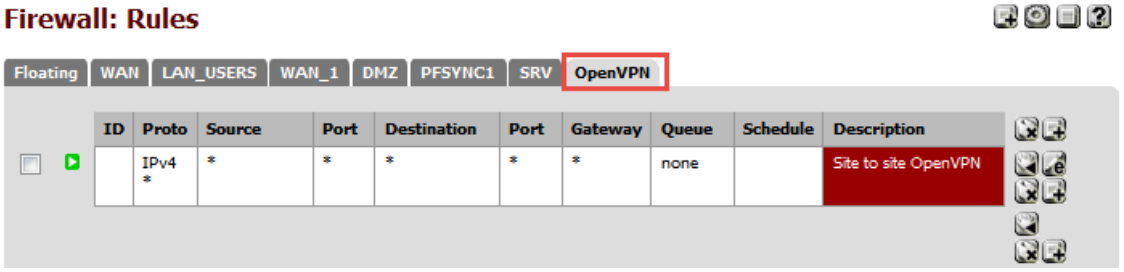

Figure 3.6: Règle de pare-feu créée sur l'interface OpenVPN.

3.3.2.2 Configuration du deuxième serveur

Nous allons maintenant nous déplacer vers le deuxième routeur Pfsense (Client OpenVPN) : À partir du client site distant de BBA on accède à l'interface Web de configuration de notre deuxième Pfsense (172.32.100.254/22) : client OpenVPN.

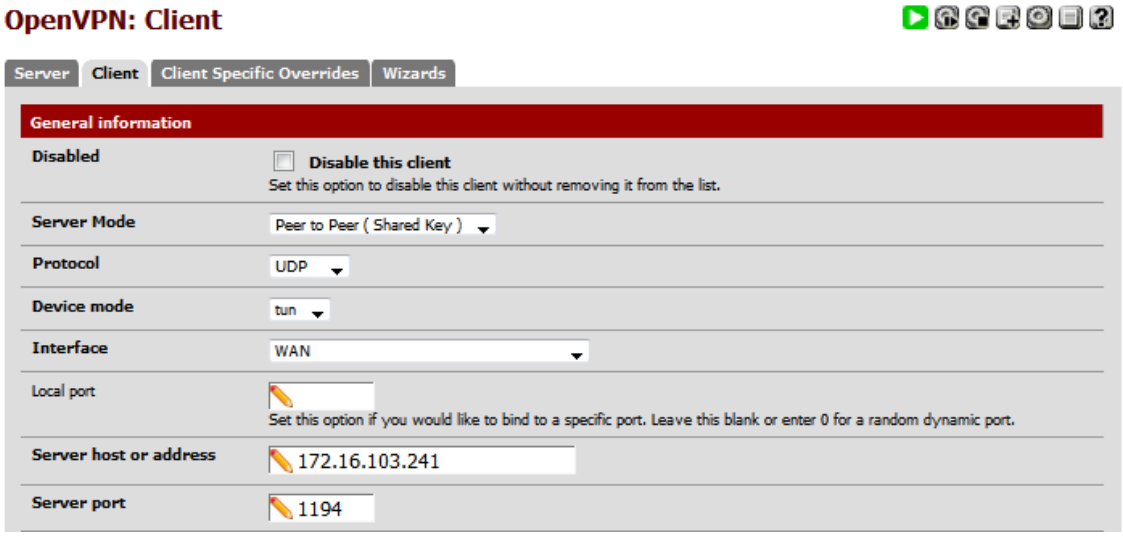

Figure 3.7: Configuration du deuxième serveur.

De la même manière que dans le premier serveur nous configurons ce deuxième, mais cette fois en récupérant le fichier contenant le secret et copier son contenu dans la zone **Shared Key** : c'est la clé partagée.

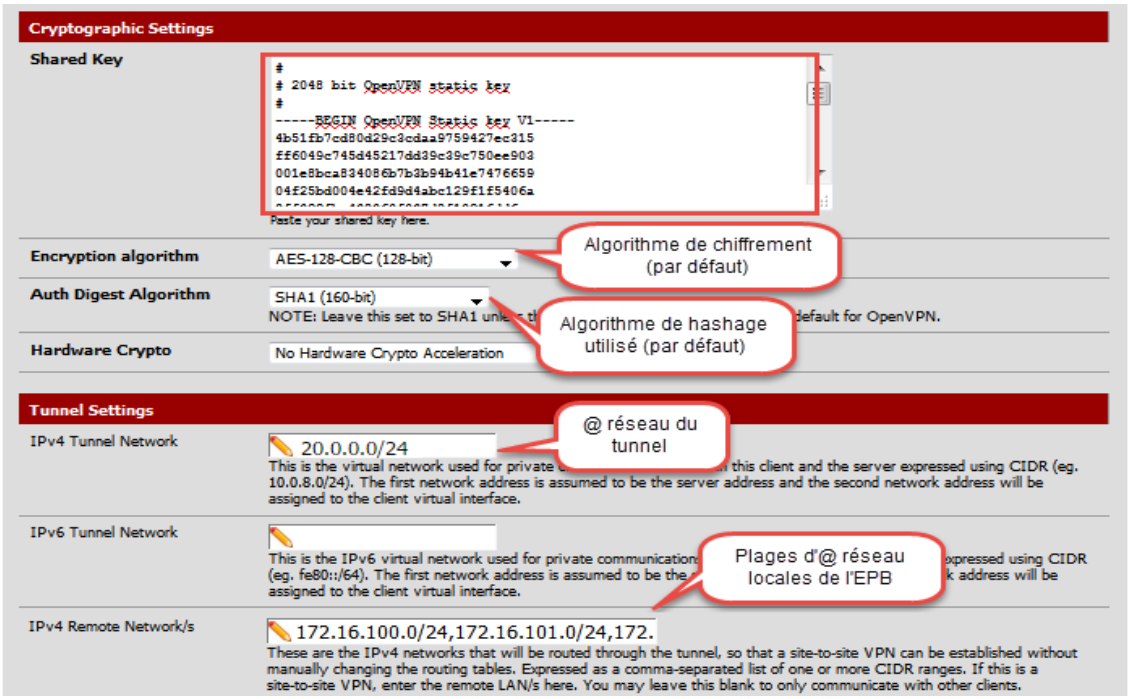

Figure 3.8: Clé partagée générée par le serveur et paramètres du tunnel.

Nous pouvons voir le client dans la liste des clients OpenVPN

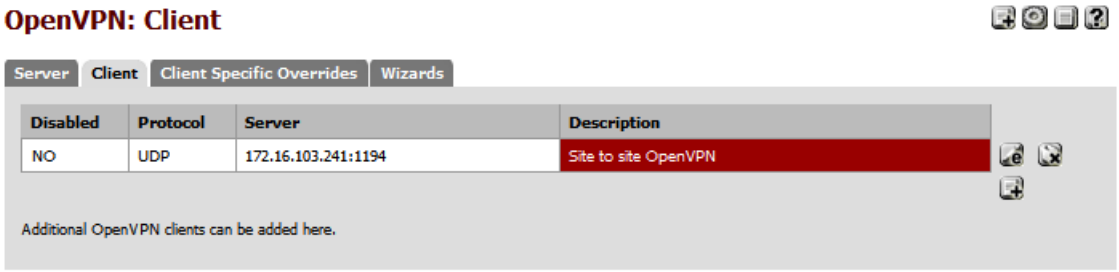

Figure 3.9: Liste des clients OpenVPN.

Les mêmes règles considérées dans le premier serveur sont aussi créées sur celui-ci avec les mêmes paramètres de configuration et sur les deux interfaces (WAN et OpenVPN).

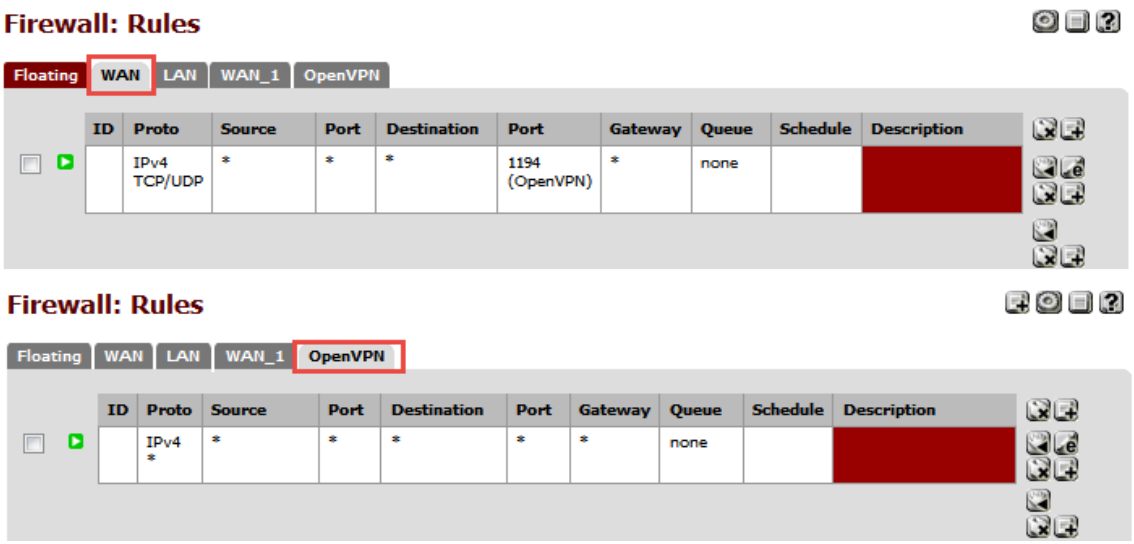

Figure 3.10: Règles de pare-feu créées sur WAN et OpenVPN.

Le client (BBA) est à présent prêt à être mit en relation avec le site de l'EPB par le biais d'Internet.

3.3.3 Test de l'état du service OpenVPN

Sur le shell d'un client du site principal de l'EPB, nous envoyons une requête " ping " vers le client BBA ayant une adresse virtuelle 20.0.0.1. Cette adresse est une adresse virtuelle et est attribuée automatiquement par OpenVPN au côté du site de BBA.

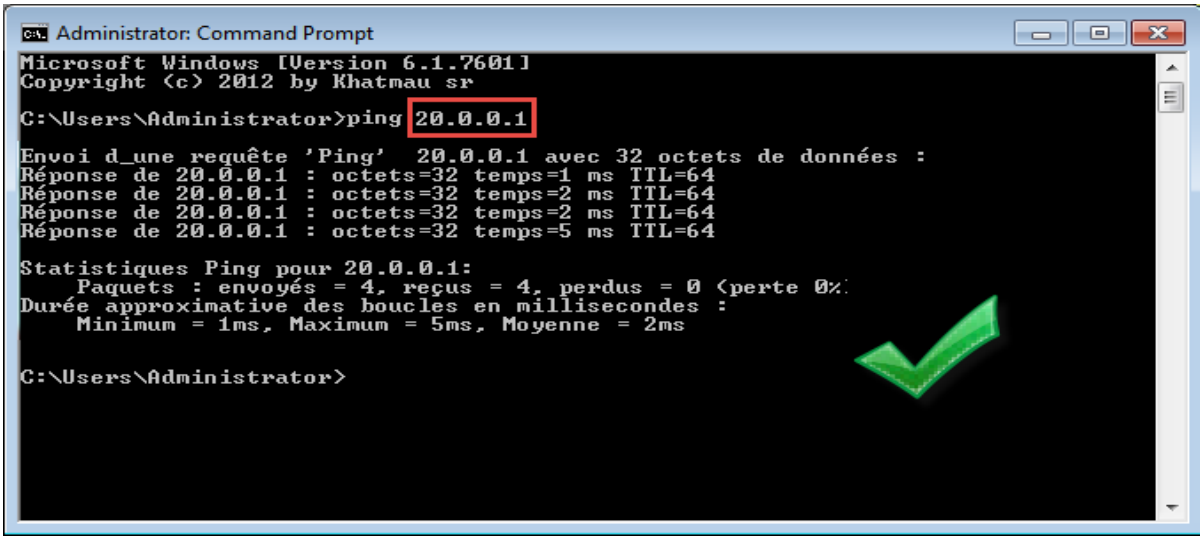

Figure 3.11: Test de fonctionnement de VPN vers le réseau de BBA

Sur le shell du client de BBA nous envoyons des requêtes “ ping ” vers le client de l'EPB ayant l'adresse virtuelle 20.0.0.2 attribuée par OpenVPN au côté du site de l'EPB.

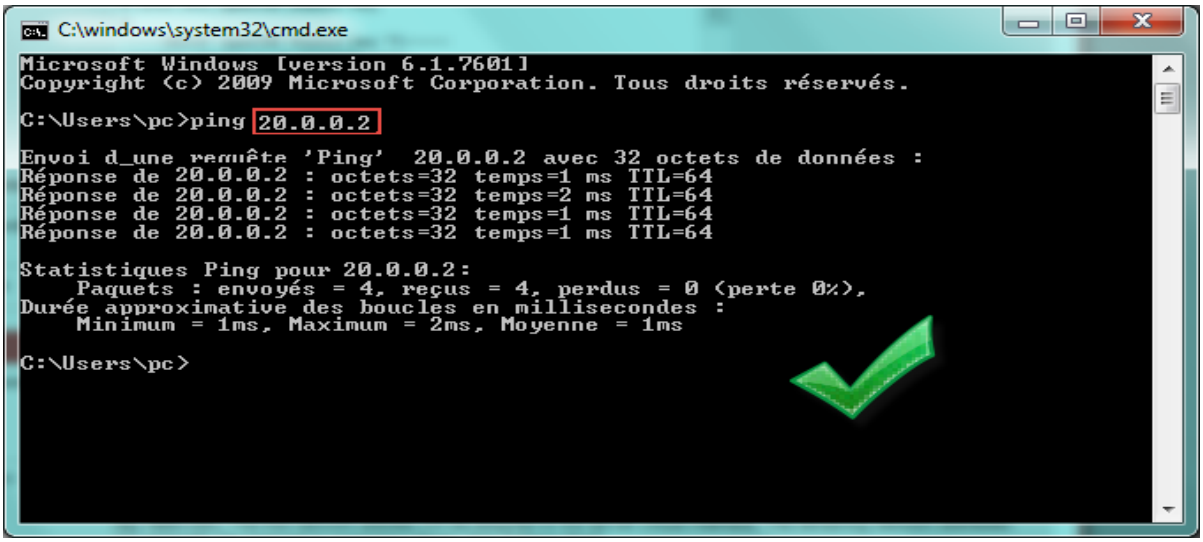

Figure 3.12: Test de fonctionnement de VPN vers le réseau de l'EPB.

Conclusion

Le besoin croissant des entreprises de communiquer entre des sites distants a donné naissance aux VPN. En effet, la raison d'être des VPN est d'offrir aux utilisateurs et aux administrateurs d'un système d'information, les mêmes conditions d'utilisation, d'exploitation et de sécurité à travers un réseau public que celles disponibles sur un réseau privé.

La mise en place de VPN site-à-site permet aux réseaux privés de s'étendre et de se relier entre eux à travers Internet. Cette solution mise en place est une politique de réduction des couts liés à l'infrastructure réseau des entreprises.

CONCLUSION GÉNÉRALE

L'informatique est devenue un outil incontournable de gestion, d'organisation, de production et de communication. Le réseau de l'entreprise met en œuvre des données sensibles, les stocke, les partage en interne, les communique parfois à d'autres entreprises ou personnes, voire les importe d'au-delà les murs. Cette ouverture vers l'extérieur conditionne des gains de productivité et de compétitivité. Il est impossible de renoncer aux bénéfices de l'informatisation, d'isoler le réseau de l'extérieur, de retirer aux données leur caractère électronique et confidentiel. Les données sensibles du système d'information de l'entreprise sont donc exposées aux actes de malveillance dont la nature et la méthode d'intrusion sont sans cesse changeantes. Les prédateurs et voleurs s'attaquent aux ordinateurs surtout par le biais d'accès aux réseaux qui relient l'entreprise à l'extérieur.

Durant le présent projet de fin de cycle, il nous a été confié la mission, au sein de l'Entreprise Portuaire de Béjaïa d'étudier et de mettre en place le pare-feu pfSense. Pour cela, notre travail a été décomposé en trois étapes majeures. La première avait pour but d'étudier le réseau LAN de l'entreprise, d'en déduire les failles de sécurité et ainsi suggérer une architecture dénouant ces problèmes.

Le second travail consistait à décrire le processus suivi pour la réalisation des solutions proposées.

Une liaison virtuelle VPN a également été mise en place et ce dans le troisième et dernier chapitre afin de lier le site principal au site distant.

L'élaboration de ce travail nous a permis, d'une part, d'approfondir nos connaissances et le savoir-faire acquis durant les quelques mois de notre formation à l'Entreprise Portuaire de Béjaïa, et d'autre part, de préparer notre intégration à la vie professionnelle et de nous nous situer sur le marché de la sécurité des réseaux.

Le travail que nous avons réalisé pourrait être complété et poursuivi sous différents aspects. En guise de perspectives nous visons :

- La virtualisation du réseau en le segmentant en VLANs.
- La mise en place d'une zone démilitarisée DMZ.
- L'établissement d'une liaison VPN Poste-à-Site.

Bibliographie

[1] Présentation de l'Entreprise Portuaire de Béjaïa, Documents internes de l'EPB.

[2] Plan de développement informatique 2015/2016, Documents internes de l'Entreprise Portuaire de Béjaïa.

[3] COSTANZO A., GRILLAT D., LEFRANCOIS L., Étude des principaux services fournis par pfSense, PfSense, 2009.

[4] The FreeBSD Project IN https://www.freebsd.org/about.html.

[5] Bernard G., Guide de mise en œuvre de pfSense v2 : Dans un cadre de déploiement spécifique, DRTIC, Mars 2012.

[6] Le Noyau : cœur du système d'exploitation IN https://doc.ubuntu-fr.org/kernel.

[7] Gateway Settings IN https://doc.pfsense.org/index.php/Gateway_Settings.

[8] Gateway Groups IN https://doc.pfsense.org/index.php/Gateway_Groups.

[9] Multi-WAN IN https://doc.pfsense.org/index.php/Multi-WAN.

[10] Firewall Rule Basics IN https://doc.pfsense.org/index.php/Firewall_Rule_Basics.

[11] Aliases IN https://doc.pfsense.org/index.php/Aliases.

[12] Schedules IN https://doc.pfsense.org/index.php/Schedules.

[13] Serveur Proxy IN http://oandreau.free.fr/supports/serveurproxy.pdf.

[14] High Avalaibility https://doc.pfsense.org/index.php/High_Availability.

[15] Squid : Optimising Web Delivery IN http://www.squid-cache.org/.

[16] Welcome to squidGuard IN http://www.squidguard.org/index.html.

[17] Ntopng : High-Speed Web-based Traffic Analysis and Flow Collection IN http://www.ntop.org/products/traffic-analysis/ntop/.

[18] TOUAHRI K., TIDJET J., Sécurité du réseau Intranet de l'université de Béjaïa : Implémentation d'une solution avec VLANs. Mémoire en vue de l'obtention du diplôme d'ingénieur d'état en Génie Informatique, 2007-2008.

[19] LEONARD P. Mobilité et Sécurité sur le réseau Réaumur : mise en place de solutions DHCP et VPN, Rapport de stage de licence RT. Bordeaux : Université de Bordeaux 1, Juin 2006.

[20] ARCHIER J-P, Les VPN : Fonctionnement, mise en œuvre et maintenance des Réseaux Privés Virtuels, Edition eni, 2013.

[21] OpenVPN Site-to-Site IN https://doc.pfsense.org/index.php/OpenVPN_Site_To_Site.

Résumé

L'informatique a atteint une prodigieuse évolution technologique dans différents domaines. L'évolution des technologies dans le monde actuel conduit de plus en plus à l'évolution du mode de travail. Les technologies peuvent rendre les taches plus souples. Cependant, la sécurité des réseaux peut en pâtir. Comment ouvrir et en même temps sécuriser les réseaux informatiques ?

Ce rapport s'attache à découvrir quels moyens existent et quelles solutions peuvent répondre aux besoins des utilisateurs qui demandent plus d'ouverture et aux administrateurs qui veulent plus de sécurité. Ce dilemme est abordé de la manière suivante : après avoir déterminé les besoins de l'entreprise, nous avons mis en place un pare-feu pfSense doté d'un système de filtrage d'URL, d'un autre pour la détection et prévention des intrusions ainsi que diverses fonctionnalités. Enfin, nous avons achevé ce travail par la création d'un tunnel VPN reliant le site de l'EPB à celui de BBA.

Mots clé : Sécurité, Pare-feu, PfSense.

Abstract

Computer technology has reached a prodigious technological developments in different areas. The evolution of technology in today's world leads more and more to the changing work mode. Technology can make tasks more flexible. However, network security may suffer. How to open and simultaneously securing computer networks?

This report seeks to find out what means exist and what solutions can meet the needs of users who demand more openness and administrators who want more security. This dilemma is addressed as follows : after determining the company's needs, we have set up a firewall pfSense with a URL filtering system , another for the detection and prevention intrusions and various features. Finally , we completed this work by creating a VPN tunnel between the site of the EPB and BBA's one.

Keywords : Security, Firewall, PfSense.