Table des matières

Liste des figures

Liste des tableaux

Introduction Générale

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. Ce besoin est accentué pour un système accessible via un téléphone public ou un réseau de données. On donne à cette collection d'outils conçus pour protéger des données et contrecarrer les pirates le nom de sécurité informatique.

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.

Il n'existe pas de frontières claires entre ces deux formes de sécurité. Par exemple, un des types d'attaque de systèmes d'information les plus médiatisés est le virus (informatique). Un virus peut être physiquement introduit dans un système via une disquette ou via Internet. Dans les deux cas, une fois le virus présent dans le système, des outils informatiques de sécurité sont nécessaires pour le détecter et le détruire.

C'est donc dans cette optique que le sujet de ce projet de mastère a été défini. Il consiste particulièrement à étudier de près le projet, d'apporter une solution permettant de faire face aux menaces pouvant affecter le réseau au sein de l'entreprise COTREL. Notre mission est de concevoir un système de sécurité composé des outils open source en assurant la haute disponibilité des services.

Pour répondre aux différentes exigences posées par le sujet, une bonne compréhension de toutes les perspectives s'avère indispensable. C'est la raison pour laquelle j'ai adopté le plan suivant :

Pour répondre aux différentes exigences posées par le sujet, une bonne compréhension de toutes les perspectives s'avère indispensable. C'est la raison pour laquelle nous avons adopté le plan suivant :

- *Le premier chapitre est un chapitre introductif consacré à une présentation générale du sujet, du cadre du projet et de l'organisme d'accueil.*

- *Le second chapitre sera consacré à l'étude de l'art de la solution de sécurité open source en assurant la haute disponibilité des services et en faisant l'implémentation de la solution firewall, serveur proxy, serveur antivirus, système de détection d'intrusions.*

- *Le troisième chapitre représente la solution à déployer.*

- *Le quatrième chapitre sera consacré à la réalisation de la solution de sécurité PFsense.*

- *Dans le dernier chapitre, on présentera des scénarios de tests afin de mettre à l'épreuve la sécurité de notre environnement.*

- *Enfin, la conclusion générale récapitulera le travail réalisé et exposera les perspectives éventuelles du projet.*

I. Présentation de l'entreprise et étude de l'existant

Dans le cadre de notre formation continue au sein de l'Université Virtuelle de Tunis pour la préparation du Diplôme Universitaire Mastère professionnel en « **N**ouvelles **T**echnologies des **T**élécommunications et **R**éseaux **N2TR »** j'ai été invité à mettre en place une solution de sécurité « firewall » au sein de COTREL suite à un stage de quatre mois.

Ce travail a été une opportunité qui m'a permis d'exercer et d'appliquer les acquis soulevés de ma formation et de me donner une approche pratique sur le domaine professionnel.

Mon projet vise à répondre aux exigences informatiques et à remédier aux problèmes d'exploitation réseau connus par l'établissement afin de garantir la sécurité et la fiabilité du système et maintenir sa qualité, sa fiabilité et sa disponibilité.

Par la suite je vais commencer par présenter l'entreprise d'accueil, l'étude de l'existant et soulever les problèmes rencontrés.

I.1 – Présentation de l'entreprise

La Compagnie Tunisienne des Ressorts à Lames (COTREL) est une société anonyme fondée en 1981, avec un capital de 8 250 000 DT dont 60% Tunisien et 40% étranger. Elle appartient au groupe Tunisien UFI group. Géographiquement, son usine et son siège social se situent dans la zone industrielle de BORJ EL CEDRIA et elle couvre une superficie totale de 30 000 m2 dont 12 000 m2 couverts.

Selon la typologie adoptée par la promotion de l'industrie, la société COTREL est classée dans le secteur « Industrie mécanique et métallurgique » dans la branche d'activité « Industrie automobile ». Elle est spécialisée dans la conception, fabrication et vente de ressorts à lames de suspension conventionnels et paraboliques pour tous véhicules motorisés ou tractés. COTREL a acquis son savoir-faire de la société japonaise NHK, premier fabricant mondial de ressorts à lames pour suspension de véhicules.

La société COTREL a signé en 2011 un partenariat avec une entreprise espagnole spécialisée dans le même secteur (FUNVERA) pour constituer une nouvelle entreprise appelée CAVEO. Ainsi que COTREL compte un effectif de plus de 502 employés dont 82 cadres.

Actuellement, la société occupe une position stratégique au cœur du marché international des ressorts à lames caractérisé par son aspect concurrentiel. En effet, elle assiste les clients dans la phase de conception des nouveaux produits, assure la bonne qualité de ses produits et montre une maîtrise de sa logistique.

Grâce à la qualité de ses produits et à son savoir-faire dans la conception et le développement, COTREL a pu conquérir des marchés dans toute l'Europe comme le montre la figure (1.1).

Figure 1.1 : les marchés de COTREL

Les clients de COTREL peuvent être répartis selon le type des ressorts à lames :

- ✓ Véhicules utilitaires légers :

  FIAT / PEUGEOT / CITROËN / VOLKSWAGEN / IVECO

- ✓ Camions moyens et poids lourds :

  IVECO / SCANIA / MAN / SICAME/DAIMLER(Mercedes)

➢ Organisation de l'entreprise

Comme la plupart des grandes entreprises industrielles, COTREL fait la distinction entre le travail de l'usine et celui de l'administration. Cependant toutes les distinctions se réunissent dans le but de satisfaire les clients en termes de qualité, coûts délais et pérennité de l'entreprise.
L'organisation de COTREL est représentée par l'organigramme (figure 1.2) suivant :

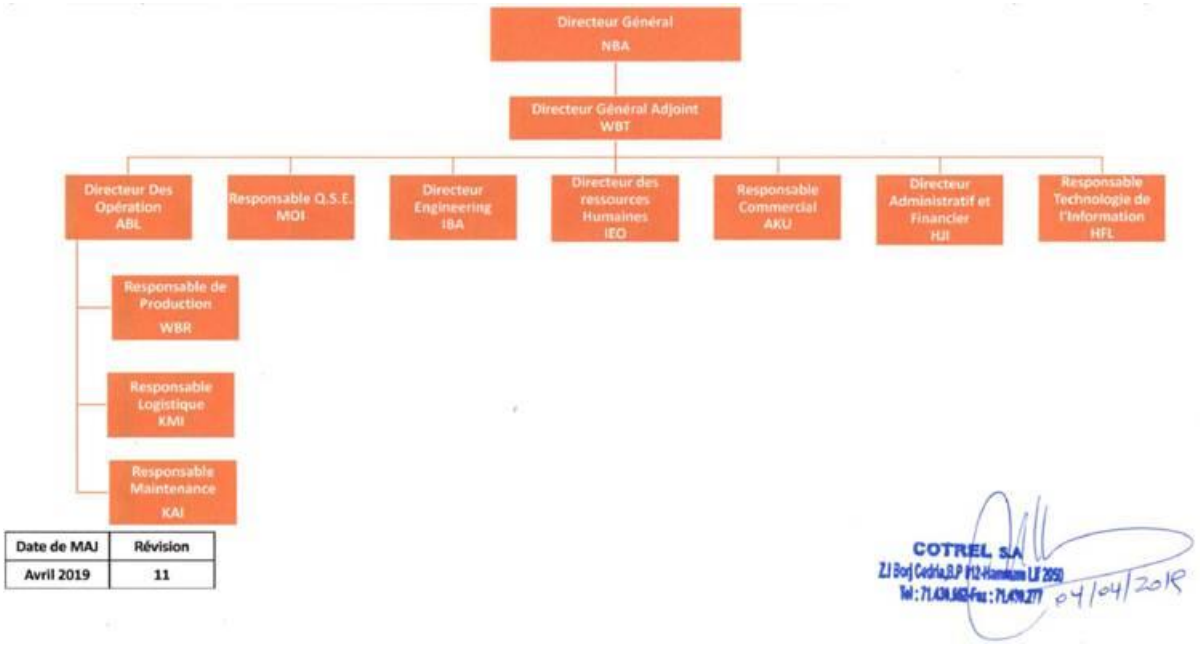


Figure1.2 : Organigramme de la société COTREL

Grâce à cette répartition structurée, COTREL assure une complémentarité entre les différents départements ce qui assure une bonne organisation amenant à une bonne qualité du produit. Chaque département assure l'exécution des tâches suivantes :

- **Le département Engineering :** *Elle assure la recherche et le développement des nouveaux produits ou bien l'amélioration des produits existant. Elle étudie l'industrialisation en développant les processus de fabrication.*

- **Le département Qualité, Sécurité et Environnement :** *Elle vise à intégrer la qualité dans toutes les fonctions de l'entreprise, atteindre le zéro défaut tout en se conformant aux normes des clients, ainsi que l'amélioration de l'environnement du travail et le recyclage des déchets tout en se conformant aux réglementations.*

- **Le département Industrielle :** *Elle assure l'organisation, la mise en œuvre, l'optimisation et le suivi de la fabrication suivant des objectifs déterminés à savoir : le coût, les délais, la qualité et la quantité.*

- **Le département Commerciale :** *Elle vise à augmenter le chiffre d'affaires et la part du marché avec des produits, services et clients diversifiés tout en ayant un rôle très important pour l'acquisition de nouveaux marchés et avoir de nouveaux clients.*

- **Le département Financière :** *son rôle consiste à assurer la gestion financière de l'entreprise. Elle s'occupe essentiellement de l'élaboration et le suivi des budgets, la tenue des comptes, la gestion de la trésorerie et l'accomplissement des opérations financières.*

- **Le département des Ressources Humaines :** *Elle sélectionne et développe le potentiel humain pour garantir l'occupation et la continuité des fonctions tout en assurant la satisfaction et la sécurité au travail du personnel.*

- **Le département Logistique :** *Elle garantit les livraisons à temps et planifie les exports tout en optimisant le niveau de stock de matière primaire, des accessoires et des produits finis, à toutes les étapes.*

- **Le département de Production :** *son rôle consiste à assurer l'optimisation, l'utilisation de la capacité et des moyens de production en garantissant l'amélioration permanente de la productivité et de la qualité.*

- **Le département de Maintenance :** *Il veille à installer et maintenir en bon état les équipements et tous les biens de COTREL tout en améliorant leurs performances et leurs durées de vie.*

- **Le département Informatique :** Les Services de l'informatique doivent s'assurer d'un choix ainsi que d'une utilisation cohérente et conviviale, dans un souci d'efficience et d'efficacité, des réseaux, des systèmes collectifs, des logiciels de gestion et des équipements ou du matériel informatique requis par la commission scolaire afin de répondre aux besoins des services et des établissements pour l'atteinte des objectifs corporatifs

I.2 - Etude de l’existant

Il est essentiel de disposer d'informations précises sur l'infrastructure réseau physique et les problèmes qui ont une incidence sur le bon fonctionnement du réseau. En effet, ces informations affectent une grande partie des décisions que je vais prendre dans le choix de la solution et de son déploiement.

L’existant est décrit selon les points suivants :

- L’antivirus utilisé possède l’architecture client/serveur et il est propriétaire. Cela montre le coût élevé dépensé pour avoir les mises à jour de manière permanente, sinon, ce dernier devient obsolète et les machines deviennent exposées facilement aux virus, vers, chevaux de Troie, et aux logiciels malveillants ayant comme effet de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté.

- Les machines des employés sont protégées par le firewall software existant par défaut au niveau de système d’exploitation Windows.

- Lenteur des machines à cause de l’état critique de l’infrastructure réseau et la congestion de la bande passante.

- Manque de stratégie de sécurité. Ce qui implique l’absence de la mise en œuvre des mécanismes de sécurité, des procédures de surveillance des équipements de sécurité, des procédures de réponse aux incidents de sécurité et des contrôles et audits de sécurité.

- Utilisation des applications de proxy pour contourner les restriction l'accès au site web

I.3 - Critique de l’existant et problèmes soulevés

Suite à une étude du système actuel utiliser au sein de COTREL, j’ai pu relever un certain nombre de risques potentiel important. Alors que l'informatique est devenue pour l'entreprise un outil

incontournable de gestion, d'organisation, de production et de communication, les données mises en œuvre par le système d'information ainsi que les échanges internes et externes sont exposées aux actes de malveillance de différentes natures et sans cesse changeants. Le réseau de l'entreprise est exposé aux risques suivants :

- Les données irrémédiablement perdues ou altérées, ce qui les rend inexploitables.
- Les données ou traitements durablement indisponibles, pouvant entraîner l'arrêt d'une production ou d'un service.
- Divulgation d'informations confidentielles ou erronées pouvant profiter à des sociétés concurrentes ou nuire à l'image de l'entreprise.
- Déclenchement d'actions pouvant provoquer des accidents physiques ou induire des drames humains.

I.4 - Cahier des charges

La solution proposée doit répondre aux attentes suivantes :

- Doit empêcher l’accès par des personnes tiers au réseau.
- Doit permettre l’accès au WAN par les salariés.
- Doit restreindre l’accès des salariés à des sites nocifs
- Doit conserver un rapport des accès réseau entrant et sortant.
- Doit être gratuit.

II. Etude de l’art : Solutions de sécurité et de filtrage

II.1 La sécurité des réseaux et des systèmes.

Le réseau de l'entreprise met en œuvre des données sensibles, les stocke, les partage en interne et les communique parfois à d'autres entreprises ou personnes.

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 ou de risquer la confidentialité des données de l’entreprise.

Les données sensibles du système d'information de l'entreprise sont donc exposées aux actes malveillants dont la nature et la méthode d'intrusion sont sans cesse changeantes.

Les hackers s'attaquent aux ordinateurs surtout par le biais d'accès aux réseaux qui relient l'entreprise à l'extérieur.

Les moyens de la sécurité adoptée :

- Portail captif (mécanisme d’authentification) : cette interface va jouer le rôle d’une passerelle sécurisée dans le but d’authentification avant l’accès Internet.
- VPN c’est un tunnel sécurisé.
- Système de détection et prévention d’intrusion réseau (SNORT) : pour protéger le système d’information de la Société contre les attaques.
- Partage de bande passante (TRAFFIC SHAPER) et supervision de bande passante (NTOP).
- Filtrage URL (SquidGuard) : va permettre à la société d’appliquer la politique de sécurité pour l’autorisation de l’accès aux sites web.
- Mise en place d’un serveur proxy (proxy cache)
- Contrôler et limiter les droits des utilisateurs.
- L’utilisation de protocoles IP sec, SSL/TLS ou encore HTTPS (protocoles réseaux permettant de sécuriser les accès distants par chiffrement des données transmises).
- Chiffrement : méthode de codage/décodage des données mettant généralement en œuvre un mécanisme de clé(s) logique(s) afin de rendre impossible la lecture d’un fichier à des tiers qui ne possèdent pas la ou les clé(s).
- Tolérance de panne : dispositif de sécurité mis en œuvre notamment au niveau des disques durs qui permet de se prémunir de la panne d’un disque en évitant l’arrêt des applications ou l’endommagement des données stockées.
- La haute disponibilité.
- Détecteur d'intrusions est un système capable de détecter une tentative d'intrusion sur votre système. Il stoppe la majeure partie des attaques recensées. L'IDS écoute le trafic réseau et analyse les paquets pour prévenir des actions suspectes et les arrêter.
- Cryptage des données.

II.2 Technologies et Solutions de sécurité

Les pares-feux sont utilisés principalement dans quatre buts :

- Se protéger des malveillances externes : En effet, pour se protéger des malveillances externes, les Firewalls écartent divers intrus :
- Les curieux qui génèrent du trafic, font plus de peur que de mal, mais qui quelquefois finissent par coûter cher,
- Les vandales qui saturent les liaisons, corrompent les données, etc.
- Les espions2.
- Éviter la fuite d'information non contrôlée vers l'extérieur.
- Surveiller les flux internes/externes : Tous les flux du trafic entre le réseau interne et externe doivent être surveillés. Cela permet d'avoir une vue sur la consommation Internet des différents utilisateurs internes et de bloquer l'accès à certains sites contenant des informations illégales.
- Faciliter l'administration du réseau : Sans firewall, chaque machine du réseau est potentiellement exposée aux attaques d'autres machines d'Internet. Les firewalls simplifient la gestion de la sécurité et donc l'administration du réseau car ils centralisent les attaques potentielles au niveau du firewall plutôt que sur le réseau tout entier.
  - ✓ De nombreux Firewalls existent sous tous les systèmes d'exploitation. Le choix s'est fait en partie du fait de la contrainte des services offerts, sa fiabilité et qu'il soit très répandu dans le monde de l'entreprise.

Notre étude comparative se base sur les Firewalls suivants :

- **Smoothwall Express** : est un projet qui a été initié au Royaume-Uni à l'été 2000 par Lawrence Manning (principal développeur de code) et Richard Morrell (Manager du projet). Leur idée de base était de créer une distribution Linux qui pouvait convertir un ordinateur personnel en un équipement pare-feu. La première version du pare-feu Smoothwall a été postée au Sourceforge.net en Août 2000. La communauté s'est élargie depuis et le produit Smoothwall a aussi évolué.

Il faut noter que la distribution Smoothwall est Open Source et distribué sous licence GPL. C'est un système d'exploitation basé sur RedHat Linux (devenu plus tard Fedora Core Project).

- **IPCop** : est à l'origine un fork de Smoothwall Express. Ceci signifie qu'IPCop est basé sur linux Redhat. La première version est sortie en décembre 2001. Aujourd'hui on est à la version 2.0.6. IPCop est distribué sous licence GPL.
- **Vyatta Community Edition** : La solution pare-feu de la société Vyatta existe en deux exemplaires. Le premier est payant, le second est libre. On note que la version commerciale est plus souvent maintenue et mise à jour que la solution libre (environ une mise à jour tous les six mois). Le produit commercialisé est en outre toujours stable ce qui n'est pas forcément le cas pour la version libre, dénommée Vyatta Community Edition et dont la dernière version est la version 6.5 issue en Octobre 2012.
- **Endian** : est une distribution de sécurité open source dont le but est d'obtenir une distribution Linux complètement dédiée à la sécurité et aux services essentiels d'un réseau afin d'offrir une protection maximale contre le vol de données, virus, spyware, spam et autres menaces Internet. Plus concrètement, Endian intègre un firewall qui va jouer le rôle d'intermédiaire entre un réseau considéré comme non sûr (Internet) et un réseau que l'on souhaite sécuriser (le réseau local par exemple), tout en fournissant des services permettant la gestion et le suivi de celui-ci qui seront gérer à travers une interface web (Unified Threat Management UTM).

Le firewall d'Endian Firewall se compose de plusieurs interfaces dont chacune peut être ou non utilisée :

- Rouge : Zone du réseau à risque (Internet).
- Verte : Zone du réseau à protéger (réseau local).
- Bleu : Zone spécifique pour les périphériques sans fil (wifi). Il n'est possible de faire communiquer l'interface Verte et l'interface Bleu qu'en créant un VPN.
- Orange : Zone démilitarisée (DMZ), cette zone isolée, hébergeant des applications mises à disposition du public. Elle est accessible de l'extérieur mais ne possède aucun accès sortant (serveur web, un serveur de messagerie, un serveur FTP public, etc.).
- **PFsense** : est basé sur une distribution FreeBSD3 adapté pour être utilisé comme un pare feu et un routeur. Le projet débuta en 2004 avec le projet m0n0wall qui s'axer plus vers des installations sur ordinateur à part entière plutôt que la mise au point du matériel embarqué de m0n0wall. PFsense inclue de nombreuses fonctions qui sont fournis par les pare feux commerciaux payants et d'autres qui ne sont disponibles que sur PFsense :
- Pare feu,
- Translation d'adresse et de port,
- Redondance,

- **CARP** : CARP sur Open BSD permet un basculement matériel. Deux ou plusieurs parent feu peut être configuré comme un groupe de basculement. Si un problème est rencontré dans le premier alors le second prend le relais. PFsense comprend également des options de synchronisations, lorsque des modifications sont apportées sur le premier, celles-ci sont synchronisées automatiquement sur le second.
- **Pfsync** : Pfsync assure la réplication des tables d'états sur tous les pares-feux se trouvant dans le groupe de basculement. En cas de problème, les connexions existantes seront maintenues car elles seront rebasculées vers un autre pare feu, évitant les perturbations du réseau.
  - Equilibrage de charge entrante et sortante,
  - VPN, IP sec, OpenVPN,
  - RRD Graphs Reporting,
  - Portail Captatif,
  - Relai et serveur DHCP.

II.3 Étude et choix de la solution

Critère	**Coefficient (1-2-3)**	**PFsense**	**Smoothwall**	**Endian**	**Vyatta**	**IP cop**
Filtrage et sécurité	3					
Avec état		x	X	X	X	X
Filtrage d'URL		X	X	X	X	X
Filtrage contenu web		X	X	X	X	X
Temps d'accès par utilisateur		-	X	-	-	-
IDS		X	X	X	X	X
Antivirus WEB (HTTP/FTP)		X	X	X	-	X
Email Antivirus/Antispam		X	X	X	-	X
Routage	3					
NAT (dynamique)		X	X	X	-	X
Port address translation		X	X	X	-	X
Politique de routage (Policy Routing)		X	-	X	X	-
Licence		BSD	GPL	GPL	GPL	GPL

Ergonomie	2					
Interface graphique		X	X	X	X	X
Taille en Mo	1	88.8	33.78	119.24	165.23	47.23
Haute disponibilité	3					
Load Balance		X	-	-	X	-
Multi Wan		X	-	X	X	-
Capacité de failover		X	-	X	X	-
Facilité de configuration	2	X	X	-	-	X
Facilité de surveillance/journaux	2	X	-	X	X	X
Performance et consommation réseau	2	X	X	X	X	X
Service	2					
Proxy web		X	X	X	X	X
Proxy POP3		-	X	X	-	-
Proxy SIP		-	X	X	-	-
DHCP		X	X	X	X	X
DNS		X	X	X	X	X
TELNET		-	-	X	X	X
SSH		X	X	X	X	X
VPN		X	X	X	X	X
QoS	1					
Priorité selon type de trafic		X	X	X	X	X
Lissage de trafic (limitation)		X	X	X	X	X
Administration	2					
Recherche de mise à jour		X	X	X	-	-
Mise à jour automatique		X	-	X	-	-
Back up		X	X	X	X	X

Add on		X	X	X	-	X
Note		**17**	**11**	**14**	**10**	**9**

Tableau 1.1: Etude comparative des Firewalls

Au vu de ce comparatif, PFsense apparait comme le meilleur compromis entre ces pare feux.
Ce qui séduit chez PFsense c'est la facilité d'installer et configurer des outils d'administration réseau. En effet, il est possible de configurer quasiment toutes les fonctionnalités des services proposés par une interface Web PHP unique : Pas d'interface graphique Gnome ou KDE4, etc. qui alourdiraient le système proposé, juste l'essentiel !
C'est cette solution qui répond le mieux au critère de :

- Disponibilité.
- Confidentialité (HTTPS authentification, IPSEC…).
- Auditabilité (système upgradable sans réinstallation, packages téléchargeables directement depuis le webGUI …).
- Mise à jour.
- Simplicité d'installation.
- Autonomie complète.
- Support : dynamisme au niveau du support.

PFsense représente une solution pare feu qui gère plusieurs services. Elle permet de consommer moins de ressources puisqu'elle possède déjà d'un serveur proxy, un serveur antivirus, et un mécanisme de détection / prévention d'intrusion.
Les services proposés

- Système de basculement par le protocole CARP.
- Proxy, Blacklist SQUID et SQUIDGuard
- IDS-IPS Snort
- Antivirus ClamAV

II.4 Présentation technique de la solution retenue

La gestion des serveurs distants et le monitoring de ses équipements étant le plus grand souci de l'administrateur. J'ai jugé nécessaire de mettre en évidence un outil pour contrôler le

fonctionnement du réseau, d'étudier les données collectées et de définir des seuils d'alertes qui peuvent servir pour le déclenchement des alertes lors de détection des problèmes.
Il s'agit donc et sans doute d'une mise en place d'un composant firewall. Notre choix porte sur le logiciel PfSense Open Source qui pourra, grâce à ses différentes fonctionnalités, d'apporter la sécurité nécessaire au réseau local de l'entreprise et de détecter les tentatives d'intrusion.
Le firewall propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau, et d'utiliser ainsi convenablement le réseau de la société. Ceci doit se réaliser sans encombrer le réseau avec des activités non essentielles.

PfSense ou « Packet Filter Sense » est un routeur/firewall open source base sur le système d'exploitation FreeBSD réputé pour son extrême stabilité et Monowall auquel il rajoute ses propres fonctionnalités.

Ce qui séduit chez Pfsense est sa facilité d'installation et de configuration des outils d'administration réseau. En effet est possible de configurer quasiment toutes les fonctionnalités de Pfsense via l'interface Gui PHP.

La distribution Pfsense met ainsi à la disposition de l'administrateur réseau une multitude d'outils open sources permettant d'optimiser ses taches.

Services proposés :

- Système de basculement (failover)
- VPN site à site avec Openvpn et Ipsec
- VPN client PPTP
- VPN point à point avec Stunnel
- Proxy et Blacklist (Squid et SquidGuard)
- ISD avec Snort
- Répartition des charges avec Loadbalancer
- Partage de la bande passante avec Traffic shaper
- Vue sur la consommation de la bande passante avec bandwithd et Ntop
- Portail captif avec captive portal
- Rapport et monitorage
- Information temps réel

III. Présentation et déploiement de la solution

III.1 Présentation de la topologie actuelle

Dans cette section je vais présenter la Topologie réseau actuelle de COTREL est d'identifier les types de connexion entre les équipements réseaux.

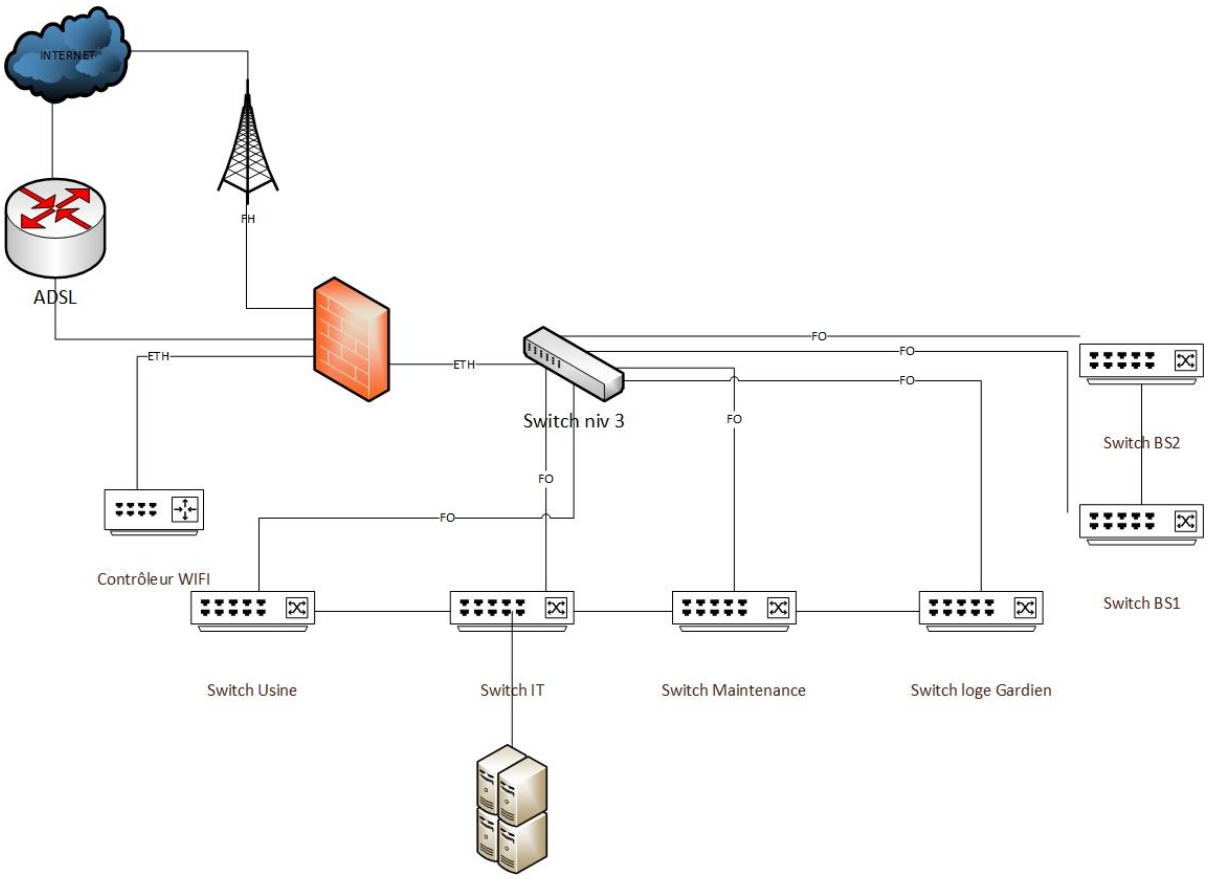


Figure 3.1 : Topologie réseau de COTREL

Comme le montre la figure ci-dessous la topologie réseau utilisée chez COTREL est une topologie Réseau en étoile. Par la suite je vais dégager les différents équipements réseaux :

- 01 switch de type CISCO Catalyst 3850 de niveau 3 pour l'interconnexion des différents switches de l'entreprise
  → Liaison en fibre Channel entre le switch Cisco et les switch HP

- 06 switch de type HP 1800 de niveau 2 pour la liaison Ethernet des utilisateurs, machines automates et points d'accès wifi.

- Firewall Watch Guard

- ADSL Global Net et faisceau hertzien de Ooredoo pour garantir la redondance et la tolérance au panne dans le cas où l'une d'entre eux ne fonctionne pas.

La partie adressage est segmenter selon les Vlans :

- Vlan administratif :
  192.168.10.1 → 192.168.10.253
  Masque sous réseau 255.255.255.0
  Gateway 192.168.10.254

- Vlan usine :
  192.168.12.1 → 192.168.12.253
  Masque sous réseau 255.255.255.0
  Gateway 192.168.12.254

- Vlan MES :
  192.168.13.1 → 192.168.13.253
  Masque sous réseau 255.255.255.0
  Gateway 192.168.13.254

- Vlan maintenance :
  192.168.14.1 → 192.168.14.253
  Masque sous réseau 255.255.255.0
  Gateway 192.168.14.254

- Vlan serveurs :
  192.168.1.1 → 192.168.1.25
  255.255.255.0
  Gateway 192.168.1.254

De même pour les SSID du WIFI

- ✓ SSID COTREL-ADM → Vlan 10

- ✓ SSID COTREL → Vlan 11 réserver pour les IT (accès RDS aux serveurs et au console d'administration)
- ✓ SSID COTREL-USINE → Vlan 12
- ✓ SSID COTREL-MAINTENANCE → Vlan 14

III.2 Présentation de la topologie

Selon le nombre des employés et la quantité de trafic réseau, COTREL est classifié au niveau des moyennes entreprises. Ainsi, l'architecture réseau qu'on va l'implémenter est composée de serveur proxy, serveur antivirus, système de détection d'intrusion. Ces composants sont mis derrière deux firewalls afin d'assurer la haute disponibilité et la tolérance aux pannes

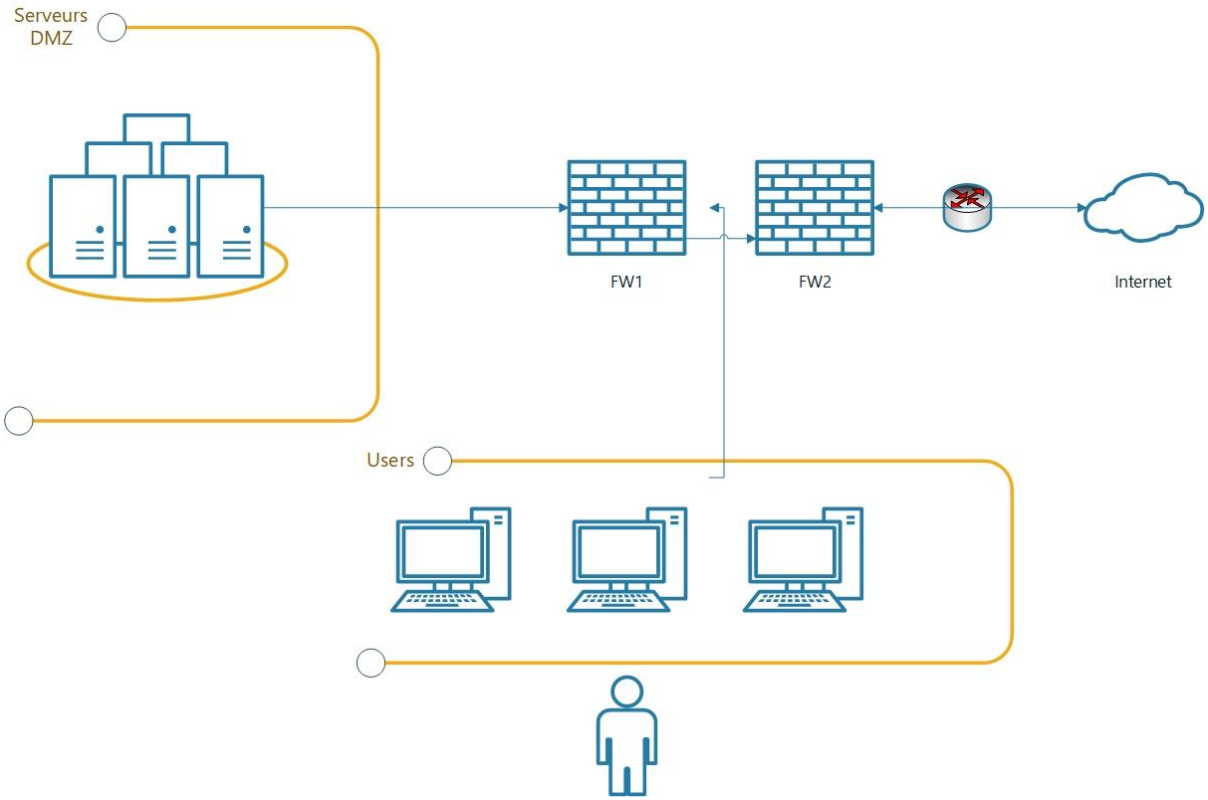


Figure 3.2 : Topologie réseau de COTREL

La Figure 2.2 représente l'architecture réseau qu'on va l'implémenter. On y distingue :

- Internet représente le réseau externe, auquel l'entreprise est reliée par le routeur du fournisseur d'accès.
- Une DMZ (zone démilitarisée) qui contient les serveurs publics de l'entreprise : serveur proxy, serveur antivirus, serveur de messagerie électronique, serveur d'impression et serveur de fichiers.
- Le réseau local, zone privée et protégée de l'entreprise.

- **La haute disponibilité**

La haute disponibilité (abrégée HA pour « high availability ») désigne une architecture informatique, ou un service, disposant d'un taux de disponibilité convenable. On entend par disponible le fait d'être accessible et rendre le service demandé. La disponibilité est aujourd'hui un enjeu très important et qu'en cas d'indisponibilité, les répercussions en termes de coûts et de production peuvent avoir un effet catastrophique. Cette disponibilité est mesurée par un pourcentage essentiellement composé de 9.
Par exemple une disponibilité de 99 % indique que le service ne sera pas disponible pendant 3,65 jours par an maximum (un tableau en dessous est fourni pour les différents taux de disponibilité). On atteint la haute disponibilité à partir de 99,9 %.

Taux de disponibilité	**Durée d'indisponibilité**
97%	11 jours
98%	7 jours
99%	3 jours et 15 heures
99.9%	8 heures et 48 minutes
99.99%	53 minutes
99.999%	5 minutes
99.9999%	32 secondes

Tableau 3.1: Correspondance entre le taux de disponibilité et la durée d'indisponibilité.

- **DMZ**

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (un serveur de messagerie, un serveur FTP, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de « zone démilitarisé » pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile.

Les serveurs situés dans la DMZ sont appelés « bastions » en raison de leur position d'avant-poste dans le réseau de l'entreprise.

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- Trafic du réseau externe vers la DMZ autorisé.
- Trafic du réseau externe vers le réseau interne interdit.
- Trafic du réseau interne vers la DMZ autorisé.
- Trafic du réseau interne vers le réseau externe autorisé.
- Trafic de la DMZ vers le réseau interne interdit.
- Trafic de la DMZ vers le réseau externe refusé.

IV. Réalisation

IV.1 Installation et configuration de PFsense

On installe PFsense comme un OS classique sur VMware, seule particularité : la configuration réseau, en effet, il faut paramétrer quatre cartes réseaux sur notre PFsense, car j'ai une interface pour le réseau local, une pour le réseau externe, une pour la DMZ et une interface de synchronisation entre les deux PFsense.

Avant de se lancer dans la configuration de PFsense, il faut configurer les Vmnet de VMware Workstation.

Les Vmnet sont des switchs virtuels qui permettent de fournir trois modes de connexion :

- Le mode Host-only qui permet de connecter des machines virtuelles entre-elles ou/et avec la machine physique.
- Le mode Bridged qui permet de connecter une machine virtuelle au réseau externe.
- Le mode NAT qui permet de se cacher derrière la machine physique et de partager sa connexion internet avec la machine virtuelle.

Donc, si en réalité pour connecter plusieurs machines physiques on doit les brancher dans le même switch, dans VMware, pour connecter des machines entre-elles, il faut les mettre dans le même Vmnet.

La configuration des Vmnet se fait grâce à l'outil "Virtual Network Editor" qui vient avec l'installation de VMware Workstation.

On a besoin de 3 réseaux C1, C2 et C3, on utilisera donc 3 Vmnet (switchs virtuels), soit Vmnet 1, 2 et 3.

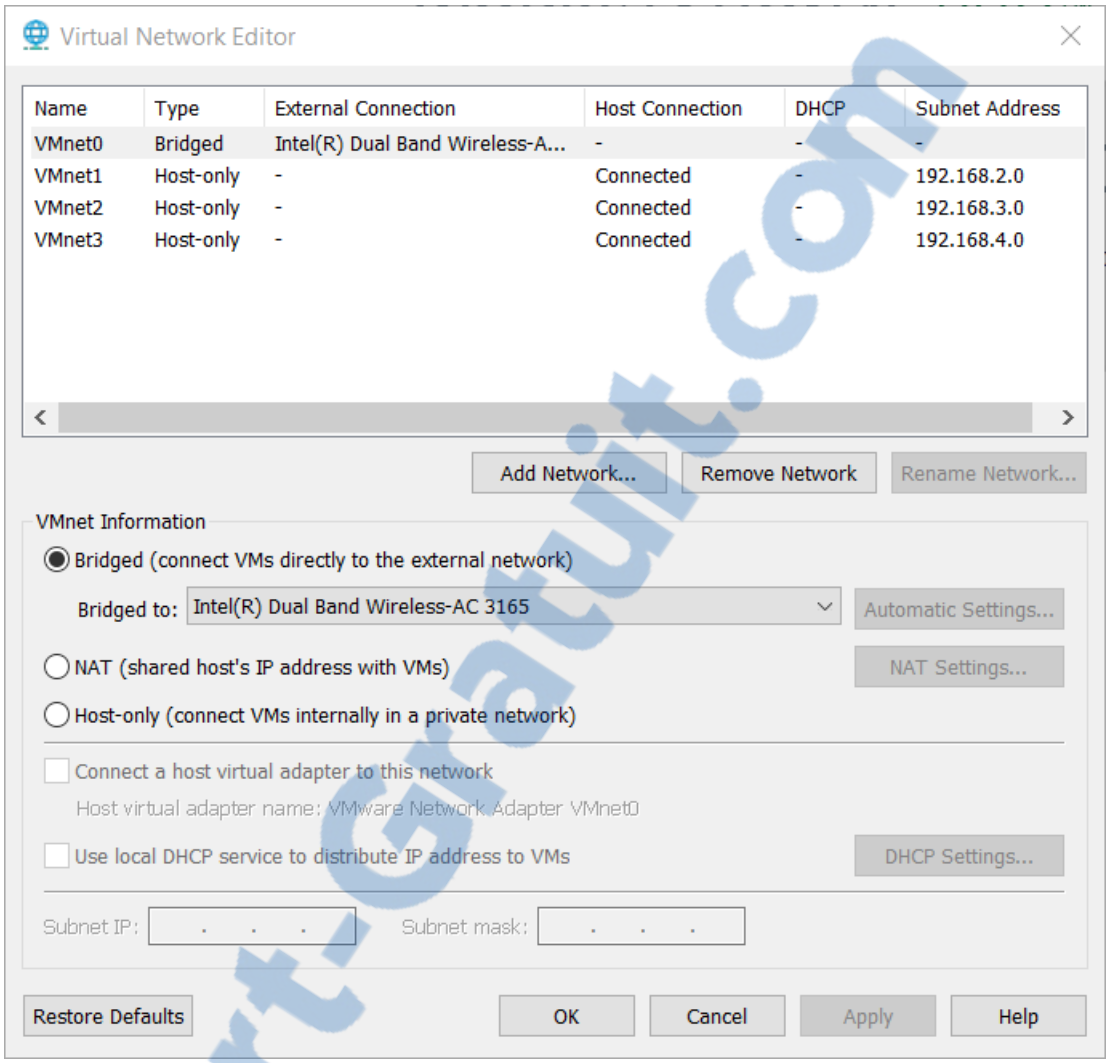


Figure 4.1: Configuration des Vmnet

Une fois PFsense installé, on doit paramétrer les interfaces.

PFsense Master

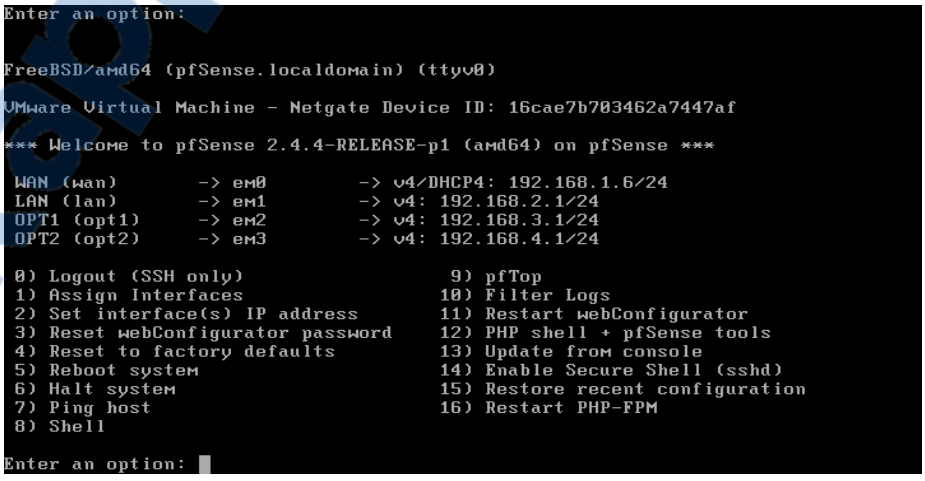


Figure 4.2: Interfaces de PFsense Master

PFsense Slave

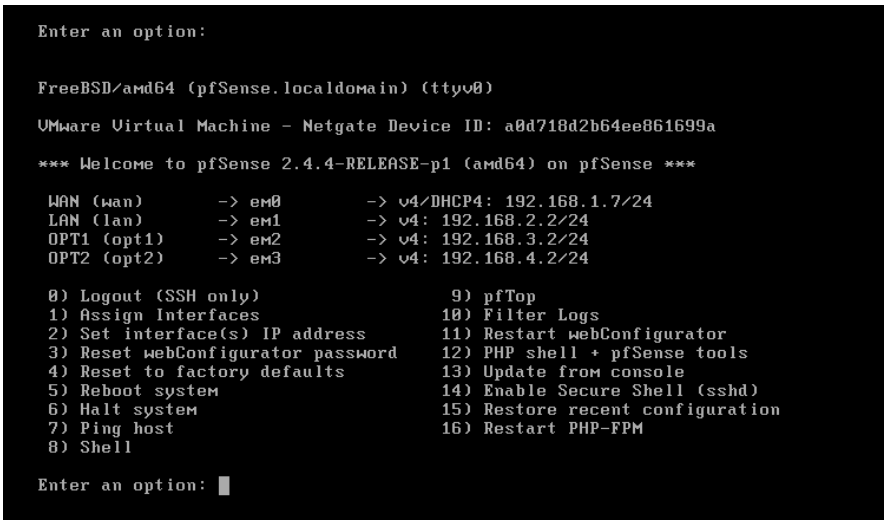


Figure 4.3: Interfaces de PFsense Slave

On lance l'interface web de configuration à travers un poste de client.

Au niveau de la barre de navigation, on tape https://adresse-ip-lan. Ensuite, on doit s'authentifier pour accéder à l'interface de PFsense.

Exemple : pour PFsense Master, on tape https://192.168.2.1.

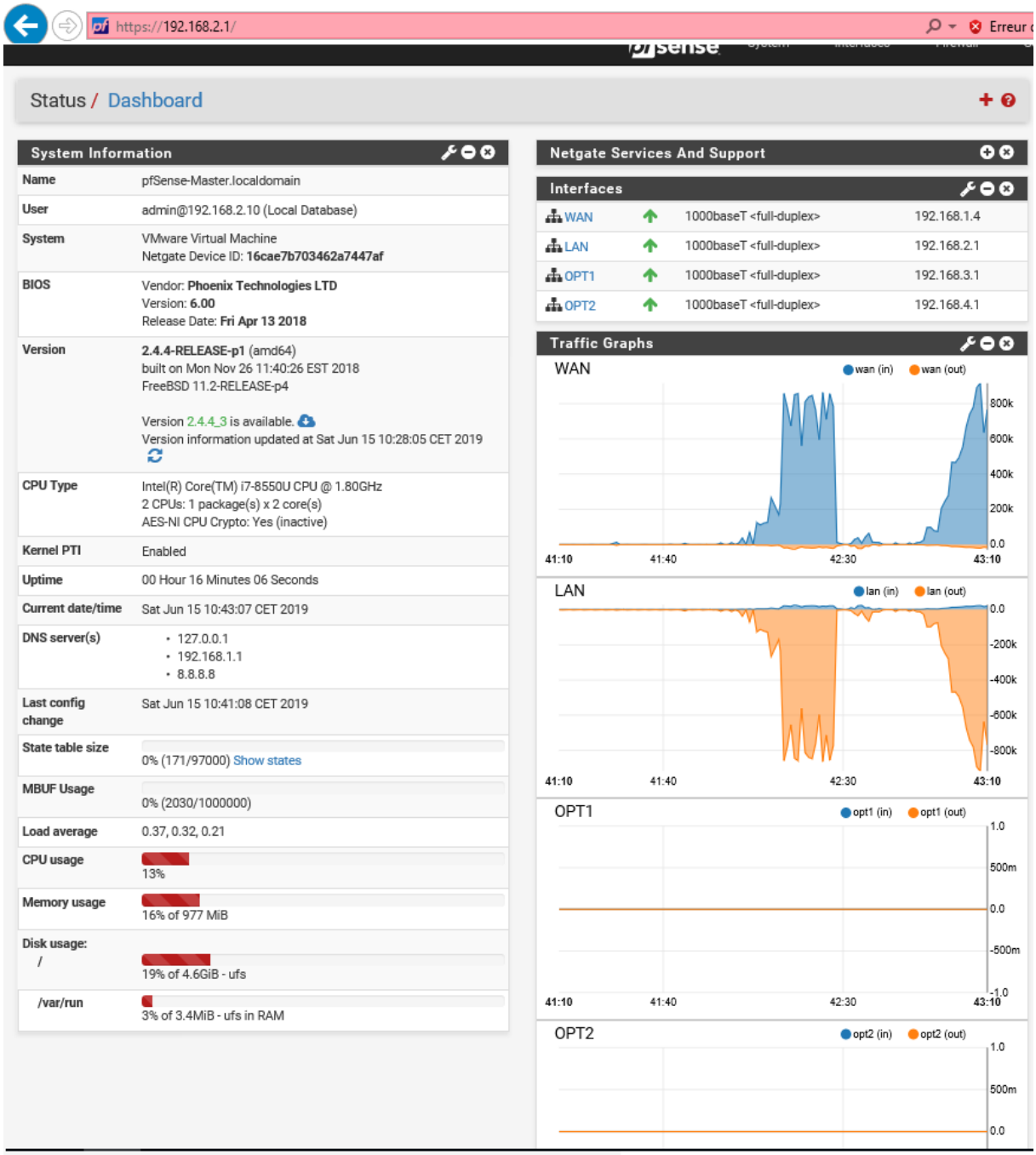


Figure 4.4: Première interface de PFsense Master

PFsense Master

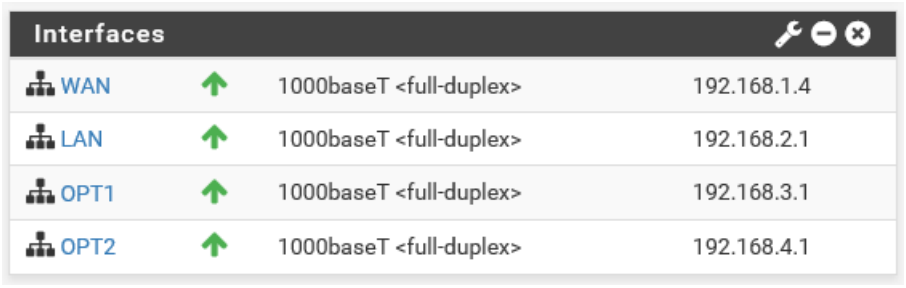


Figure 4.5: Adressage réseau de PFsense Master

PFsense Slave

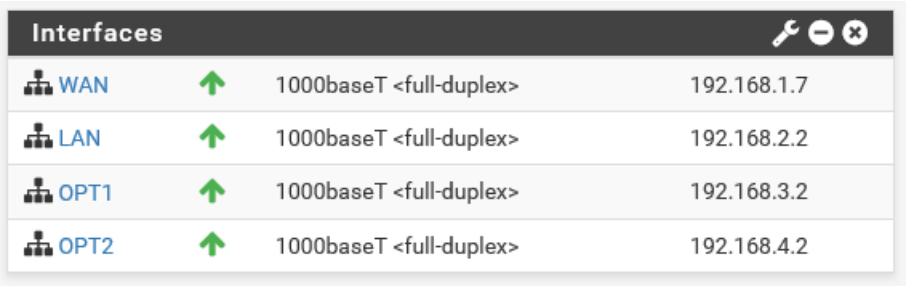


Figure 4.6: Adressage réseau de PFsense Slave

IV.2 Mise en place de la solution dual firewall

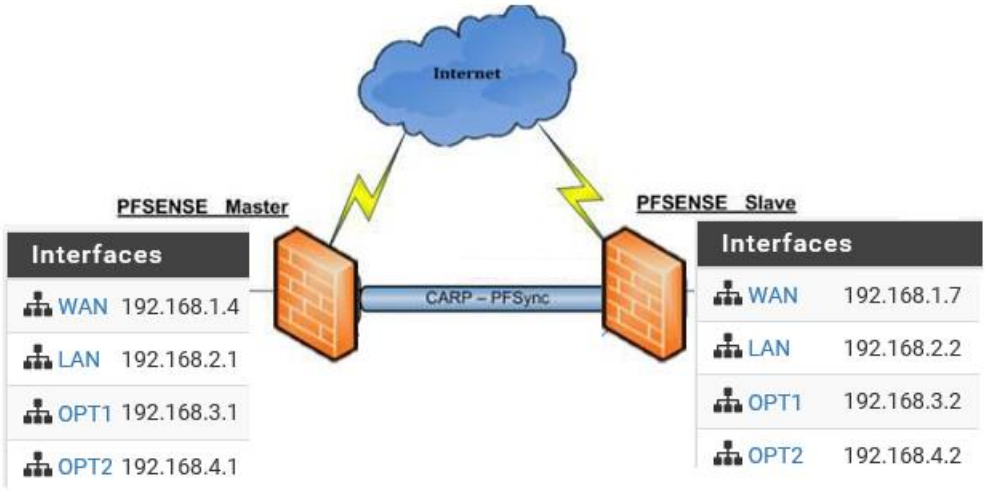


Figure 4.7: PFsense en haute disponibilité

Une fois que les Firewalls fonctionnent, je vais commencer par distinguer leurs noms (hostnames) dans le menu « General Setup », j'aurai : master-pfsense et slave- pfsense.

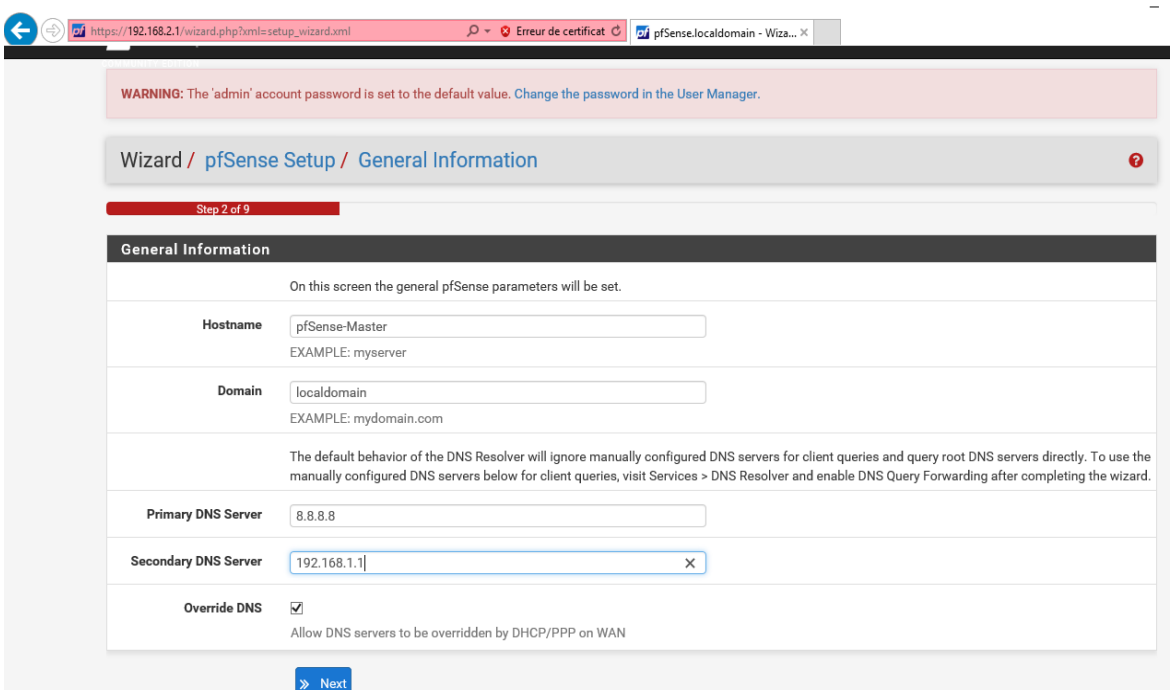


Figure 4.8: General Setup de master-pfsense

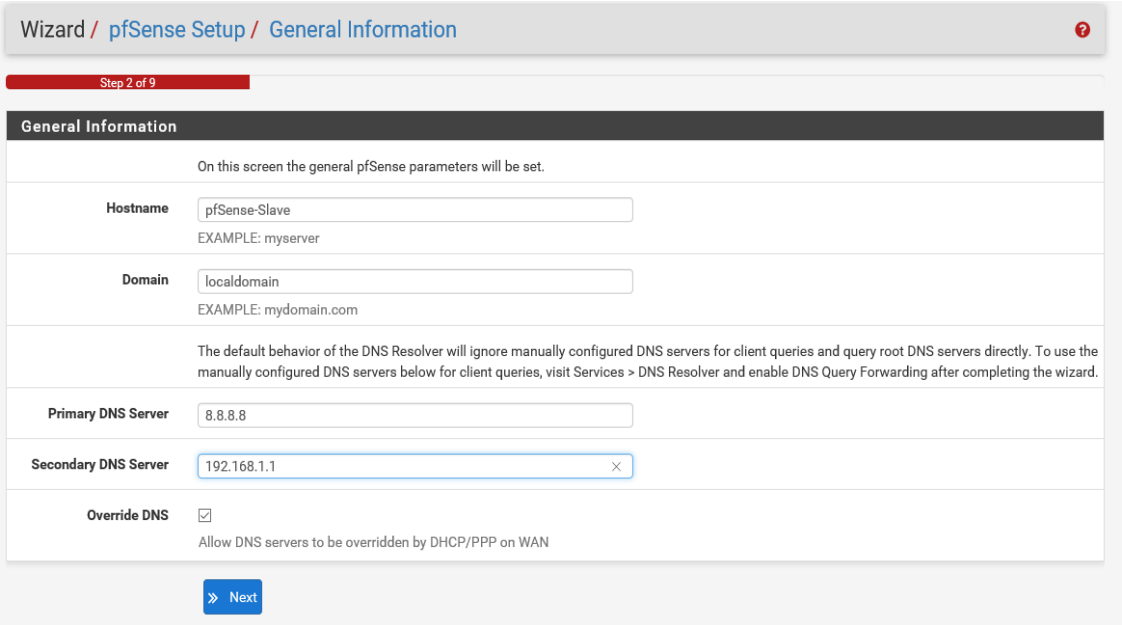


Figure 4.9: General Setup de slave-pfsense

Je configure ensuite les interfaces dans le menu « Interfaces » « Assign » :

- Pour le Firewall Maitre :
  - WAN : 192.168.1.6/24
  - LAN :192.168.2.0/24
  - SYNC : 192.168.4.1/24
- Pour le Firewall Esclave :
  - WAN : 192.168.1.7/24
  - LAN : 192.168.2.2/24
  - SYNC : 192.168.4.2/24

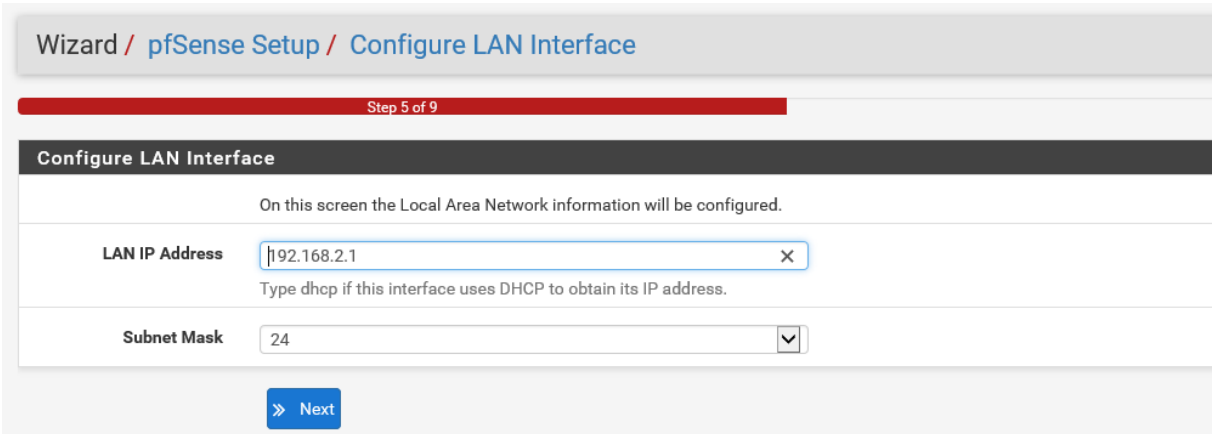


Figure 4.10: Configuration de l'interface LAN

Je dois configurer une règle pour permettre la communication entre les deux interfaces de synchronisation "SYNC". Dans le menu « Firewall > Rules » puis sur l'interface SYNC je clique sur le « + » afin d'ajouter une règle.

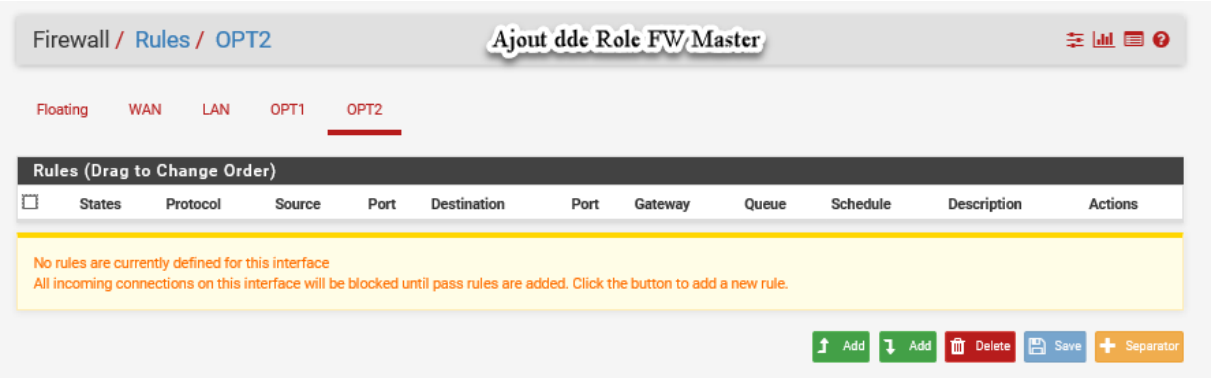


Figure 4.11: Règle de communication entre les interfaces SYNC

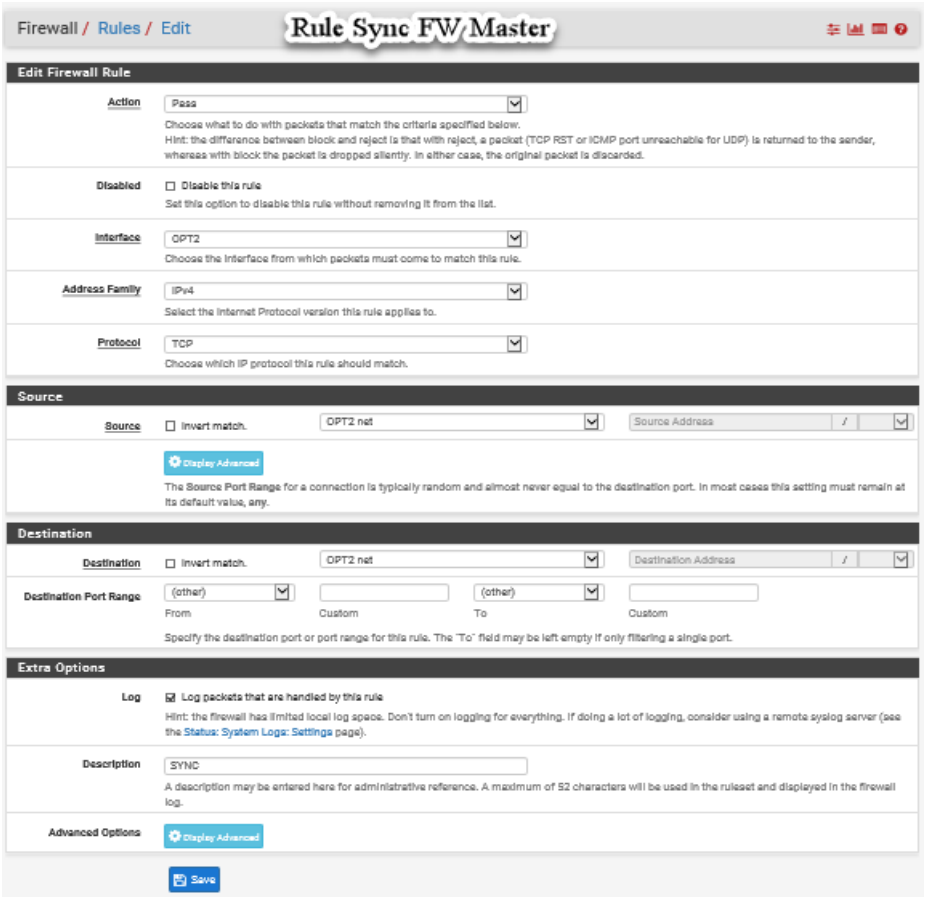


Figure 4.12: Règle de communication entre les interfaces SYNC

Il faut répéter cette opération sur le deuxième Firewall. Pour vérifier la communication entre les interfaces SYNC des deux Firewalls, on utilise la commande Ping.

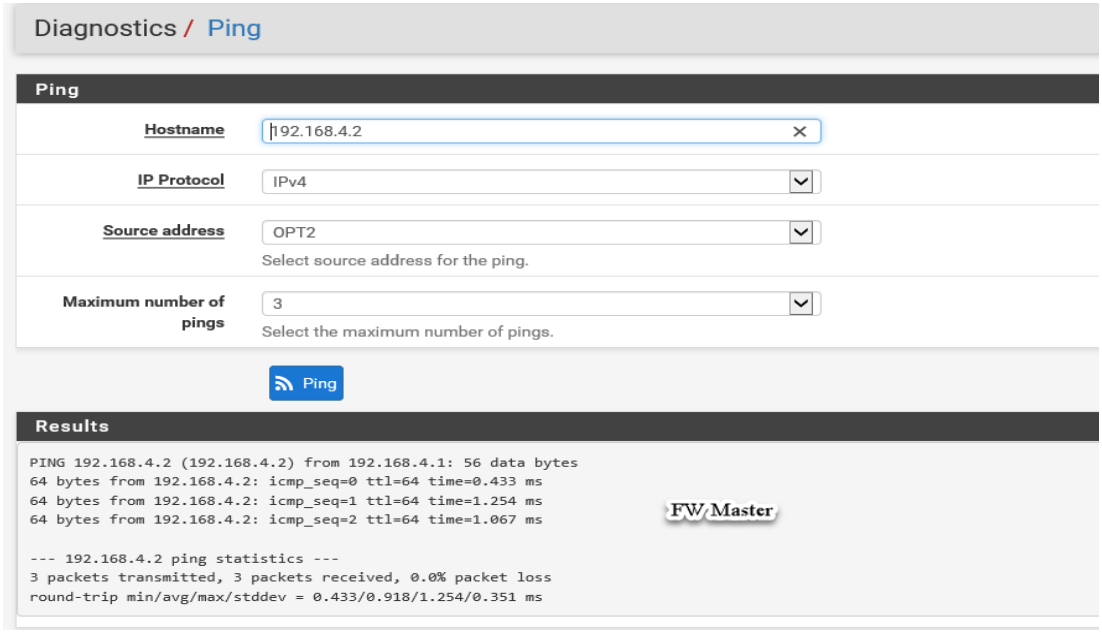


Figure 4.13: Test de Ping entre les interfaces SYNC

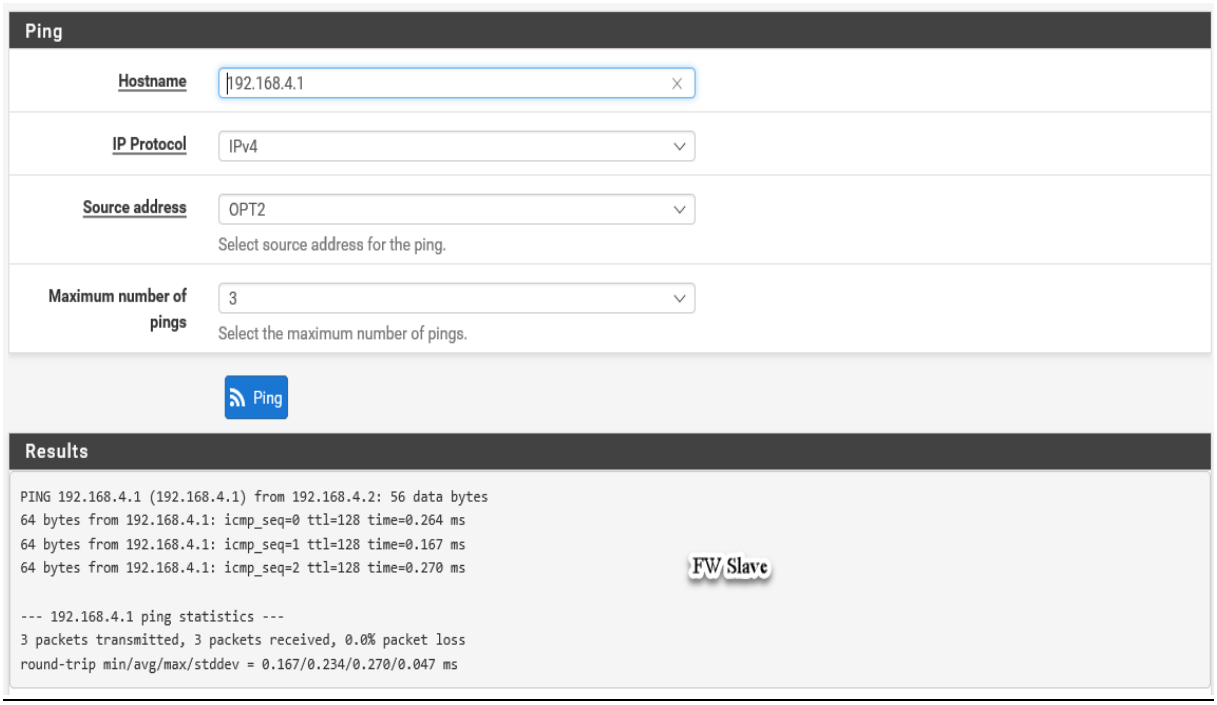


Figure 4.14: Test de Ping entre les interfaces SYNC

Configuration de la synchronisation

Sur le Firewall Maitre, je me rends dans le menu « Firewall > Virtual IP » puis dans l'onglet « CARP Settings ». On sélectionne la case « Synchronize States » puis sélectionnons

l'interface SYNC.

Je vais introduire l'IP du firewall Esclave dans « pfsync Synchronise peer IP » et « Synchronize Config to IP ». Ainsi, le compte admin et le mot de passe du firewall esclave respectivement dans « Username » et « Password ».

On sélectionne ensuite toutes les cases concernant les fonctions que je souhaite synchronisées.

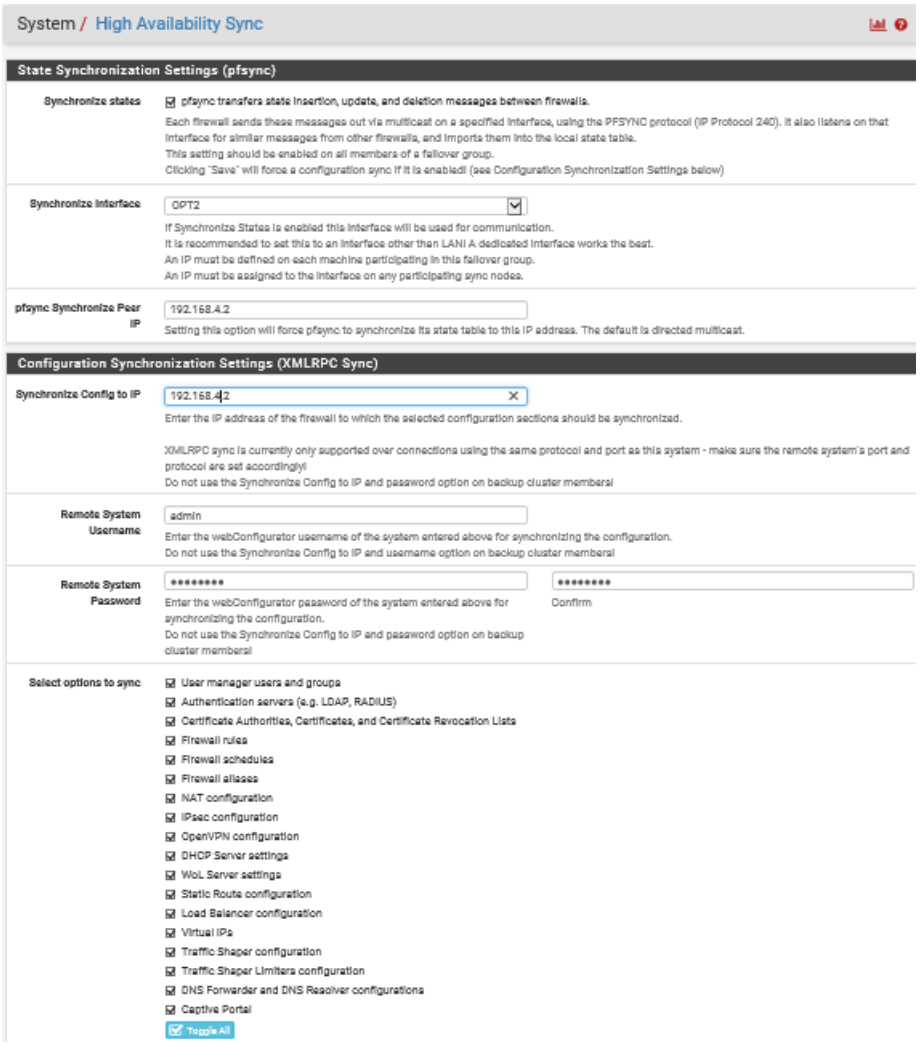


Figure 4.15: Configuration de CARP sur master-PFsense

Je répète la même opération sur le Firewall Esclave, **à la différence** qu'ici :

- Il faut rentrer l'IP du Firewall Maitre dans « pfsync Synchronise peer IP »
- Ne pas renseigner d'IP dans « Synchronize Config to IP »
- Laisser à vide « Username » et « Password »

Par contre, il fait sélectionner les mêmes cases concernant les services à synchroniser.

Configuration des interfaces virtuelles

Sur le firewall Maitre, je me rends dans l'onglet « Virtual IPs » juste à côté de « CARP Settings ». J'ajoute alors une interface virtuelle en cliquant sur le « + ».
On choisit la case « Carp » et sélectionnons l'interface qui va être considéré comme interface virtuelle (ici WAN). Ensuite, j'entre l'adresse IP Virtuelle que se partagerons les deux firewalls sur cette interface (ici 192.168.1.200).

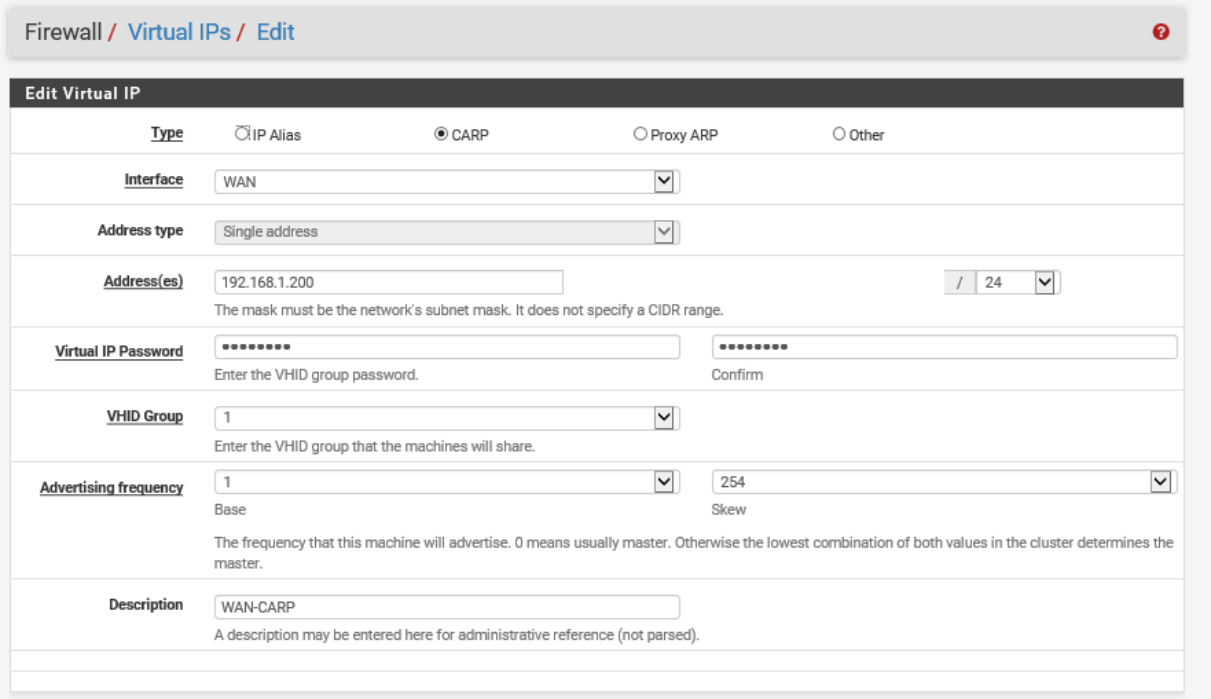


Figure 4.16: Configuration de l'adresse IP virtuelle de l'interface WAN

J'ai répété la même opération sur l'interface LAN et l'interface DMZ (toujours sur le Firewall maître). Si tout s'est bien passé, je dois voir que cette configuration a été dupliquée sur le Firewall esclave.

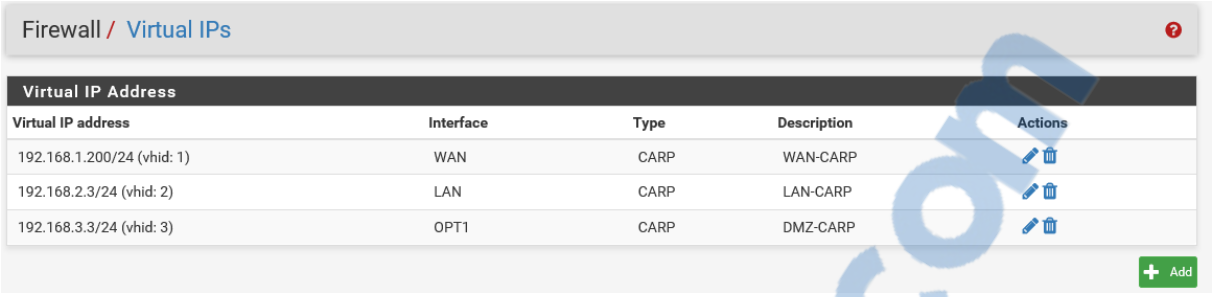


Figure 4.17: Liste des adresses IP virtuelles

Il faut maintenant paramétrer le NAT afin que le flux sortant des firewalls utilise L'interface WAN Virtuelle plutôt que physique.

Pour cela, je vais sur le menu « Firewall > NAT » puis dans l'onglet « Outbound ».

Je sélectionne la case « Manual Outbound NAT rule generation » et je clique sur Save.

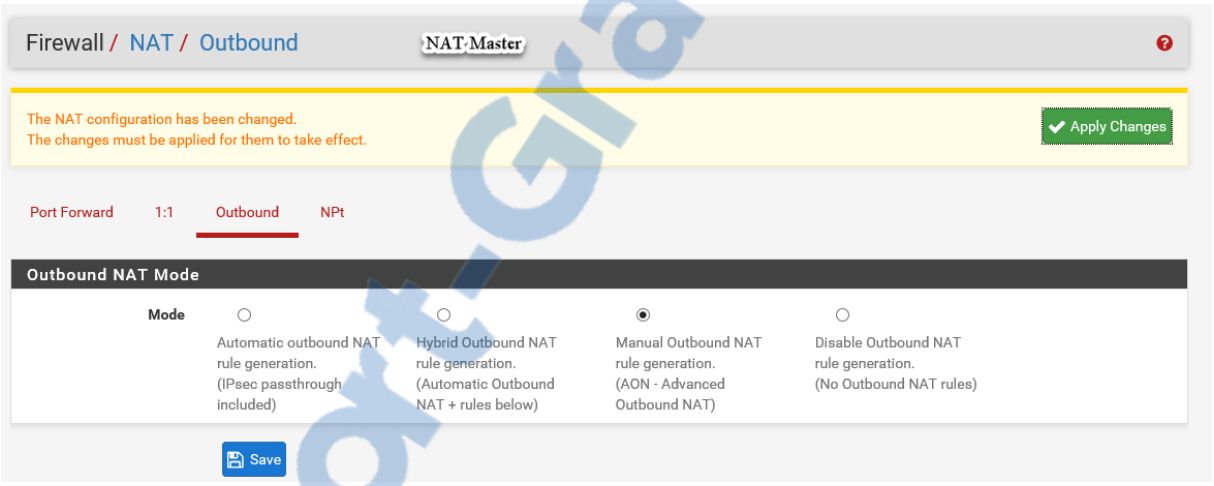


Figure 4.18: Paramétrage de NAT

Vérification du dual firewall

Si mes configurations ont bien été dupliquées, c'est que ma solution de haute disponibilité fonctionne correctement.

Je peux toutefois la vérifier sous le menu « Statuts » CARP (failover) » sur chacun des Firewall.

Sur le maître :

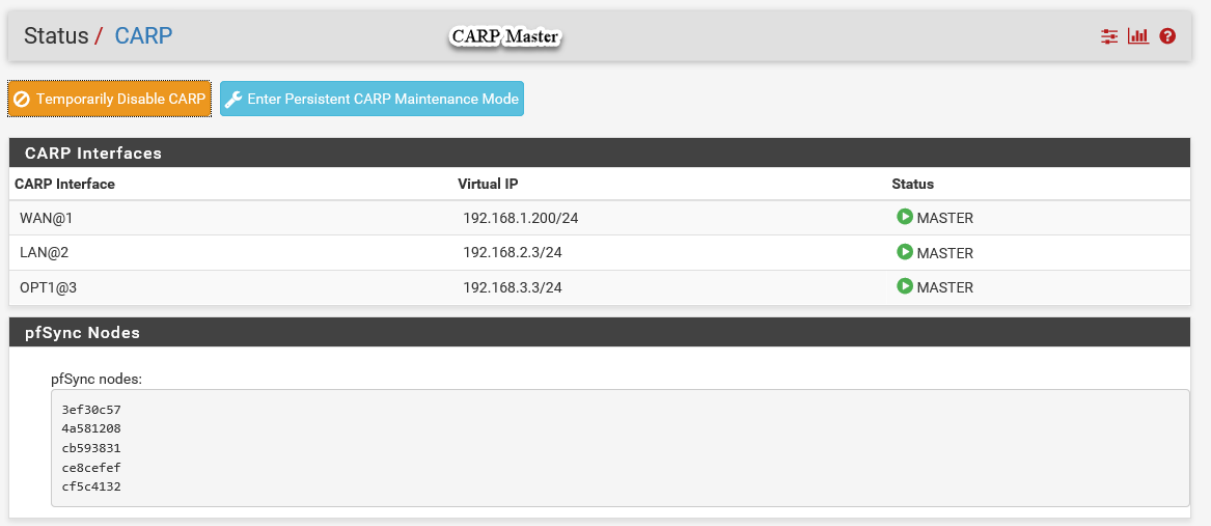


Figure 4.19: Statue de CARP sur PFsense-Master

Sur l'esclave :

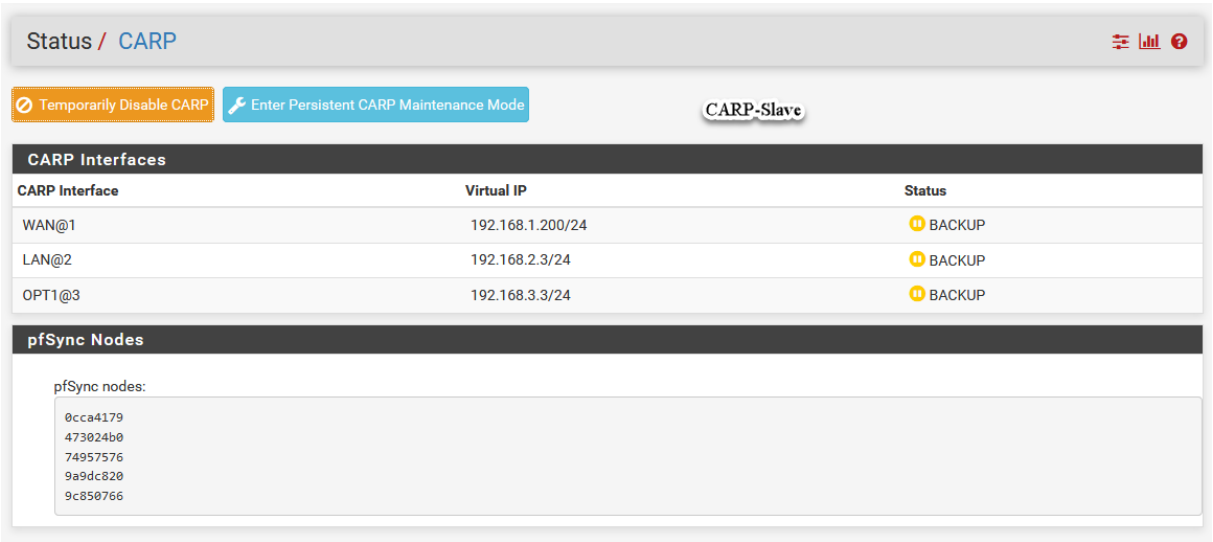


Figure 4.20: Statue de CARP sur PFsense-Slave

Au niveau de la configuration réseau, il faudra que des trois côtés (WAN, LAN et DMZ), les passerelles par défauts soient les virtuelles (192.168.1.200, 192.168.0.3 et 192.168.2.3).

IV.3 Serveur proxy

Le proxy retenu est Squid, qui est une solution libre et le plus utilisé par le monde de l'entreprise.

Squid est un logiciel libre distribué sous licence GNU GPL. C'est un serveur mandataire et un reverse proxy capable d'utiliser les protocoles FTP, HTTP et

HTTPS.

Squid garde les métadonnées et plus particulièrement les données les plus fréquemment utilisées en mémoire. Il conserve aussi en mémoire les requêtes DNS, ainsi que les requêtes ayant échoué.

SquidGuard est à installer en complément de Squid il permet de télécharger des blacklists et de filtrer le contenu du Web.

IV.3.1 Installation du serveur proxy sous PFsense

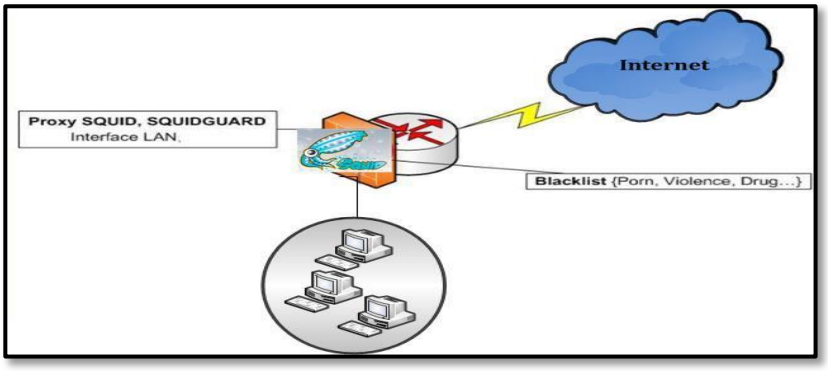


Figure 4.21: Maquette de mise en place de Squid

Le serveur mandataire Squid et SquidGuard existent sur PFsense sous forme de package à installer.

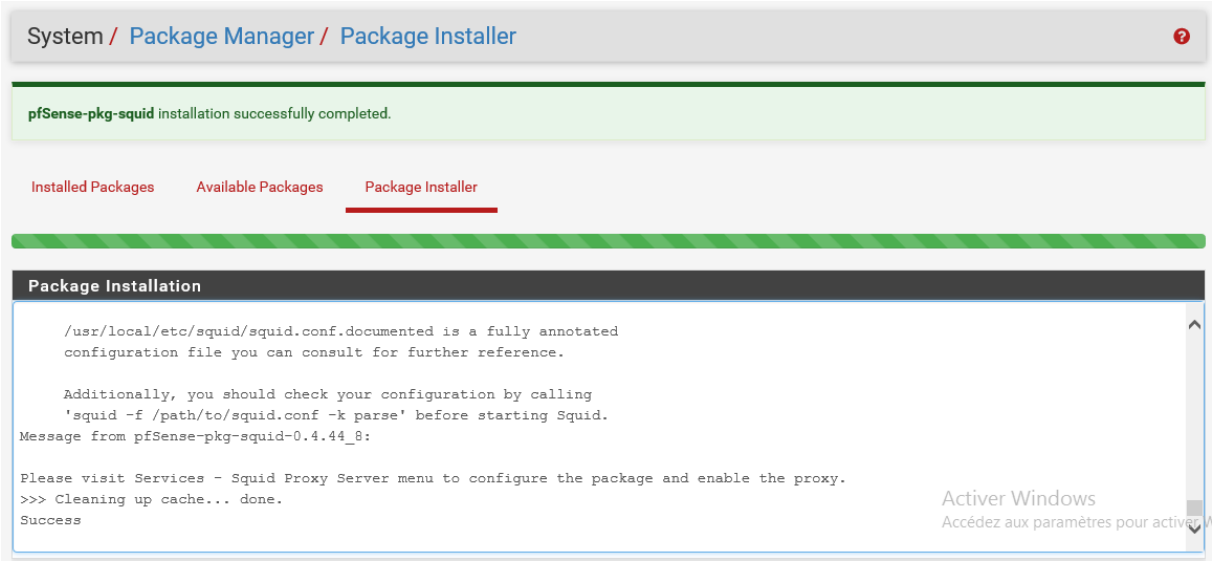


Figure 4.22: Installation de Squid

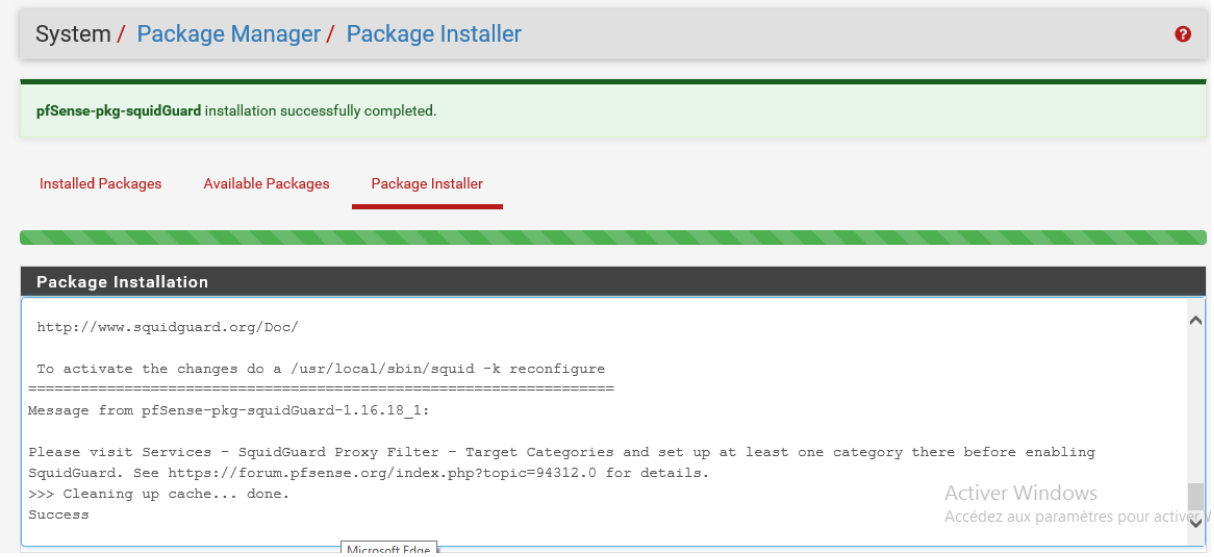


Figure 4.23: Installation de SquidGuard

Pour confirmer que les packages ont été installés, il est préférable de redémarrer les deux firewalls. Ensuite, on remarque que ces deux packagent sont ajoutés au niveau de System > Package > Installed Packages.

IV.3.2 Configuration de Squid et SquidGuard sous PFsense

Une fois Squid et SquidGuard ont été installés, je vais configurer maintenant les paramètres du serveur proxy.

Je choisis Services > Proxy Server. Dans l'onglet Général, on définit les paramètres suivants : l'option d'interface proxy doit être réglé sur "LAN", et parce qu'on veut que Squid fonctionne avec authentification des clients, on choisit « Allow users on interface ».

Squid utilise par défaut le port 3128, mais dans notre cas on va utiliser le port 3128.

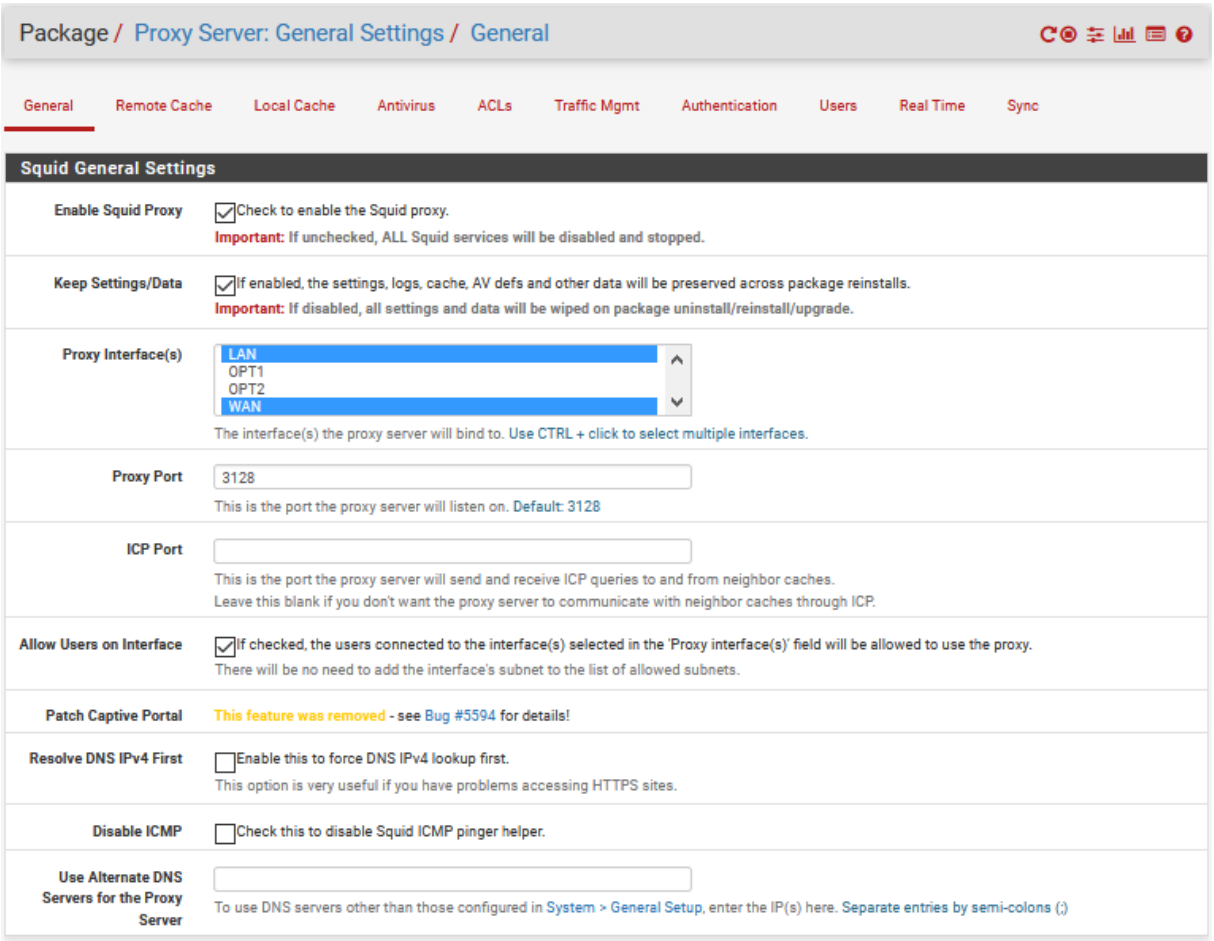


Figure 4.24: Configuration de Squid sous PFsense

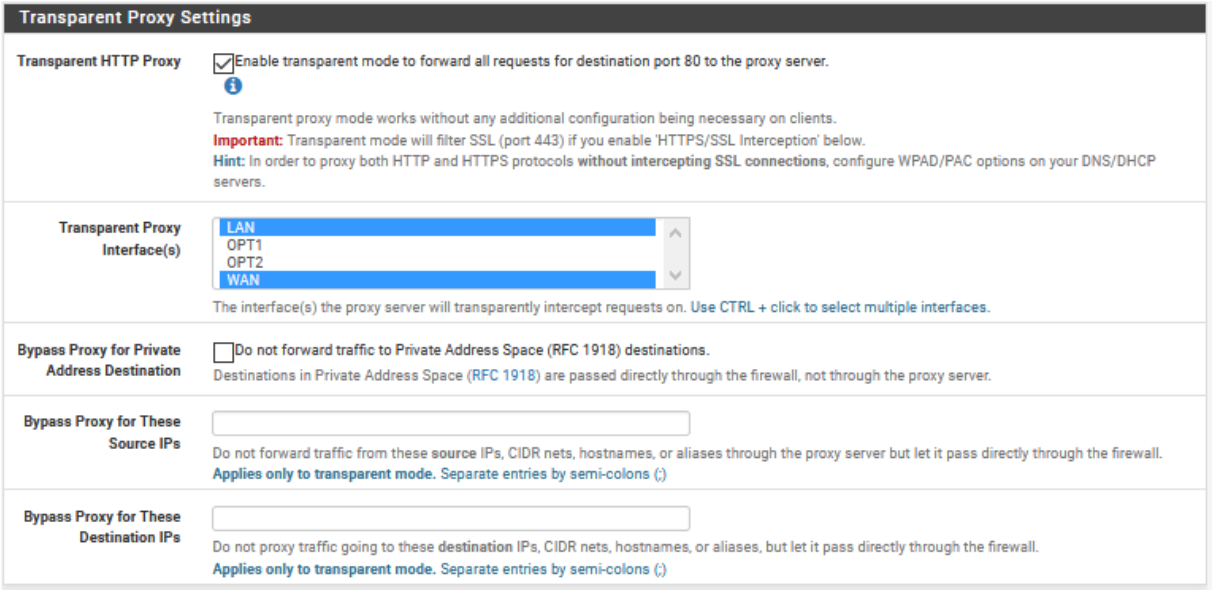


Figure 4.25: Configuration de Squid sous PFsense

Ensuite, on choisit l'onglet « Cache Mgnt », par défaut, la taille du disque dur cache

est réglé sur 100Mb, Mais on peut l'augmenter et cela dépendra de la taille de notre disque.

Figure 4.26: Configuration de Squid sous PFsense

Au niveau de l'onglet « Access Control », on ajoute les sous réseaux autorisés à utiliser le serveur proxy. En plus, j'ai pu spécifier la liste des sites web autorisés « Whitelist » et les sites refusés « Blacklist » afin que le réseau local ne puisse pas y accéder.

Figure 4.27: « Access Control » de Squid

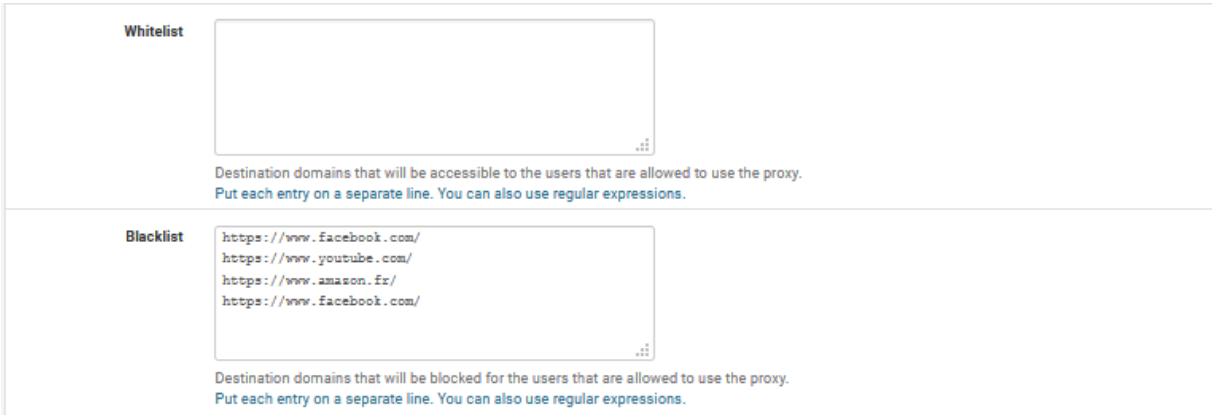


Figure 4.28: « Whitelist » et « Blacklist » de Squid

L'onglet « Local User » permet d'ajouter des utilisateurs pour l'authentification, en Spécifiant leur Login et Password.

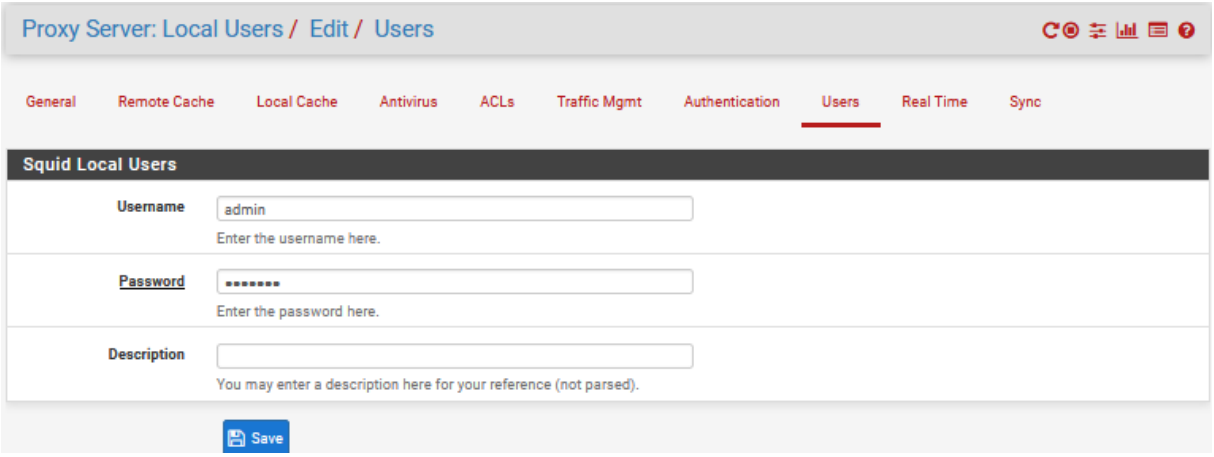


Figure 4.29: Authentification sous Squid

Configuration de SquidGuard

Maintenant, on passe à la configuration de SquidGuard à travers le menu service > proxy filter.

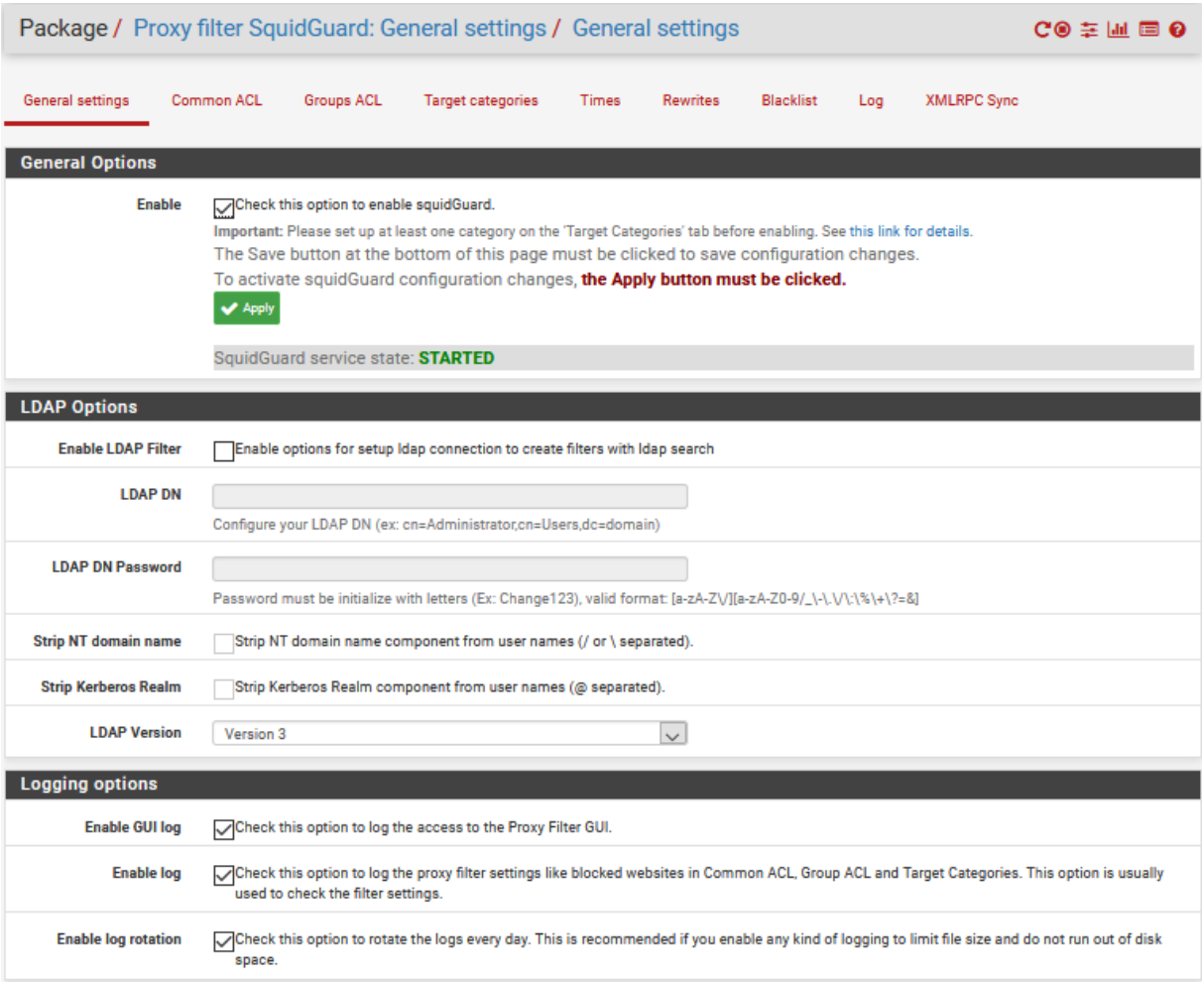


Figure 4.30: « General Settings » de SquidGuard

On reste sur l'onglet Paramètre généraux et on sélectionne la case d'activation de la liste noire. Dans Blacklist URL, on ajoute le lien suivant : http://www.shallalist.de/Downloads/shallalist.tar.gz afin de télécharger les données de liste noire.

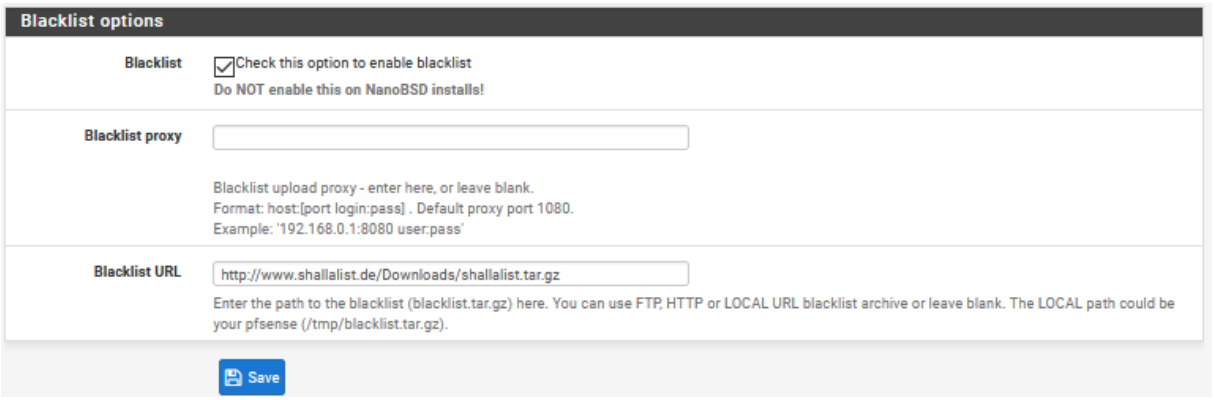


Figure 4.31: Ajout de la liste noire

La blacklist téléchargée m'a permis de filtrer le web par catégorie, en choisissant « Whitelist » ou « deny » ou « allow » pour chaque catégorie.

Restreindre l'accès par le temps

Pour ce faire, on doit d'abord déterminer l'intervalle de temps. Dans notre exemple, on a fait un intervalle en semaine, l'accès est autorisé de 12h à 13 h.

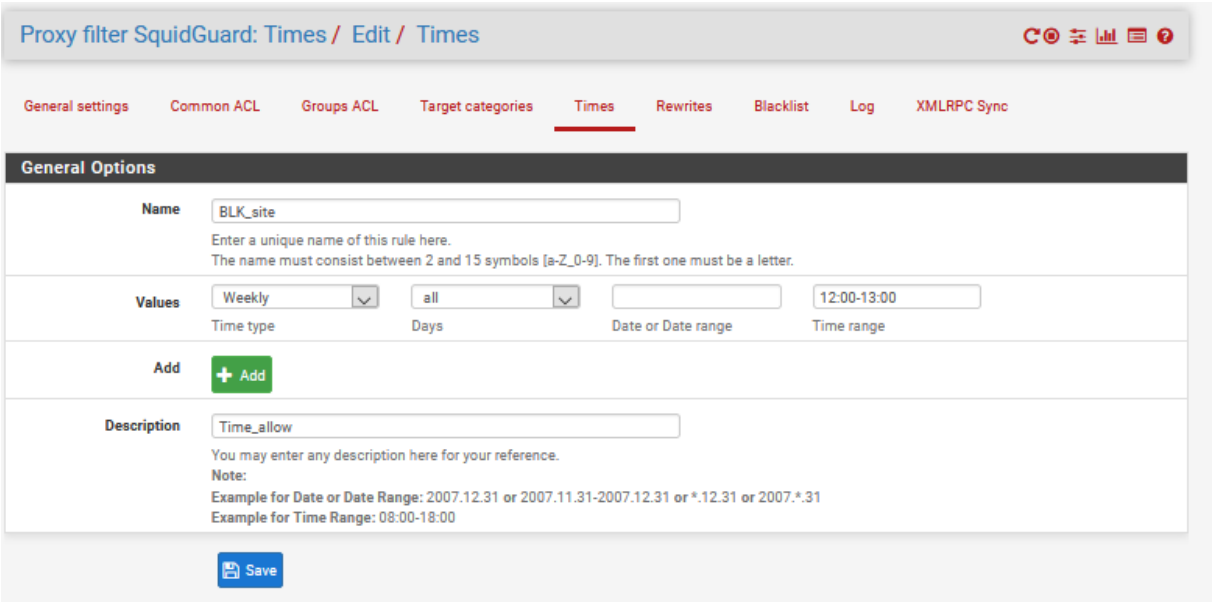


Figure 4.32: Restreindre l'accès par le temps

Catégories de paramètres individuels pour les entreprises

Cela se fait dans l'onglet « Groups ACL ». On fait des règles pour les machines des clients pour qu'il n'utilise pas « Facebook » et « Youtube » pendant les heures de travail, ainsi autoriser l'accès à ces derniers pendant la pause.

On indique l'intervalle des adresses IP dans le champ « client (source) » et on peut Spécifier l'intervalle de temps pré-créé à l'étape précédente (Restreindre l'accès par le temps).

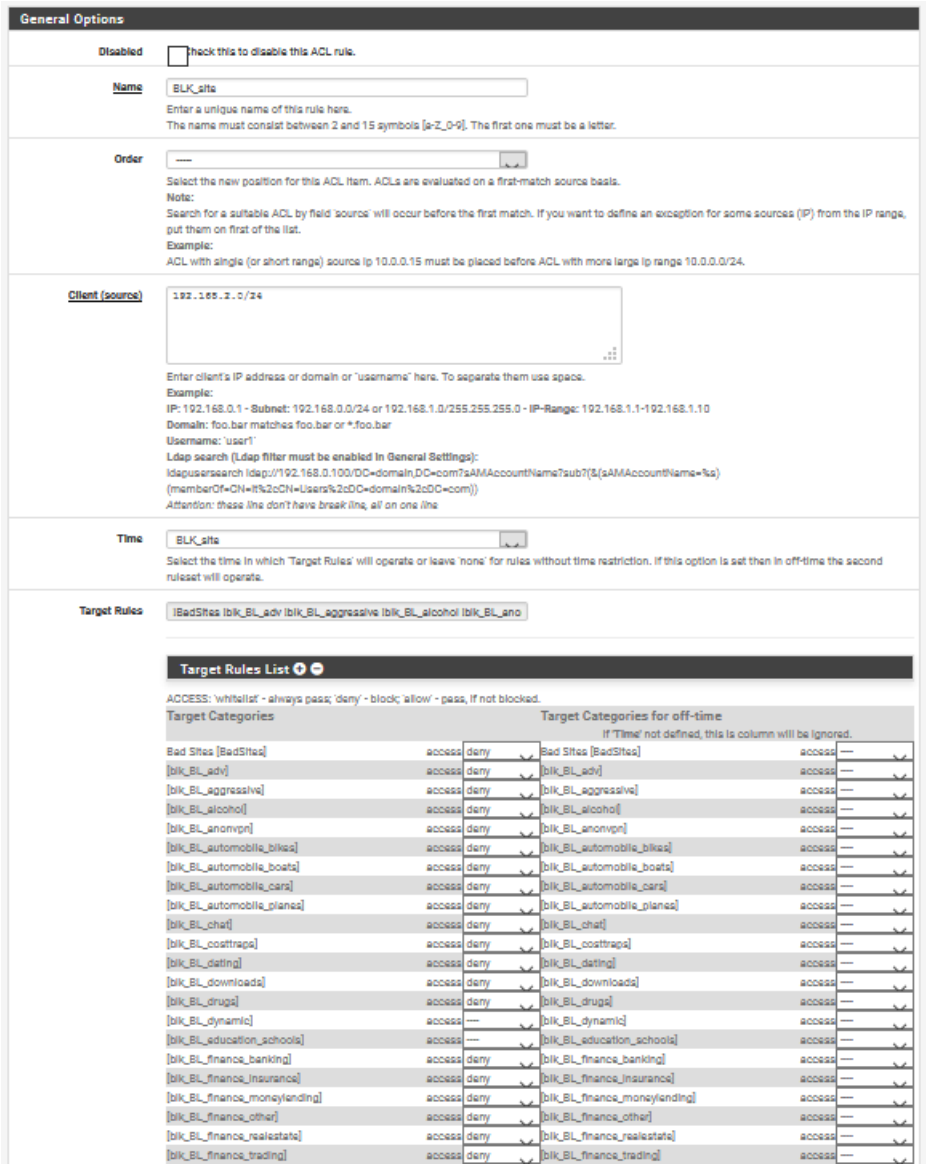


Figure 4.33: Configurer « Groups ACL »

Les catégories de sites seront présentées sur deux colonnes. La colonne de gauche indique les catégories de filtrage dans laquelle j'ai fixé l'intervalle de temps, et la colonne de droite est à l'opposé - à d'autres moments.

Cela est fait par le menu Firewall > NAT > Port Forward. On ajoute la règle suivante :

- Interface : LAN
- Adresse source : Any
- Port source : Any
- Adresse destination : 192.168.2.2 « this firewall »
- Port destination : 8080

- Adresse NAT : 127.0.0.1
- Port NAT : 8080
- Static port : No

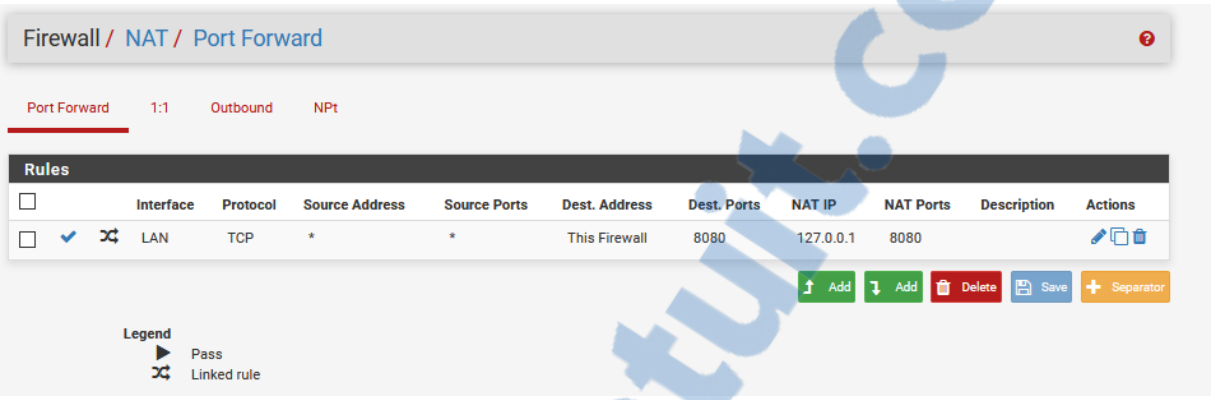


Figure 4.34: Configuration de « Port Forward »

On répète les mêmes étapes de configuration de serveur proxy sur le deuxième Firewall.

Il est possible de rajouter le module HAVP, qui est un serveur Proxy spécialement dédié au scan antivirus sur des flux HTTP. Ce proxy est couplé avec l'antivirus et il permet de protéger le réseau local de certains sites hébergeant des virus.

IV.4 Solution antivirale

IV.4.1 Choix de l'antivirus

Un antivirus permet, comme son nom l'indique, de bloquer et supprimer les virus. La plupart de ces virus arrivent par le biais d'Internet sur les machines hôtes. Il paraissait donc indispensable d'intégrer la protection contre ces menaces dans notre solution de sécurité.

Par virus nous entendons les « vers » et « chevaux de Troie », les « spywares », etc.

Notre tâche était donc d'installer et de configurer un antivirus, car ces derniers représentent une menace directe pour le matériel.

L'antivirus proposé implémente aux moins les fonctionnalités suivantes :

- Exécution en tâche de fond,
- Détection automatique,
- Mise à jour automatique.

L'antivirus que j'ai choisi est ClamAV. En effet, de nombreux antivirus existent sur

le marché mais rares sont ceux totalement libres et gratuits.

ClamAV est un logiciel libre (GPL), son moteur antivirus conçu pour des chevaux de Troie, virus, détection des logiciels malveillants et autres menaces malveillantes. Il fournit un démon de haute performance pour le balayage mutli-thread, des utilitaires de ligne de commande pour le balayage du fichier de la demande, et un outil intelligent pour les mises à jour automatiques de signatures. Le moteur antivirus est la bibliothèque libclamav.

IV.4.2 L'anti-virus ClamAV

Le Squid Proxy server est un proxy avec le moteur d'antivirus ClamAV.

C'est avec le HTTP que la majorité des virus se transmettent par l'Internet. Le Squid Proxy server est spécialement dédié à une utilisation avec ClamAV et plus exactement sa librairie. Il peut être couplé avec d'autre antivirus, mais ClamAV reste l'antivirus pour lequel il a été conçu. La particularité de Squid Proxy server est qu'il permet à l'antivirus de commencer à scanner les fichiers en cours de téléchargement pour limiter au maximum le temps d'attente sur la machine hôte.

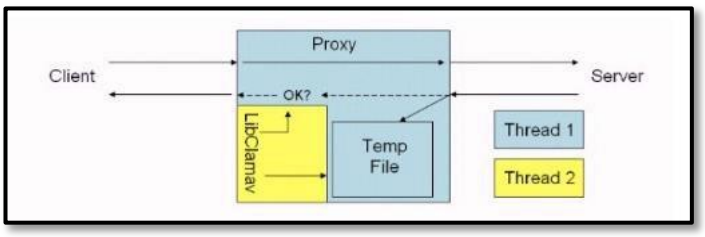


Figure 4.35: Principe de fonctionnement de HAVP

IV.4.3 ClamAV sous PFsense

4.3.1 Installation de ClamAV

Pour commencer, Le Squid Proxy server paquets intègre la solution antivirus de PFsense.

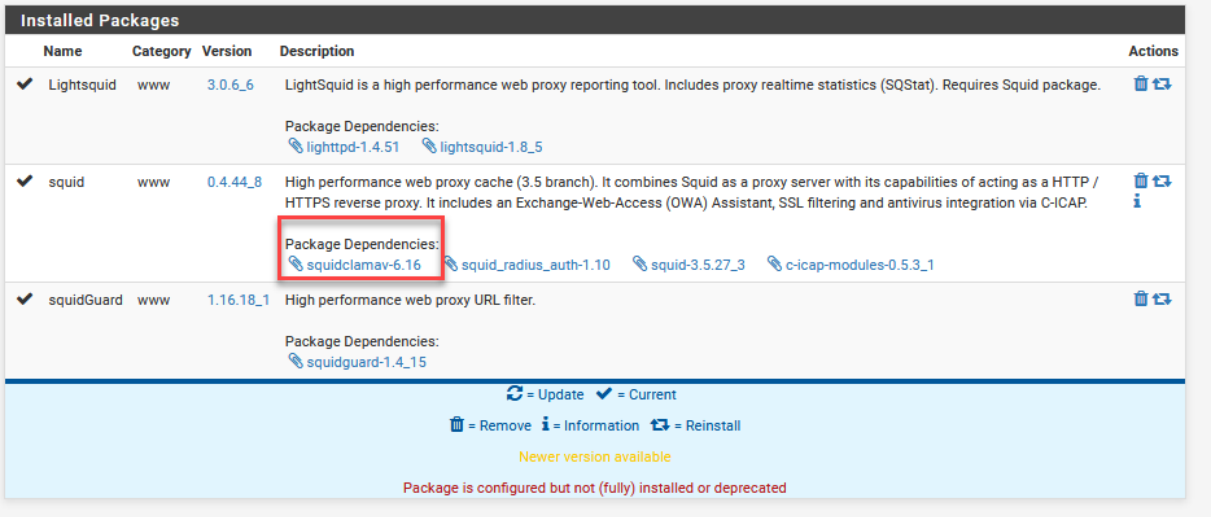


Figure 4.36: Installation de ClamAV antivirus sous PFsense

4.3.2 Configuration de HTTP proxy et ClamAV sous PFsense

Une fois que j'ai installé le Squid Proxy server, il y a quelques paramètres qui doivent être changé sous ClamAV pour qu'il fonctionne correctement. Je Clique sur l'entrée Squid Proxy server dans le menu des services pour accéder aux paramètres ClamAV.

Dans mon cas, je le configure comme parent du proxy Squid, c'est à dire qu'il se retrouve en amont de ce dernier.

Il est possible de chaîner ClamAV et Squid afin d'avoir simultanément un proxy antivirus et la possibilité de conserver Squid. Cette méthode permet de continuer d'utiliser Squid en frontal, avec ses autorisations et ses ACL et c'est Squid qui demandera à ClamAV les pages web.

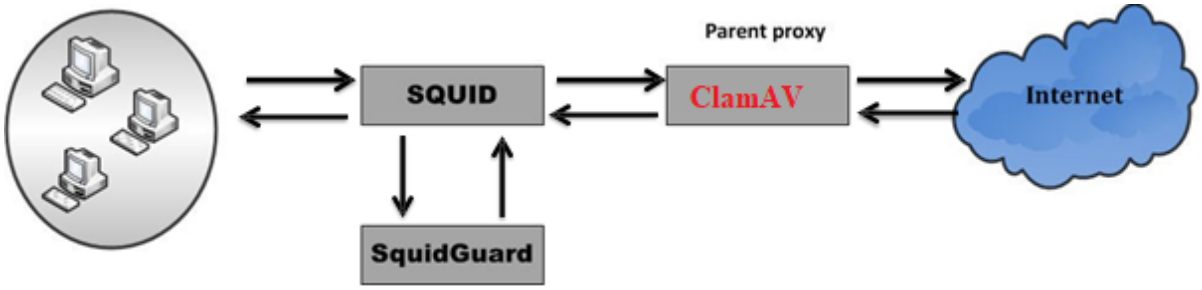


Figure 4.37: Chaînage Squid-HAVP

Je m'assure que l'interface de proxy est réglée sur LAN. Le numéro de port par

défaut est 3125 et il doit être différent de celui utilisé en Squid.

Pour permettre mises à jour automatiques des définitions de virus, je choisis l'onglet « Setting ». Je recommande que la mise à jour de base antivirus se produire toutes les 6 heures. C'est aussi une bonne idée de choisir un miroir de téléchargement régionale qui se trouve près de chez moi, choisir un miroir proche permettra aux définitions de télécharger beaucoup plus rapide.

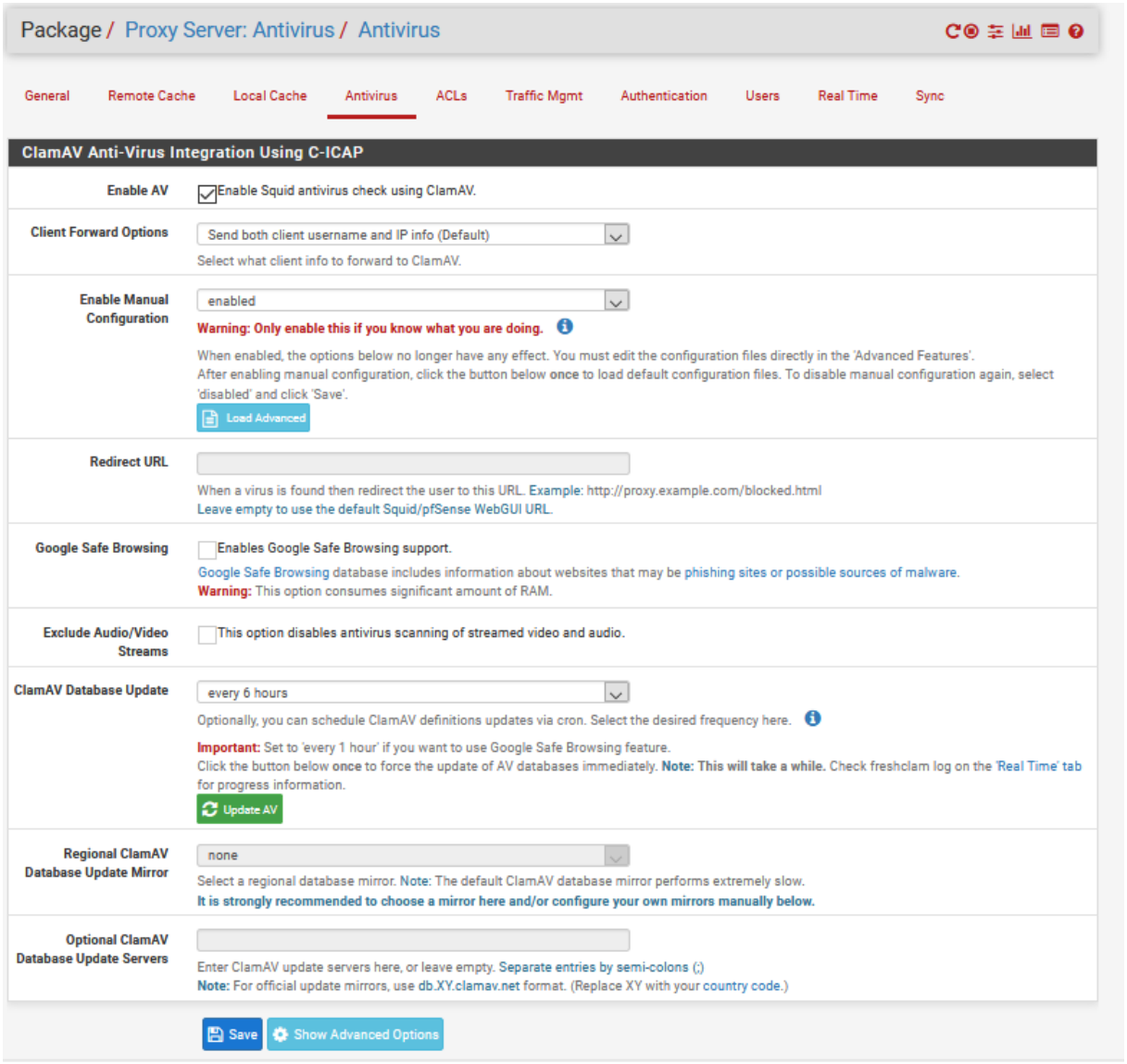


Figure 4.38: Mise à jour de la base antivirus

A ce point, ClamAV devrait être opérationnel. Je vérifie son état pour s'assurer que tous les services ont démarré et le fichier de définition a été téléchargé.

C-ICAP Virus Table

C-ICAP - Virus Logs

Date-Time	Message	Virus	URL	Host	User
16.06.2019 20:57:54	VIRUS FOUND	Eicar-Test-Signature	http://www.eicar.org/download/eicar.com	192.168.2.11	-
16.06.2019 20:56:03	VIRUS FOUND	Eicar-Test-Signature	http://www.eicar.org/download/eicar.com	192.168.2.11	-
16.06.2019 20:55:46	VIRUS FOUND	Eicar-Test-Signature	http://www.eicar.org/download/eicar.com	192.168.2.11	-
16.06.2019 20:53:27	VIRUS FOUND	Eicar-Test-Signature	http://www.eicar.org/download/eicar.com	192.168.2.11	-

C-ICAP Access Table

C-ICAP - Access Logs

Date-Time	Message
16.06.2019 20:59:48	127.0.0.1 127.0.0.1 REQMOD squid_clamav 204
16.06.2019 20:59:47	127.0.0.1 127.0.0.1 REQMOD squid_clamav 204
16.06.2019 20:59:47	127.0.0.1 127.0.0.1 REQMOD squid_clamav 204
16.06.2019 20:59:47	127.0.0.1 127.0.0.1 REQMOD squid_clamav 204
16.06.2019 20:59:47	127.0.0.1 127.0.0.1 REQMOD squid_clamav 204
16.06.2019 20:59:46	127.0.0.1 127.0.0.1 REQMOD squid_clamav 204
16.06.2019 20:59:46	127.0.0.1 127.0.0.1 REQMOD squid_clamav 204
16.06.2019 20:59:46	127.0.0.1 127.0.0.1 REQMOD squid_clamav 204
16.06.2019 20:59:46	127.0.0.1 127.0.0.1 REQMOD squid_clamav 204
16.06.2019 20:59:46	127.0.0.1 127.0.0.1 REQMOD squid_clamav 204

C-ICAP Server Table

C-ICAP - Server Logs

Date-Time	Message
16.06.2019 20:57:54	squidclamav.c(1488) generate_response_page: Sun Jun 16 20:57:54 2019
16.06.2019 20:56:03	squidclamav.c(1488) generate_response_page: Sun Jun 16 20:56:03 2019
16.06.2019 20:55:45	squidclamav.c(1488) generate_response_page: Sun Jun 16 20:55:45 2019
16.06.2019 20:53:16	squidclamav.c(1488) generate_response_page: Sun Jun 16 20:53:16 2019
16.06.2019 13:19:48	squidclamav.c(614) squidclamav_end_of_data_handler: Sun Jun 16 13:19:48 2019
16.06.2019 13:19:48	squidclamav.c(1709) dconnect: Sun Jun 16 13:19:48 2019
16.06.2019 13:18:54	squidclamav.c(614) squidclamav_end_of_data_handler: Sun Jun 16 13:18:54 2019
16.06.2019 13:18:54	squidclamav.c(1709) dconnect: Sun Jun 16 13:18:54 2019
16.06.2019 13:18:54	squidclamav.c(614) squidclamav_end_of_data_handler: Sun Jun 16 13:18:54 2019
16.06.2019 13:18:54	squidclamav.c(1709) dconnect: Sun Jun 16 13:18:54 2019

freshclam Table

Status / Services

Services

Service	Description	Status	Actions
c-icap	ICAP Inteface for Squid and ClamAV integration	✓	
captiveportal	Captive Portal: Local	✓	
clamd	ClamAV Antivirus	✓	
dhcpd	DHCP Service	✓	
dpinger	Gateway Monitoring Daemon	✓	
lightsquid_web	Lightsquid Web Server	✓	
ntpd	NTP clock sync	✓	
squid	Squid Proxy Server Service	✓	
squidGuard	Proxy server filter Service	✓	
syslogd	System Logger Daemon	✓	
unbound	DNS Resolver	✓	

Figure 4.39: Démarrage de HTTP Antivirus Proxy + Antivirus Server

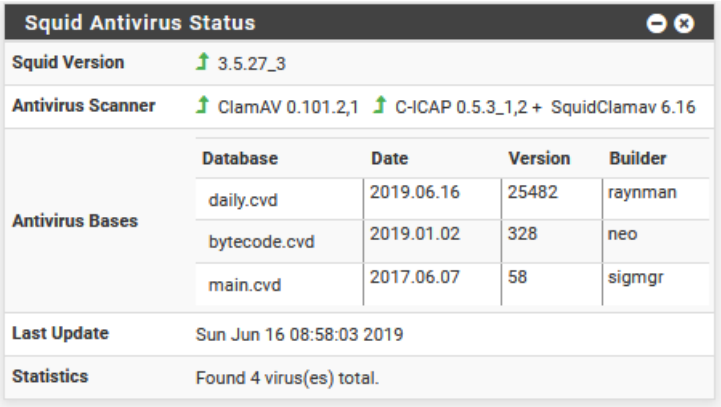


Figure 4.40: statut ClamAV

Maintenant que j'ai réalisé l'implémentation des outils de sécurisation de notre réseau informatique, je passe à la présentation des tests de pénétration en mettant en place leur intérêt vu la haute exposition de l'infrastructure réseau aux risques liés à la sécurité informatique.

Dans ce chapitre, je réaliserai un audit de sécurité d'un réseau en effectuant un scan de vulnérabilité et un balayage des ports ouverts sur une machine donnée ou sur un réseau tout entier afin de déterminer ces vulnérabilités.

V.Réalisation de scan réseau

Dans cette partie, je réalise l'implémentation des outils open source permettant le scan de port et le scan de vulnérabilité. Les premières victimes d'une attaque réussie sont les données, le temps de fonctionnement, et la réputation d'une société. A partir de là, on remarque l'importance de scan de vulnérabilité.

V.1 Les systèmes d'exploitation dédiés sécurité

Sur le marché on trouve plusieurs systèmes d'exploitation orientés sécurité, ils servent à regrouper le plus grand nombre d'outils de sécurité dans un seul système pour simplifier la tâche des experts sécurité et leurs faire gagner du temps dans l'installation et la configuration des outils.

La plupart de ces systèmes sont des distributions Linux personnalisées. Ci-dessous, la liste des distributions les plus connues :

- Matriux.
- BlackUbuntu.
- Vacarm Linux.
- Samurai Web Testing Framework.
- BackTrack.

V.2 Choix du système d'exploitation le plus adéquat

Le seul critère de choix est la popularité et le nombre d'utilisateurs dans le monde. Les développeurs de BackTrack ont réussi à faire de cette distribution-là plus connue dans le domaine du pentesting à l'aide de différente communauté et la mise en place de plusieurs certifications dans les différents domaines de la sécurité informatique en se basant sur leur produit.

Figure 4.41: Logo BackTrack

BackTrack est une distribution linux orientée sécurité, son but est de regrouper les outils nécessaires et utiles pour tester la sécurité d'un système réseau. Basé sur Slackware jusqu'à la version 3 et Ubuntu dans les versions ultérieures et margé sa richesse en termes d'outils, BackTrack offre un environnement très extensible et personnalisable ; installation de nos propres outils si nécessaire, l'ajout d'autre outils, configuration et personnalisation des outils, etc.

Les outils de tests sont classés par catégorie (Voir Figure 3.9) : collecte d'informations, évaluation des vulnérabilités, outils d'exploitation, investigations, etc. Sous chaque catégorie, les outils sont classés par le type des cibles (architecture réseau, système, base de données, serveur web, applications, etc.).

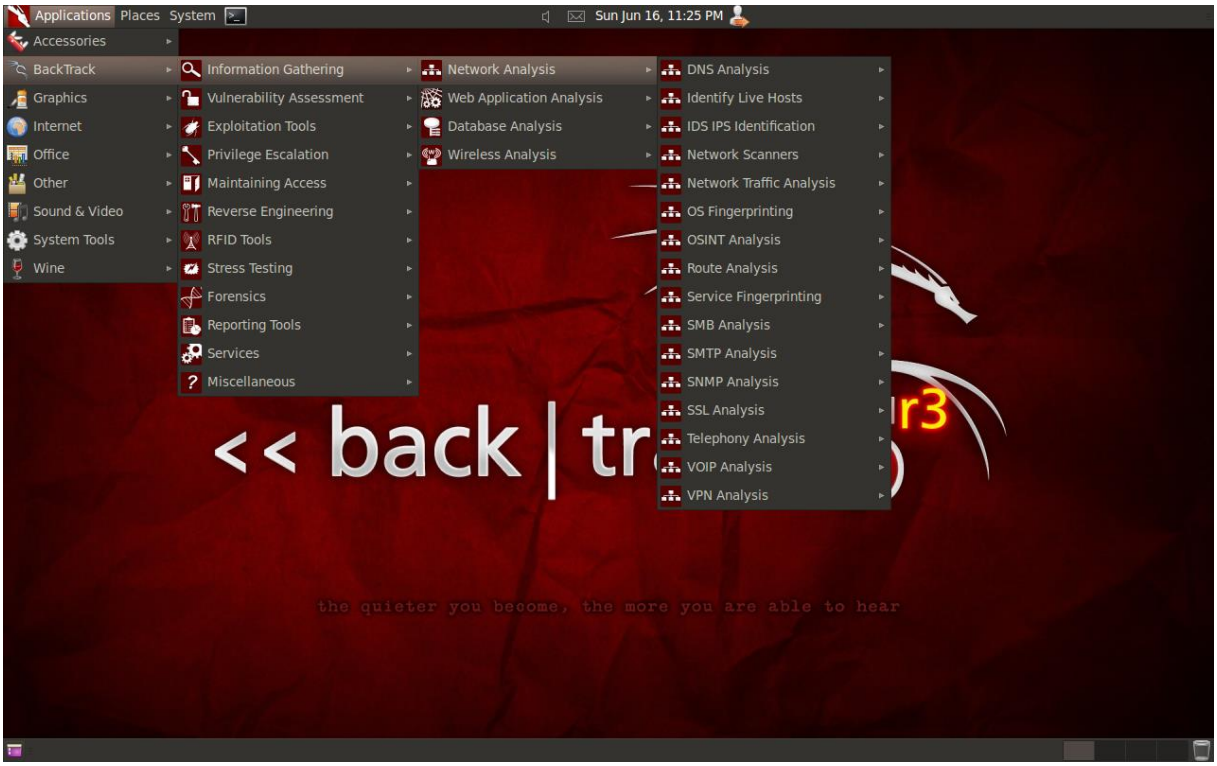


Figure 4.42: Menu de BackTrack

V.3 Scan des ports

V.3.1 Outils de tests

L'outil le plus adéquat dans notre cas est « Nmap ». Ce dernier permet la réalisation des différents types de scan des ports et assure la détection de services et d'OS. Un autre avantage du nmap est la possibilité de créer des scripts personnalisés afin d'automatiser des tâches, par exemple script de détection et exploitation des vulnérabilités, découverte du réseau, amélioration de la détection des versions, etc.

Afin de simplifier la tâche et de fournir des résultats clairs, j'utilise « Zenmap », l'interface graphique du « nmap ». Il fournit plusieurs profils prédéfinis de scan où chaque profil est caractérisé par une commande nmap et une suite d'options permettant la réalisation d'un type e de scan spécifique. Sinon il est possible de créer un nouveau profil.

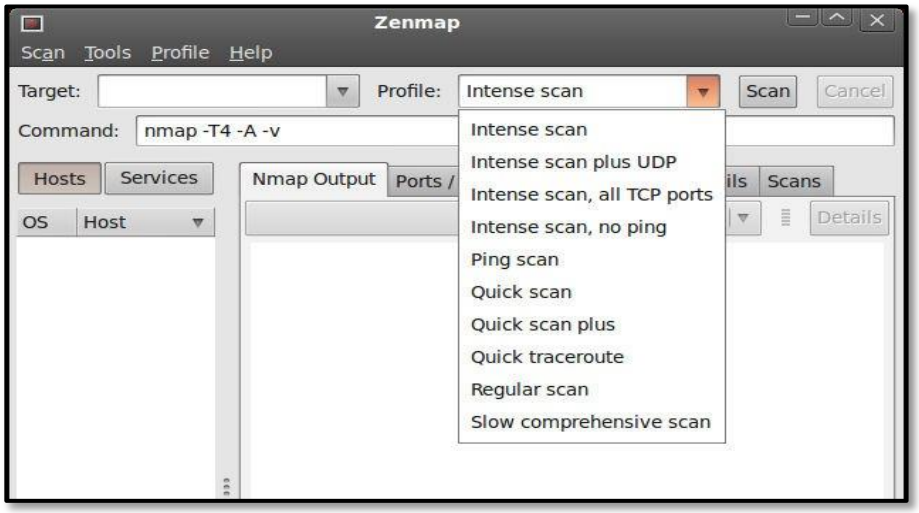


Figure 4.43: interface Zenmap

V.3.2 Tests réalisés

Pour assurer le bon fonctionnement des services de l'infrastructure réseau de COTREL, les différents ports des services doivent être ouverts et fonctionnels. J'ai exécuté les tests suivants pour déterminer les ports ouverts lors de la phase « collecte d'information » du pentesting et vérifier l'état des machines.

Syn Scan

Connu aussi par le nom de « stealth Scan », ce type de scan a pour but principal de déterminer l'état des ports dans la cible. Pour lister les ports ouverts, j'utilise la commande suivante :

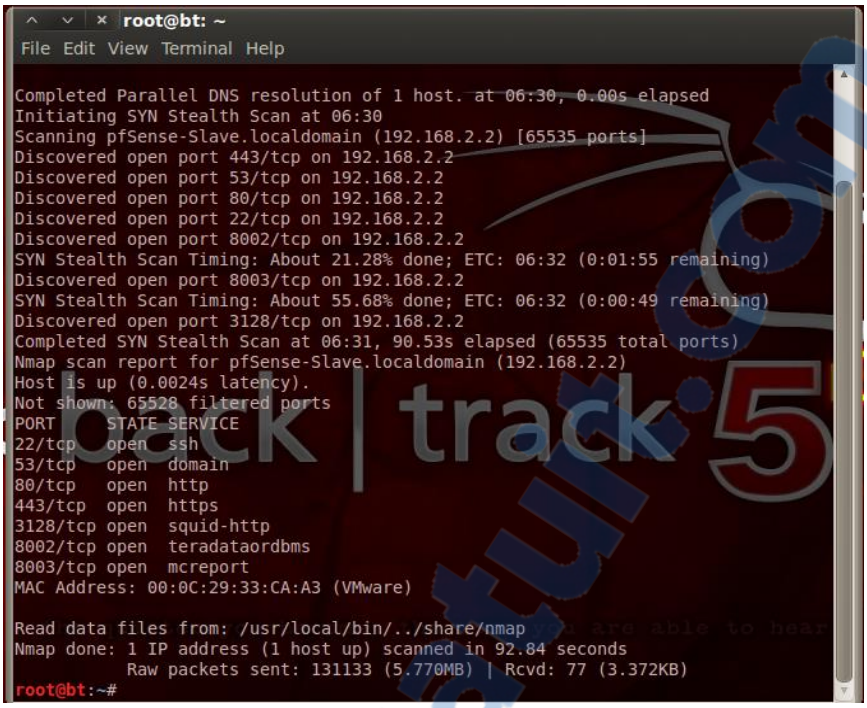


Figure 4.44: test nmap

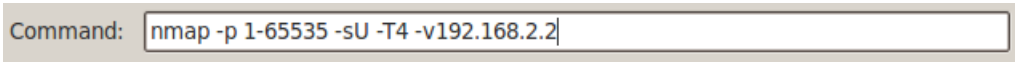
- -p : les ports à scanner.
- -sS : Syn scan
- -T4 : vitesse de scan.
- -v : mode verbeuse qui affiche en temps réel l'exécution de scan et génère plus d'information.

Remarque :

- Je peux choisir un ou plusieurs ports mais dans notre cas il est préférable de tester tous les ports.
- Sous nmap plusieurs options entrent en jeu dans la configuration de la vitesse du scan, l'option -T simplifie cette tâche en offrant plusieurs modes de scan. L'option « -Tx » avec x peut varier de 0 à 5 :
  - Paranoid (0) : Envoi d'un paquet toutes les 5 minutes.
  - Sneaky (1) : Envoi d'un paquet toutes les 15 secondes.
  - Polite (2) : Envoi d'un paquet toutes les 0.4 secondes.
  - Normal (3) : Niveau par défaut. Optimise la durée du scan en minimisant sa durée sans perte de paquet.
  - Agressive (4) : Attente d'une réponse pendant un maximum de 1.25 secondes au maximum.
  - Insane (5) : Attente d'une réponse pendant un maximum de 0.3 secondes.
- Le Syn. Scan est caractérisé par sa vitesse puisqu'il peut balayer des milliers de ports par seconde.

UDP Scan

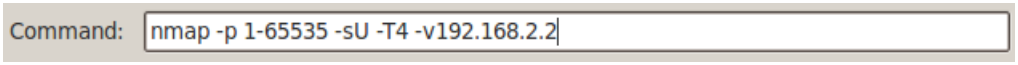
Ce scan permet de savoir s'il y a des services qui utilisent le protocole UDP.



sU : UDP Scan.

Remarque : Le scan UDP est très lent par rapport au SYN Scan.

ACK Scan



X- **mas Scan**

FIN Scan

Null Scan

Je peux minimiser le temps de scan en spécifiant les numéros des ports à scanner, ce type du scénario est conseillé pour le UDP Scan vu qu'il est le plus lent des scans. Je peux également fixer les numéros des ports ou utiliser Nmap par défaut.

Zenmap présente les résultats de scan d'une façon claire en mettant en évidence les Informations importantes (Voir Figure 3.11).

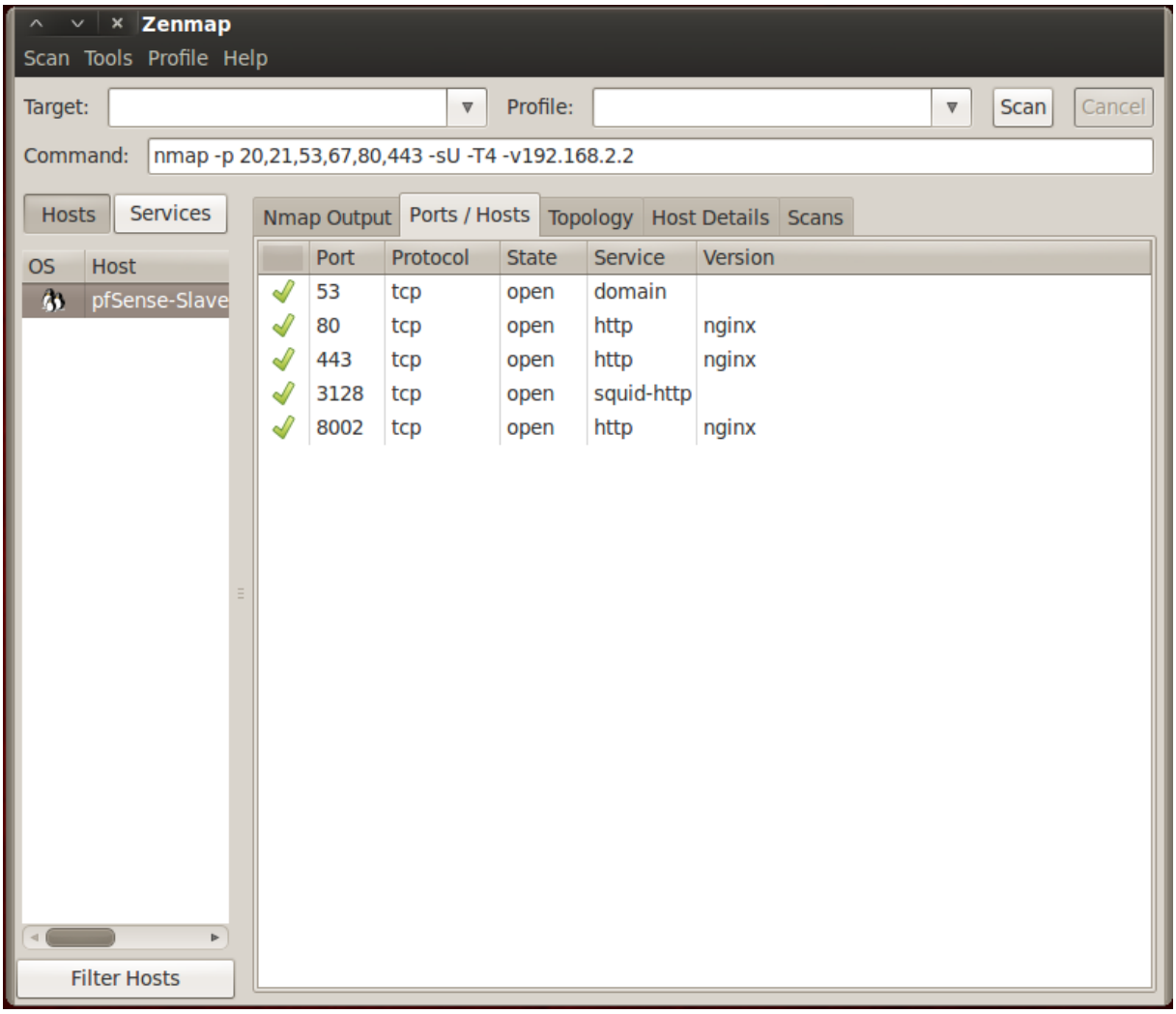


Figure 4.45: Résultat d'un scan de port

V.2 Scan de vulnérabilités

V.2.1 Outils de tests

L'outil le plus adéquat dans notre cas est « OpenVas » (Open Vulnerability Assessment System). C'est un scanner de vulnérabilité open source et le fork libre de Nessus lorsque ce dernier est devenu un logiciel propriétaire lors de son passage à la version 3.

OpenVAS permet aux administrateurs l'audit des réseaux et la recherche des vulnérabilités sur divers systèmes Windows, Linux, Unix. Cet outil signale les failles potentielles du matériel scanné (machine, équipement réseau). Le résultat du scan fournira :

- La liste des vulnérabilités par niveaux de criticité,
- Une description des vulnérabilités,
- La méthode ou un lien qui indique la solution de problème.

Principe de fonctionnement

OpenVas fonctionne grâce un système de 3 modules. C'est à dire que je dispose d'un OpenVas client, OpenVas serveur et un OpenVas NVT Feed Service. Comme le montre le schéma ci-dessous :

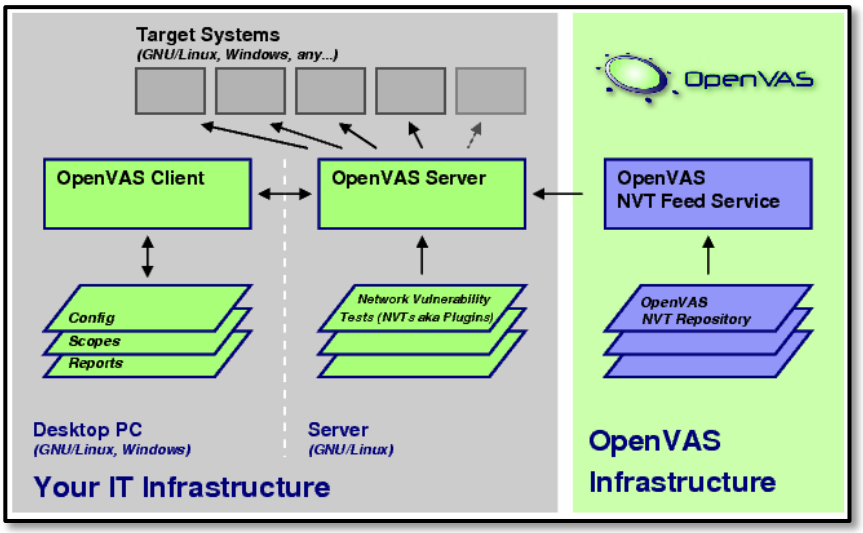


Figure 4.46: Les modules d'OpenVas

Le principe de fonctionnement de l'outil est le suivant :

1) Le client OpenVAS se connecte et s'identifie au serveur.
2) Le client et le serveur s'échangent leurs certificats afin de crypter les données et que le serveur authentifie le client.
3) Le serveur informe le client des différents tests et options disponibles.
4) Le client envoie les différents paramétrages au serveur.
5) Réalisation du scan : les plug-ins de tests analysent la cible en se reposant sur une base de données des vulnérabilités connues.
6) Les informations récoltées ainsi que leurs analyses sont affichées à l'utilisateur.

V.2.2 Installation et configuration d'OpenVas

Sous BackTrack, OpenVas est installé par défaut, il ne reste que sa configuration.

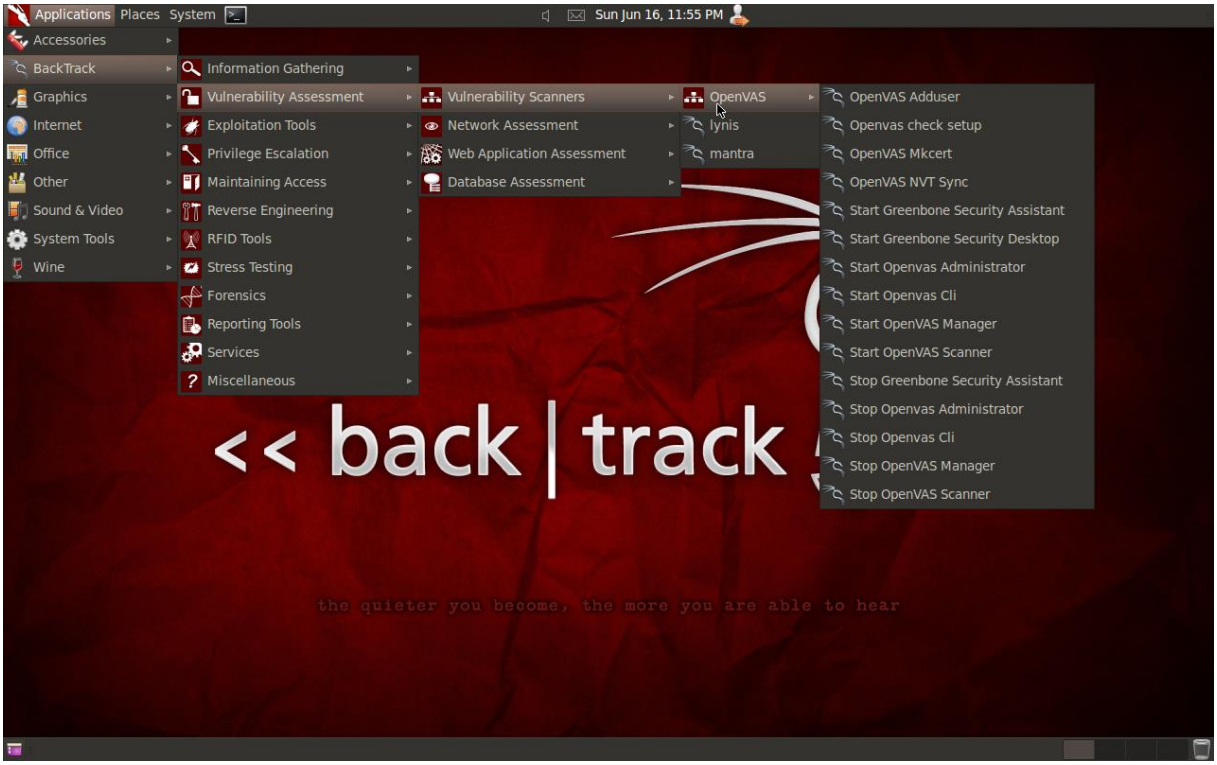


Figure 4.47: Menu de BackTrack

Plusieurs étapes sont nécessaires pour la réalisation d'un scan de vulnérabilités avec OpenVas :

<u>Etape 1</u> : Création d'utilisateur

Je vais créer un utilisateur pour pouvoir s'identifier et utiliser le client.

J'utilise la commande « **openvas-adduser »** et je suis les instructions.

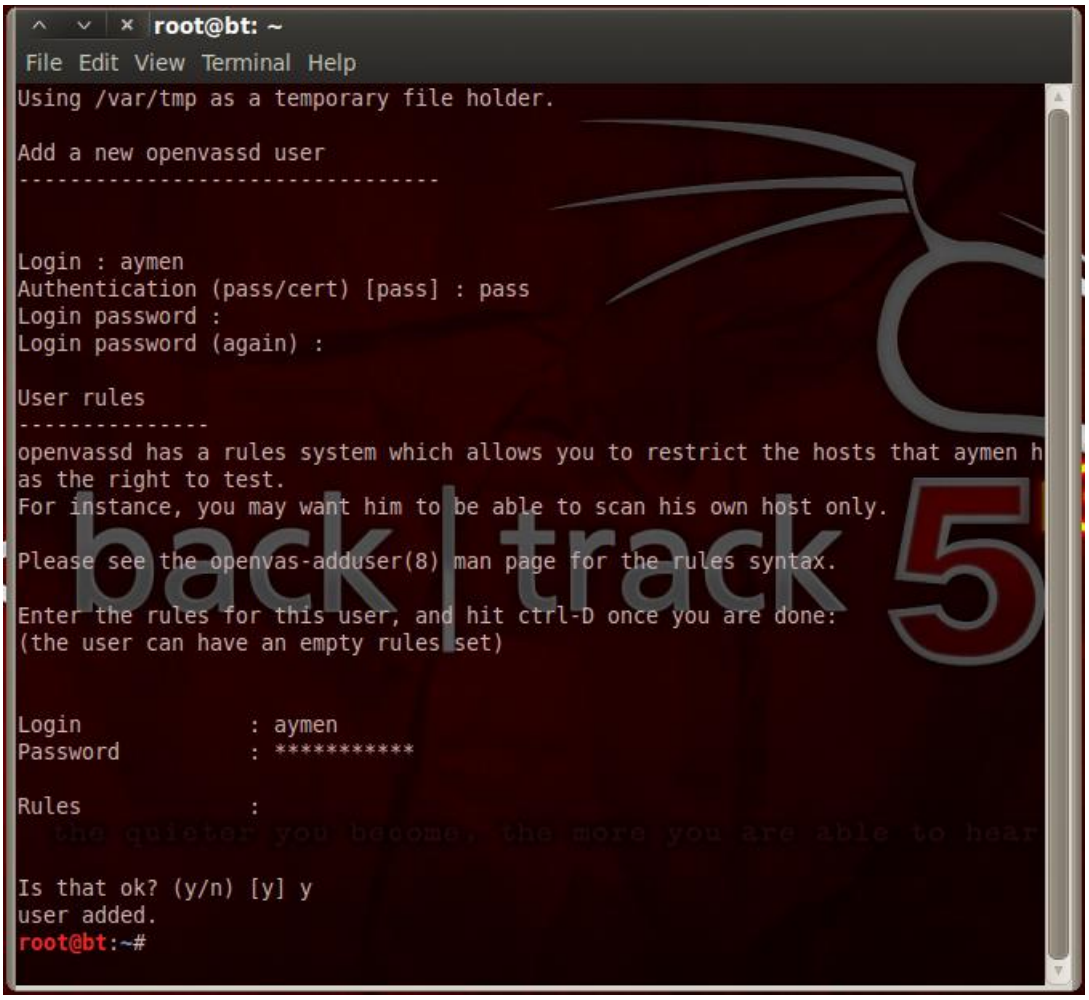


Figure 4.48: Création d'utilisateur OpenVas

Ici j'ai la possibilité de s'authentifier par mot de passe ou par certificat. Ainsi, je peux définir des règles pour cet utilisateur.

Pour les règles appliquées à cet utilisateur je les ai laissés en blanc en appuyant sur CTRL-D Cela signifie que cet utilisateur sera en mesure d'exécuter des tâches sans aucune restriction.

Etape 2 : Construction des certificats

C'est ici que je vais créer dans un premier temps notre certificat SSL. Il va me permettre la communication de notre client avec notre serveur. En effet leur communication n'est possible que par une communication SSL chiffrée. Pour cela j'utiliserai la commande **« openvas-mkcert »** qui va me générer deux certificats, un certificat d'autorité local (CA) et un autre pour le serveur qui est signé par la CA.

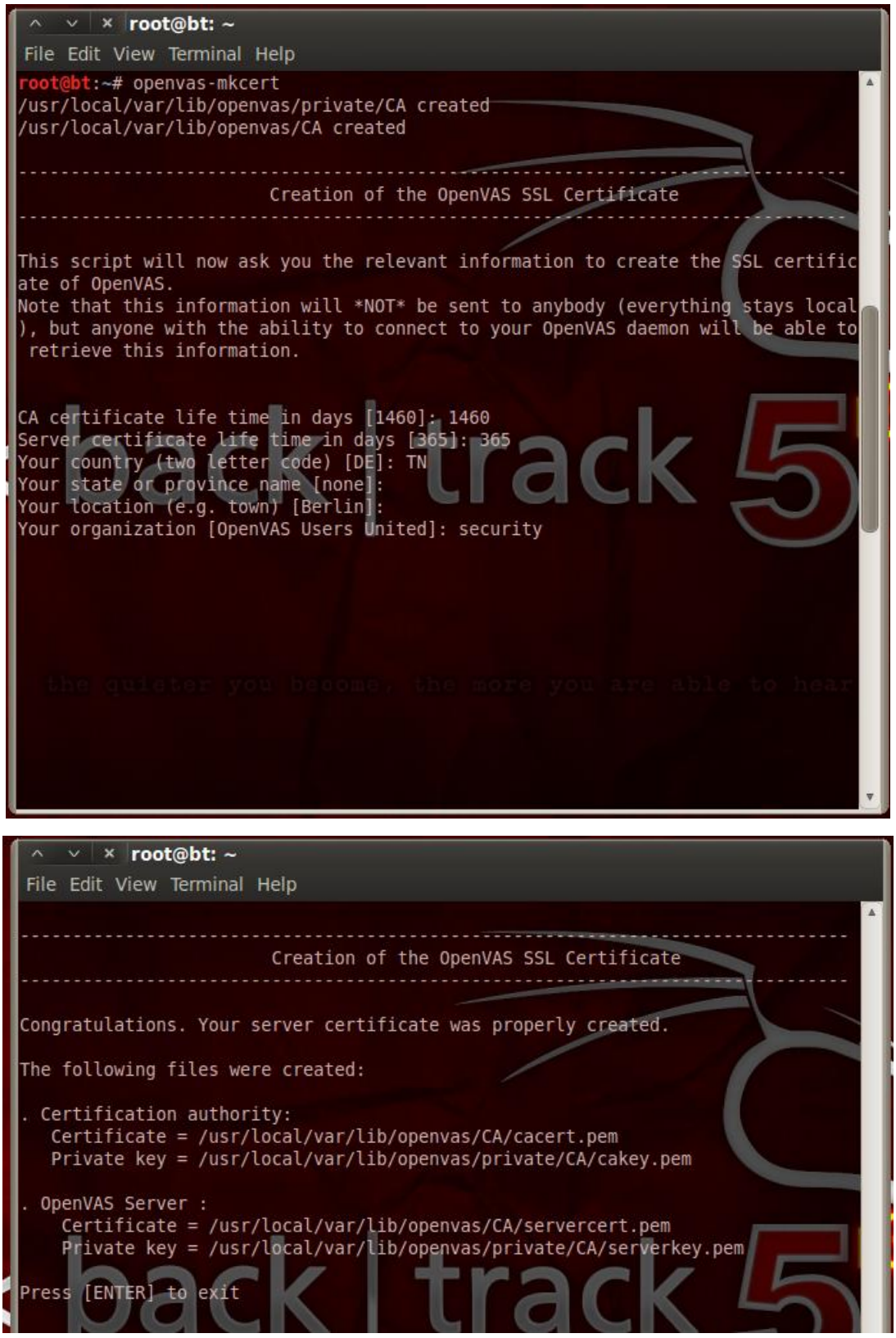


Figure 4.49: Création de certificat

<u>Etape 3</u> : Synchronisation de NVT

A ce stade, j'ai besoin de la dernière série de NVT. Ce module permettant de garder la base de données du serveur à jour afin de détecter les vulnérabilités.

J'utilise la commande **« openvas-nvt-sync »**.

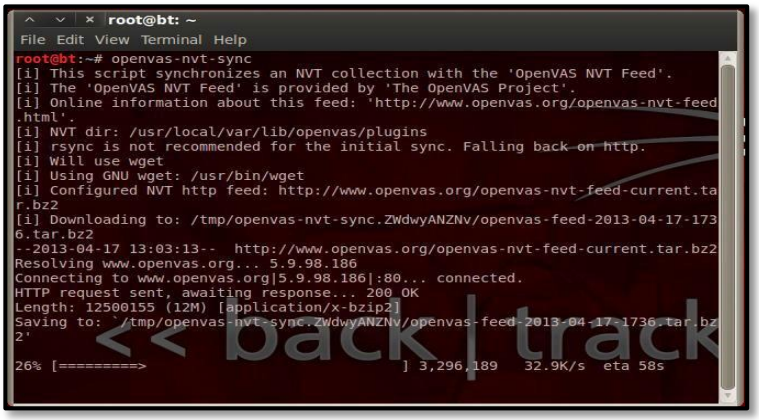


Figure 4.50: Chargement de module NVT

Maintenant que j'ai créé nos certificats, nos utilisateurs, et que notre serveur est à jour, je vais l'utiliser.

Etape 4 : Démarrage de scanner

Le module OpenVas server est le cœur même de cet outil. En effet c'est lui qui est chargé d'effectuer les tests de vulnérabilités et de faire le rapport. Les différents tests se présentent sous formes de plugins. J'utilise la commande **« openvassd »** ou bien le menu pour démarrer le serveur et charger les plugins.

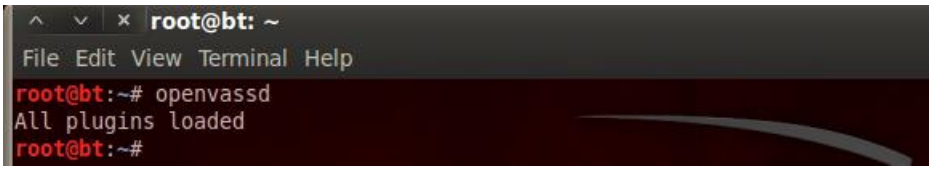


Figure 4.51: Démarrage d'OpenVas Server

Etape 5 : Configuration d'OpenVas Manager

J'opte pour la création d'un certificat client pour le gestionnaire OpenVas par la commande

« Openvas-mkcert-client –n om –i ».

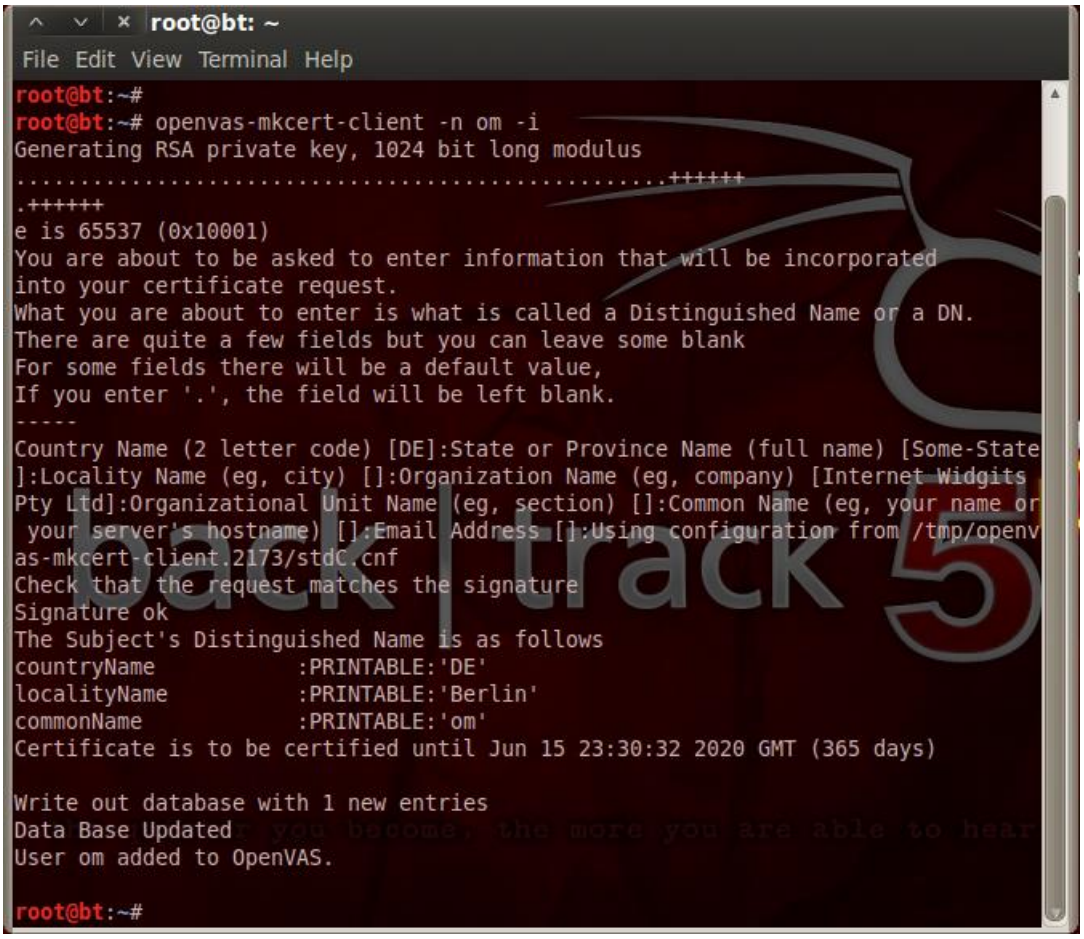


Figure 4.52: Certificat client d'OpenVas Manager

Etape 6 : Reconstruire la Base De Données

A cause de ce nouveau certificat, notre base de données est hors de « date » pour ainsi dire. Chaque fois que j ' exécute la synchronisation NVT à tirer les plus récents, je dois reconstruire la base de données à nouveau. Cela se fait avec une simple commande « Openvasmd --rebuild ».

Etape 7 : Configurer OpenVas Administrateur

Je dois créer un utilisateur administratif nommé admin qui me permet d'exécuter toutes nos analyses. Ceci est fait en exécutant la commande suivante **« openvasad- c 'add_user'-n admin -r Admin »**.

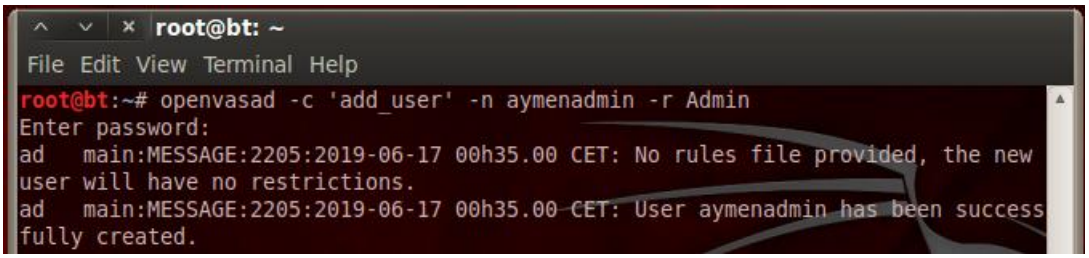


Figure 4.53: Reconstruction de la Base De Données

Etape 8 : Démarrer OpenVas Manager

L'OpenVas Manager fonctionne comme un démon en arrière-plan. J'utilise localhost pour l'écoute et le port par défaut 9390. Ceci est fait en exécutant la commande

« Openvasmd -p 9390 -a 127.0.0.1 »

Etape 9 : Démarrer OpenVas Administrateur

Ceci est fait par ma commande **« openvasad –a 127.0.0.1 –p 9393 ».**

Etape 10 : Démarrer Greenbone Security Assistant

Enfin, je fais le démarrage de Greenbone Security Assistant. Cela est exécuté comme un démon en arrière-plan. J'utilise la commande **« gsad –http-only –listen=127.0.0.1 –p 9392 »**.

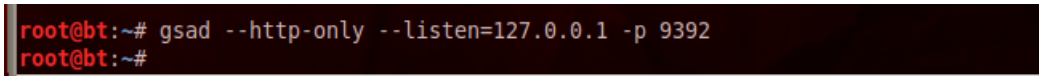


Figure 4.54: Démarrage de Greenbone Security Assistant

A ce stade, notre installation est pratiquement terminée. Maintenant, je vais réaliser le scan de vulnérabilité d'une machine qui possède l'adresse IP 192.168.0.30.

V.2.3 Test d'utilisation d'OpenVas

Je peux utiliser l'interface OpenVas client selon deux méthodes :

1) je démarre l'interface cliente à travers le navigateur web en tapant http://127.0.0.1:9392.

Ensuite, j'introduis le login et le mot de passe.

Figure 4.55: Interface d'authentification de Greenbone Security Desktop

D'abord, je dois spécifier notre cible afin de lancer le scan de vulnérabilité.

Cela est fait par la création de « New Target », comme le montre la Figure 3.22.

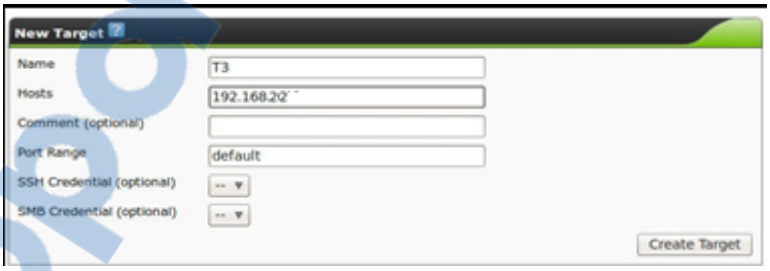


Figure 4.56: Création « New Target »

Ensuite, je fais la création d'une nouvelle tâche en indiquant le type de scan et l'adresse IP de la victime.

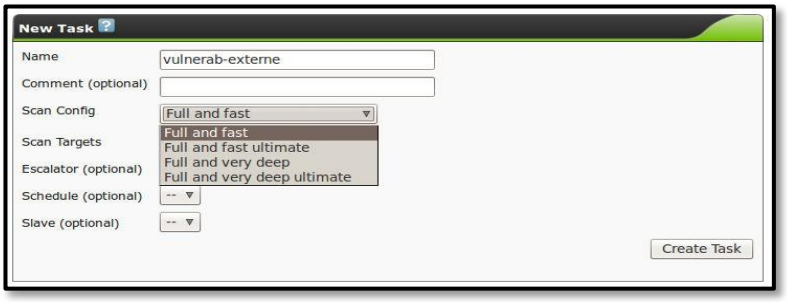


Figure 4.57: Création de « New Task »

Par la suite, je lance le scan et cela peut durer plusieurs minutes.

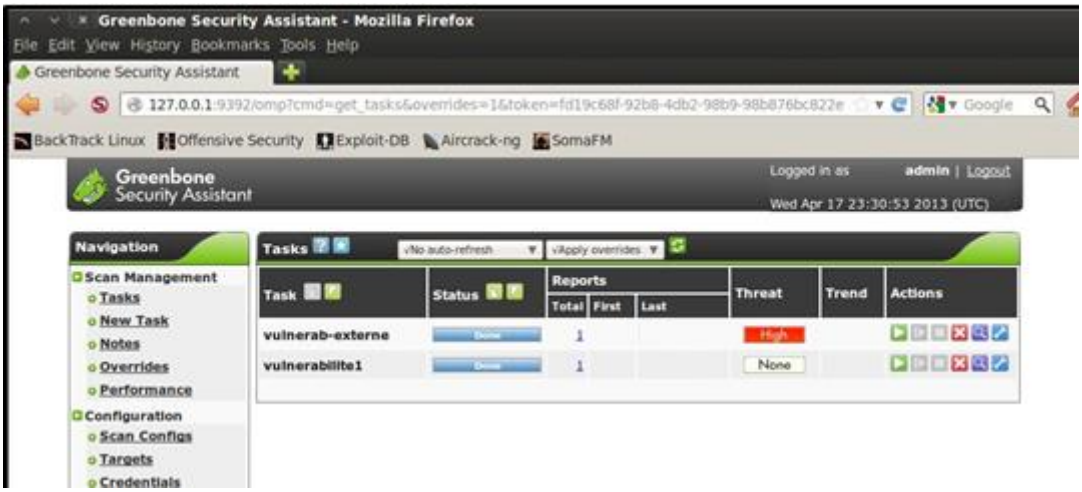


Figure 4.58: Scan de vulnérabilité

OpenVAS va lancer une batterie de tests de vulnérabilités sur la machine et générer un rapport dans lequel il décrit les vulnérabilités trouvées et les solutions existantes.

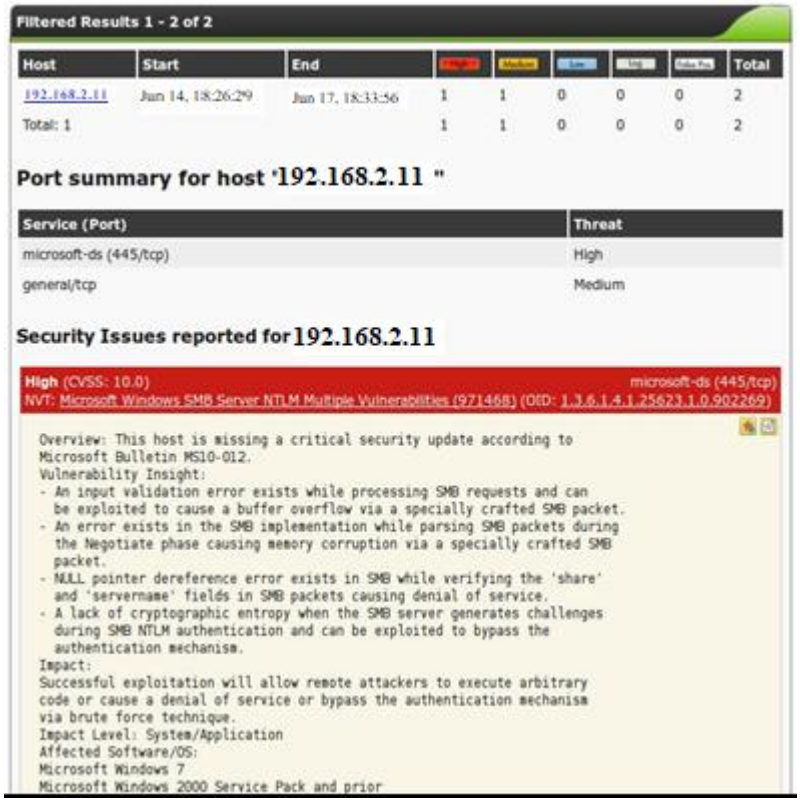


Figure 4.59: Rapport de scan

Les vulnérabilités sont classées en trois catégories :

- Les vulnérabilités critiques
- Les avertissements
- Les notes

Un traitement sur ces rapports pourra me permettre de lui attribuer un indice de criticité.

- Si une vulnérabilité classée « critique » est présente dans le rapport, ce dernier a une criticité de 3.
- Si une vulnérabilité classée « avertissement » est présente dans le rapport, ce dernier a une criticité de 2.
- Si une vulnérabilité classée « note » est présente dans le rapport, ce dernier a une criticité de 1.
- Si le rapport ne contient aucune vulnérabilité, il a une criticité de 0.

2) Je démarre l'interface OpenVas cliente à travers Greenbone Security Desktop.

Ce dernier se trouve au niveau de menu de Back Track. Il offre les mêmes fonctionnalités de l'interface web. Mais son avantage se trouve au niveau de l'affichage de tableau de bord qui montre la classification des vulnérabilités à travers les graphes.

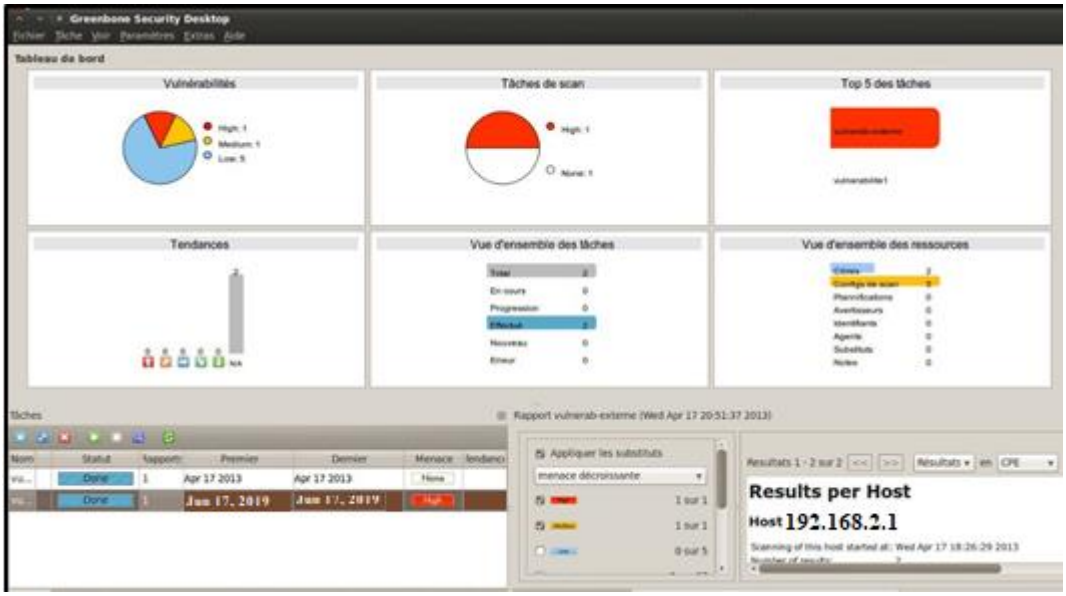


Figure 4.60: Scan de vulnérabilité par Greenbone Security Desktop

Après avoir étudié et exploité les scanners réseau existant sur le marché, je m'intéresse à la conception et développement d'une application de balayage réseau spécifique à l'entreprise.

VI. TEST DE LA SOLUTION DE SECURITE

Ce chapitre est consacré à la réalisation des différents scénarios de tests afin de mettre à l'épreuve la sécurité de notre environnement et qualifier sa résistance à un certain niveau d'attaque.

VI.1 Les attaques

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

Une attaque est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel, erreur de configuration, etc.) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Sur l'Internet, des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques.

Un scénario d'intrusion sur un système peut se décomposer en six actions élémentaires, enchaînées selon un processus itératif :

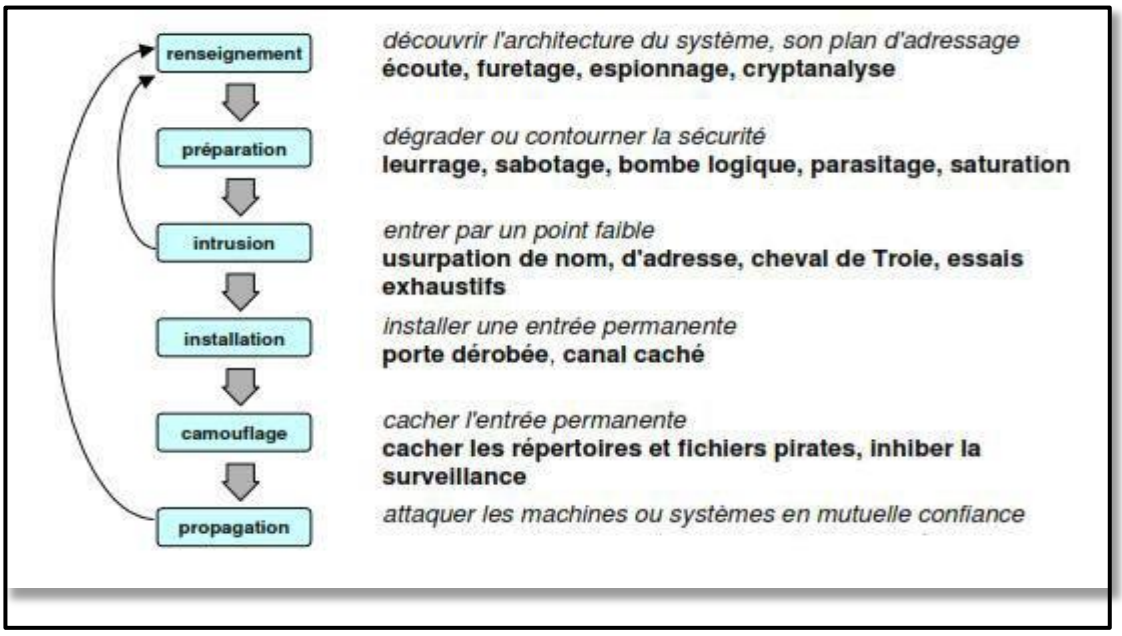


Figure 5.1: Déroulement d'une attaque.

VI.2 Les scénarios de tests

VI.2.1 Scénario 1 : Attaque scan de ports

Comme déjà vu au niveau du chapitre 3 « Etude et test des outils de scan », le scan de ports (ou balayage de ports) consiste à tenter d'ouvrir une connexion sur chaque port TCP (ou UDP) d'une machine afin de déterminer les services qu'elle propose et trouver ainsi d'éventuelles vulnérabilités comme un service comportant une faille connue. Le scan des ports appartient à la phase de reconnaissance.

Ainsi, il est considéré par les pare feux et les systèmes de sécurité en général comme une attaque à proprement parler même s'il ne s'agit que d'une découverte de services. Cependant, cette découverte donne en général les informations de base nécessaires pour l'attaque de la machine.

Outils de test

Pour réaliser l'attaque de scan de ports, je vais utiliser Nmap. Ce dernier un scan de port TCP et UDP, en ligne de commande est aussi en mode graphique. Il permet de détecter si une machine est sur un réseau, d'identifier les services qui tournent dessus et même d'en déduire dans certain cas le type d'operating system.

Procédure de l'attaque

Au niveau de la machine de l'attaquant, je réalise le scan des ports afin de récupérer la Liste des ports TCP ouverts et le type du système d'exploitation utilisé.

J'utilise la commande suivante :

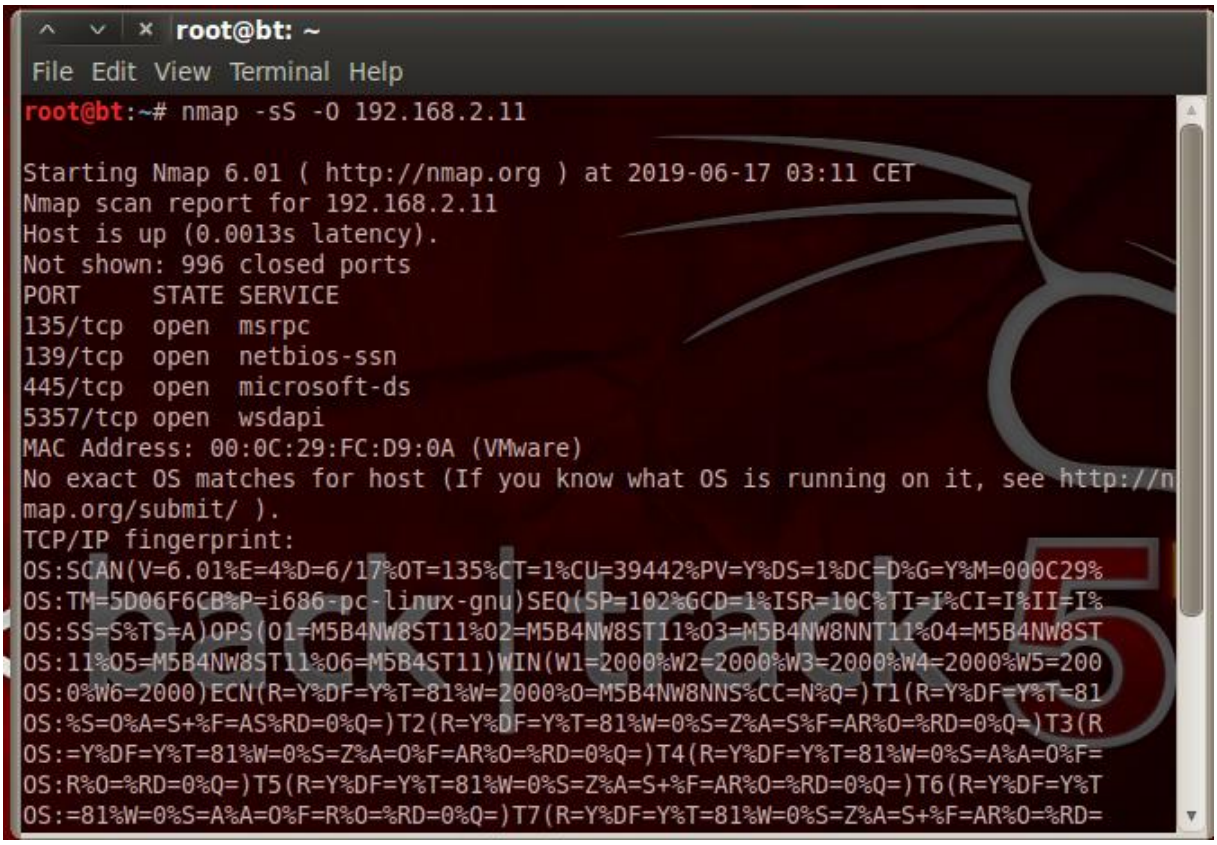


Figure 5.2: Scan des ports de la machine victime

Ce test m'affiche la liste des ports ouverts avec le nom de service, l'adresse physique de la machine victime et le système d'exploitation utilisé. Toutes ces informations forment un moyen pour réaliser le pentest et rendre le système exploitable par les intrus.

VI.2.2 Scénario 2 : Attaque Déni de Service

Un « déni de service » (Denial of Service ou DoS) est une attaque réalisée dans le but de rendre indisponible durant une certaine période le ou les services ou ressources d'une organisation. Généralement, ce type d'attaque à lieu contre des machines et serveurs d'une entreprise afin qu'ils deviennent inaccessibles pour leurs clients.

Le but d'une telle attaque n'est pas d'altérer ou de supprimer des données, ni même de voler quelconque information. Il s'agit ici de nuire au fonctionnement d'un service ou à la réputation d'une société qui offre un service sur Internet en empêchant le bon fonctionnement de celui-ci.

Principe : envoyer une très grande quantité de paquets, dont la taille est relativement importante, en même temps, voire sur une longue période.

Le principe du Distributed Denial of Service (DDoS) consiste à utiliser une grande quantité de postes « Zombies » dans l'intention de paralyser la réponse de machine victime.

Outil de test :

LOIC (Low Orbit Ion Cannon) est un outil dédié pour les attaques de type DDOS, déjà utilisé par « Anonymous » lors de leurs attaques sur les sites gouvernementaux pendant la révolution Tunisienne en décembre 2010 et beaucoup d'autres attaques utilisées un peu partout dans le monde.

Pour effectuer cette attaque, il tente d'attaquer par déni de service distribué (DDOS) le site ciblé en inondant le serveur avec des paquets TCP, des paquets UDP, ou des demandes HTTP avec l'intention de perturber le service d'un hôte particulier.

Procédure de l'attaque Déni de service :

Le fonctionnement basique de LOIC est le suivant : L'utilisateur fourni une IP ou une URL, règle le port, le type d'attaque.

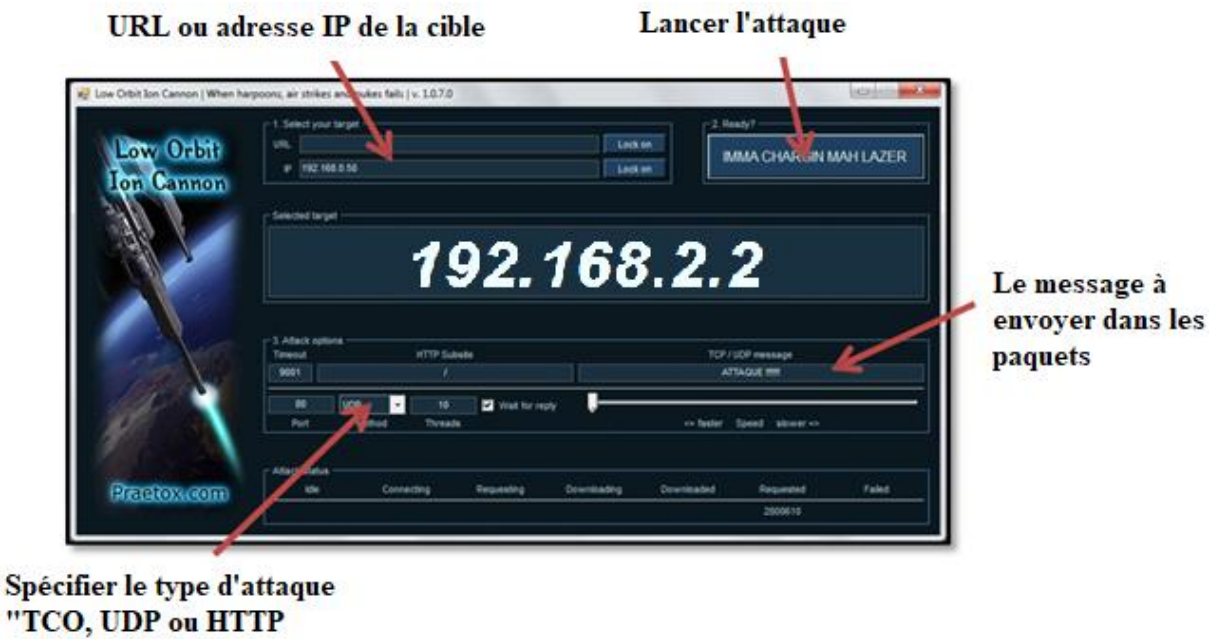


Figure 5.3: Attaque Déni de service par LOIC

VI.2.3 Scénario 3 : Attaque ARP poisoning par Man in the middle

L'ARP poisoning est une technique utilisée en informatique pour attaquer tout réseau local utilisant le protocole de résolution d'adresse ARP. Cette technique peut permettre à l'attaquant de détourner des flux de communication transitant sur un réseau lui permettant de les écouter, de les corrompre, mais aussi d'usurper une adresse IP ou de bloquer du trafic.

Man in the middle est un scénario d'attaque dans lequel un attaquant écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties.

Cette usurpation d'adresse IP se fait en envoyant un paquet ARP empoissonné à la machine A afin qu'il envoie ses paquets à l'attaquant C, alors qu'ils étaient destinés à la victime B.

Da manière analogue, l'attaquant C envoie un paquet ARP empoissonné vers la

Machine B afin qu'elle envoie ses paquets à l'attaquant C au lieu de les envoyer à la machine

A. L'attaquant C détourne le flux de données entre les machines A et B et il peut voir les données qui transitent en clair entre les deux machines.

Dans cette technique, je retrouve une autre technique qui est le spoofing.

L'IP spoofing est une technique qui a pour ambition d'usurper une adresse IP d'une machine cible et qui est généralement employé pour obtenir un accès non autorisé sur une machine.

L'émetteur malveillant envoie des messages à l'ordinateur cible en utilisant une adresse IP qui semble indiquer que le message provient d'une machine de confiance.

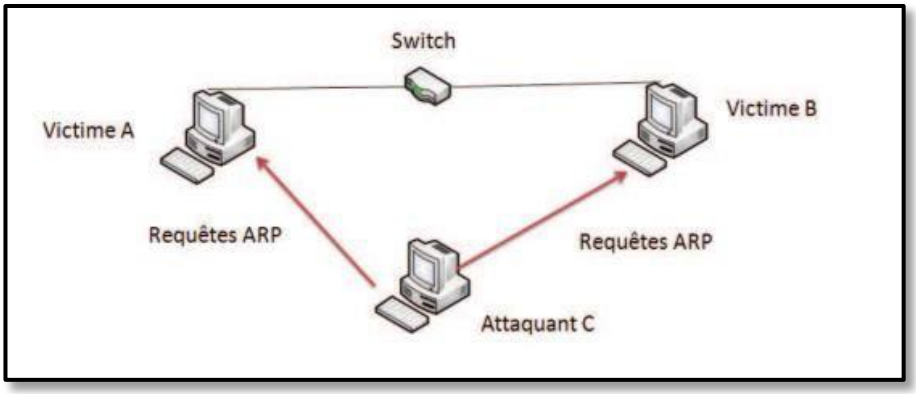


Figure 5.4: Schéma d'ARP poisoning.

Outil de test :

Les outils comme "Dsniff", "Arpoisson" et "Ettercap" peuvent être utilisés pour effectuer des attaques ARP spoofing. Notre choix est fixé sur l'utilisation d'Ettercap.

Ettercap est un utilitaire réseau aux multiples fonctionnalités. A sa naissance, l'utilisation la plus courante que j'en faisais été de sniffer (capturer les paquets) des réseaux LAN. Dorénavant, il est également possible de réaliser des attaques de type Man In The Middle (MITM ou "Homme au milieu).

Ettercap est doté de plugins facilitant la recherche de mots de passe. Pour cela, il suffit simplement qu'une session d'un protocole non sécurisé ait lieu, et Ettercap détecte toutes les informations sensibles. De nombreux protocoles sont supportés (FTP, HTTP, telnet,).
Il est également composé de fonctions intéressantes sur le réseau comme l'injection de requêtes, soit à envoyer au client, soit à envoyer au serveur. Je peux également réaliser des analyses d'hosts intéressantes et des identifications sur les machines.

C'est un projet libre, qui peut être utilisé au travers d'un mode graphique, et d'un mode Texte simple, ou interactif avec des menus.

Procédure de l'attaque ARP poisoning :

Pour lancer Ettercap j'utilise le menu de Back Track > Privilege Escalation > Protocol Analysis > Network Sniffers > ettercap-gtk.

Figure 5.5: Lancement d'Ettercap à partir le menu de Back Track

Il faut en premier lieu spécifier ce que je souhaite "sniffer" : pour ce faire, je choisis le mode à partir du menu.

- Unified : sur une seule carte réseau
- Bridged : sur deux cartes réseau

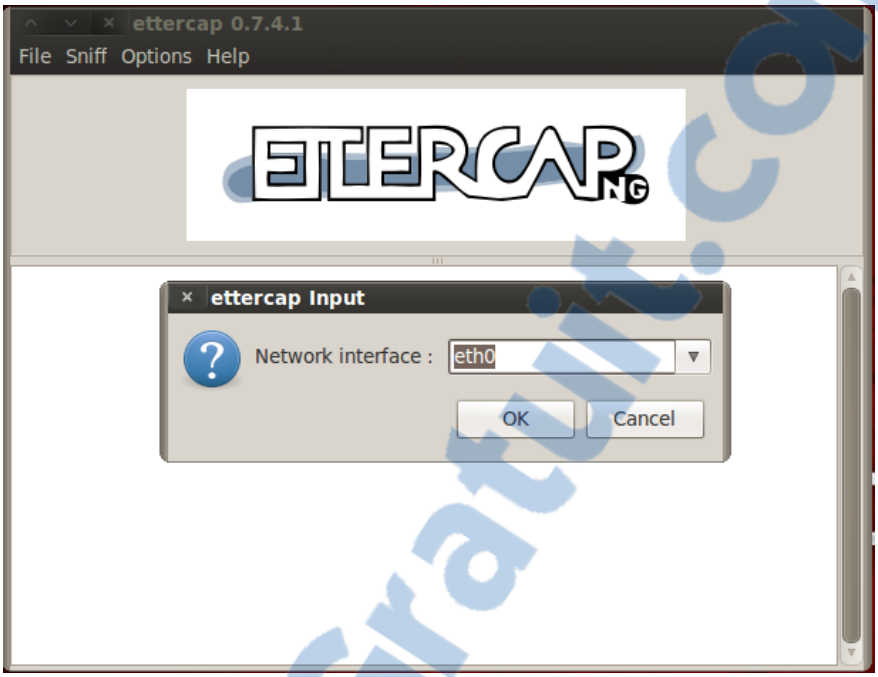


Figure 5.6: Choisir l'interface de sniff

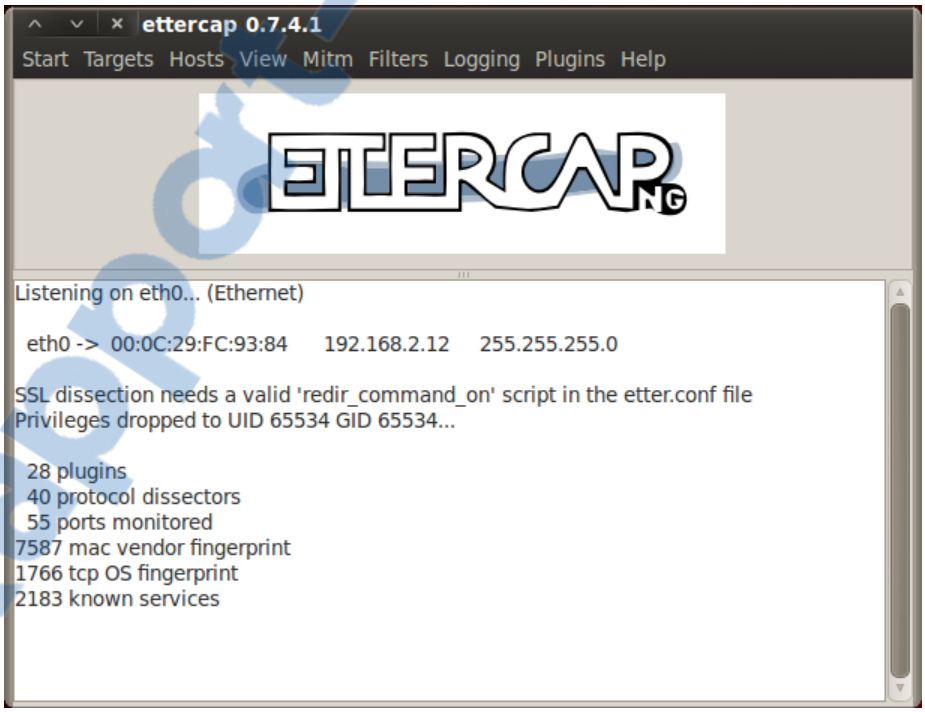


Figure 5.7: Sniff sur l'interface eth1

Afin de réaliser de l'ARP Poisoning, il faut tout d'abord scanner la plage IP correspondant au réseau local du poste, afin de déterminer les hôtes en ligne. Le bouton Scan for Host réalisera cette action.

Les hôtes en ligne seront alors ajoutés dans la "Host List". Target1 et Target2 représentent la liste des ordinateurs entres lesquels j'm'immisce. Ensuite, je sélectionne ARP Poisoning dans le menu Mitm.

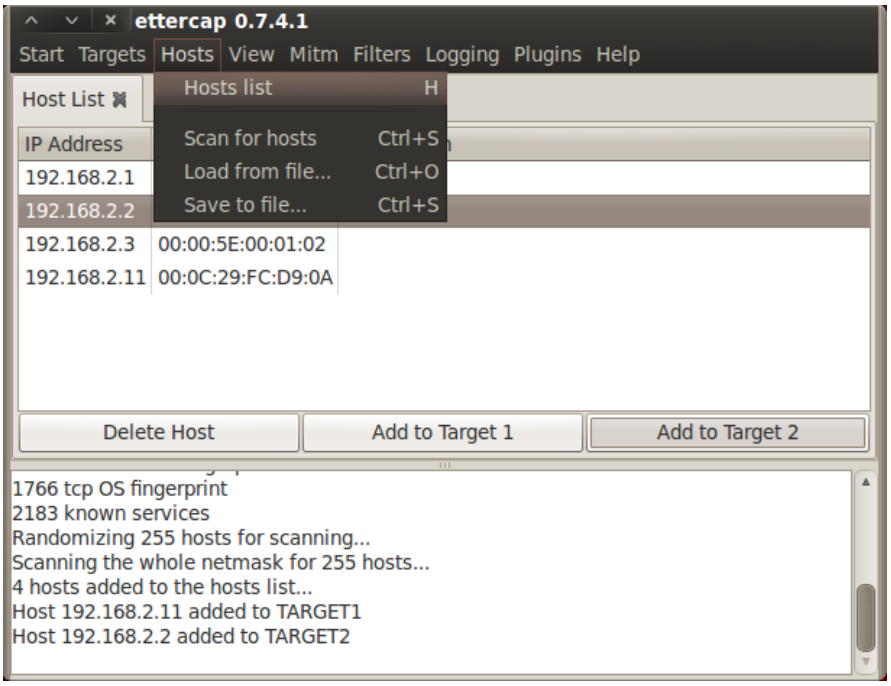


Figure 5.8: Sélection des cibles

Pour commencer l'attaque, je choisis start sniffing de menu start.

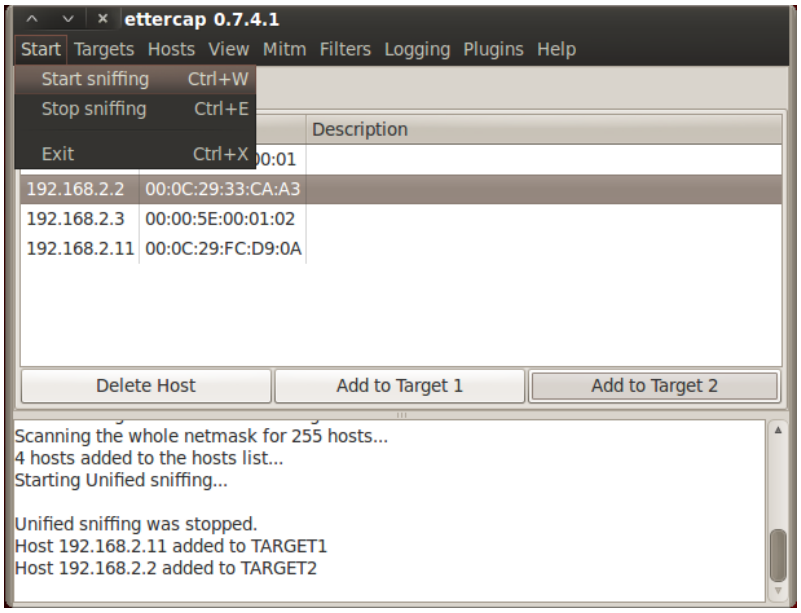


Figure 5.9: Lancement de l'attaque ARP Poisoning

Je peux utiliser Ettercap avec d'autres outils ainsi qu'avec les plugins. Par exemple, le plugin chk_poison indiquera si l'ARP poisoning fonctionne bien ce qui est fort appréciable.

Figure 5.10: Test de fonctionnement de l'attaque ARP Poisoning

Lorsque la victime consulte le site www.commentcamarche.net et elle fait introduire

son login / mot de passe, l'attaquant peut visualiser le paquet envoyé en indiquant les informations relatives à cet utilisateur.

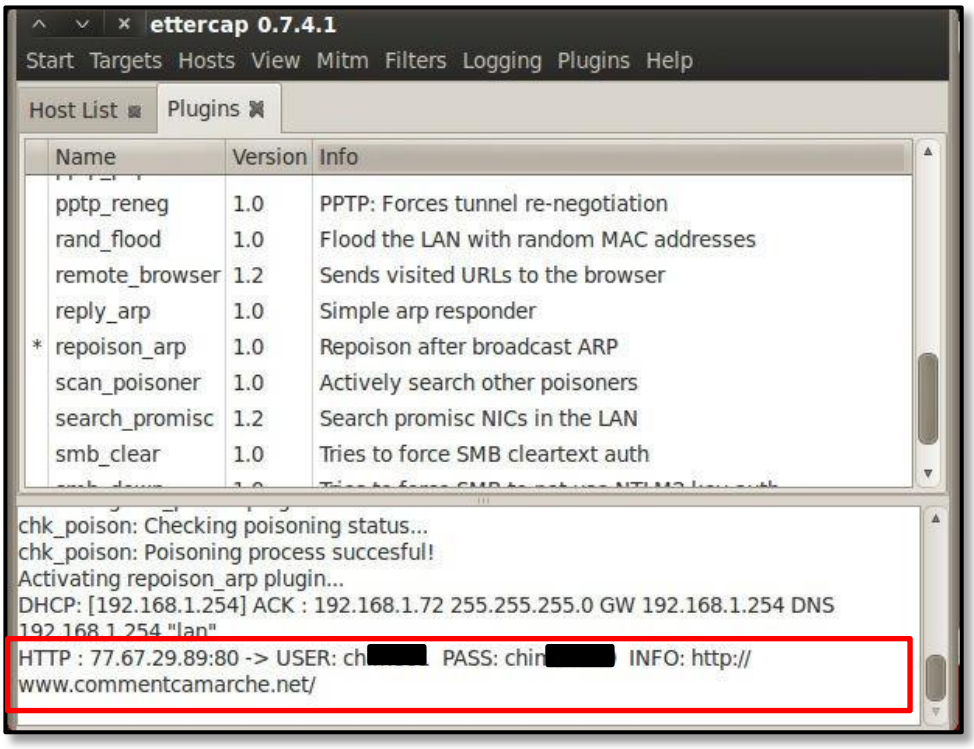


Figure 5.11: Sniff des paquets

VI.3 Test de la haute disponibilité

L'adresse IP d'un utilisateur de réseau LAN est 192.168.2.11.

Je fais la commande Ping avec option –t de PC de l'utilisateur vers google.fr

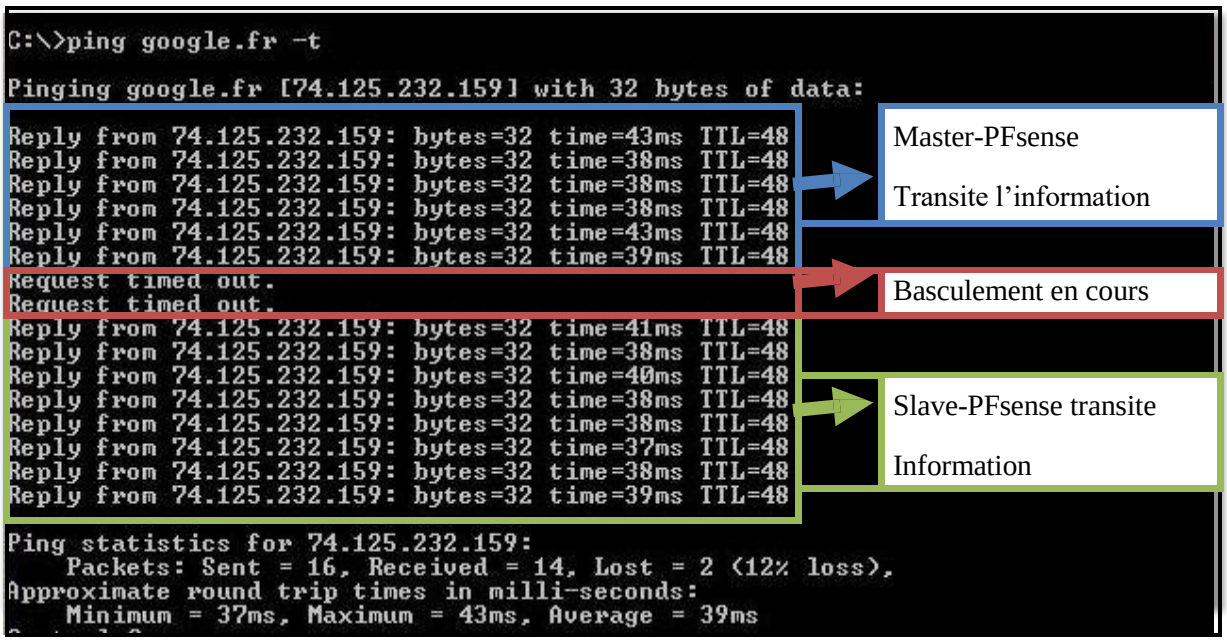


Figure 5. 12 : Test de la solution dual Firewall

Le firewall principale "Master-PFsense" transite l'information au départ, c'est lui la Passerelle par défaut du réseau local.

Débranchons-le maintenant du LAN ou du WAN, si tout va bien, le basculement s'effectue (10 secondes Max) et l'information retransite au travers Slave-PFsense en attendant que Master-PFsense soit reconnecté et opérationnel.

VI.4 Test de la solution antivirale

Pour tester l'antivirus ClamAV, je tente de télécharger le fichier test Eicar test à partir eicar.org.

Le fichier de test n'est pas un véritable virus, le fichier contient une signature normalisée qui est utilisée pour tester les logiciels antivirus. Si HAVP (Http Antivirus proxy) et l'antivirus fonctionnent correctement, alors je dois être redirigé vers une page qui montre que l'accès est refusé.

Figure 5. 13 : Test de la solution antivirale

VI.5 Test de fonctionnement du serveur proxy

D'abord, il faut faire la configuration du serveur proxy au niveau le navigateur de Chaque machine cliente en spécifiant l'adresse IP et le port.

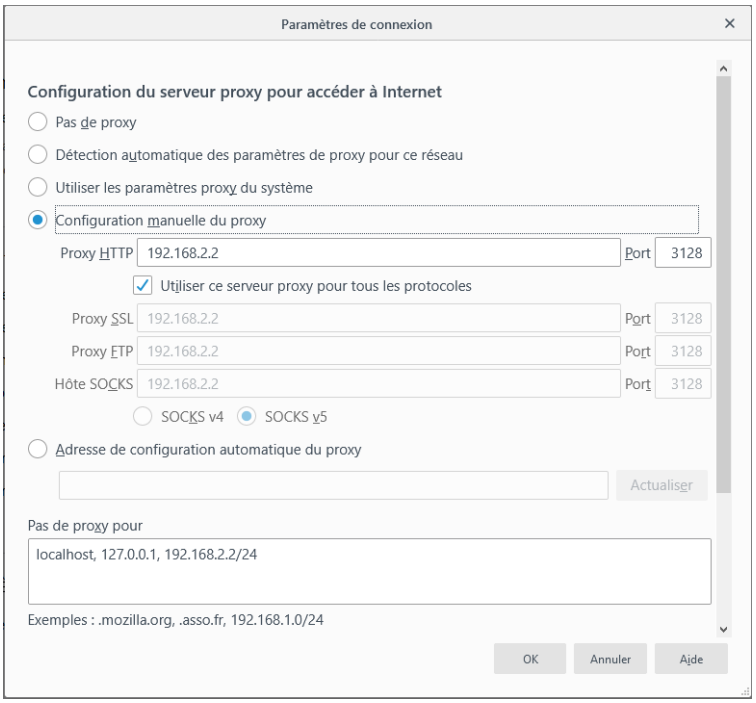


Figure 5.14: Configuration de serveur proxy au niveau du client

Lors de l'ouverture de navigateur, l'interface d'authentification ci-dessous s'affiche. Chaque client doit indiquer son Login et Password pour pouvoir utiliser la connexion Internet.

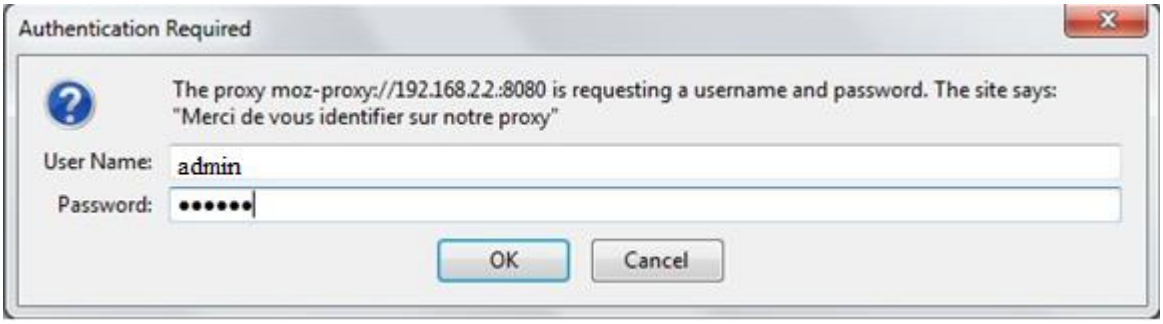


Figure 5.15: Authentification niveau proxy

La copie d'écran ci-dessous montre bien que l'accès au site www.youtube.com est interdit puisqu'il se trouve au niveau de Blacklist de squid.

Figure 5.16: Accès interdit au site www.youtube.com

Ainsi, je peux consulter le fichier log des pages web visitées par les clients à travers SquidGuard.

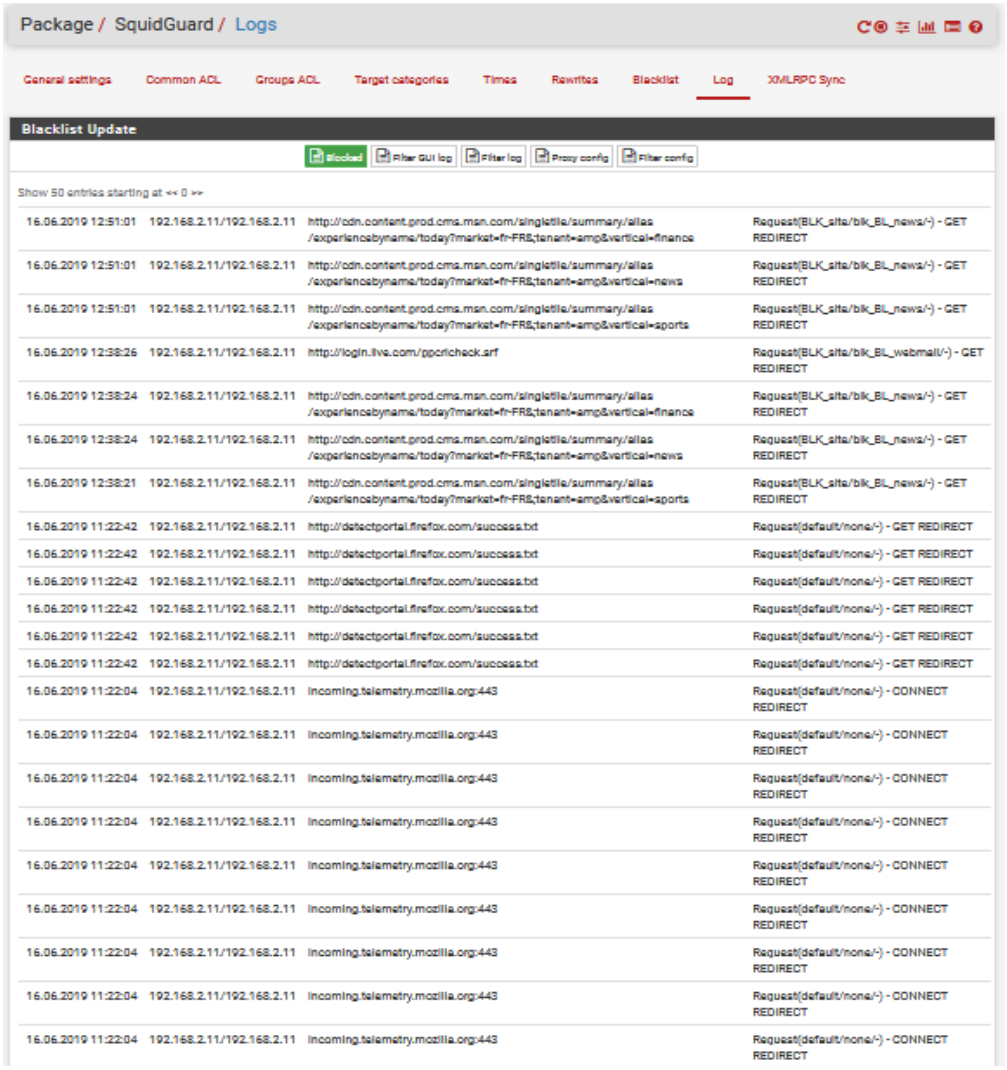


Figure 5.17: Fichier log de SquidGuard

VI.6 Test du système de détection d'intrusion

Au cœur de la réalisation des attaques présentées au début du chapitre, notre système de détection d'intrusion Snort est en mode écoute du trafic réseau.

Il possède un fichier de log /var/log/snort/alert dans lequel je trouve toutes les tentatives d'attaque réalisé sur notre réseau.

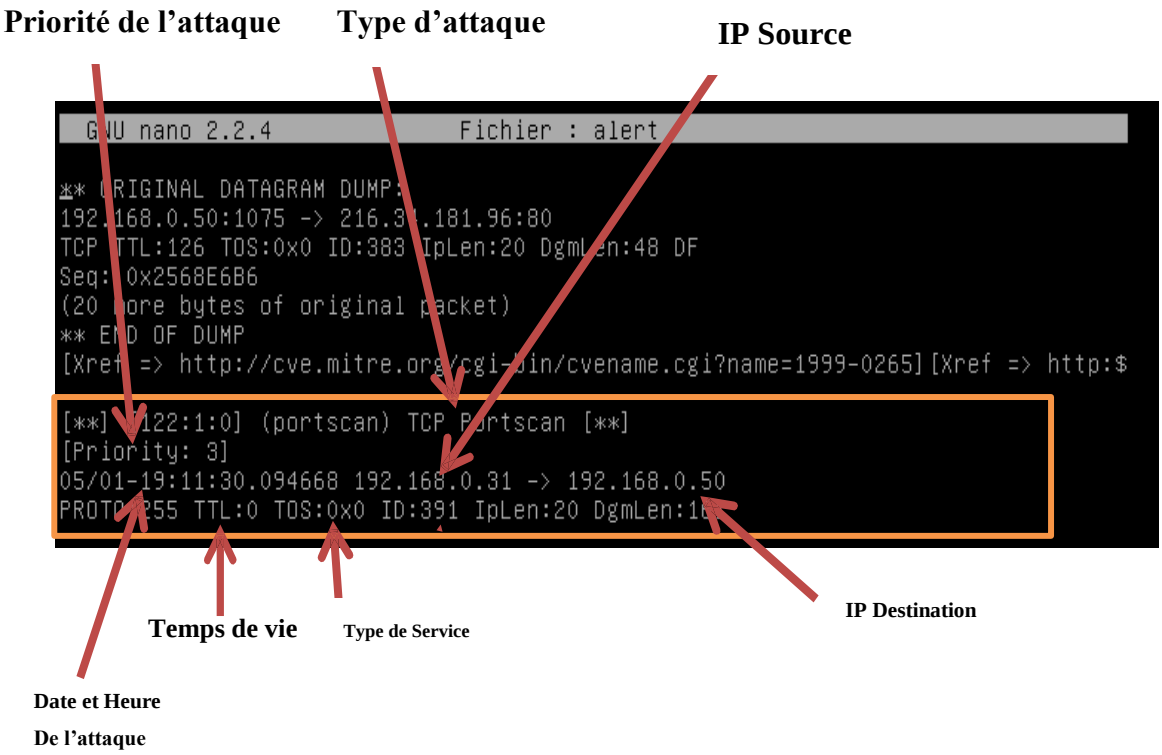


Figure 5. 18 : Analyse d'une alerte de Snort

Pour visualiser les paquets qui transitent sur notre réseau lors de l'attaque, je peux utiliser Wireshark. C'est l'analyseur réseau le plus populaire du monde. Cet outil extrêmement puissant fournit des informations sur des protocoles réseaux et applicatifs à partir de données capturées sur un réseau (voir figure 5.19).

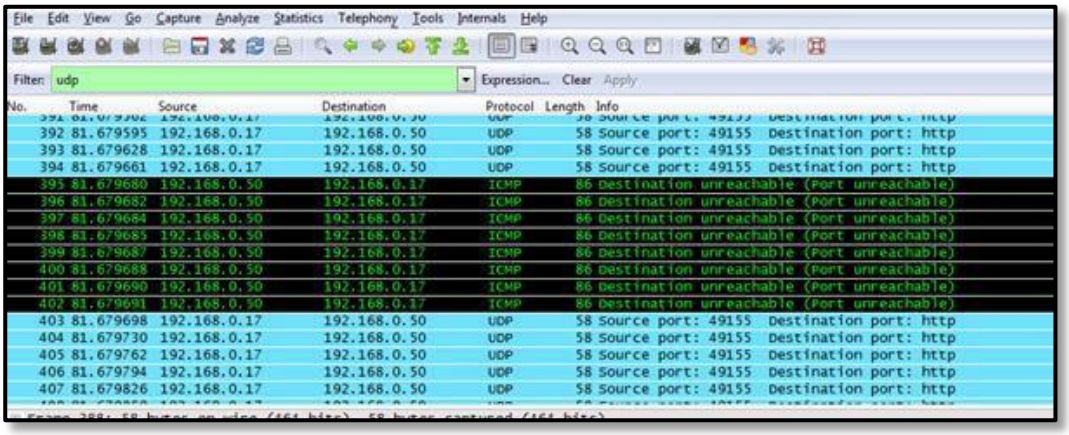


Figure 5.19: Analyse des paquets de l'attaque Déni de service

Conclusion Générale

Notre projet avait pour objectif la mise en place d'une solution de sécurité open source pour le réseau informatique de COTREL, afin d'éliminer les vulnérabilités et de contrer les attaques qui peuvent engendrer un certain nombre de risques potentiel important.

Ce projet comporte deux volets. Dans le premier, je procéderai à une étude des outils open source chargés de défendre les ressources d'un système d'information afin d'assurer la haute disponibilité des services et empêcher les personnes malveillantes ayant l'intention de se glisser dans le système informatique à partir des failles de sécurité.
Je fais appel à une installation et une configuration des mécanismes, des services, et des procédures que je nomme communément solution ou mesures de sécurité : Firewall, serveur proxy, serveur antivirus, système de détection d'intrusion.

Je tiens à préciser que ce projet m'a permis de prendre conscience des menaces et des risques de réseau informatique. De plus, ce projet m'a offert l'occasion d'approfondir nos connaissances sue les notions de sécurité informatique.

Du point de vue général, ce projet m'a aussi permet d'acquérir un savoir non négligeable et d'améliorer notre aptitude à communiquer, collaborer et s'adapter avec l'environnement professionnel.

En termes de perspectives, des améliorations sont possible pour augmenter la performance de cette solution selon l'apparition de nouvelle technologie, prenons l'exemple de la sécurité de la voix sur IP. Sinon, l'envoi de mail lors de détection d'attaque par le mécanisme Snort sera d'un grand avantage.

ANNEXES

La virtualisation

En informatique, on appelle virtualisation l'ensemble des techniques matérielles et/ou logiciels qui permettent de faire fonctionner sur une seule machine plusieurs systèmes d'exploitation et/ou plusieurs applications, séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes.

1. Les objectifs de la virtualisation

La virtualisation peut avoir de nombreux intérêts pour une entreprise :

- Utilisation optimale des ressources d'un parc de machines.
- Installation, déploiement et migration facile des machines virtuelles d'une machine physique à une autre.
- Economie sur le matériel par mutualisation.
- Sécurisation et/ou isolation d'un réseau.
- Isolation des différents utilisateurs simultanés d'une même machine.
- Allocation dynamique de la puissance de calcul en fonction des besoins de chaque application à un instant donné.
- Diminution des risques liés au dimensionnement des serveurs lors de la définition de l'architecture d'une application, l'ajout de puissance étant alors transparente.

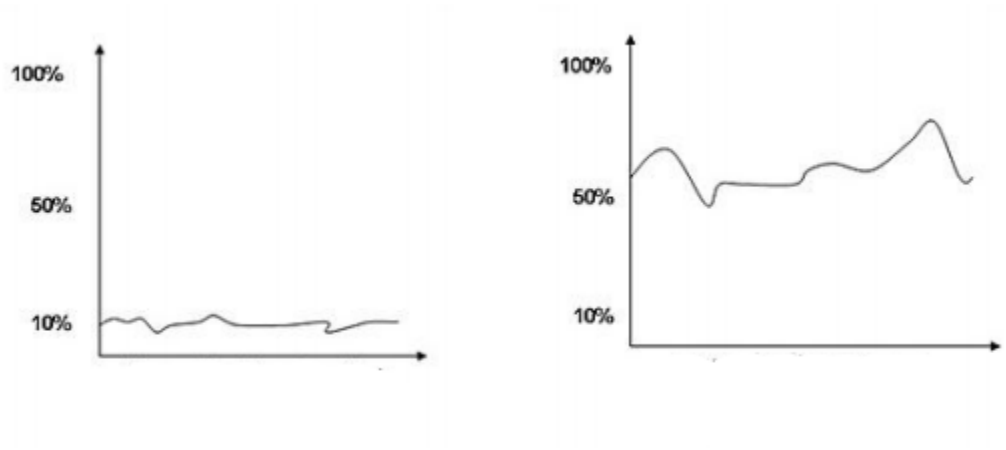


Figure A.1: Taux d'utilisation des serveurs

2. Choix du logiciel de virtualisation du marché

Il existe un grand nombre de logiciels de virtualisation, chacun ayant ses avantages et ses inconvénients. De plus, certains d'entre eux se déclinent en différentes versions (à usage professionnel ou personnel). Cependant, peu de ces logiciels ont atteint un niveau de stabilité suffisant que pour être utilisé en entreprise.

➢ **VMWare** est une entreprise spécialisée dans le domaine des technologies de virtualisation de systèmes informatiques. Elle développe et distribue des logiciels servant à virtualiser des systèmes d'exploitation. Ses produits sont disponibles pour de nombreux systèmes d'exploitation hôtes, dont les distributions GNU/Linux, Microsoft Windows et Apple Mac OS, et prennent en charge plusieurs familles de systèmes d'exploitation invités.

Parmi ces produits on trouve :

- VMware Workstation (propriétaire) : c'est un logiciel à destination des professionnels. tout comme VMware Player, il permet de créer des machines virtuelles et de les exécuter en même temps au-dessus d'un système d'exploitation hôte. Il propose toutefois quelques fonctionnalités plus poussées dont l'utilisateur final a rarement besoin, mais fort utiles aux professionnels de gestion de réseaux informatiques.

- VMware server : Cette solution de virtualisation délie l'application serveur, faisant fonctionner des machines virtuelles, et la console d'administration, qui crée et gère les propriétés des machines virtuelles. VMWare Server s'adresse avant tout aux administrateurs de serveurs informatiques.

➢ **Windows VirtualPC :** c'est un logiciel gratuit d'émulation et de virtualisation. Il permet d'émuler un système d'exploitation sur une architecture matérielle différente de celle à laquelle il était initialement destiné.

➢ **Oracle VM VirtualBox** (anciennement VirtualBox) : c'est un logiciel open source de virtualisation publié par Oracle. Il est également la seule solution professionnelle qui est librement disponible en tant que logiciel Open Source sous les termes de la GNU General Public Licence (GPL).

Ma solution de sécurité est implémentée avec le logiciel de virtualisation VMware Workstation puisque j'ai déjà une idée sur son utilisation et il représente la solution la plus fiable pour la gestion de réseaux informatiques.

LISTE DES ACRONYMES

A	
ACL	Access Control List
ARP	Address Resolution Protocol
B	
BSD	BSD: Berkeley Software Distribution License
C	
CARP	Common Address Redundancy Protocol
CVE	Common Vulnerabilities and Exposures
CUPS	Common Unix Printing System
D	
DMZ	Demilitarized Zone
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOS	Denial Of Service
DDOS	Distributed Denial Of Service
F	
FAI	Fournisseur d'Accès à Internet
FTP	File Transfer Protocol
G	
GPL	General Public License
GFI	Groupe Français d'Informatique
H	
HA	High Avaibility
HTTP	HyperText Transfer Protoco
HTTPS	HyperText Transfer Protocol Secure
HAVP	HTTP AntiVirus Proxy
HIDS	Host Intrusion Detection System
I	
IP	Internet Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ICMP	Internet Control Message Protocol
IMAP	Internet Message Access Protocol
N	
NAT	Network Address Translation
NVD	National Vulnerability Database
NVT	Network Vulnerability Tests
NNTP	Network News Transfer Protocol
NIDS	Network Intrusion Detection System
O	
OpenVas	Open source Vulnerability Assessment Scanner
OSVDB	Open Source Vulnerability Database
OS	Operating System
P	
PFsense	Packet Filter Sense
PHP	Hypertext Preprocessor
POP3	Post Office Protocol
S	
SSH	Secure SHell
SIP	Session Initiation Protocol
SAAS	Software As A Service
SSL	Secure Sockets Layer
SMTP	Simple Mail Transfer Protocol
SMB	Server Message Block
T	
TCP	Transmission Control Protocol
TTL	Time To Live
U	
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team
UDP	User Datagram Protocol
UML	Unified Modeling Languag
V	
VPN	Virtual Private Network
W	
WAN	Wide Area Network

ملخص
الهدف من هذا العمل هو إنشاء حل لسلامة شبكة الكمبيوتر شركة كوترل باستخدام خدمات
" آليات والأدوات مفتوحة المصدر و التي يتم استدعاؤها عادة "حل "أو "تدبير للسلامة الإلكترونية
يتكون هذا المشروع من عنصرين .في المرحلة الأولى، أجرينا التثبيت وآليات التكوين الضرورية لحماية موارد النظام
المعلومات ومنع الأشخاص الخبيثة التي تنوي اقتحام النظام .في الجزء الثاني، قمنا لمسح الشبكة استنادا إلى
دراسة الأدوات مفتوحة المصدر موجود في السوق .وبالتالي، علينا أن ندرس ضعف أنظمة الكمبيوتر لتحديد المخاطر
ونقاط الضعف التي قد تشكل خطرا على النظام

الكلمات الرئيسية :هجوم، إقتحام، مسح، جدار الحماية، مكافحة الفيروسات، الإنذار، الضعف، المخاطر و المصدر
المفتوح

Résumé :

L'objectif de ce travail est la mise en place d'une solution de sécurité open source pour le réseau informatique de COTREL, en faisant appel à des services, des mécanismes, des outils et des procédures que l'on nomme communément "solutions" ou "mesures de sécurité".
Ce projet comporte deux volets. Dans le premier, j'ai procédé à une installation et une configuration des mécanismes nécessaires pour la protection des ressources du système d'information et empêcher les personnes malveillantes ayant l'intention de s'introduire dans le système. Dans le deuxième volet, j'ai utilisé des applications de scannage réseau en se basant sur l'étude des outils open source existant sur le marché. Ainsi, j'ai étudié la vulnérabilité du système informatique, afin de dégager les risques et les failles qui peuvent présenter un danger pour le système testé.

Mots clés : Attaque, intrusion, scan, port, firewall, serveur, proxy, antivirus, IDS, IPS, alerte, vulnérabilité, risque, JAVA, Open Source.

Abstract :

The objective of this work is the establishment of a security solution for the open source computer network of COTREL by using services, mechanisms, tools and procedures that are called commonly "solution" or "security measure".
This project has two components. In the first, i performed an installation and configuration mechanisms necessary for the protection of information system resources and prevent malicious persons intending to break into the system. In the second part, i has use a network application scanning based on the study of existing open source tools on the market. Thus, i study the vulnerability of computer systems to identify risks and vulnerabilities that may pose a danger to the system under test.

Keywords : attack, pentest, scan, port, firewall, server, proxy, anti-virus, IDS, IPS, alert, vulnerability, risk, JAVA, Open Source.