V0.1.0

Etude des principaux services fournis par PfSense

Pour la communauté PfSense :
http://www.pfSense.org
http://forum.pfsense.org

Rédacteurs : **Anthony COSTANZO**
Damien GRILLAT
Lylian LEFRANCOIS

Objet :	**Etude des principaux services fournis par PfSense**
Rédigé par :	Anthony COSTANZO, Damien GRILLAT, Lylian LEFRANCOIS

Diffusion		
Nom	**Société**	**Diffusion**
Communauté PfSense		1

Historique des modifications			
Version / Evolution	Date	Etat	Description de la modification
v0.1.0	01/02/2009	Beta	Première version du document distribuée

Synthèse :	Ce document présente les principaux services délivrés par la version v1.2.2 de Pfsense. Les améliorations attendues en v2.0 seront abordées dans la mesure des informations connues à ce jour. N'hésitez pas à contribuer à l'amélioration de ce document ! la partie « Ce qu'il reste à faire » est fait pour cela !

Pour cela nous vous demandons d'utiliser le forum Français de PfSense pour proposer vos remarques / suggestions ou modifications.

http://forum.pfsense.org/index.php?board=7.0

REMERCIEMENTS

Nous remercions les membres du forum PfSense.org pour leur disponibilité et leur participation. Un merci spécial pour ccnet et Juve.

Nous remercions également d'avance toutes les personnes qui aideront à tenir vivant ce tutorial en le corrigeant et en proposant des évolutions.

Cette partie comportera aussi toutes les personnes ayant participé à l'amélioration du document proposé.

SOMMAIRE

INTRODUCTION

Nous avons décidé d'étudier les principaux services fournis par l'excellent routeur/Pare feu PfSense. Ce système Open source est basé sur le système d'exploitation FreeBSD, réputé pour être extrêmement stable. De plus, PfSense ne réinvente pas la poudre puisqu'il reprend le cœur du Routeur/Firewall m0n0wall (http://m0n0.ch/wall/) et y ajoute ses propres fonctionnalités. C'est précisément de cette partie dont nous allons traiter dans ce document.

La distribution PfSense propose en cela une multitude d'outils Open Sources permettant à l'administrateur réseau d'optimiser ses tâches.

En ce début d'année 2009 PfSense va sortir un livre blanc payant nommé« Guide Book : the definitive Guide » qui relate de tout ce qui concerne PfSense. Notre volonté n'est pas de le copier mais d'avoir une approche basée sur le retour d'expérience. Ainsi nos parties sont constituées d'une présentation de la technologie concernée, des solutions techniques associées (comparaison si besoin) et d'une mise en pratique. Notre analyse est en somme la problématique suivante : comment mettre en place tel ou tel service intégré à PfSense en pratique ?

Ce document est non immuable, c'est une ébauche de livre blanc sur PfSense en Français qui est vouée à s'enrichir de vos idées ou de votre vécu. Nous comptons par exemple sur votre participation pour traiter de tous les services présents dans PfSense. Cette première version traite des principaux services utilisés, n'oublions pas les autres… ☺. Pour les autres motivés un portage de notre premier tutorial sur PfSense est à faire (Mise à jour + migration), le lien http étant : http://forum.pfsense.org/index.php?topic=1452.new

La première partie de ce document traite de la présentation de PfSense et énonce brièvement les services aujourd'hui étudiés.

La deuxième partie de ce document développe les principaux services proposés par PfSense v1.2.2. Nous nous attacherons d'ailleurs à préciser les améliorations attendues en v2.0.

Nous conclurons enfin sur notre retour d'expérience et sur le devenir de ce document.

1 PRESENTATION GENERALE DE PFSENSE

1.1 GENERALITES

PfSense, ou « **P**acket **F**ilter **Sense** » est un Firewall / routeur proposé en Live CD d'environ 50Mo (installable à la manière d'Ubuntu par exemple). PfSense est basé sur un système d'exploitation BSD, réputé pour sa stabilité et sur m0n0wall qui est aussi un Firewall / Routeur Open Source (http://m0n0.ch/wall/) mais conduit par un autre projet.

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 KDE, etc… qui alourdiraient le système proposé, juste l'essentiel !

Pour aller plus loin : http://www.pfsense.org/

1.2 LES SERVICES PROPOSES

Ce qui est traité dans ce document :

- Système de basculement (Failover) par le protocole **CARP**
- VPN site à site **OpenVPN** et **IPSec**
- VPN client **PPTP**
- Proxy et Blacklist **SQUID** et **SQUIDGuard**
- IDS-IPS **Snort**
- Répartition de charge avec **LoadBalancer**
- Vue sur la Consommation de Bande Passante avec **Bandwithd** et **Ntop** pour plus de détails
- VPN point à point **Stunnel**
- Partage de bande passante **Traffic Shaper**

Ce qui est à rajouter (en se basant sur la v1.2.2) :

- **Captive Portal** (Portail captif)
- Installation et configuration de base de PfSense
- Sécurisation de PfSense

1.3 INDEX DES VERSIONS DE LOGICIELS ET OS

- PfSense : v1.2.2 (06/01/2009) ➔ des références seront faites sur la v2.0 prévue pour début 2009
- VMWare Workstation : v6.5.0 build 118166
- Windows Server 2003 Standard
- Windows XP SP1

2 PORTAIL CAPTIF

2.1 PRESENTATION

Un portail captif est une structure permettant un accès rapide à Internet. Lorsqu'un utilisateur cherche à accéder à une page Web pour la première fois, le portail captif capture la demande de connexion par un routage interne et propose à l'utilisateur de s'identifier afin de pouvoir recevoir son accès. Cette demande d'authentification se fait via une page Web stockée localement sur le portail captif grâce à un serveur HTTP. Ceci permet à tout ordinateur équipé d'un navigateur HTML et d'un accès WiFi de se voir proposer un accès à Internet. La connexion au serveur est sécurisée par SSL grâce au protocole HTTPS, ce qui garanti l'inviolabilité de la transaction. Les identifiants de connexion (identifiant, mot de passe) de chaque utilisateur sont stockés dans une base de données qui est hébergée localement ou sur un serveur distant. Une fois l'utilisateur authentifié, les règles du Firewall le concernant sont modifiées et celui-ci se voit alors autorisé à utiliser son accès pour une durée limitée fixée par l'administrateur. A la fin de la durée définie, l'utilisateur se verra redemander ses identifiants de connexion afin d'ouvrir une nouvelle session.

Fonction type d'un portail captif :

Client : http://www.cesi.fr (en passant par le portail…)

↪ *Portail :* redirection vers la page d'authentification locale

↪ *Client :* Login+MdP

↪ **SI OK** : *client :* http://www.cesi.fr

Remarque : Maintenant **il faut que cette redirection fonctionne avec tous les protocoles applicatifs**.

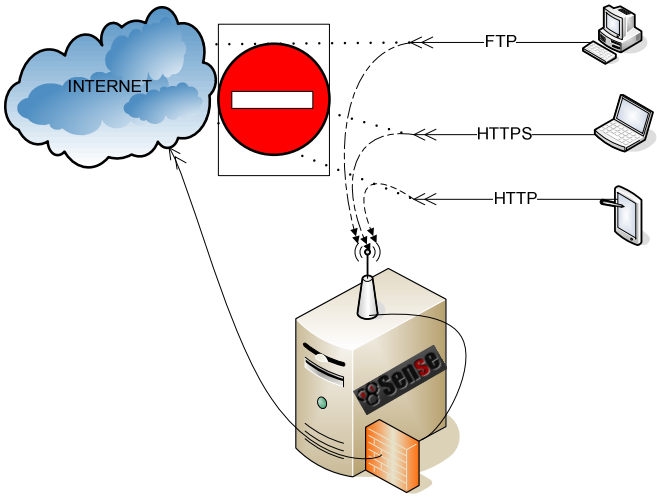
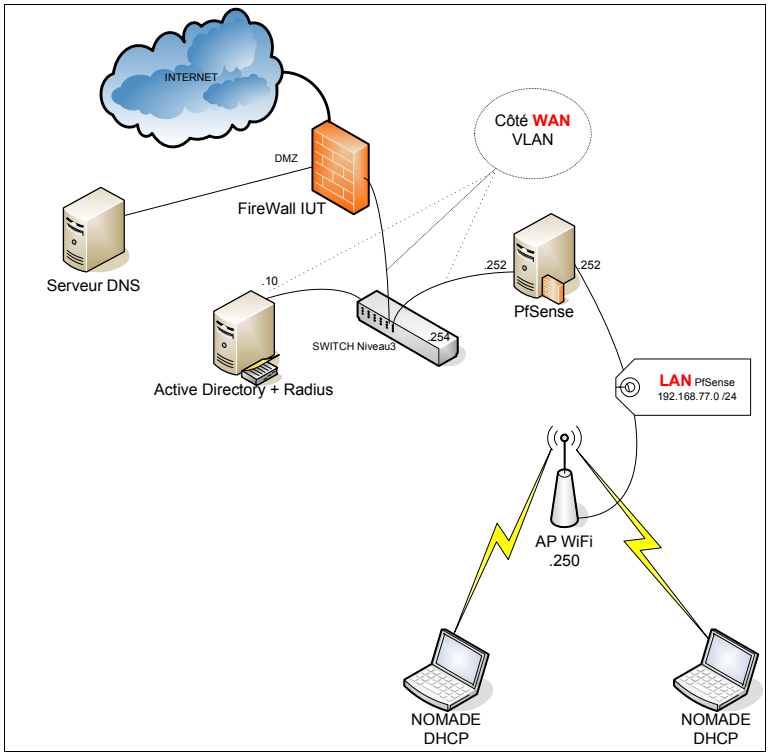


Schéma théorique d'un portail captif

Interprétation : Quoi que désire faire le client, s'il veut surfer sur le WEB il devra d'abord passer par le portail captif afin de s'authentifier.

La différence entre un simple FireWall et un portail captif réside dans le fait que le portail captif ne refuse pas une connexion, il la redirige vers une page d'authentification.

2.2 SCHEMA



2.3 CONFIGURATION SERVEUR

2.3.1 Configuration de PfSense

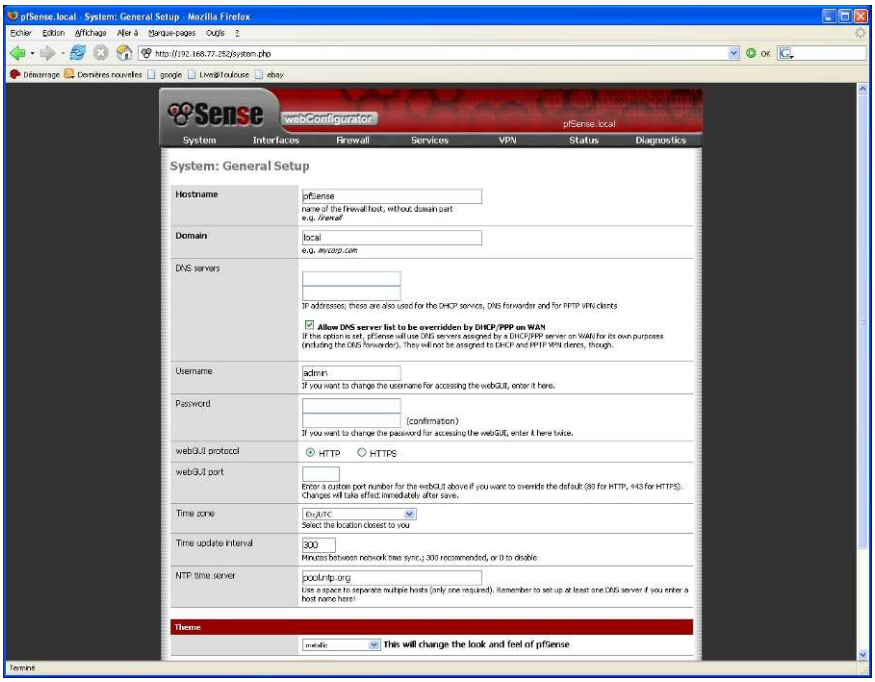
2.3.1.1 Les principaux paramètres

Nous allons maintenant configurer PfSense.
Avant tout, nous vous conseillons de changer l'IP sur la machine de PfSense directement, pour plus de simplicité par la suite. Pour cela, dans le menu de PfSense, tapez le choix *2 Set LAN IP address.*

Entrer l'adresse IP correspondant à votre LAN.

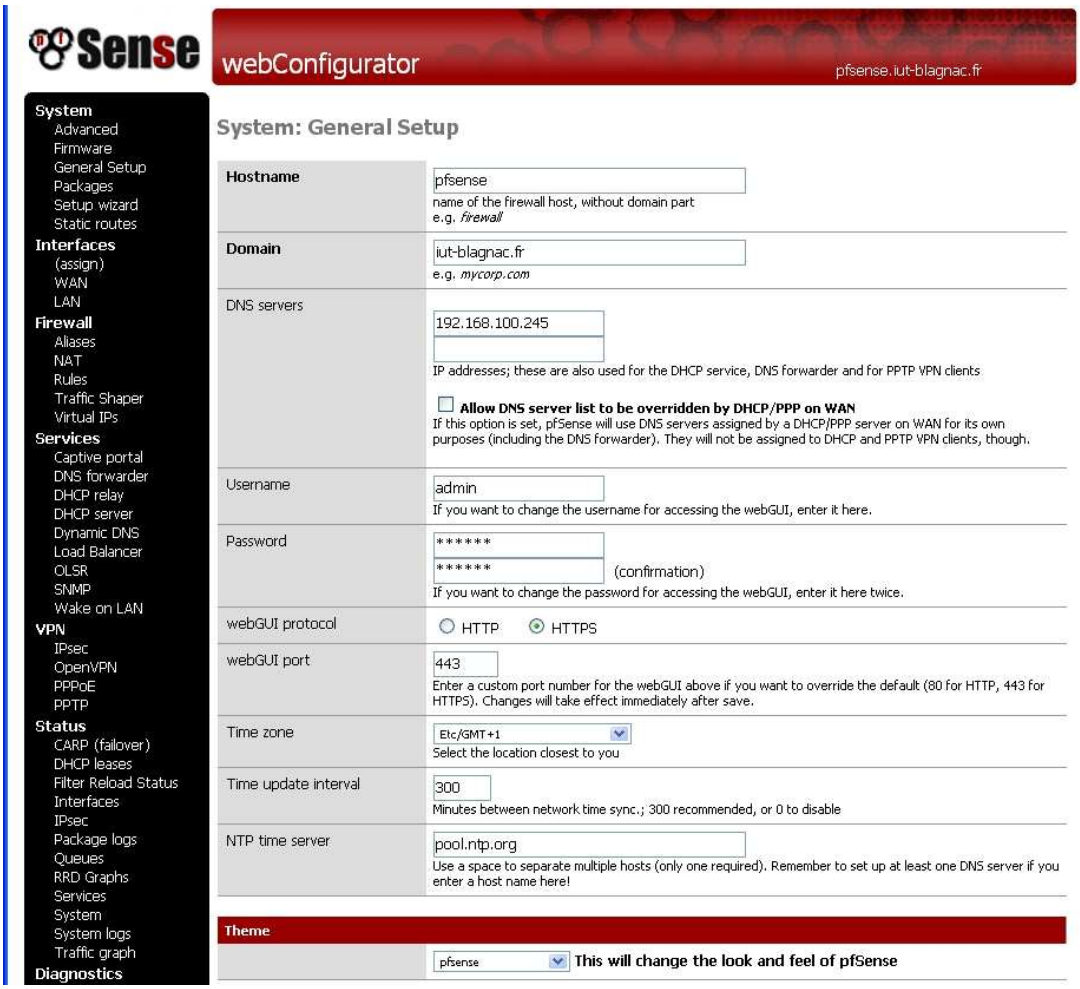
```
Enter the new LAN IP address: 192.168.77.252

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN subnet bit count: 24

Do you want to enable the DHCP server on LAN [y|n]?  y
Enter the start address of the client address range: 192.168.77.10
Enter the end address of the client address range: 192.168.77.100

The LAN IP address has been set to 192.168.77.252/24.
You can now access the webGUI by opening the following URL
in your web browser:

http://192.168.77.252/

Press ENTER to continue.
```

Nous allons pouvoir maintenant configurer Pfsense via l'interface Web.
Connectez une machine sur la carte réseau de Pfsense (coté LAN, tout est bloqué coté WAN par défaut). N'oubliez pas de changer l'IP de votre machine.
Ouvrez ensuite votre navigateur Web, puis entrez http://ip_pfsense.
Dans notre cas, nous ferons http://192.168.77.252.
Entrez ensuite le login (par défaut *admin*, mot de passe : *pfsense*).
Allez ensuite dans *System*, puis *General Setup.*

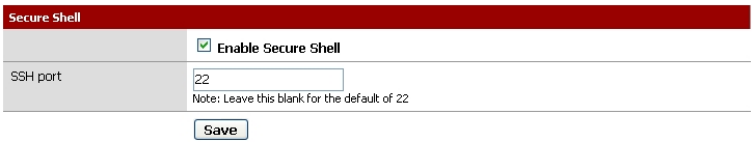


Ici se trouve la configuration générale de Pfsense. Entrez ici le nom de la machine, le domaine et l'IP du DNS. Attention, il vous faut décocher l'option se trouvant dessous (*Allow DNS server list to be overridden by DHCP/PPP on WAN*). En effet, cette option provoque des conflits puisque les DNS des clients n'est plus Pfsense, mais un DNS du WAN inaccessible par le LAN.
Ensuite, modifiez le nom et le mot de passe du compte permettant de se connecter sur Pfsense.
Vous pouvez ensuite activer l'accès à ces pages, via une connexion sécurisée SSL. Pour cela, activer l'HTTPS. Entrez le port 443 dans *webGui port* (correspondant à SSL).
Vous pouvez ensuite modifier le serveur NTP et le fuseau horaire pour régler votre horloge.
Enfin, nous vous conseillons de changer le thème d'affichage de Pfsense. En effet, le thème par défaut (metallic), comporte quelques bugs (problème d'affichage, lien disparaissant). Mettez donc le thème "*Pfsense*".

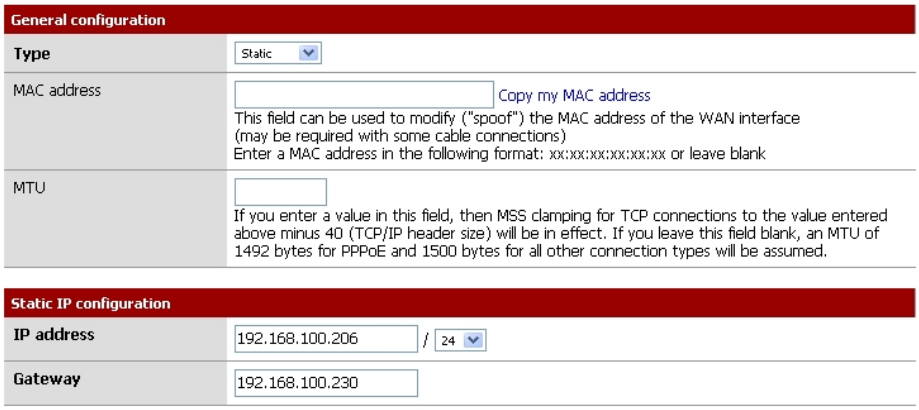
Vous devriez donc avoir une interface comme ceci :



Ensuite, toujours dans "system", allez dans *Advanced*. Ici, nous pouvons activer la connexion SSH afin de l'administrer à distance sans passer par l'interface graphique (en effet, pour une configuration accrus, il vaut mieux passer par le Shell).

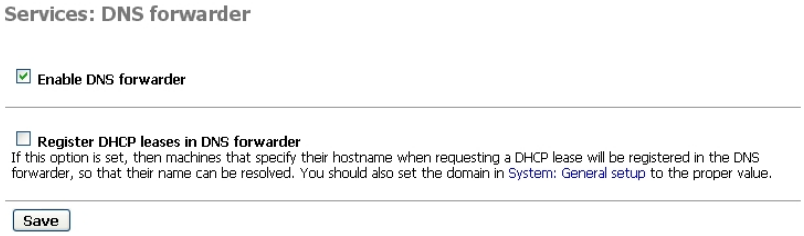


Nous allons maintenant configurer les interfaces LAN et WAN en détail.
Pour cela, allez dans Interface, puis WAN pour commencer. Entrez ici l'adresse IP de la carte réseau coté WAN, ainsi que l'adresse IP de la passerelle.

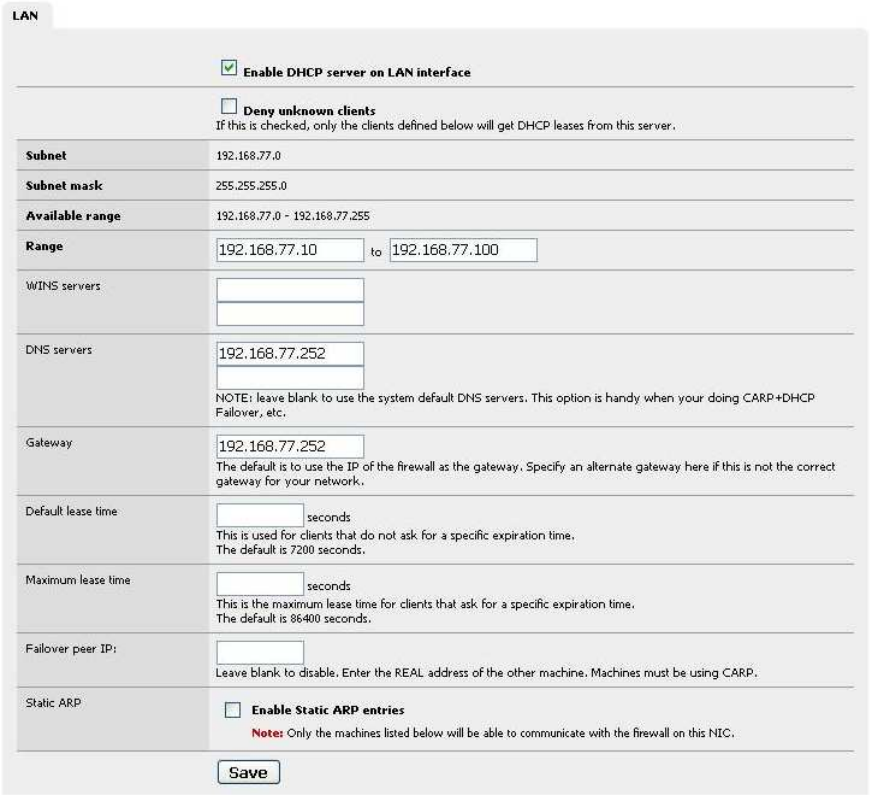


Configurer ensuite la carte LAN (elle doit être normalement bien configuré, mais vous pouvez faire des modifications par la suite ici) :

Allez ensuite dans la section *DNS forwarder*. Activez ensuite l'option *Enable DNS forwarder*. Cette option va permettre à Pfsense de transférer et d'émettre les requêtes DNS pour les clients.



Il ne reste plus qu'à configurer le serveur DHCP pour le LAN, afin de simplifier la connexion des clients. Pour cela, allez dans la section *DHCP server*.
Cochez la case *Enable DHCP server on LAN interface*. Entrez ensuite la plage d'adresse IP qui sera attribuée aux clients. Dans notre cas, notre plage d'IP sera 192.168.77.10 – 192.168.77.100.
Il faut par la suite entrer l'IP du serveur DNS qui sera attribuée aux clients. Ici, il vous faut entrer l'IP du portail captif. En effet, nous avons définie plus haut que Pfsense fera lui-même les requêtes DNS.
Pour finir, entrez l'adresse de la passerelle pour les clients. Celle-ci sera le portail captif : 192.168.7.252.
Voici donc ce que vous devriez avoir :



Voila, Pfsense est correctement configuré. Pour le moment il sert uniquement de Firewall et de routeur. Nous allons maintenant voir comment activer l'écoute des requêtes sur l'interface LAN et obliger les utilisateurs à s'authentifier pour traverser le Firewall.

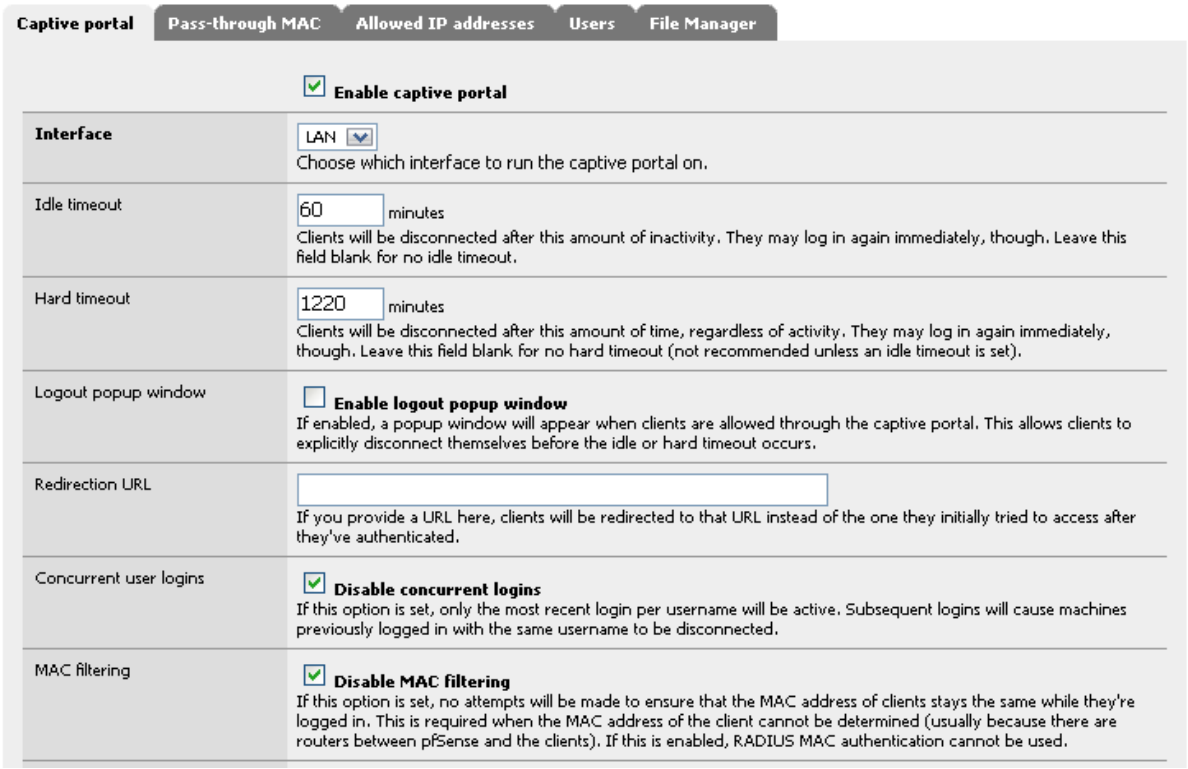
2.3.2 Le portail captif

2.3.2.1 Paramètres généraux

Nous allons désormais voir la procédure afin de mettre en place le portail captif. Pour cela, allez dans la section *Captive portail*.
Cochez la case *Enable captive portail*, puis choisissez l'interface sur laquelle le portail captif va écouter (LAN dans notre cas).
Dans les 2 options suivantes, nous allons définir les temps à partir desquelles les clients seront déconnectés. *Idle Timeout* définie le temps à partir duquel un client inactif sera automatiquement déconnecté. Hard Timeout définie le temps à partir duquel un client sera déconnecté quelque soit sont état.
Nous avons choisi de mettre 1h pour l'inactivité, et 12h pour les déconnexions brutales.

Ensuite, nous pouvons activer ou pas un popup qui va servir au client de se déconnecter. Nous avons préféré ne pas mettre cette option, car de nombreux utilisateurs utilisent des anti-popup et donc ne verront pas ce message.
Il est possible ensuite de rediriger un client authentifié vers une URL spécifique. Nous avons préféré de ne rien mettre afin de laisser la liberté au client de gérer leur page de démarrage.

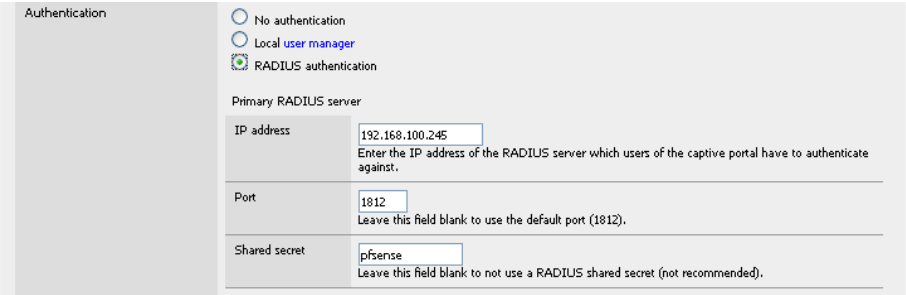
Le paramètre suivant *Concurrent user logins*, permet d'éviter les redondances de connexions. En effet, l'utilisateur pourra se connecter sur une seule machine à la fois. Cela va donc limiter les usurpations d'identité pour se connecter.
Enfin il est possible de filtrer les clients par adresse MAC.



Ensuite vient la méthode d'authentification.
3 possibilités s'offre à nous :

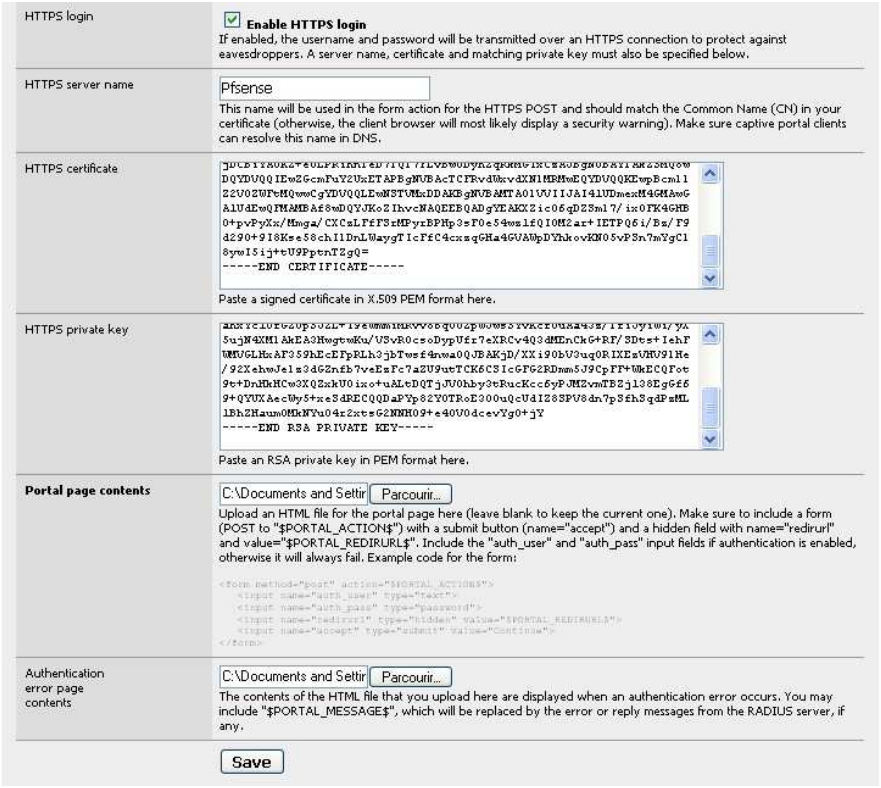
- Sans authentification, les clients sont libres
- Via un fichier local
- Via un serveur RADIUS

Pour des raisons de sécurités, nous avons mis en place un serveur RADIUS. Pour plus de détail sur l'installation de Radius, reportez-vous à la partie consacrée à la sécurisation du portail.



Il est possible par la suite de sécuriser l'accès au portail captif. Cette mise en place est décrite dans la partie consacrée à la sécurisation du portail.

Enfin, vous pouvez importer une page web qui servira de page d'accueil, ainsi qu'une autre page en cas d'échec d'authentification.



Si vous avez des images insérer sur vos pages web, allez dans l'onglet *File Manager* et télécharger vos images.

Les autres onglets ne sont pas utilisés dans notre cas, mais pour information, l'onglet *Pass-through MAC* sert à définir les adresses MAC autorisé à traverser Pfsense. *Allowed IP address* sert à définir les adresses IP autorisées à sortir. Et enfin l'onglet *Users* sert dans le cas où l'on a choisi l'option *Local Manager* vu plus haut, et est donc utilisé pour stocker les comptes valides.

Voila, le portail captif est en marche. Cependant, cette configuration comporte quelques failles, dans le sens l'accès aux pages web n'est pas crypté. Les données concernant le login passe donc en clair et peut être visible de tous. Nous allons voir maintenant comment sécuriser cet accès.

2.3.2.2 L'authentification

L'authentification est un point névralgique de PfSense puisque cette dernière définit l'autorisation ou non d'accès vers l'extérieur d'un utilisateur, une sorte de portail mécanique fermé dont il faut avoir la clé pour l'ouvrir…

PfSense embarque plusieurs types d'authentification possibles :

1) Une base locale en XML « local manager » ou sont inscrits les utilisateurs. (annexe 5)
2) Un serveur embarqué FreeRadius (annexe 6)
3) Un serveur Radius externe de type Microsoft IAS (Internet Authentification Service)

Choix du protocole d'authentification

RADIUS (Remote Authentification Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification. C'est le standard utilisé aujourd'hui car très malléable et très sécurisé.

PfSense intègre par défaut un serveur radius libre (FreeRadius) couplé à une base locale. Nous avons fait le test et il fonctionne bien (annexe 6).

Cependant nous avons abandonné cette solution pour deux principales raisons :

- Notre maquette est déjà doté d'un annuaire Active Directory, il reste juste à sécuriser l'accès à cet annuaire en utilisant le protocole Radius intégré à Microsoft Server 2003 (voir partie 3.2)
- Le serveur FreeRadius embarqué ne dispose pas de toutes les fonctionnalités que propose un Radius (spécification du media utilisé, groupes, etc….)

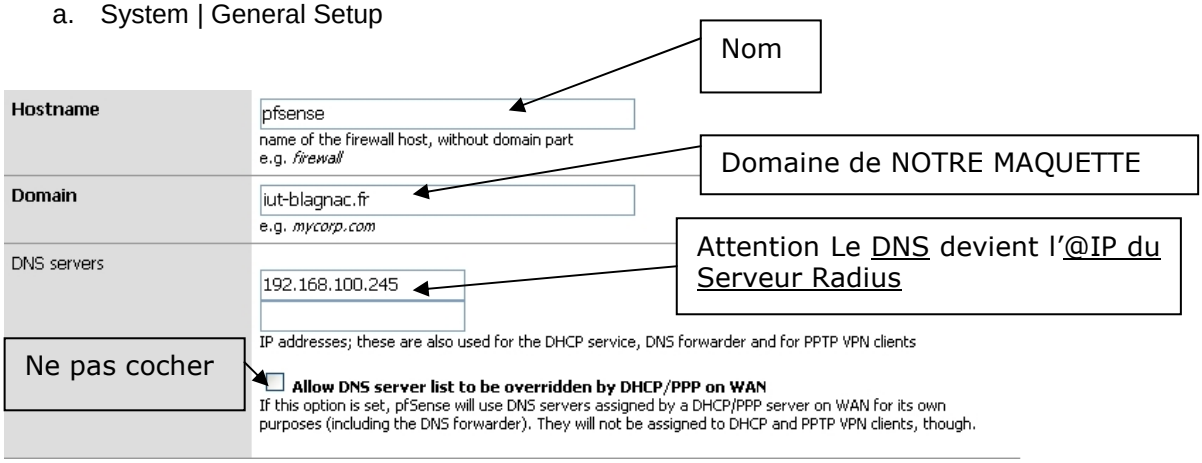
Ajout de l'authentification Radius d'IAS Microsoft Server2003 à PfSense

2 parties à considérer

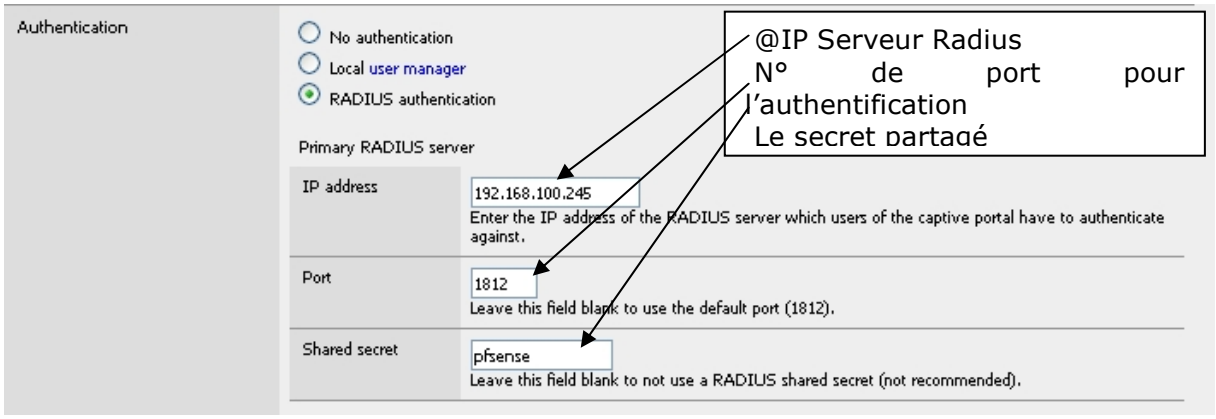
a. Configuration de PfSense
b. Configuration de Server 2003

a. Configuration de l'authentification sous PfSense

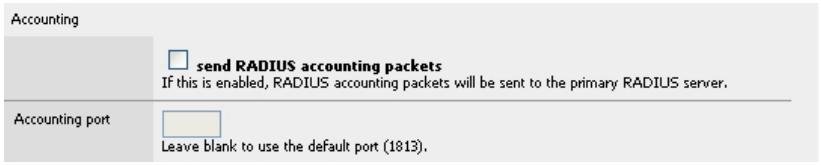
a. System | General Setup



- Services | Captive portal



Il y ensuite la possibilité de créer des statistiques pour Radius : l'Accounting



Puis Option intéressante, la ré-authentification de l'utilisateur toutes les minutes. Nous avons choisi cette option car elle évite le « Man In The Middle ». En effet si un pirate pas gentil venait à s'interposer entre 2 stations alors le laps de temps que pourrait jouir le méchant pirate serait au maximum égal à la prochaine authentification (Une minute), donc seules les 2 stations connaissent le secret partagé+ MdP crypté (le login ne l'est pas…) =>attaque finie.

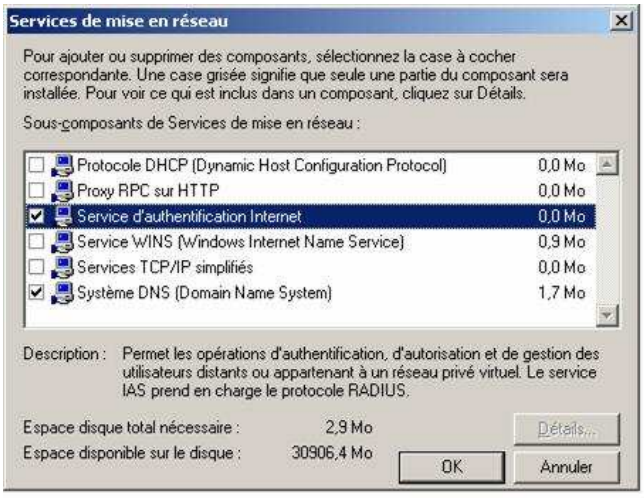
b. RADIUS sous Windows Server 2003 Enterprise Edition

- Ne pas oublier de joindre le domaine Notre iut-blagnac.fr sur le serveur Radius. Si ce n'est pas le cas une réinstallation d'Active Directory est nécessaire. Le fait de joindre le Radius dans le domaine évite à l'utilisateur lors son authentification de faire 'user@autre_domaine.fr' mais seulement 'user'
- Ne pas oublier que le serveur Radius sera désormais le DNS de PfSense
- Une configuration par défaut comme celle-ci utilise les ports
    - 1812 pour l'authentification
    - 1813 pour l'accounting (stats pour Radius)

Installation du serveur radius

Pour installer le service Radius appelé aussi Service d'authentification Internet, chez Microsoft, il faut aller dans :

- Démarrer | Panneau de configuration | Ajout/Suppression de programmes | Ajouter ou supprimer des composants Windows | Services de mises en réseau | Service d'authentification Internet.

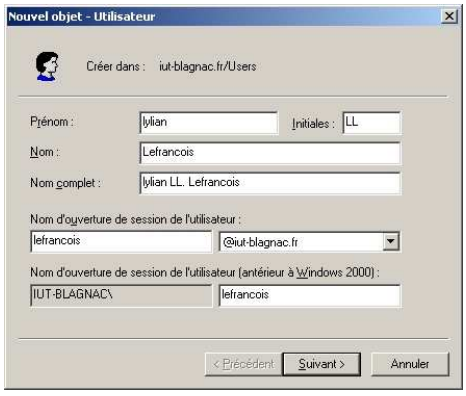


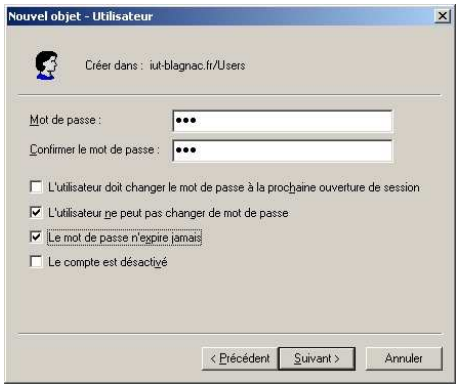
- Cliquer sur OK, l'installation s'effectue en sélectionnant les paramètres par défaut.

Créer un compte utilisateur dans Active Directory

- Pour créer un compte utilisateur dans l'Active Directory, cliquer sur Démarrer | Outils d'administration | Utilisateurs et ordinateurs Active Directory
- Dans le dossier Users, cliquer avec le bouton droit de la souris sur Nouveau | Utilisateur

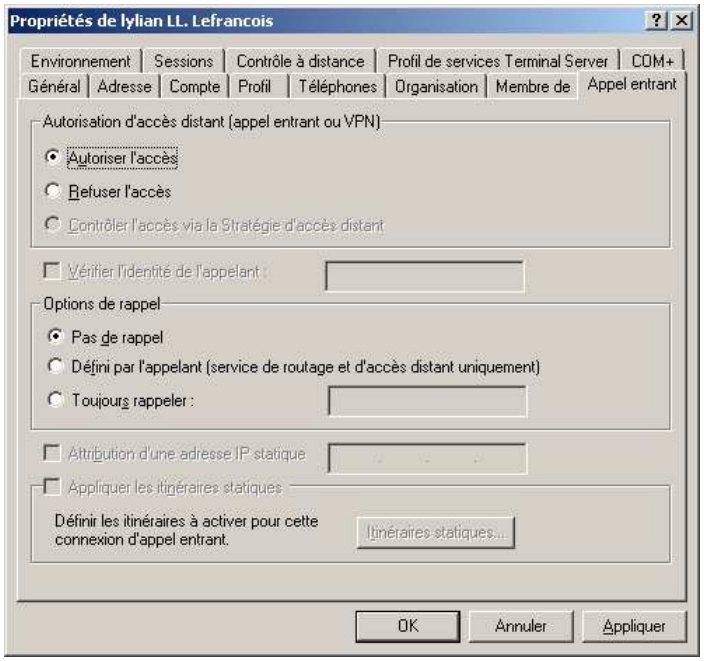
- Créer l'utilisateur nommé « lefrancois » ainsi :





Remarque : Si vous avez l'erreur suivante reportez vous annexe 4

- Editer les propriétés de lefrancois, pour autoriser l'accès distant :

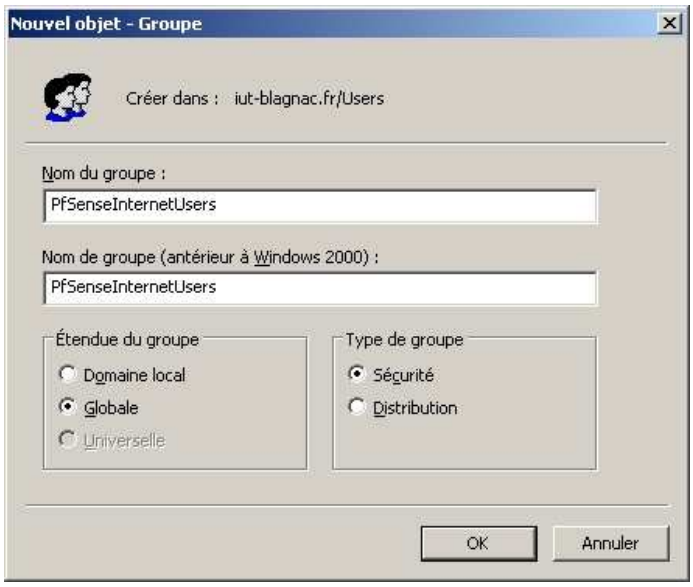


- Sélectionner Autoriser l'accès dans la section Autorisation d'accès distant (appel entrant ou VPN)

Créer un groupe de sécurité global dans Active Directory

Pour créer un groupe de sécurité global dans l'Active Directory, cliquer sur :

- Démarrer | Outils d'administration | Utilisateurs et ordinateurs Active Directory
- Dans le dossier Users, cliquer avec le bouton droit de la souris sur Nouveau | Groupe

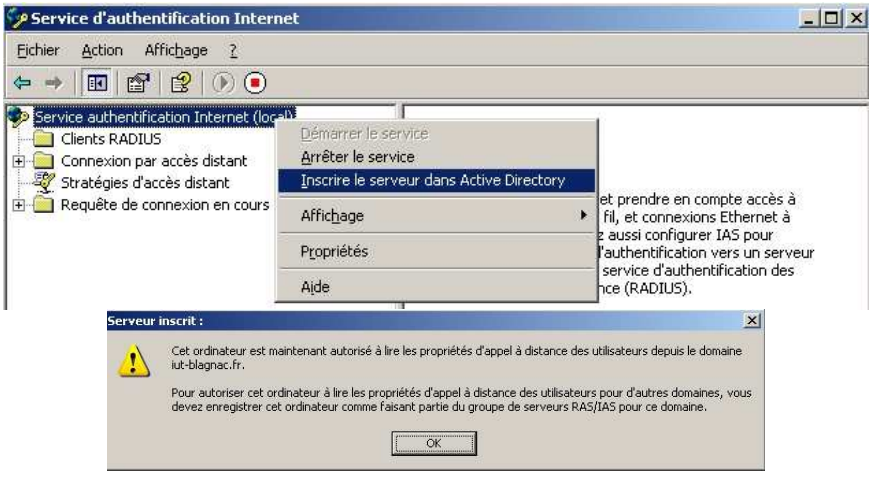


- Nous allons créer un groupe PfSenseInternetUsers puis **ajouter l'utilisateur à ce groupe**.

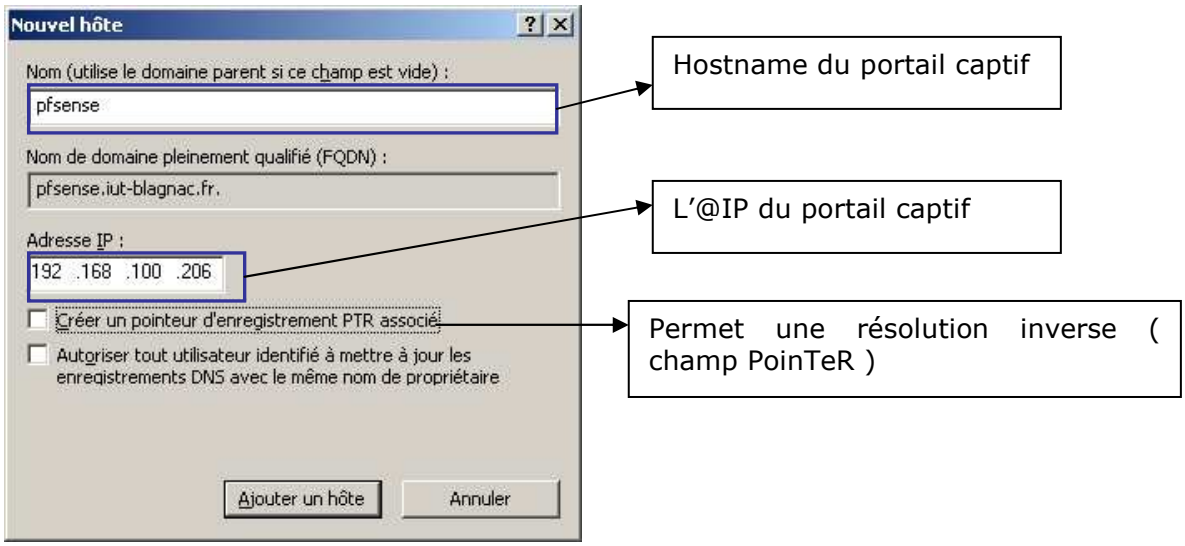
Renseigner PfSense dans le DNS du Serveur Radius

En effet lorsque PfSense utilise un serveur Radius externe ce dernier devient le serveur DNS de PfSense. Il faut donc indiquer dans le serveur Radius le chemin LUI---PfSense.

- Démarrer | programmes | outils d'administration | DNS
- En premier renseigner le service authentification dans Active Directory



- Dans le dossier IUT-BLAGNAC.FR créer un nouvel hôte (A)

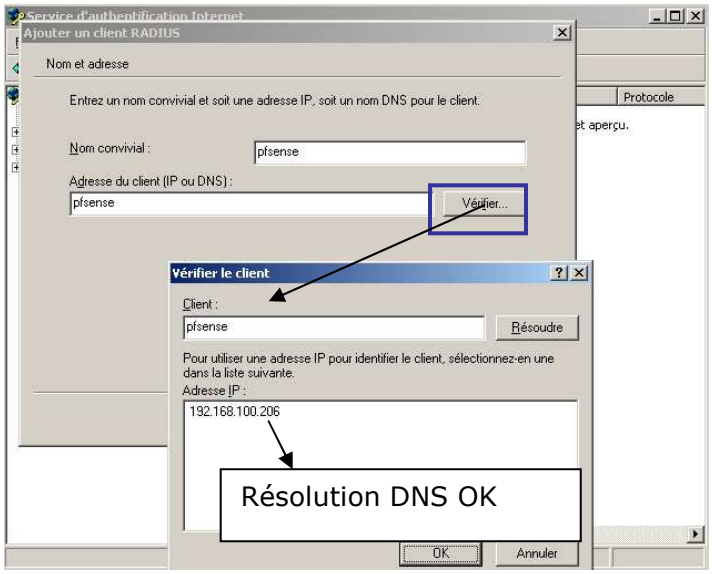


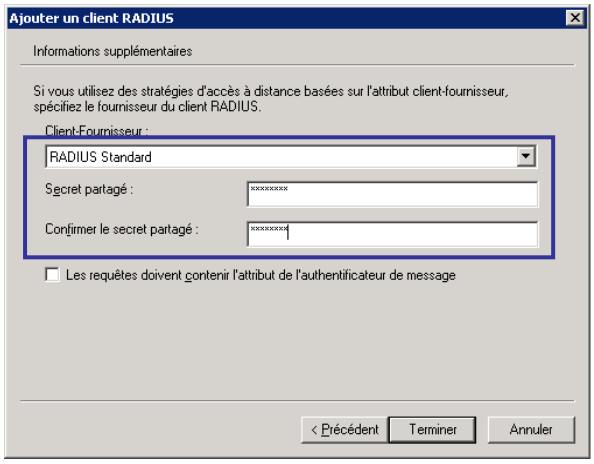
Paramétrer le service IAS

Dans l'interface d'administration du Service d'authentification Internet, Ajouter un client Radius :

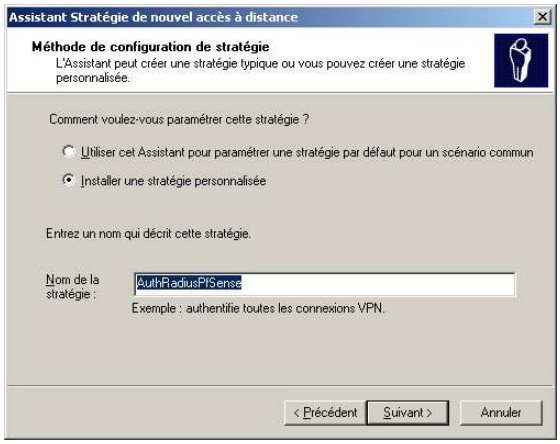
Renseigner le nom de PfSense, son adresse IP et Définir le secret partagé entre PfSense et le serveur Radius, dans notre exemple nous choisirons **PfSense comme secret partagé.**

Remarque : Les secrets partagés sont utilisés pour vérifier que les messages RADIUS, à l'exception du message de requête d'accès, sont envoyés par un périphérique compatible RADIUS configuré avec le même secret partagé. Les secrets partagés vérifient aussi que le message RADIUS n'a pas été modifié en transit (intégrité du message). Le secret partagé est également utilisé pour crypter certains attributs RADIUS, tels que User-Password et Tunnel-Password.



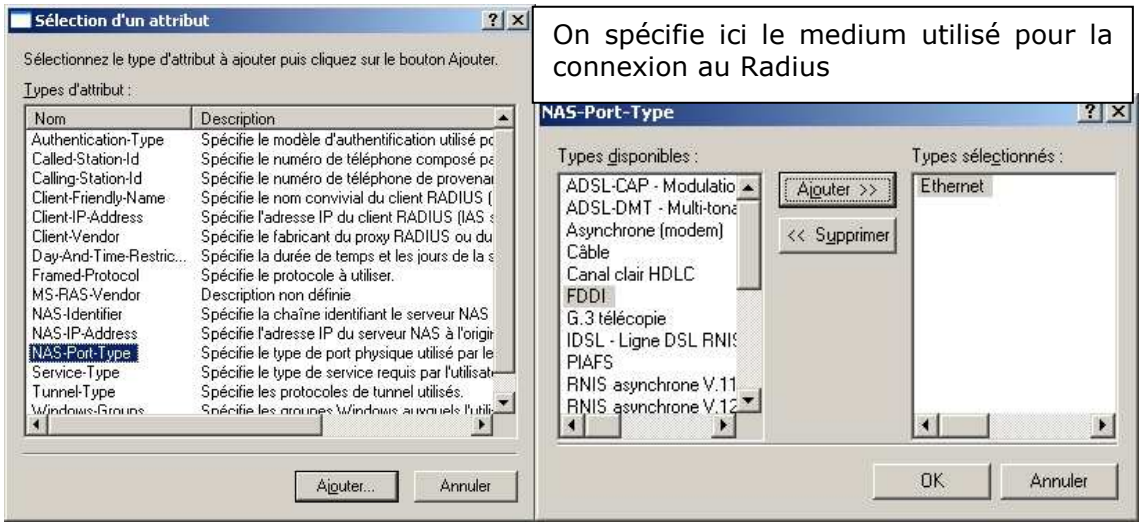


Ajoutons une nouvelle stratégie d'accès distant personnalisée:

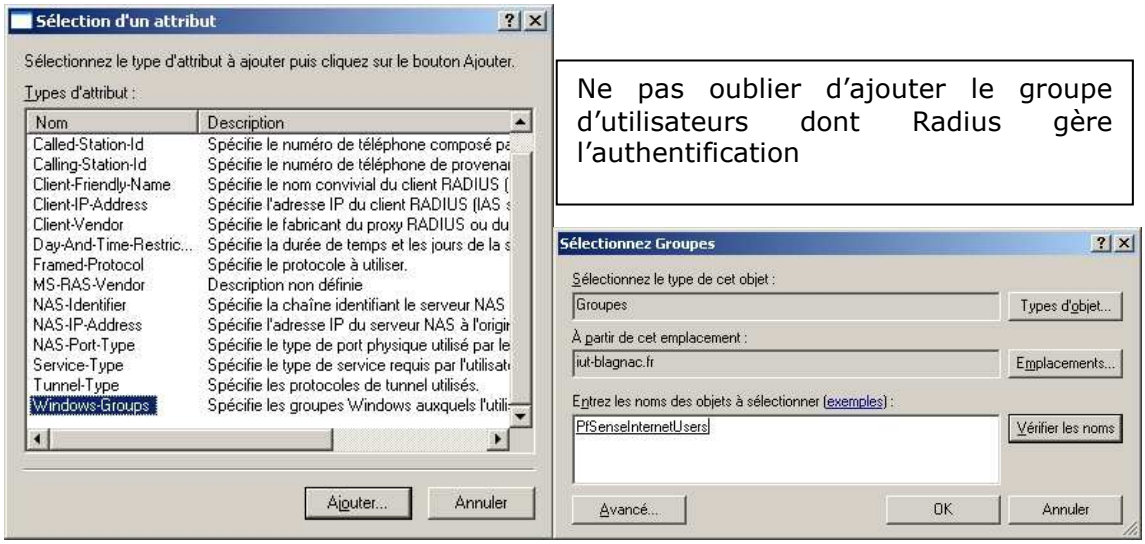


Création d'une nouvelle stratégie définissant comment le serveur Radius doit fonctionner (avec quels paramètres…)

Le NAS (Network Access Identifier) est la machine qui reçoit la demande d'authentification du client WiFi (ici la machine Pfsense)

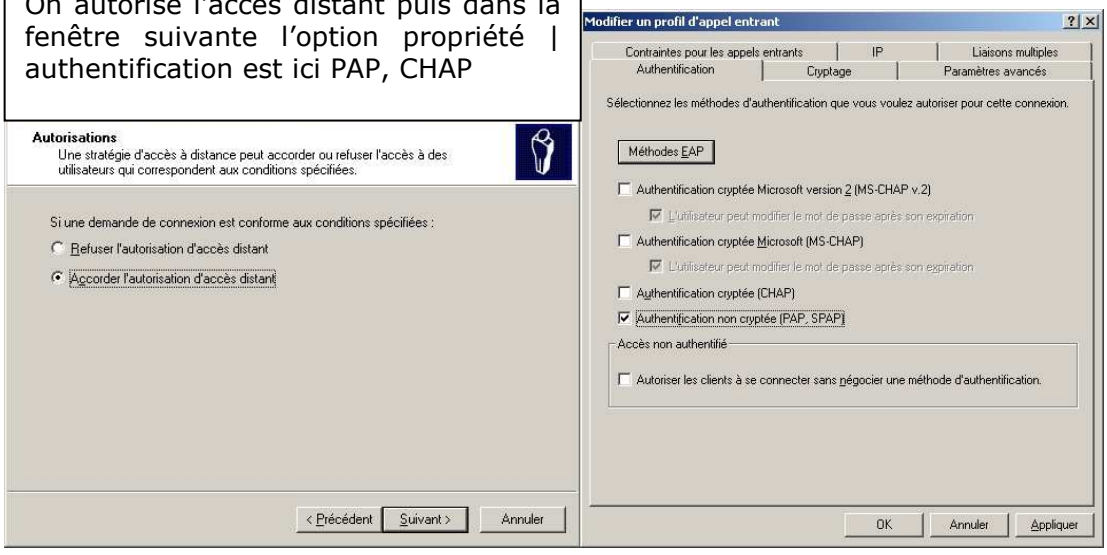


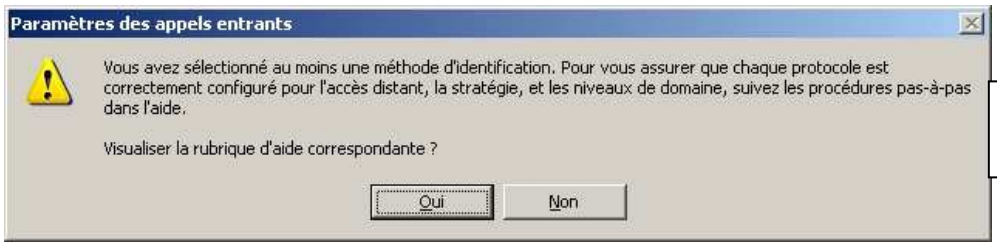
On spécifie ici le medium utilisé pour la connexion au Radius



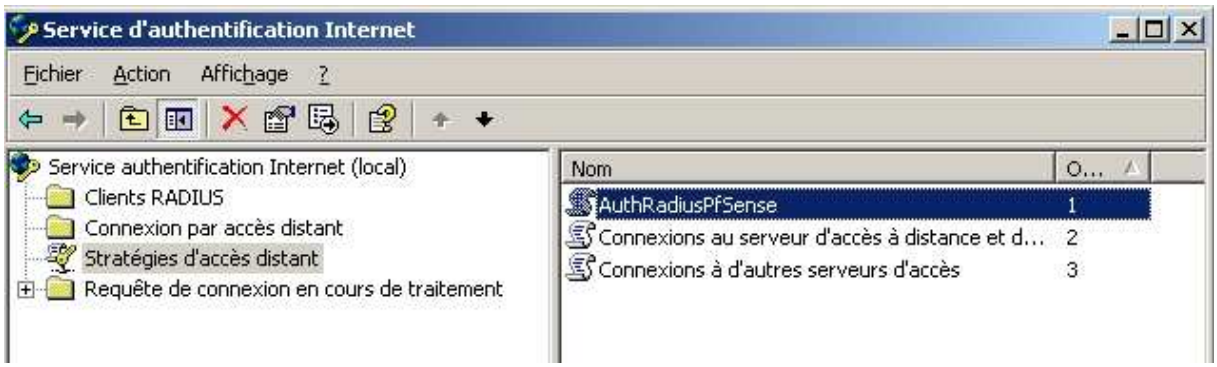
Ne pas oublier d'ajouter le groupe d'utilisateurs dont Radius gère l'authentification

On autorise l'accès distant puis dans la fenêtre suivante l'option propriété | authentification est ici PAP, CHAP

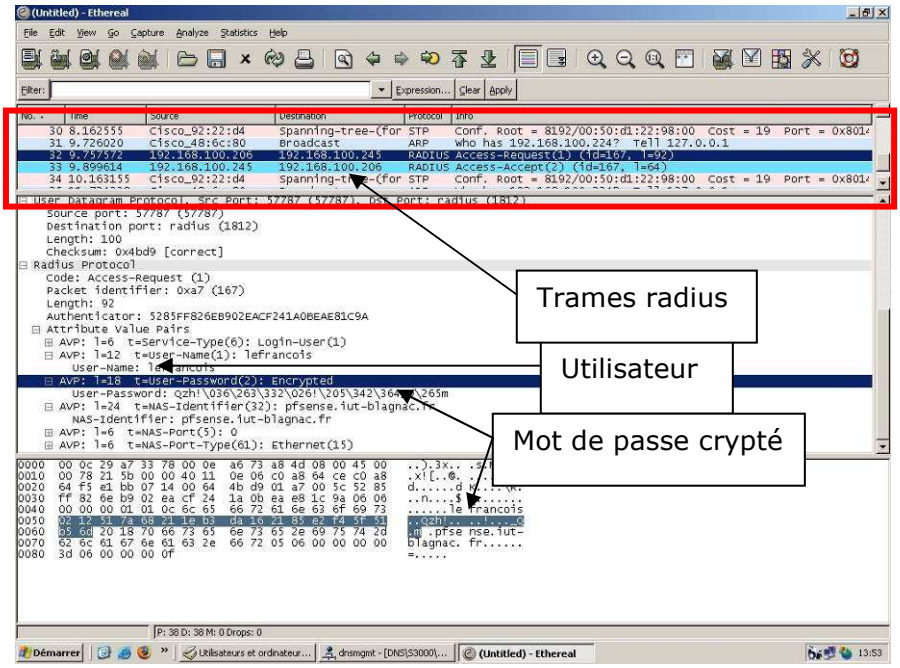




Pas obligatoire…



Avec un analyseur de réseau….test fait sur le serveur Radius



2.3.3 Sécurisation de PfSense

PfSense, à son installation, est dénué de toute sécurité. C'est assez embêtant dans la mesure où par exemple un mot de passe en clair serait facilement interceptable. Plusieurs étapes sont à prendre en compte :

- L'accès au Web Gui (l'interface d'administration)

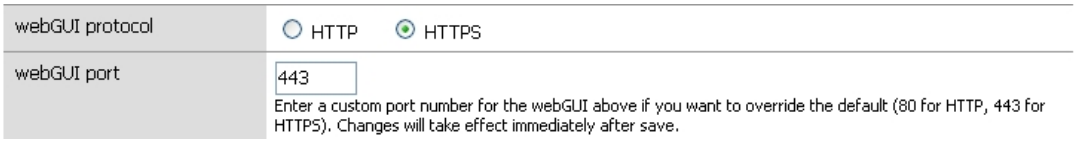
- L'authentification de l'utilisateur
- L'après authentification, Une communication cryptée

2.3.3.1 *L'accès sécurisé au Web Gui*

Pour cette sécurisation, vous aurez besoin d'un certificat. Une connexion HTTPS sera établie.
Si vous n'avez pas de certificat, reporter vous plus haut afin d'un créer un.

Si le certificat est présent dans la section *Advanced* (vu précédemment), allez dans le menu *General Setup.*

Sélectionnez HTTPS dans *WebGUI protocol* et mettez le port 443 (SSL) dans *WebGUI port*.



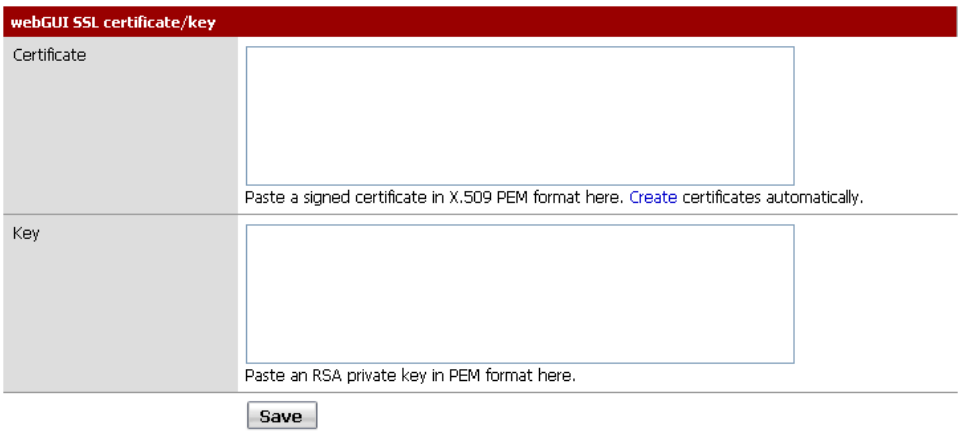
Voila, l'accès à Pfsense est entièrement sécurisé !

2.3.3.2 *L'authentification sécurisée de l'utilisateur*

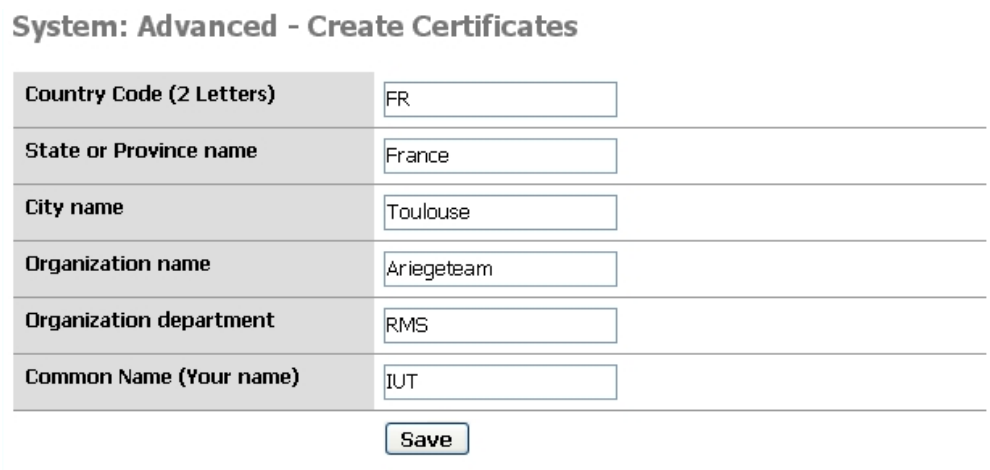
Pfsense permet des gérer un accès sécurisé au portail captif via SSL. L'accès se fera donc via une connexion HTTPS. Le client devra simplement télécharger un certificat pour la mise en place du tunnel crypté.

Configuration de Pfsense.

Avant d'activer l'HTTPS, il faut tout d'abord créer un certificat. Pour cela, Pfsense intègre un module pour leur génération.
Allez sur la section *System*, *Advanced***.**
Descendez ensuite la partie *webGUI SSL*. Ici vous pourrez créer votre certificat, cliquer sur *Create*



Entrer ensuite les informations demandées, et cliquer sur *Save*.



Vous avez maintenant votre certificat de créée. Cliquer sur *Save* afin de garder ce certificat.

Revenez ensuite sur cette page, et récupérez les clés. Nous nous en servirons pour l'accès sécurisé au portail.
Allez ensuite dans la section *Captive Portail.*
Activer le HTTPS, donner le nom de la machine et coller les clés créées plus haut.

Cliquer sur Save.
Voila, l'authentification est maintenant sécurisé.
Nous allons voir maintenant comment sécurisé l'accès à Pfsense pour l'administrateur.

2.4 CONFIGURATION CLIENT

La solution installée a été faite de sorte à ce que la mise en place du portail captif soit la plus transparente possible pour les utilisateurs.

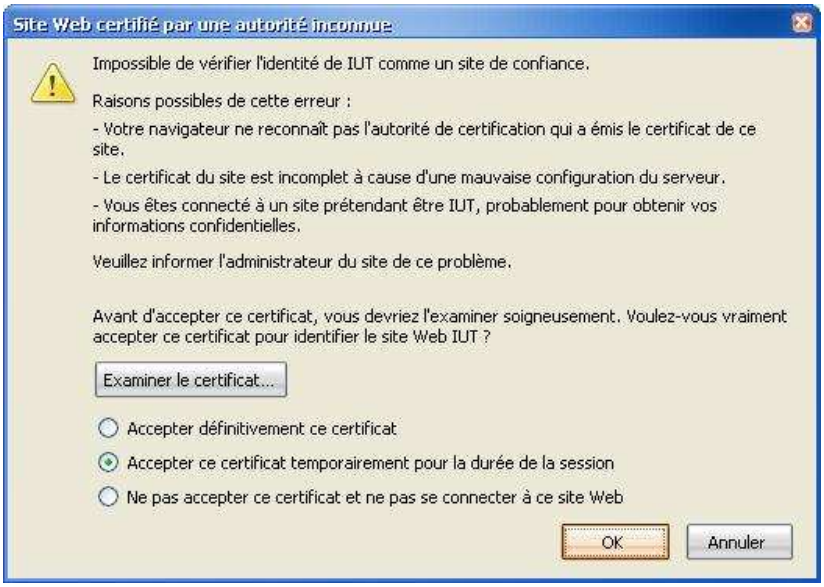
Nous allons donc voir maintenant la procédure de connexion d'un client WiFi.

Tout d'abord, le client choisira le SSID du WiFi de l'NOTRE MAQUETTE (WiFi_NOTRE MAQUETTE dans notre cas), et se connectera à ce réseau.

Le client devra se mettre en IP automatique. C'est-à-dire que l'adresse IP sera fournie par Pfsense.

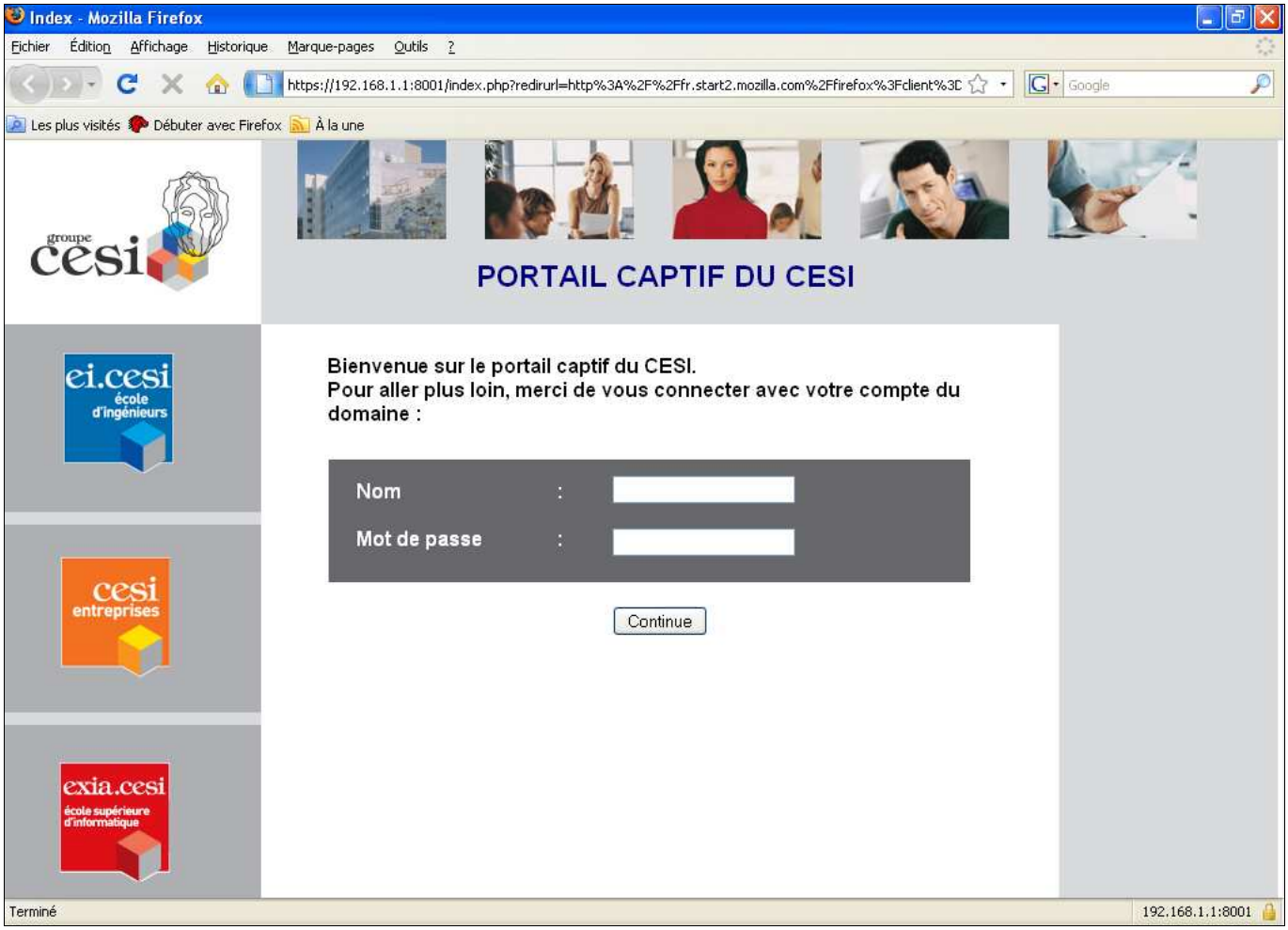
On voit bien ci-dessous que l'IP a bien été transmise de façon automatique.

L'utilisateur devra ensuite, tout simplement, ouvrir un navigateur web (comme s'il voulait surfer sur le web).
Il aura ensuite la charge de télécharger le certificat fourni automatiquement. Il aura donc une fenêtre comme celle-ci apparaître :

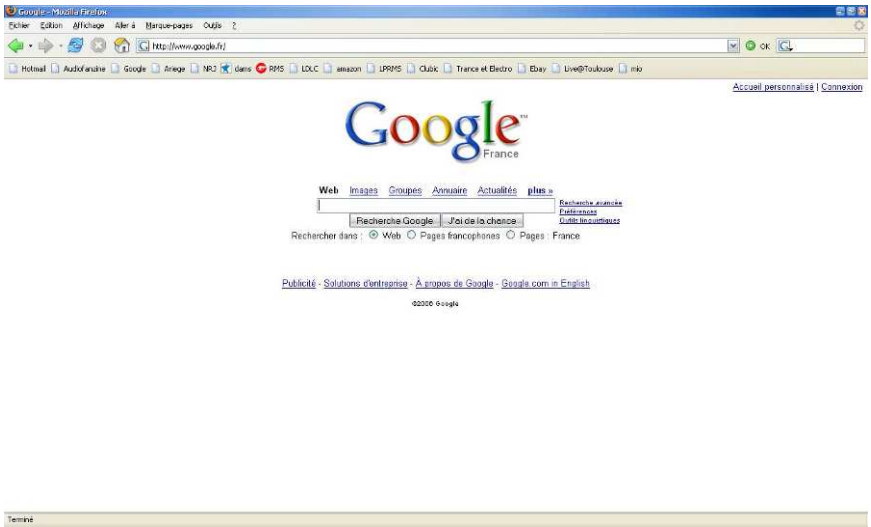


Dans certains cas, il aura le message suivant :

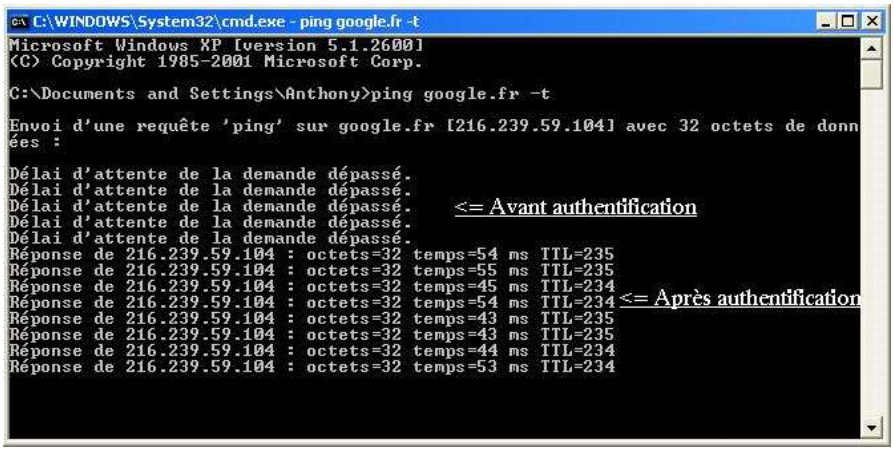
Il suffit de mettre "OK" et de passer à la suite.
Le client sera automatiquement redirigé vers la page html d'authentification. Il devra alors entrer ici son login et mot de passe.



Si le login est bon, il pourra alors surfer sur Internet !



2.4.1 Test de fonctionnement



3 VPN CLIENT

3.1 INTRODUCTION

Le VPN client consiste à connecter un nomade informatique à son entreprise via un tunnel sécurisé. Il faut voir ce tunnel comme un tuyau hermétique de bout en bout fermé à ses extrémités par deux portes verrouillées avec une même clef. A l'intérieur il y a de l'information qui transite de façon sécurisée puisque personne ne peut regarder ce qu'il y a dans le tuyau. Les personnes pouvant voir le contenu du tuyau se trouvent donc à l'extrémité de ce dernier et possèdent tous deux la même clef.

Plusieurs technologies disponibles dans PfSense permettent de mettre en place un VPN client:

- OpenVPN (http://openvpn.net/)
- IPSec (http://tools.ietf.org/html/rfc4301)
- PPTP (http://www.ietf.org/rfc/rfc2637.txt)

NB: A l'heure actuelle (v1.2.2) il manque toujours L2TP. La version 2.0 devrait l'embarquer.

A terme ce chapitre devrait contenir toutes les technologies de VPN disponibles dans PfSense. Néanmoins nous commencerons par notre chouchou, à savoir OpenVPN.

PS : Cette version V1.0 Beta n'aborde que le VPN client PPTP couramment utilisé par les entreprises. La suite pour bientôt…

3.2 PPTP

3.2.1 Présentation

Le **P**oint-**T**o-**P**oint **T**unneling **P**rotocol (PPTP) est un protocole d'encapsulation s'appuyant sur le protocole PPP pour la communication. Ce protocole ne peut travailler que sur des réseaux IP. Historiquement parlant, ce protocole a été implémenté pour la première fois par Cisco, il fut ensuite repris par Microsoft dans ses systèmes Windows. Une spécification fut publiée dans la Request For Comments (RFC) 2637 en juillet 1999, parmi les auteurs on citera à nouveau Microsoft, mais également l'équipementier 3Com, ainsi que d'autres sociétés moins connues (Ascend Communications, Copper Mountain Networks, ECI Telematics, etc…).

Fonctionnement général d'un VPN avec PPTP

Le protocole PPTP consiste en deux flux de communication entre le client et le serveur, s'appuyant directement sur le protocole IP :

- Le premier flux a pour rôle la gestion du lien entre les deux parties, il s'agit là d'une connexion sur le port 1723 du serveur en TCP.
- Le second flux concerne les données échangées entre les deux parties, bien entendu ce flux peut et doit être chiffré, ce dernier transite en utilisant le protocole GRE (**G**eneral **R**outing

Encapsulation, protocole de niveau 3 qui permet d'établir des tunnels IP sur de l'IP). Son usage est destiné aux **communications entre 2 routeurs**).

PPTP ne concerne que le transport des données, un de ces deux protocoles intervient ensuite pour sécuriser l'authentification, il faut en effet être certain que c'est la bonne personne qui se connecte au serveur VPN !

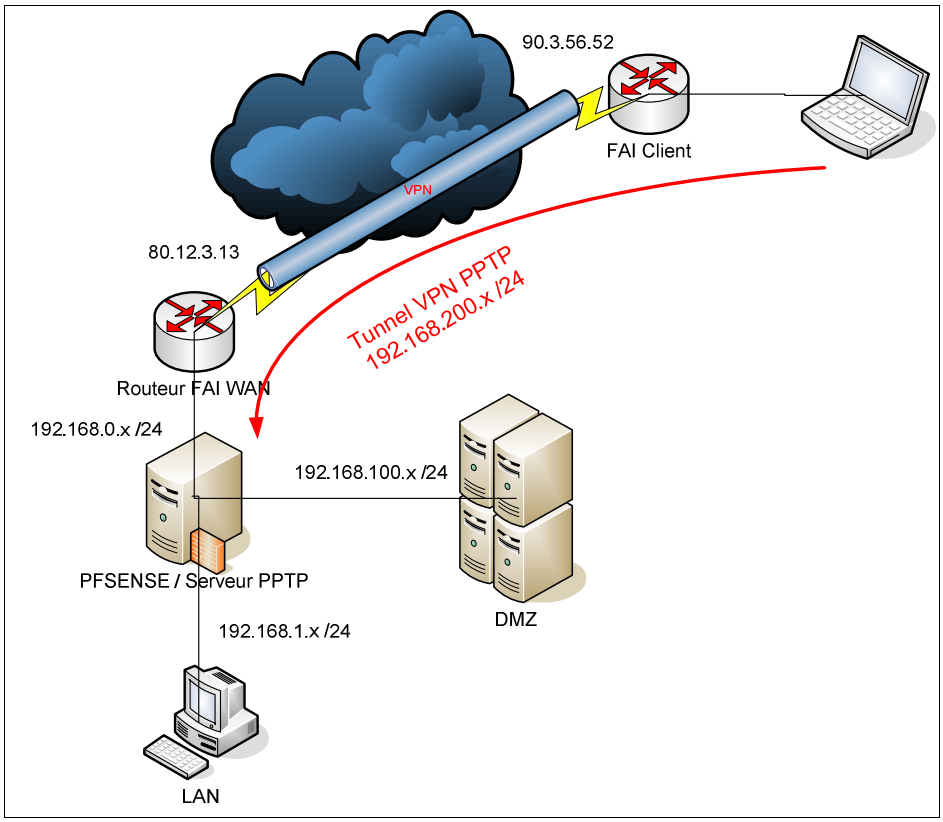
- **P**assword **A**uthentification **P**rotocol (PAP) : ce protocole décrit dans la RFC 1994 consiste à mettre en place une authentification entre le client et le serveur VPN. Les informations d'authentification (nom d'utilisateur et mot de passe) transitent en clair, ce qui n'est pas l'idéal si l'on veut sécuriser au maximum...
- **C**hallenge **H**andshake **A**uthentification **P**rotocol (CHAP) : ce protocole consiste en un mécanisme d'authentification crypté, il est donc sécurisé. Un protocole basé sur ce dernier, développé par Microsoft, est aussi utilisé : MS-CHAP.

L'authentification effectuée, il faut désormais sécuriser la communication au sein du VPN; comme pour l'authentification, la sécurisation des données repose sur un protocole de PPP : Compression Control Protocol. Différents types de cryptage sont utilisés, qu'ils soient symétriques ou asymétriques. Les algorithmes RSA (DES, RC4 et IDEA) et les clés publiques (Public Key Infrastructure, PKI) entre autres.

3.2.2 Limitation

Le protocole PPTP, étant une extension du protocole PPP, ne permet par contre pas de réaliser des liaisons multipoints. Il est limité à des connexions entre deux points. Ces deux points peuvent être n'importe où dans le monde.
Autre limitation, ce protocole ne permet que des VPN sur un réseau IP. Ceci est du à l'utilisation du protocole GRE pour l'encapsulation des trames.

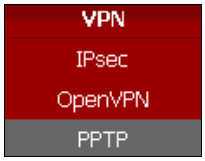
3.2.3 Schéma



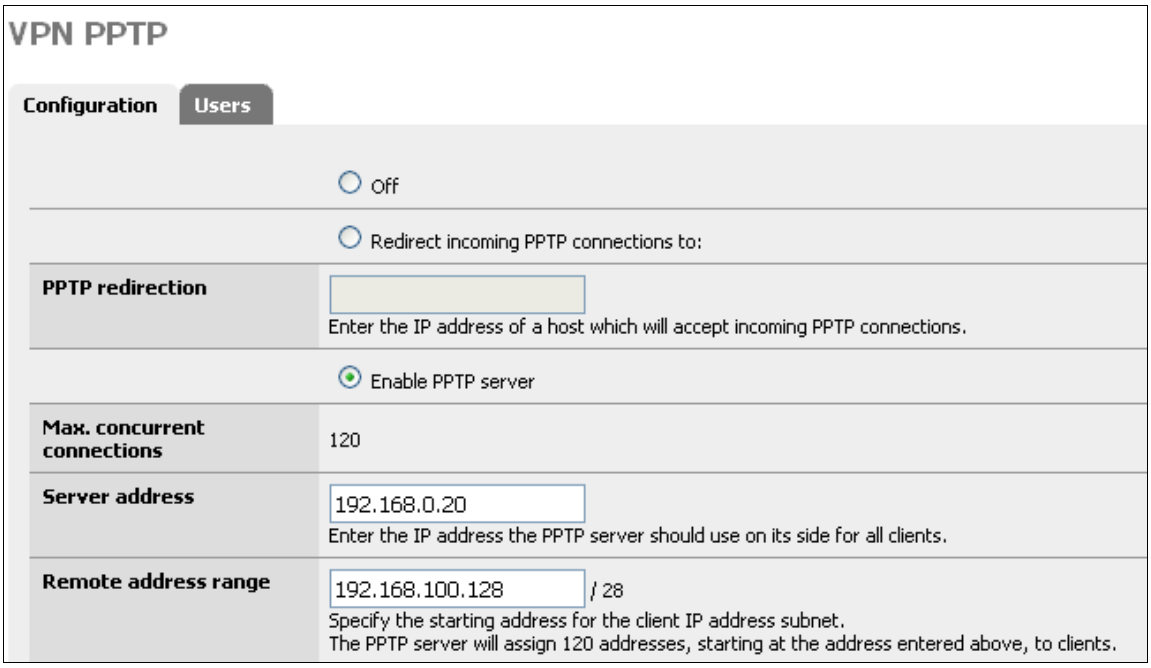
Sur notre maquette, nous avons placé une partie LAN, une DMZ, le WAN et une connexion à distance. Le tout est géré par Pfsense.
Le but est de montrer ici, que sur une architecture classique, nous pouvons créer des connexions sécurisées à distance sur notre LAN / DMZ. Nous allons voir maintenant comment le configurer.

3.2.4 Configuration Serveur

Sur Pfsense, le serveur PPTP est déjà installé. Pour le configurer, aller dans VPN puis PPTP.



Vous arrivez sur cette page de configuration :



Différents choix s'offre à nous ici :

- OFF : Désactive toutes requêtes PPTP
- Redirect incoming PPTP connections : Permet de rediriger les connexions PPTP vers un serveur externe. Il suffit ici d'entrer l'adresse IP de la machine.
- Enable PPTP server : Active le serveur interne à Pfsense. Nous allons détailler cette partie.

Vous voyez en dessous « Max concurrent connections ». Par défaut, le nombre est limité à 16. Vous vous posez maintenant la question de savoir comment arriver à 120 comme dans notre cas. Patience, nous y venons juste après.

Entrer ensuite l'adresse IP du serveur. Ici : 192.168.0.20 est l'adresse WAN de PFsense (vers le routeur).
« Remote address range » sert à spécifier la plage d'adresse que recevront les clients sur leurs tunnels. Ici encore, le masque n'est pas modifiable via l'interface Web.

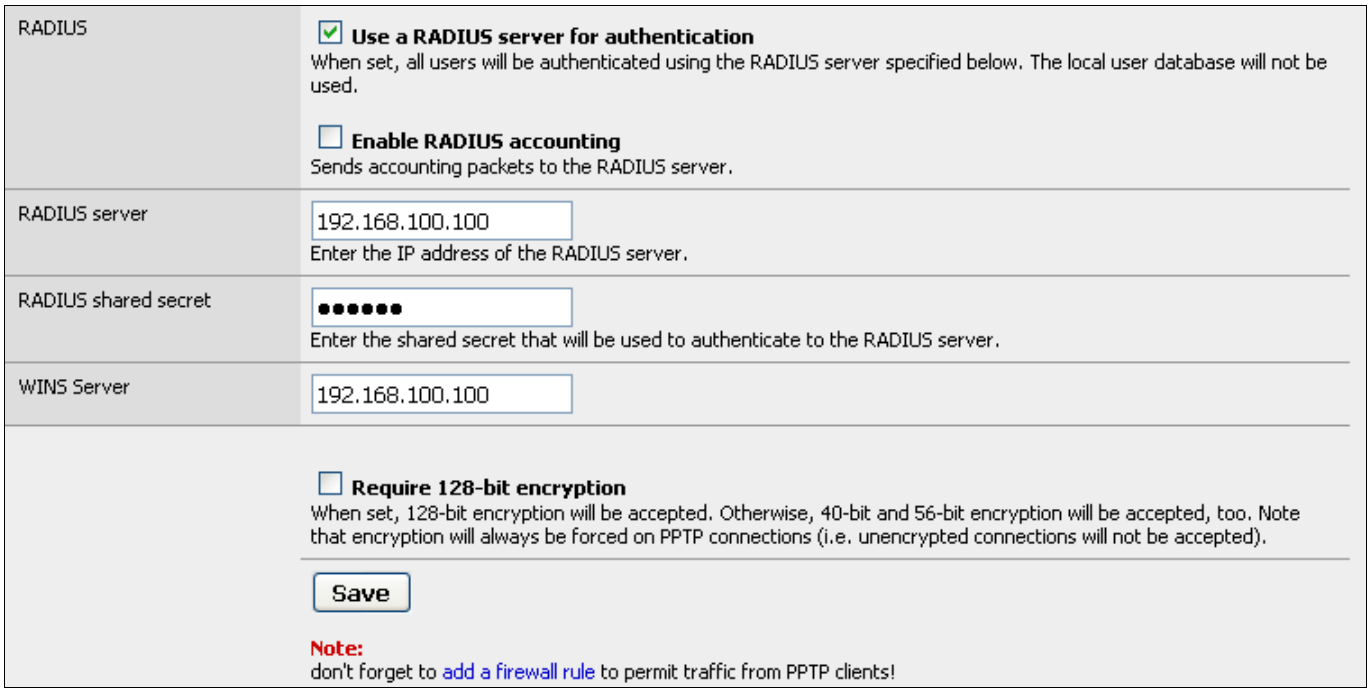
Pour modifier les 2 paramètres (connexion et masque), il faut aller le changer dans un fichier de configuration.
Aller dans « /etc/inc/ » et éditer le fichier « globals.inc ».

Faites défiler le fichier jusqu'à atteindre « n_pptp_units ». Cela correspond au nombre de connexions possible. Modifier la valeur 16 par votre nombre (ici 120). Idem pour le subnet (maque) juste en dessous (ici 28).

```
    "cf_path" => "/cf",
    "cf_conf_path" => "/cf/conf",
    "www_path" => "/usr/local/www",
    "xml_rootobj" => "pfsense",
    "pppoe_interface" => "ng0",
    "n_pptp_units" => 120,  /* this value can be overriden in pptp->n_pptp_units
 */
    "pptp_subnet" => 28,   /* this value can be overriden in pptp->pptp_subnet
*/
    "n_pppoe_units" => 16, /* this value can be overriden in pppoe->n_pppoe_unit
s */
    "pppoe_subnet" => 28,  /* this value can be overriden in pppoe->pppoe_subnet
  */
    "debug" => false,
    "latest_config" => "3.0",
    "nopkg platforms" => array("cdrom"),
```

Sauvegarder le fichier et recharger le page Web. Vous verrez les modifications appliquées.

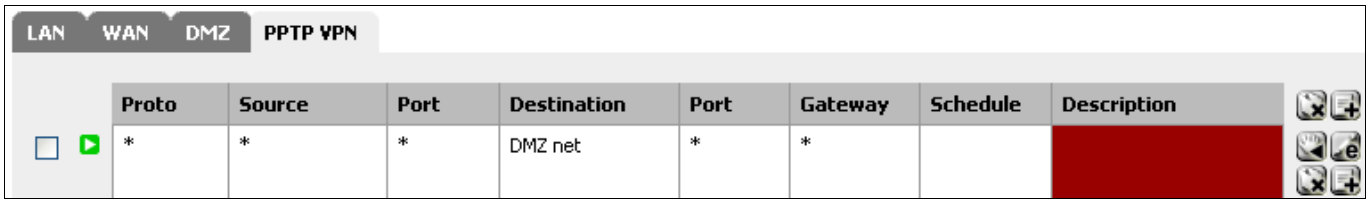
Par la suite, vous avez le choix entre l'authentification locale et un serveur Raduis. Dans notre cas, nous allons nous greffer sur l'AD déjà existant et le serveur RADIUS. Pour configurer le contrôleur de domaine, reportez-vous à la section « Portail Captif ».



Une fois l'AD configuré, cocher la case « Use a RADIUS server for authentification ». L'option « Enable RADIUS accounting » est facultative. L'accounting RADIUS est le moyen de garder trace des informations de connexion. Les informations reçues par ce biais permettent de réaliser tout un ensemble de statistiques d'usage, de consommation et dimensionnement.

Entrer ensuite l'adresse IP du serveur RADIUS ainsi que la clé secrète. Enfin, entrer l'adresse du serveur WINS (en général celui du contrôleur de domaine).

Sauvegarder la configuration. Le serveur est opérationnel.
Attention : Pfsense ajoute une interface dans le Firewall pour les connexions PPTP. Comme toute connexion par défaut, les règles bloquent tout le trafic. N'oublier donc pas d'ajouter une règle afin d'autoriser un trafic. Dans notre exemple, nous donnons uniquement l'accès à la DMZ.



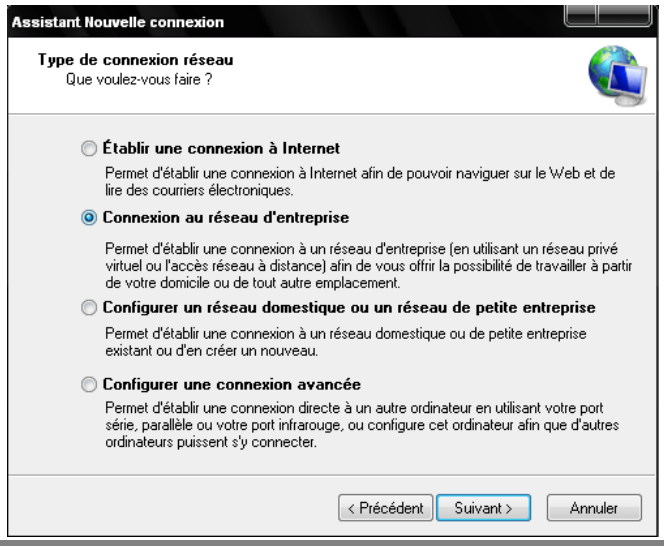
NOTE : Afin de permettre les connexions à distance, n'oublier pas de configurer votre routeur WAN pour ajouter une règle NAT : All IP externe vers 80.12.3.13 : 1723 (port PPTP) => 192.168.0.20 (ip wan pfsense) : 1723 (port PPTP).

Maintenant que le serveur est opérationnel, nous allons voir comment se connecter avec le client.

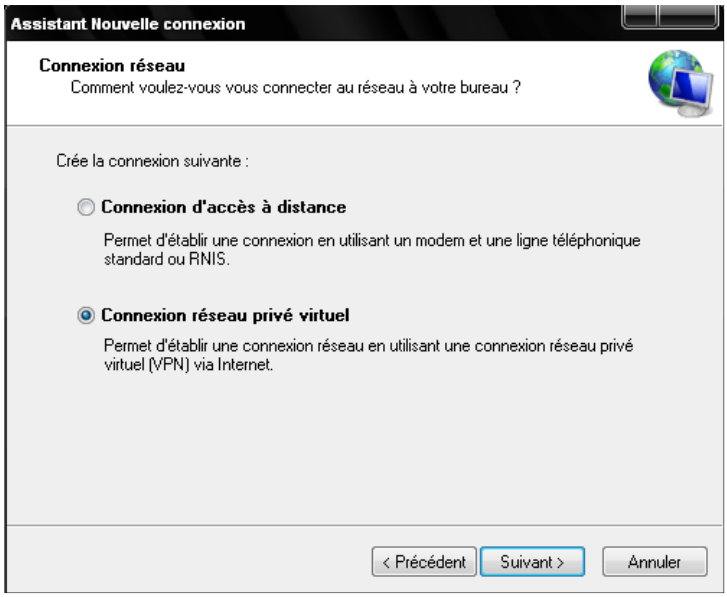
3.2.5 Configuration Client

La configuration client sous Windows est assez simple. Ceci est entièrement géré en natif dans l'OS. Nous allons vous montrer sous Windows XP comment le paramétrer.

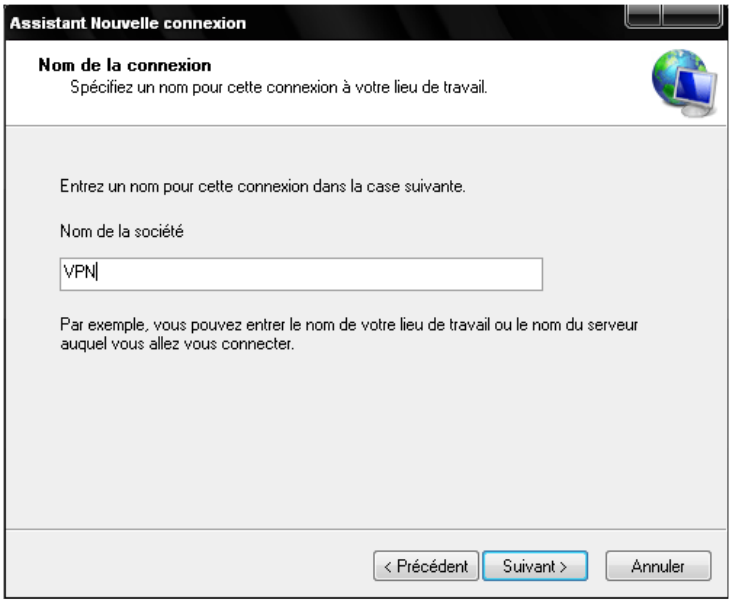
Dans les favoris réseau, nous allons créer une nouvelle connexion.



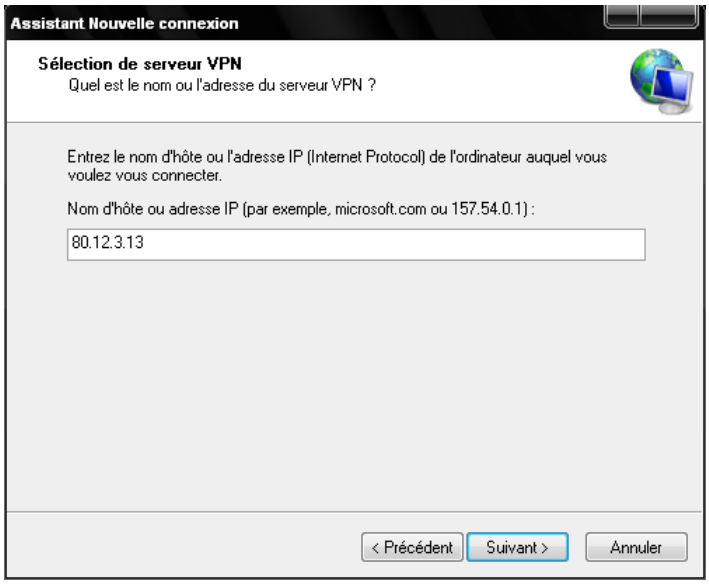
Cliquer sur « connexion au réseau d'entreprise ».



Sélectionner « Connexion réseau privé virtuel ».



Ajouter un nom pour cette connexion. Ici nous mettrons VPN.



Ajouter l'IP du serveur. En tant que client, vous n'avez accès qu'au lien WAN du routeur de la société. Vous pouvez mettre ici une adresse IP ou un nom DNS. Les règles NAT et configuration de PFSense se chargeront de transmettre la trame au sein du réseau de l'entreprise.

Une fois la connexion créée, lancer la et entrer un compte valide du contrôleur de domaine.

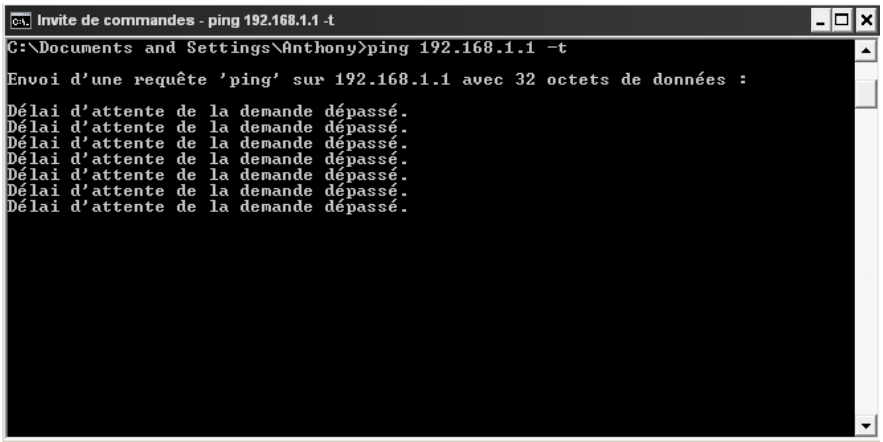
Une fois connecté, vous accédez au réseau de l'entreprise. Vous remarquerez dans les propriétés que votre connexion a bien reçu l'adresse définie dans PFSense.

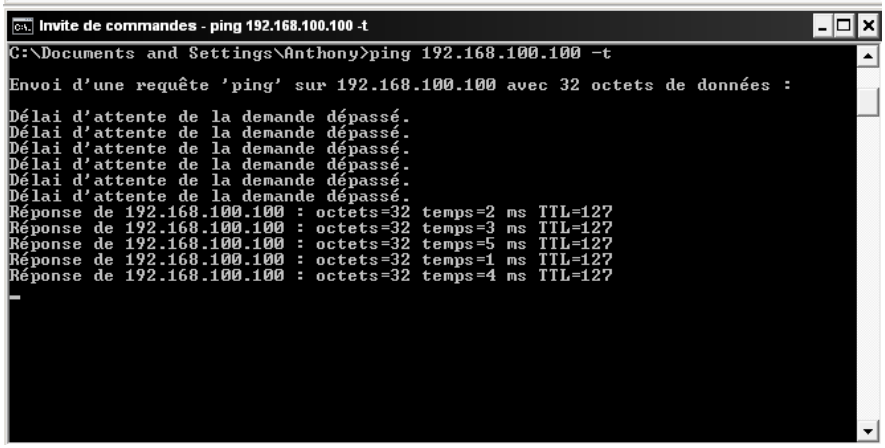
Nom du périphérique	Miniport réseau étendu (PPTP)
Type de périphérique	vpn
Type de serveur	PPP
Transports	TCP/IP
Authentification	MS CHAP V2
Cryptage	MPPE 128
Compression	(Aucun)
Trame multi-lien PPP	Inactif
Adresse IP du serveur	192.168.0.20
Adresse IP du client	192.168.100.129

3.2.6 Test de fonctionnement

Ci-dessous, 2 PING ont été réalisés : 1 vers le LAN, 1 vers la DMZ.
Nous avons précédemment donné l'accès uniquement à la DMZ dans le firewall. Une fois la connexion établie, le PING vers le LAN n'aboutie toujours pas, alors que la DMZ répond bien.

Vous avez maintenant un accès à l'entreprise à partir d'un nomade. Gardez à l'esprit qu'une fois le VPN créé, tout votre trafic réseau traversera ce tunnel, y compris votre accès Internet, et vous serez soumis aux règles de la société.





4 VPN SITE A SITE

4.1 INTRODUCTION

Le VPN site-à-site consiste à relier deux ou plusieurs sites distants par un tunnel sécurisé. Il faut voir ce tunnel comme un tuyau hermétique de bout en bout fermé à ses extrémités par deux portes verrouillées avec une même clef. A l'intérieur il y a de l'information qui transite de façon sécurisée puisque personne ne peut regarder ce qu'il y a dans le tuyau. Les personnes pouvant voir le contenu du tuyau se trouvent donc à l'extrémité de ce dernier et possèdent tous deux la même clef.

Plusieurs technologies disponibles dans PfSense permettent de mettre en place un VPN site-à-site:

- OpenVPN (http://openvpn.net/)
- IPSec (http://tools.ietf.org/html/rfc4301)
- PPTP (http://www.ietf.org/rfc/rfc2637.txt)

NB: A l'heure actuelle (v1.2.2) il manque toujours L2TP. La version 2.0 devrait l'embarquer.

A terme ce chapitre devrait contenir toutes les technologies de VPN disponibles dans PfSense.

4.2 PRE-REQUIS

Avant de configurer votre VPN, vérifiez que vous avez bien tenu compte des pré-requis. Cela peut parfois vous épargner pas mal de temps perdu ☺ .

- ✓ PfSense doit être correctement installé et configuré dans le réseau local.
- ✓ Les deux sous réseaux distants doivent impérativement être différents. En effet dans le cas ou A et B possèdent le même sous réseau, chaque requête depuis un PC sous réseau A vers un autre dans le sous réseau B sera bouclée automatiquement dans le sous réseau source, à savoir ici le sous réseau A. le Pare feu PfSense domaine A ne sera jamais donc sollicité pour router la requête.
- ✓ Un autre cas, variante de celui cité précédemment, consiste à monter un VPN entre deux Hôtes respectivement de domaine A et B. Nous déconseillons fortement ce type de configuration dans le sens ou l'administrateur ne peut pas contrôler le contenu de l'information par ses éléments de filtrage. Ainsi une attaque, un virus, etc. peuvent être lancés depuis le serveur X dans le domaine A vers le serveur Y dans le domaine B sans que les éléments de filtrage de A ou B puissent interférer.
- ✓ Si PfSense n'est pas la passerelle par défaut du LAN ou il est installé, il est indispensable de créer une redirection de trafic VPN entre la passerelle par défaut du LAN concerné et PfSense.
- ✓ Attention !, la mise en place d'un VPN site-à-site implique la prolifération de mauvaise information, notamment les virus et attaques… Pensez à vous munir d'outils de protection avant de mettre en place un VPN intersites. Cela peut paraître évident mais combien de fois s'est-on retrouvé infectés à cause d'un site partenaire…

4.3 CHOIX DE LA TECHNOLOGIE

Le tableau suivant récapitule brièvement ce qui est aujourd'hui supporté par une technologie et pas l'autre.

	OpenVPN	IPSec	PPTP
Clients mobiles	Oui	Ne supporte pas NAT-T ce qui empêche l'utilisation de client mobiles derrière du NAT.	Oui
Utiliser IP statiques ou dynamiques	Static IP : OUI Dynamic IP : v2.0	Static IP : OUI Dynamic IP : Un seul point final autorisé	Static IP : OUI Dynamic IP : OUI
Filtrage de traffic VPN	Prevu dans la v2.0	Oui	Oui
Types d'authentification	Shared Key, Certificat	Pre Shared Key, Certificat	local user database, RADIUS server (Authentication, Accounting)
Restrictions	-	-	2 IP publiques minimum pour du PPTP via utilisateurs en interne si PfSense est serveur PPTP
Fonctionnalités du mécanisme non encore implémentées dans PfSense	Celles manquantes dans la v2.0	DPD, XAuth, NAT-T, et autres	-

Analyse : Chacun possède ses avantages et inconvénients. En effet IPSec parait être la solution la plus viable aujourd'hui de par ses services proposés (OpenVPN attend la v2.0 de PfSense pour être vraiment opérationnel et PPTP n'est plus vraiment dédié au Site-à-site).

4.4 OPENVPN

4.4.1 Présentation

OpenVPN est un logiciel libre permettant de créer un réseau privé virtuel (VPN).

Ce logiciel, disponible dans PfSense, permet à des pairs de s'authentifier entre eux à l'aide d'une clé privée partagée à l'avance ou de certificats. Pour chiffrer ses données OpenVPN utilise le protocole SSLv3 de la librairie OpenSSL aussi présente dans PfSense.

4.4.2 Limitations d'OpenVPN

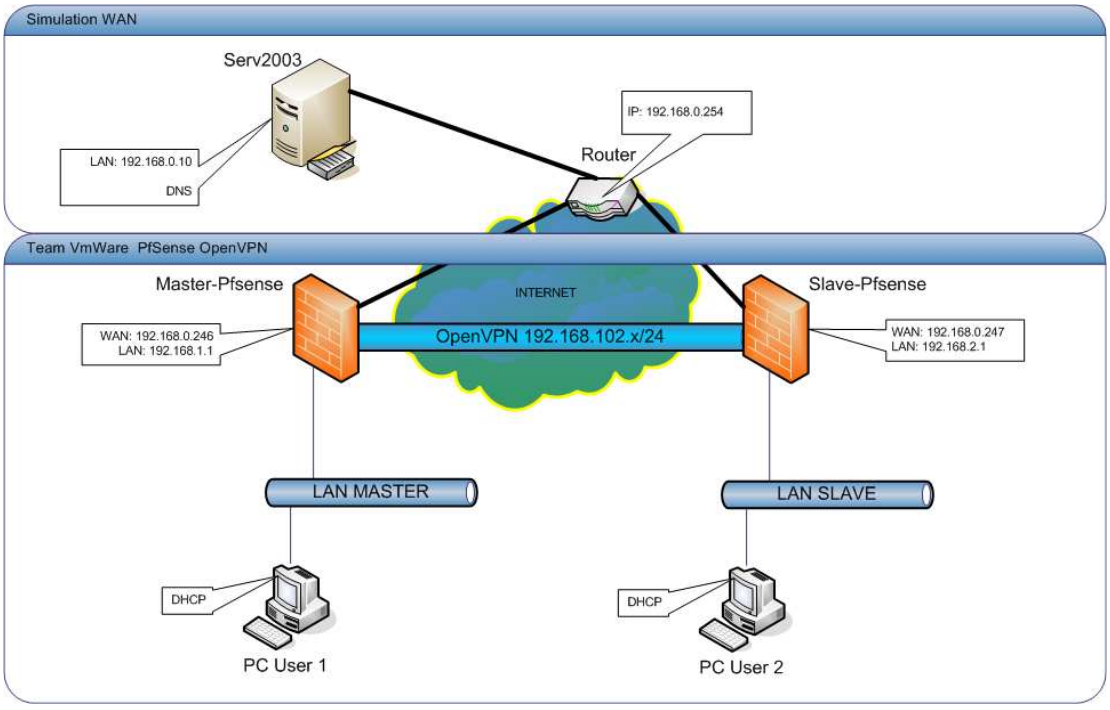
Voir la partie *Choix de la technologie* dans ce chapitre.

4.4.3 Schéma général

Après avoir vérifier les pré-requis en début de ce chapitre, nous pouvons désormais passer à la partie schéma général.

Matériel utilisé

- VmWare Workstation 6.5 avec :
  - Un Master-PfSense v1.2.2
  - Un Slave-PfSense v1.2.2
  - Un PC User 1 XP Pro
  - Un PC User 2 XP Pro
- Matériels WAN (DNS et Passerelle)



4.4.4 Configuration du Serveur

Création du Serveur OpenVPN sur **Master-PfSense**

Aller dans l'onglet **VPN > OpenVPN | Server** et Cliquer que la case « **+** » pour créer un nouveau Serveur openVPN.

Remplir les champs suivants :

- **Protocol** : UDP
- **Local port** : 1194 (port par défaut)
- **Address pool** : 192.168.102.0/24 (sous réseau des clients VPN, ici pour le Slave-PfSense)
- **Remote Network** : 192.168.2.0/24 (sous réseau du site distant)
- **Cryptography** : BF-CBC (128-bit) . A noter que la loi française fixe la limite de taille des clés à 128 bits (2 puissance 7) pour les particuliers, les entreprises doivent quant à elle faire une demande si elles souhaitent avoir recours à des clés d'une taille supérieure.
- **Authentication method** : Shared Key (si pas de PKI)

Remarque : La v2.0 intègrera un espace de management de certificats. Pour utiliser un certificat pour un VPN entre deux PfSense vous devez au minimum générer le certificat en v1.2.x.

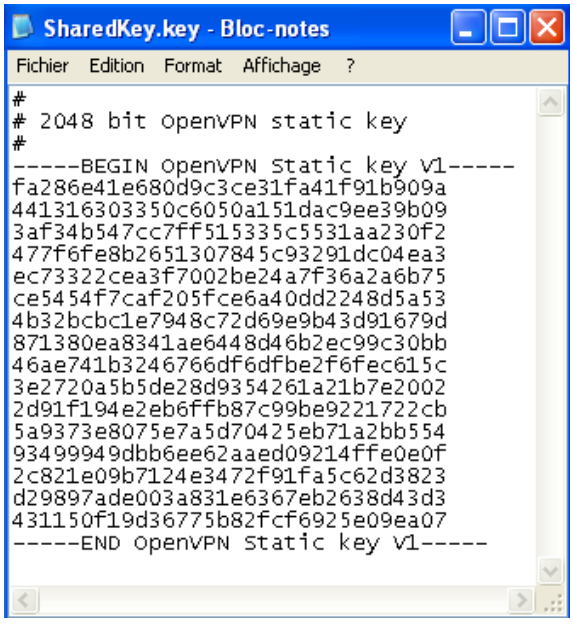
Pour générer la Shared Key vous pouvez utiliser le logiciel OpenVPNGui (http://openvpn.se). Choisissez par défaut la version « Package » qui embarque tous les drivers utiles.

a. Installer OpenVPNGui

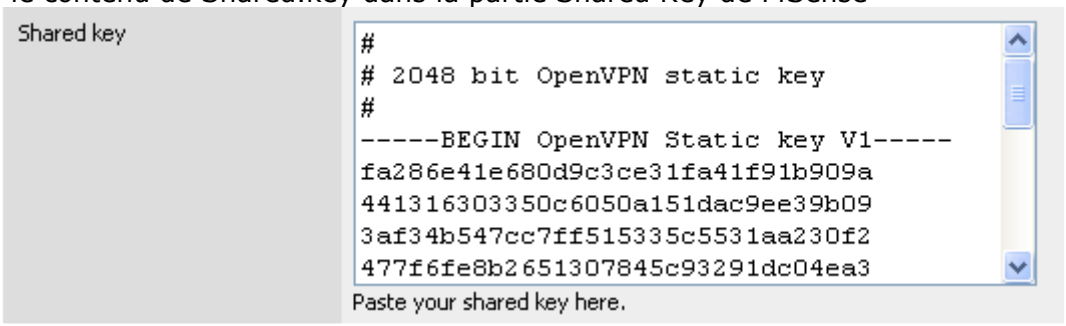
b. Ouvrir une fenêtre DOS et taper les commandes suivantes:
   - CD C:\Program Files\OpenVPN\easy-rsa\
   - openvpn --genkey --secret SharedKey.key

```
C:\Program Files\OpenVPN\easy-rsa>openvpn --genkey --secret SharedKey.key

C:\Program Files\OpenVPN\easy-rsa>_
```

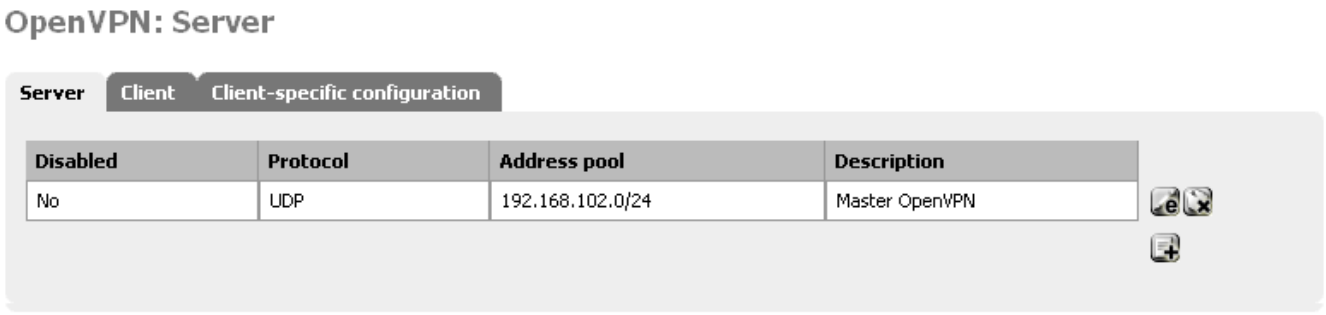
c. Récupérer le contenu du fichier Shared.key crée dans le dossier « C:\Program Files\OpenVPN\easy-rsa »



d. Coller le contenu de Shared.key dans la partie Shared Key de PfSense



- **LZO compression** : Cocher la case si vous voulez utiliser la compression de paquets.
- ***DHCP-Opt.: DNS-Domainname*** : ici vous pouvez entrer le nom de domaine local que vous utilisez
- ***DHCP-Opt.: DNS-Server*** : entrez ici les IPs des serveurs DNS de votre domaine séparés par des points virgules
- Cliquer sur **Save**



4.4.5 Configuration du client

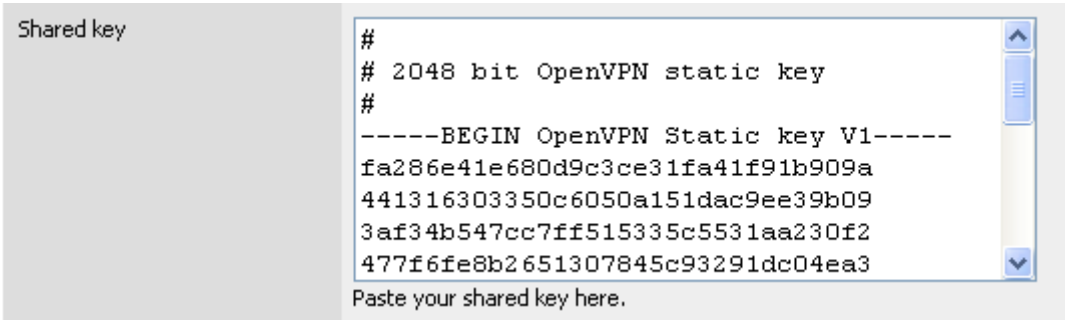
Création du Client OpenVPN sur **Slave-PfSense**

Aller dans l'onglet **VPN > OpenVPN | Client** et Cliquer que la case « **+** » pour créer un nouveau client openVPN.

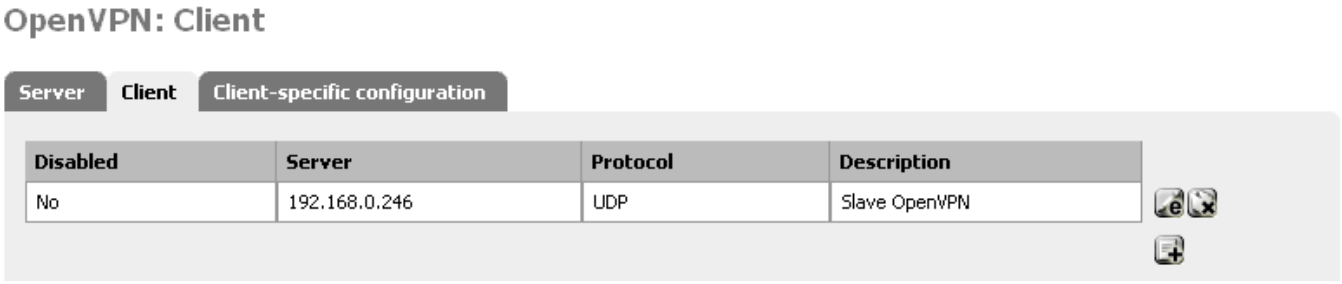
Remplir les champs suivants :

- **Protocol** : UDP
- **Local port** : 1194 (port par defaut)
- **Address pool** : 192.168.102.0/24 (sous réseau des clients VPN, ici pour le Slave-PfSense)
- **Remote Network** : 192.168.1.0/24 (sous réseau du site distant)
- **Cryptography** : BF-CBC (128-bit) . A noter que la loi française fixe la limite de taille des clés à 128 bits (2 puissance 7) pour les particuliers, les entreprises doivent quant à elle faire une demande si elles souhaitent avoir recours à des clés d'une taille supérieure.
- **Authentication method** : Shared Key

a. Coller le contenu de Shared.key du serveur OpenVPN dans la partie Shared Key de PfSense



- **LZO compression** : Cocher la case si vous voulez utiliser la compression de paquets.
  NB : Si vous choisissez la compression n'oubliez pas de cocher la case correspondante ET sur le Master-PfSense ET sur le Slave-PfSense.
- ***DHCP-Opt.: DNS-Domainname*** : ici vous pouvez entrer le nom de domaine local que vous utilisez
- ***DHCP-Opt.: DNS-Server*** : entrez ici les IPs des serveurs DNS de votre domaine séparés par des points virgules
- Cliquer sur **Save**



4.4.6 Test de fonctionnement

@IP PC User 1 (LAN MASTER) : 192.168.1.198
@IP PC User 2 (LAN SLAVE) : 192.168.2.245

Commande PING De PC User 1 vers PC User 2

```
C:\Documents and Settings\dasm>ping 192.168.2.245

Envoi d'une requête 'ping' sur 192.168.2.245 avec 32 octets de données :

Réponse de 192.168.2.245 : octets=32 temps=3 ms TTL=126
Réponse de 192.168.2.245 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.2.245 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.2.245 : octets=32 temps=2 ms TTL=126
```

Commande PING De PC User 2 vers PC User 1

```
C:\Documents and Settings\dasm>ping 192.168.1.198

Envoi d'une requête 'ping' sur 192.168.1.198 avec 32 octets de données :

Réponse de 192.168.1.198 : octets=32 temps=8 ms TTL=126
Réponse de 192.168.1.198 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.1.198 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.1.198 : octets=32 temps=1 ms TTL=126
```

4.5 IPSEC

4.5.1 Présentation

IPsec (Internet Protocol Security) est un ensemble de protocoles (couche 3 modèle OSI) utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP.
Son objectif est d'authentifier et de chiffrer les données : le flux ne pourra être compréhensible que par le destinataire final (chiffrement) et la modification des données par des intermédiaires ne pourra être possible (intégrité). Pour plus de détail ➔ http://fr.wikipedia.org/wiki/IPsec .

4.5.2 Limitations

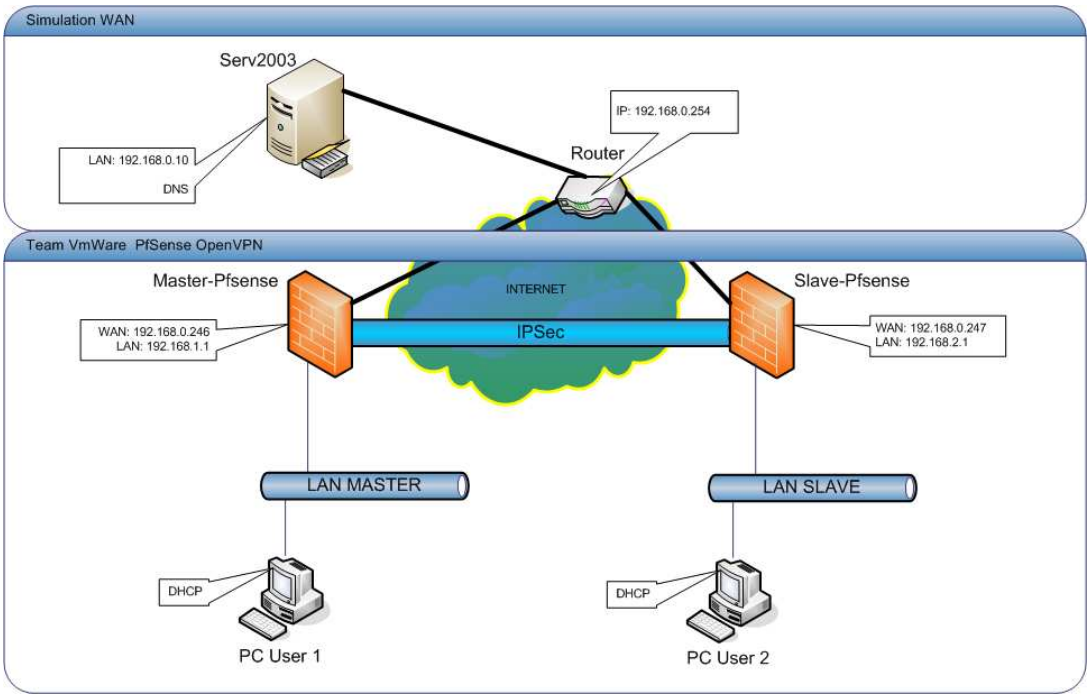
Voir la partie *Choix de la technologie* dans ce chapitre.

4.5.3 Schéma général

Après avoir vérifier les pré-requis en début de ce chapitre, nous pouvons désormais passer à la partie schéma général.

Matériel utilisé

- VmWare Workstation 6.5 avec :
  - Un Master-PfSense v1.2.2
  - Un Slave-PfSense v1.2.2
  - Un PC User 1 XP Pro
  - Un PC User 2 XP Pro
- Matériels WAN (DNS et Passerelle)



4.5.4 Configuration du serveur

Création du Serveur IPSec sur **Master-PfSense**

Aller dans l'onglet **VPN > IPSec | Tunnels** et Cliquer sur la case « **+** » pour créer un nouveau serveur IPSec en mode *Tunnel*.
Le mode *Transport*, notamment utilisé pour le Host-To-Host n'est pas utilisable dans PfSense 1.2.2. Pas de problèmes le mode *Tunnel* est très utilisé pour le *LAN-to-LAN* car il offre une protection contre l'analyse de trafic et les adresses source et destination sont toutes masquées.

Remplir les champs généraux suivants :

- **Interface** : WAN
- **Local subnet** : LAN subnet (sous réseau LAN de Master-PfSense)
- **Remote subnet** : 192.168.2.0/24 (sous réseau LAN de Slave-PfSense)
- **Remote gateway** : 192.168.0.247 (@IP WAN Slave-PfSense)
- **Description**: Ici votre description, par exemple *Tunnel IPSEC Master-Slave PfSense*

Passons à la configuration de la phase 1 IPSec (authentication)

- **Negociation mode** : agressive (il existe aussi *main*, plus sécurisé mais moins rapide)
- **My identifier** : My IP address (si vous avez une IP WAN statique), sinon votre DynDNS, Nom de domaine, FQDN utilisateur ou autre adresse IP WAN.
- **Encryption algorithm** : Blowfish (plus rapide que les autres !), 3DES pour la compatibilité avec d'autres matériels mais plus lent… etc. Lorque vous choissisez un algorithme d'encryption d'un côté du Tunnel IPSec, vous devez choisir le même de l'autre côté !
- **Hash Algorithm** : SHA1 (le même algorithme de hachage sur les deux extrémités du Tunnel).
- **DH Key Group** : 2 (1024 bit est un bon compromis entre vitesse et sécurité)
- **Lifetime** : 28800 (Partie importante !, ce temps, en secondes, en détermine la durée de vie de la phase 1 avant sa réinitialisation).
- **Pre-Shared Key** : [votre secret partagé] (Attention case sensitive), utilisez par exemple une clé comme IPSec@PfSense09TeamAr1ège . Si vous avez une PKI utilisez un certificat et RSA signature…

Configuration de la phase 2 (SA / Key Exchange)

- **Protocol** : ESP (une règle Firewall sera crée pour autoriser en entrée ESP)
- **Encryption algorithms** : Blowfish (le plus rapide en encryption). Rijndael (AES) pour du secret, Rijndael 256 pour du top secret selon la NSA, 3DES pour la meilleure compatibilité. Décochez les autres possibilités.
- **Hash algorithms** : SHA1 (le même algorithme de hachage sur les deux extrémités du Tunnel)
- **PFS key group** : 2 (1024 bit est un bon compromis entre vitesse et sécurité)
- **Lifetime** : 86400 (C'est le temps de validité de la clé d'encryption avant qu'elle ne soit régénéré. 86400 s, soit 1 jour est amplement suffisant pour le compromis paranoïa de hacking de la clé d'encryption / sécurité.

Configuration du Keep Alive (Message vérifiant la bonne connectivité entre 2 hôtes, ex ping !)

- **Automatically ping host** : 192.168.0.10 (preferez une @IP WAN fixe :-s)

Cliquez sur **Save** pour finaliser la configuration du serveur IPSec.

4.5.5 Configuration du client

La particularité du mode Tunnel d'IPSec est qu'en réalité vous créez deux serveurs et n'avez donc pas de relation Maître-Esclave.

La configuration de **Slave-PfSense** est donc très simple. Répétez les étapes de la partie Configuration du serveur faite précédemment en changeant bien sur les paramètres suivants:

- **Remote subnet** : 192.168.1.0/24 (sous réseau LAN de Master-PfSense)
- **Remote gateway** : 192.168.0.246 (@IP WAN Master-PfSense)

Réutilisez les autres valeurs, ne les changez surtout pas !

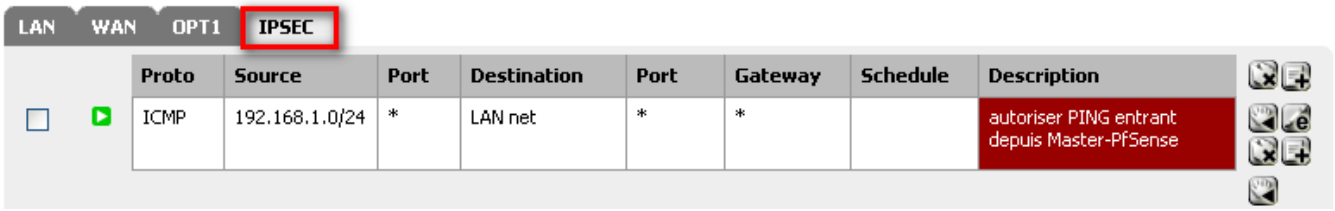
4.5.6 Créer les règles de Pare-feu

Voilà, IPSec est configuré sur nos deux pare-feu PfSense et pourtant quand je PING un hôte distant à travers le VPN, rien ne se passe…pourtant j'ai tout autorisé en WAN pour mon test…

Voilà le cas type d'une personne qui n'a pas lu la partie du le filtrage de trafic VPN dans notre tableau comparatif sur les VPN site-à-site ^^.

En effet PfSense, tellement qu'il est bien dirait Sarkozy, permet le filtrage de trafic VPN IPSec via l'interface IPSec dans les Rules.

Exemple : sur **Slave-PfSense** :



Ainsi je crée ma Rule n'autorisant que les personnes du domaine LAN Master-PfSense à me Pinguer sur une de mes machines dans mon LAN Slave-PfSense.

Cela veut dire que tout le reste est interdit !

Il faut donc paramétrer les flux autorisés en entrée à chaque extrémité du tunnel IPSec. Cette tâche est laissée libre au lecteur.

4.5.7 Test de fonctionnement

Vous devez créer de l'activité dans le tunnel IPSec crée pour voir apparaître le SAD.
La SAD (Security Association Database) est une database contenant les associations de sécurité (SA).

@IP PC User 1 (LAN MASTER) : 192.168.1.198
@IP PC User 2 (LAN SLAVE) : 192.168.2.245

Commande PING De PC User 1 vers PC User 2

```
C:\Documents and Settings\dasm>ping 192.168.2.245

Envoi d'une requête 'ping' sur 192.168.2.245 avec 32 octets de données :

Délai d'attente de la demande dépassé.
Réponse de 192.168.2.245 : octets=32 temps=13 ms TTL=126
Réponse de 192.168.2.245 : octets=32 temps=2 ms TTL=126
Réponse de 192.168.2.245 : octets=32 temps=3 ms TTL=126
```

Remarque : On voit bien au premier PING l'initialisation d'activité du Tunnel IPSec. Dès lors, on voit par exemple sur les figures suivantes (Status | IPSec) que la SAD-SPD sur **Master-PfSense** est bien crée et que donc le PING peut passer.

Status: IPsec

Overview | SAD | SPD

Source	Destination	Description	Status
192.168.0.246	192.168.0.247 192.168.2.0/24	Tunnel IPSEC Master-Slave PfSense	

Dans le résumé du status IPSec, on voit que le tunnel est bien activé (status au vert…)

Diagnostics: IPSec: SA

Overview | SAD | SPD

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
192.168.0.246	192.168.0.247	ESP	0e593ca6	blowfish-cbc	hmac-sha1
192.168.0.247	192.168.0.246	ESP	0748b906	blowfish-cbc	hmac-sha1

On voit ici la SAD contenant les SA. Une SA étant constitué d'une entête SPI (Security Parameter Index),tag d'identification en entête de paquet, + @IPDestination. Pour aller plus loin : http://en.wikipedia.org/wiki/IPsec#Security_Association

Diagnostics: IPSec: SPD

Overview | SAD | SPD

Source	Destination	Direction	Protocol	Tunnel endpoints
192.168.2.0/24	192.168.1.0/24	▶	ESP	192.168.0.247 - 192.168.0.246
192.168.1.0/24	192.168.2.0/24	◀	ESP	192.168.0.246 - 192.168.0.247

▶ incoming (as seen by firewall)

◀ outgoing (as seen by firewall)

Ici les routes des sous réseaux apparaissent dans la SPD (Security Policy Database)

Commande PING De PC User 2 vers PC User 1

```
C:\Documents and Settings\dasm>ping 192.168.1.198

Envoi d'une requête 'ping' sur 192.168.1.198 avec 32 octets de données :

Réponse de 192.168.1.198 : octets=32 temps=8 ms TTL=126
Réponse de 192.168.1.198 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.1.198 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.1.198 : octets=32 temps=1 ms TTL=126
```

5 LE BASCULEMENT (FAILOVER)

5.1 PRESENTATION

Le **basculement** (en anglais, failover qui se traduit par passer outre à la panne) est la capacité d'un équipement à basculer automatiquement vers un chemin réseau alternatif ou en veille.

Cette capacité existe pour tout type d'équipements réseau: du serveur au routeur en passant par les pare-feu et les commutateurs réseau (switch). Le basculement intervient généralement sans action humaine et même bien souvent sans aucun message d'alerte. Le basculement est conçu pour être totalement transparent.

Il existe deux modes principaux de basculement :

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

Source wikipedia.fr

PfSense permet la mise en place d'un système de basculement Actif-Passif, et surement bientôt Actif-Actif (v2.0 ?).

Le **basculement (pour l'instant Actif-Passif)** est rendu possible grâce au protocole **CARP** (Common Address Redundancy Protocol). CARP est un protocole permettant à un groupe d'hôtes sur un même segment réseau de partager une adresse IP, ce qui crée donc un groupe de redondance. Au sein de ce groupe, un hôte est désigné comme "maître". Les autres membres sont appelés "esclaves". L'hôte maître est celui qui "prend" l'adresse IP partagée. Il répond à tout trafic ou requête ARP à l'attention de cette adresse. Chaque hôte peut appartenir à plusieurs groupes de redondance. Chaque hôte doit avoir une seconde adresse IP unique.

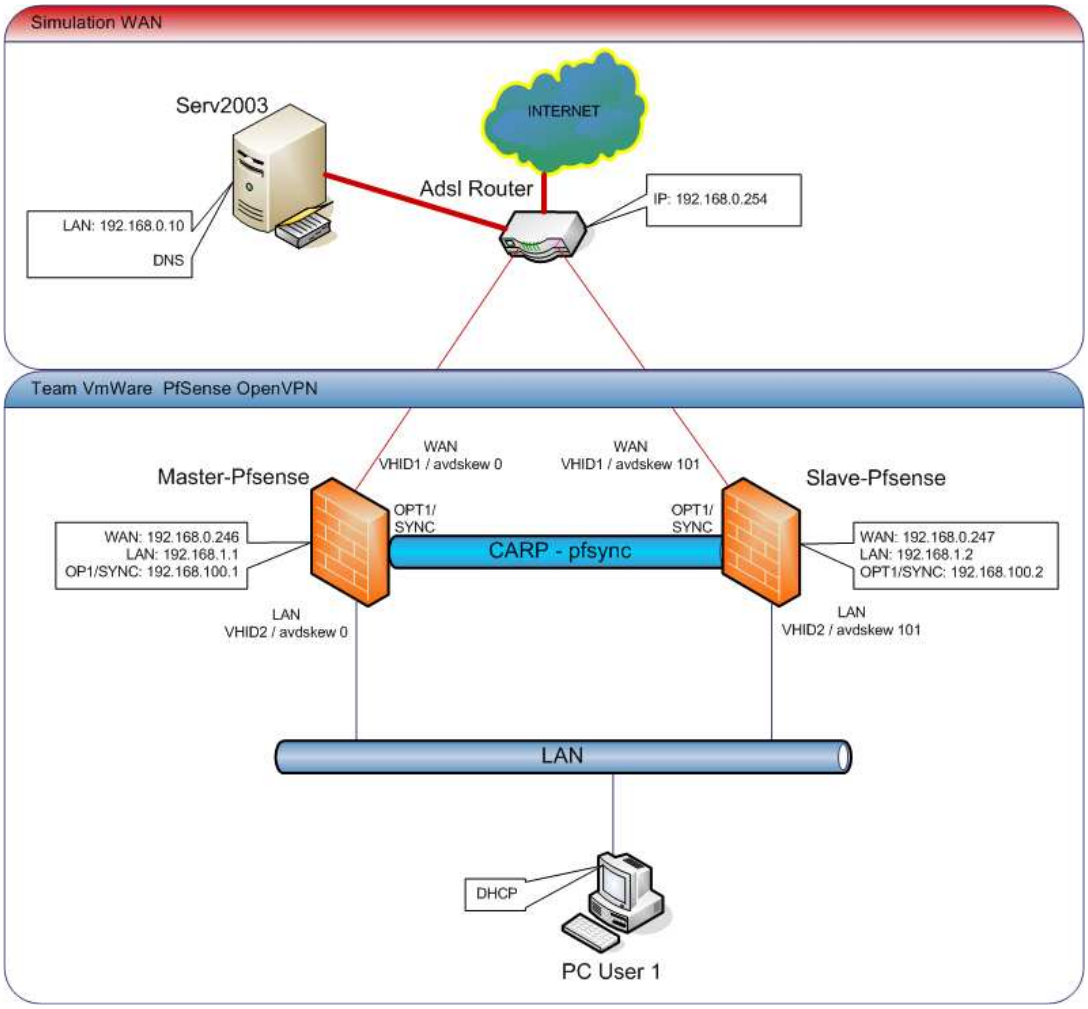
Une utilisation commune de CARP est la création d'un groupe de pare-feu redondants. L'adresse IP virtuelle attribuée au groupe de redondance est désignée comme l'adresse du routeur par défaut sur les machines clientes. Dans le cas où le pare-feu maître rencontre une panne ou est déconnecté du réseau (mise à jour par exemple), l'adresse IP virtuelle sera prise par un des pare-feu esclaves et le service continuera à être rendu sans interruption.
C'est justement de type de configuration avec deux pare-feu PfSense v1.2.2 que nous allons déployer et expliquer dans ce tutorial.

Remarque préalable : Un tutorial vidéo CARP existe aussi en ligne :
http://pfsense.bol2riz.com/tutorials/carp/carp-cluster-new.htm

5.2 SCHEMA GENERAL

Matériel utilisé

- VmWare Workstation 6.5 avec :
  - Un Master-PfSense v1.2.2
  - Un Slave-PfSense v1.2.2
  - Un PC User 1 XP Pro
- Matériels WAN (DNS et Passerelle)



Remarque : Vérifiez que vous possédez une interface optionnelle OPT configurée sur chaque pare-feu PfSense. Ces interfaces sont utilisées pour faire transiter l'information CARP-Pfsync.

Description du schéma

Le cluster partage l'adresse IP publique 192.168.0.248. Le NAT Outbound avancé sur PfSense est paramétré pour utiliser cette adresse en passerelle WAN par défaut.
Le cluster partage l'adresse IP privée 192.168.1.254. Ainsi un client utilisera uniquement cette adresse IP LAN en passerelle.
Master-PfSense utilise le mécanisme pfsync « XMLRPC sync » pouvant synchroniser automatiquement **SA** configuration sur Slave-PfSense (NAT, Rules, etc.) et paramétrer « nodes (informations de status), advskew (hiérarchie dans le cluster) et vhid (groupe de cluster) ».

5.3 CONFIGURATION DU BASCULEMENT MAITRE-ESCLAVE

5.3.1 Créer les Rules sur l'interface OPT1

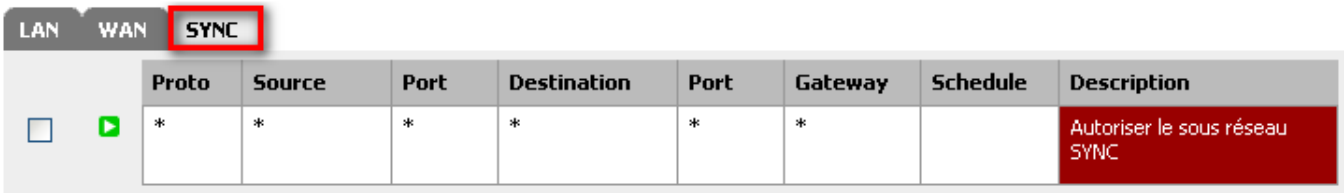
Commençons notre configuration du Failover sur le Maître, à savoir **Master-PfSense**.

Il faut tout d'abord créer une Rule sur l'interface OPT1/SYNC pour autoriser les flux CARP&pfsync à transiter sur le segment CARP (voir schéma général).

Aller dans l'onglet **Firewall > Rules | SYNC** et Cliquer sur la case « **+** » pour créer une nouvelle Rule.

Remplir les champs généraux suivants :
- **Action** : Pass
- **Interface** : SYNC
- **Protocol** : Any
- **Description** : Autoriser le sous réseau SYNC

Cliquez sur **Save** pour valider.
Cliquez sur **Apply Changes** pour appliquer votre Rule.



Répétez ces étapes de configuration sur l'esclave, à savoir **Slave-PfSense**.

5.3.2 Créer les Virtual IPs

A. Nous devons premièrement configurer CARP.

Sur l'esclave (**Slave-PfSense**), aller dans l'onglet **Firewall > Virtual IPs | CARP Settings.**

Remplir les champs généraux suivants :
- **Synchronize Enabled** : Cocher cette case pour autoriser l'échange de messages (pfsync)
- **Synchronize Interface** : SYNC

Cliquez sur **Save** pour valider.

Sur le Maître (**Master-PfSense**), aller dans l'onglet **Firewall > Virtual IPs | CARP Settings.**

Remplir les champs généraux suivants :
- **Synchronize Enabled** : Cocher cette case pour autoriser l'échange de messages (pfsync)
- **Synchronize Interface** : SYNC

- **Synchronize rules** : Cocher cette case. Vous pourrez ainsi répliquer vos Rules Maître sur le Slave via PfSync. En somme, grâce à cette option magique vous n'avez plus qu'à seulement configurer les Rules sur Master-PfSense, elles seront automatiquement crées sur Slave-PfSense. Dans notre cas nous avons seulement 2 Pare feu et n'avons donc pas coché la case Synchronize Rules sur Slave-PfSense. Dans le cas ou vous disposez d'un second ou énième Backup, activez cette option autant de fois que nécessaire…
- **Synchronize nat** : Cocher la case pour synchroniser le NAT. Même remarque que précédemment.
- **Synchronize Virtual IPs** : Cocher cette case.
- **Synchronize to IP:** 192.168.100.2 (@IP Backup)
- **Remote System Password:** [votre mot de passe WebGUI Backup]

Cliquez sur **Save** pour valider.

B. Nous pouvons maintenant configurer les IP virtuelles.

Sur le maître (**Master-PfSense**), aller dans l'onglet **Firewall > Virtual IPs | Virtual IPs.**

Cliquez sur la case « **+** » pour créer une nouvelle IP virtuelle WAN.

Remplir les champs généraux suivants :

- **Type** : Cocher la case « CARP »
- **Interface** : WAN
- **IP Address** :
  - **Type** : Single Address
  - **Address** : 192.168.0.248/24 (@IP WAN non utilisée)
- **Virtual IP Password** : [votre mot de passe] (Password du groupe VHID)
- **VHID Group** : 1 (Numéro de groupe VHID partagé par les Pare-feu)
- **Advertising Frequency** : 0 (0=Master, 0+1+*n* pour backup). Plus la valeur de *n* est basse, plus le backup se trouve proche derrière le Master : Master(0)➔Backup1(1 car n=0)➔Backup2(2 car n=1)➔…

Remarque: Lorsque vous voudrez mettre en place un système Actif/Actif la valeur **Advertising Frequency** du Master et Slave sera la même, à savoir « 0 ».

- **Description**: WAN-CARP

Cliquez sur **Save** pour valider.

Cliquez de nouveau sur la case « **+** » pour créer une nouvelle IP virtuelle LAN.

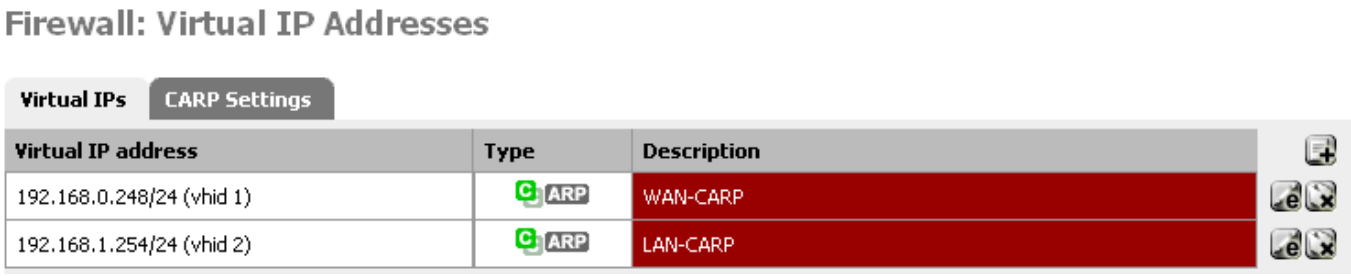
Remplir les champs généraux suivants :

- **Type** : Cocher la case « CARP »
- **Interface** : LAN
- **IP Address** :
  - **Type** : Single Address
  - **Address** : 192.168.1.254/24 (@IP LAN non utilisée)
- **Virtual IP Password** : [votre mot de passe] (Password du groupe VHID)
- **VHID Group** : 2 (Numéro de groupe VHID partagé par les Pare-feu)
- **Advertising Frequency** : 0 (0=Master, 0+1+*n* pour backup). Plus la valeur de *n* est basse, plus le backup se trouve proche derrière le Master : Master(0)➔Backup1(1 car n=0)➔Backup2(2 car n=1)➔…

Remarque: Lorsque vous voudrez mettre en place un système Actif/Actif la valeur **Advertising Frequency** du Master et Slave sera la même, à savoir « 0 ».

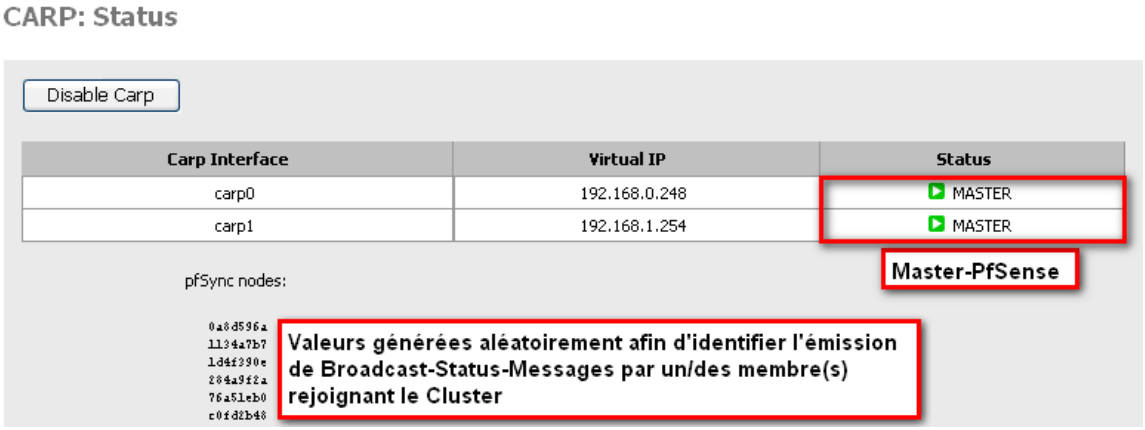
- **Description**: LAN-CARP

Cliquez sur **Save** pour valider.
Cliquez sur **Apply Changes** pour appliquer vos IPs virtuelles.

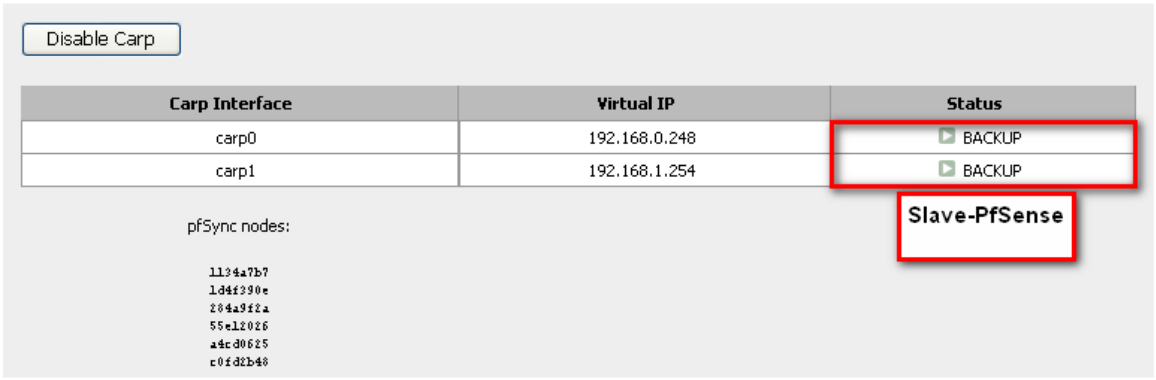


5.3.3 Vérification du fonctionnement de CARP

Sur le Master (Master-PfSense) : **Status | Failover**

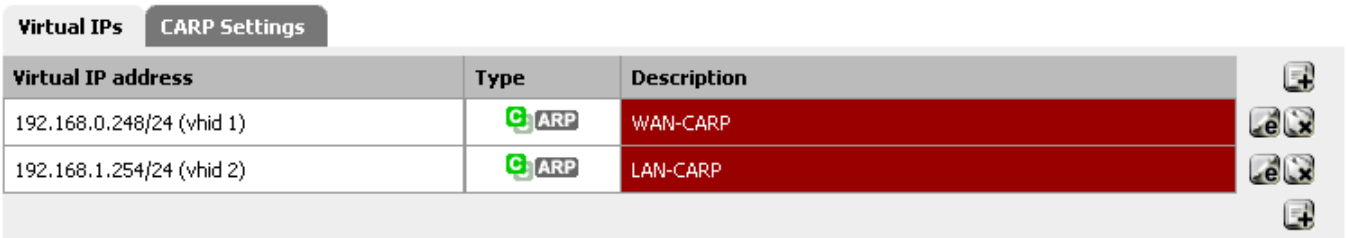


Sur le Slave (Slave-PfSense) : **Status | Failover**



NB : Si vous avez un Status « Disabled » cliquez sur la case *Enable Carp*.

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



5.3.4 Configuration du mapping NAT pour faire du failover WAN stateful.

Nous allons créer une règle NAT sur l'interface WAN pour définir notre interface virtuelle WAN-CARP comme destination par défaut. Comme cette adresse IP WAN est partagée par nos deux Pare feu, si un problème survient sur le Master nous n'aurons pas de coupure sur des communications préalablement établies car le Slave possède la même adresse IP WAN que le Master.

Sur le maître (**Master-PfSense**), aller dans l'onglet **Firewall > NAT | Outbound.**

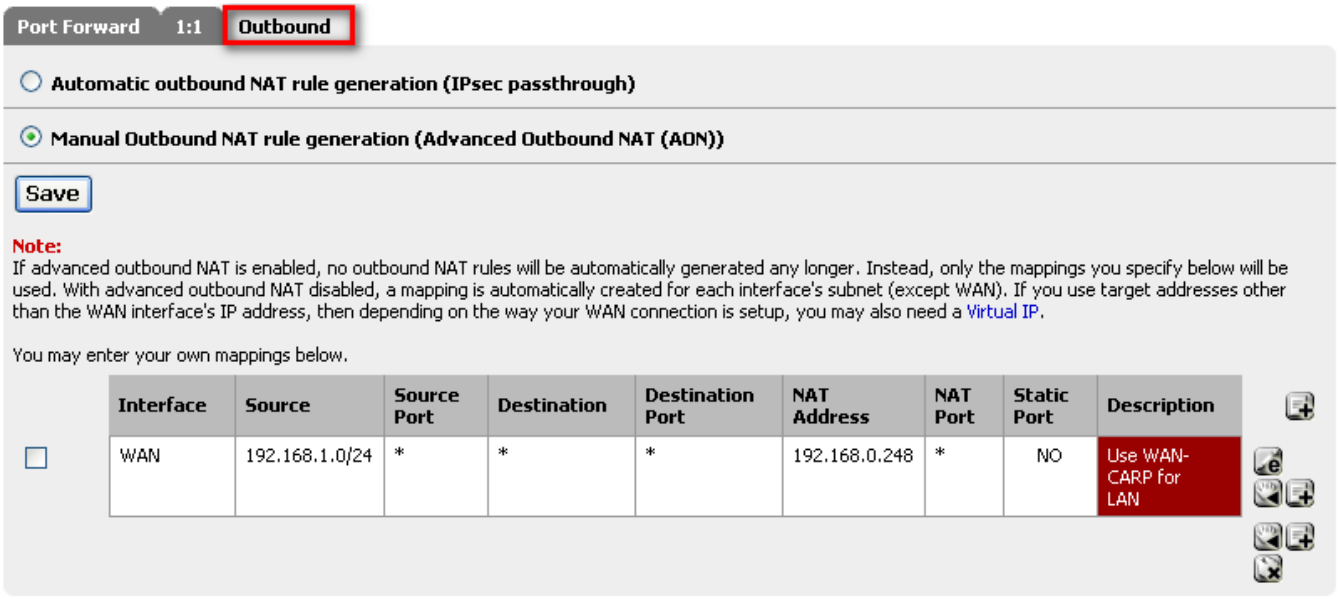
Cliquez sur la case « **Manual Outbound NAT rule generation (Advanced Outbound NAT (AON))** ».

Vous voyez apparaître une règle par défaut « **Auto created rule for LAN** » qu'il vous faut éditer :

Changer ***uniquement*** les champs généraux suivants :

- **Translation** : 192.168.0.248 (WAN-CARP) (nouvelle @IP par défaut de l'interface WAN)
- **Description** : Use WAN-CARP for LAN

Cliquez sur **Save** pour valider.
Cliquez sur **Apply Changes** pour appliquer votre règle NAT.



NB : PfSense, tellement qu'il est toujours bien, a donc répliqué automatiquement cette règle NAT sur **Slave-PfSense** grâce à Pfsync.

5.3.5 Modifier votre serveur DHCP

La mise en place d'un système de basculement (Failover) implique la modification de certains paramètres IP.

Ainsi, deux cas se présentent :

- Vous avez PfSense en DHCP ➔ Suivez l'explication ci-après
- Vous avez votre propre DHCP, modifiez la valeur suivante:
  - **Passerelle par défaut** : 192.168.1.254 (@IP LAN-CARP)

A. Si votre DHCP est PfSense :

Sur le maître (**Master-PfSense**), aller dans l'onglet **Services > DHCP Server | LAN.**
Changer au moins les champs généraux suivants :

- **Gateway** : 192.168.1.254 (LAN-CARP)
- **Failover peer IP** : 192.168.1.2 (@IP LAN Slave-PfSense pour le DHCP Failover)

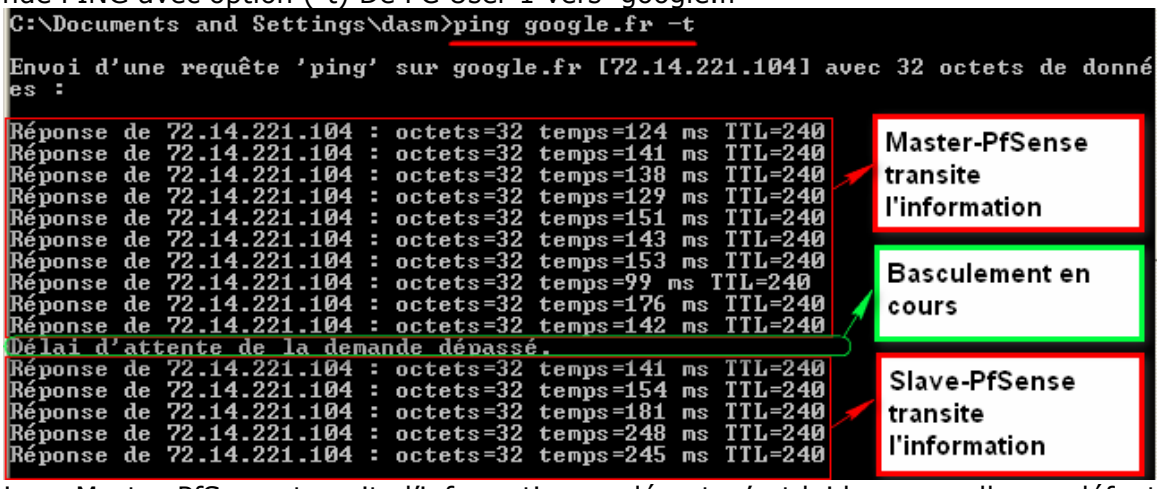
Sur **Slave-PfSense**:
Aller dans l'onglet **Services > DHCP Server | LAN.**
Changer au moins les champs généraux suivants :

- **Gateway** : 192.168.1.254 (LAN-CARP)
- **Failover peer IP** : 192.168.1.1 (@IP LAN Master-PfSense pour le DHCP Failover)

Remarque : Vous devez avoir les mêmes configurations DHCP sur les deux Pare-feu, moyennant les changements précédents. Si vous voyez d'autres champs à modifier (par ex le DNS), faites le toujours sur les deux Pare feu.

5.3.6 Test de fonctionnement

@IP PC User 1 (LAN) : 192.168.1.198
Commande PING avec option (-t) De PC User 1 vers google.fr



Explication : Master-PfSense transite l'information au départ, c'est lui la passerelle par défaut LAN. Débranchons le maintenant du LAN ou du WAN ; si tout va bien le basculement s'effectue (5 secondes Max) et l'information re-transite au travers Slave-PfSense en attendant que Master-PfSense soit reconnecté et opérationnel.

6 DETECTION ET PREVENTION D'INTRUSIONS RESEAUX : SNORT

6.1 INTRODUCTION

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

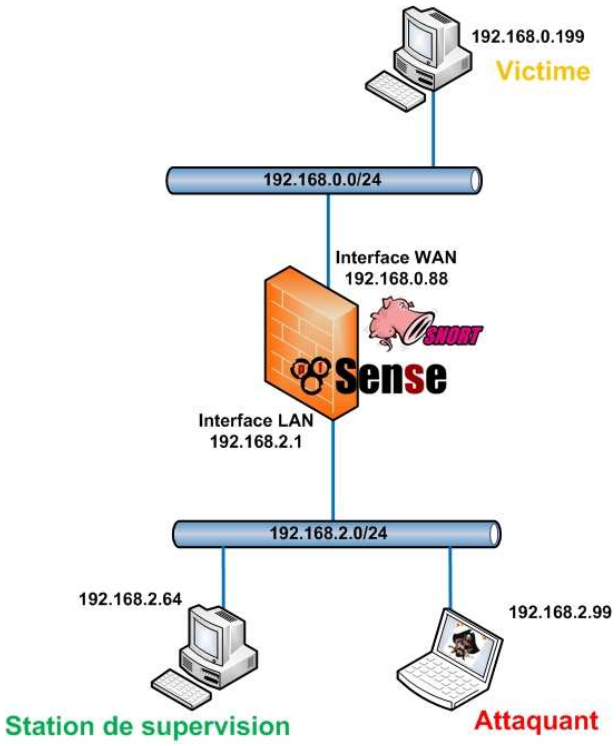
SNORT peut fonctionner en quatre modes différents : SNIFFER (capture et affichage des paquets, pas de log), PACKET LOGGER (capture et log des paquets), NIDS (analyse le trafic, le compare à des règles, et affiche des alertes) puis IPS (détection d'attaques et prévention de celles-ci).

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

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

6.2 MAQUETTE DE TEST

Voici la maquette qui nous permettra de tester SNORT afin de mettre en avant ses fonctions de NIDS et d'IPS :



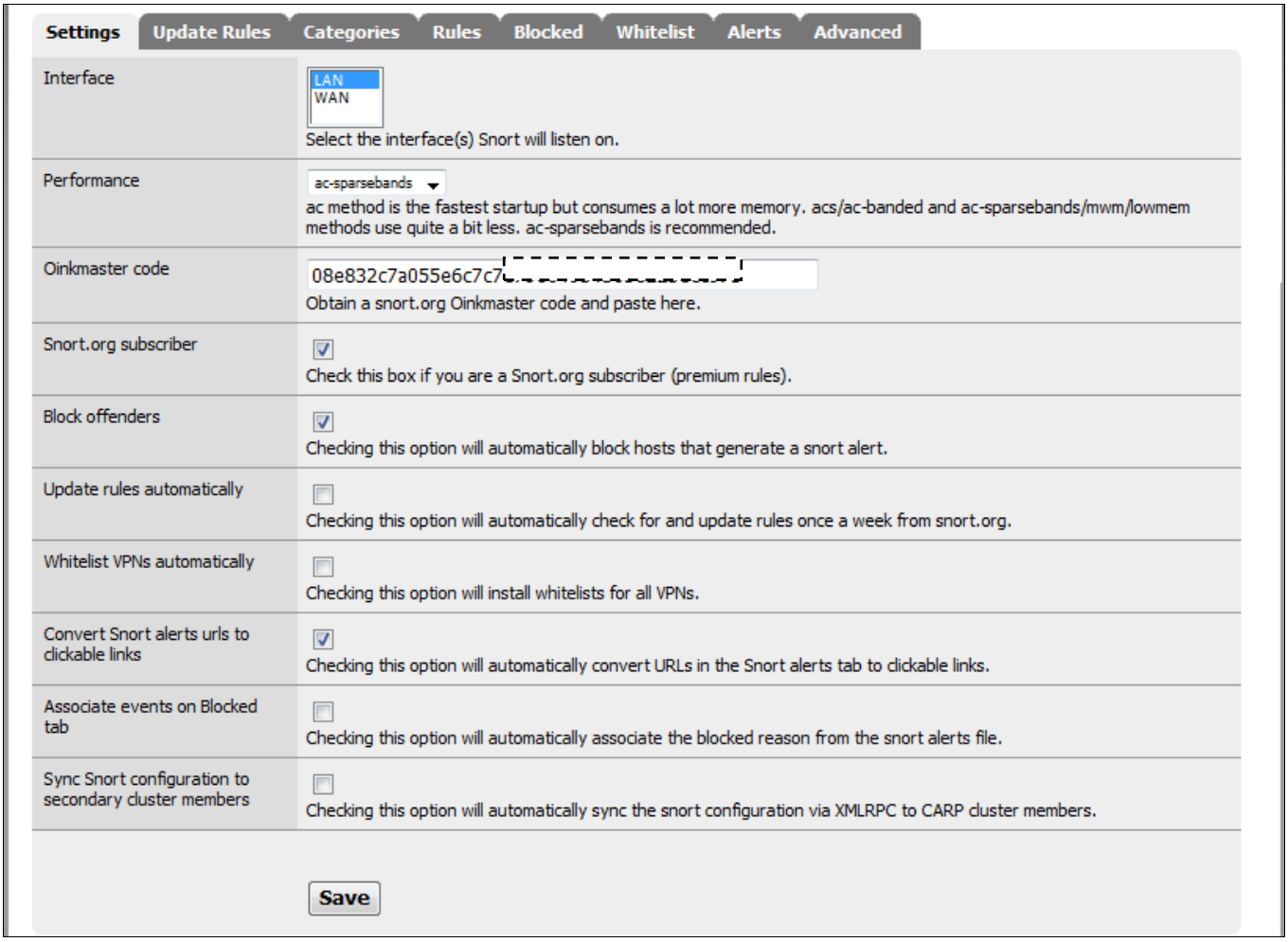
6.3 INSTALLATION ET CONFIGURATION DE SNORT

La première étape est l'installation du package SNORT dans pfSense (system->packages->SNORT) :

snort	Security	No info, check the forum	2.8.2.1_1	Snort is a libpcap-based packet sniffer/logger which can be used as a lightweight network intrusion detection system. It features rules based logging and can perform content searching/matching in addition to being used to detect a variety of other attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more.

La seconde étape importante, est la création d'un compte sur http://snort.org, afin de pouvoir récupérer les règles prédéfinies en temps voulu… nous y revenons par la suite.

L'installation étant maintenant faite, nous allons configurer SNORT (Services->SNORT) :



Interface	Nous spécifions ici l'interface de pfSense sur laquelle SNORT écoutera l'ensemble du trafic. Ici, conformément au schéma précédent : LAN
Performance	Nous indiquons ici la méthode de recherche utilisée par SNORT sur les paquets analysés. « ac-sparsebands » est la méthode recommandée.
Oinkmaster code	Code récupéré via votre compte sur SNORT.org qui vous permettra de télécharger les règles SNORT pré établies.
Snort.org subscriber	Cocher cette case si vous utilisez bien un Oinkmaster code.
Block offenders	Elément important de la configuration, puisque le fait de cocher cette case bloquera automatiquement tout hôte déclenchant une alerte sur l'interface d'écoute (fonction IPS de SNORT). Voir plus bas pour des détails complémentaires.
Update rules automatically	Mise à jour automatique des règles SNORT.
Whitelists VPNs automatically	Ajouter automatiquement les VPN pré configurés dans pfSense à la whitelist, afin d'éviter tout refus de connexion ou blacklistage.
Convert Snort alerts urls to clickable links	Les alertes apparaissent sous la forme de liens hypertextes.
Associate events on Blocked tab	Lier la raison du blocage à l'hôte bloqué dans l'onglet « blocked ».
Sync Snort configuration to secondary cluster members	Synchroniser la configuration de SNORT avec tous les membres du cluster CARP s'il en existe un.

Validez ensuite en cliquant sur le bouton « save » en bas de page. SNORT va ensuite automatiquement télécharger les règles (premium rules) depuis snort.org grâce à votre Oinkmaster code :

Toutes les règles ainsi téléchargées sont regroupées sous forme de catégories dans l'onglet « Categories », à vous de sélectionner celles qui correspondent aux attaques que vous désirez détecter sur votre réseau. Nous concernant, afin de tester l'efficacité de la solution, nous nous contentons de la règle « scan.rules » qui nous permettra de détecter et bloquer un attaquant effectuant un scan de port sur un hôte distant.

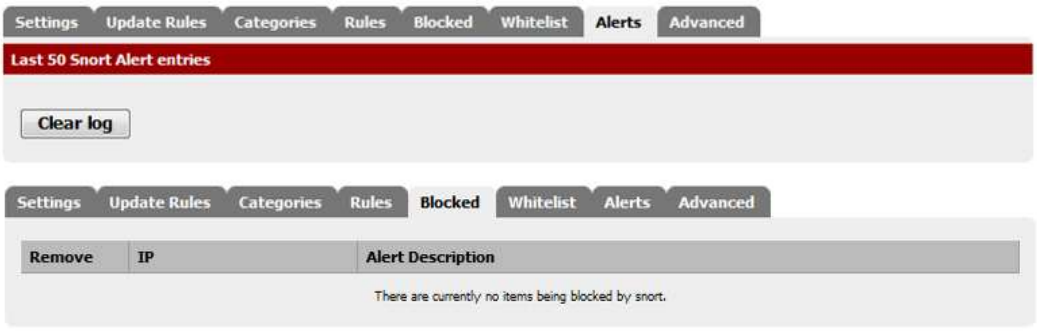
L'étape suivante consiste à paramétrer les règles présentent dans la catégorie que nous venons de sélectionner :

Category:
scan.rules
There are 21 rules in this category.

SID	Proto	Source	Port	Destination	Port	Message
613	tcp	$EXTERNAL_NET	10101	$HOME_NET	any	SCAN myscan
616	tcp	$EXTERNAL_NET	any	$HOME_NET	113	SCAN ident version request
619	tcp	$EXTERNAL_NET	any	$HOME_NET	80	SCAN cybercop os probe
621	tcp	$EXTERNAL_NET	any	$HOME_NET	any	SCAN FIN
622	tcp	$EXTERNAL_NET	any	$HOME_NET	any	SCAN ipEye SYN scan
623	tcp	$EXTERNAL_NET	any	$HOME_NET	any	SCAN NULL
624	tcp	$EXTERNAL_NET	any	$HOME_NET	any	SCAN SYN FIN
625	tcp	$EXTERNAL_NET	any	$HOME_NET	any	SCAN XMAS
1228	tcp	$HOME_NET	any	$EXTERNAL_NET	any	SCAN nmap XMAS
630	tcp	$EXTERNAL_NET	any	$HOME_NET	any	SCAN synscan portscan
626	tcp	$EXTERNAL_NET	any	$HOME_NET	any	SCAN cybercop os PA12 attempt
627	tcp	$EXTERNAL_NET	any	$HOME_NET	any	SCAN cybercop os SFU12 probe
634	udp	$EXTERNAL_NET	any	$HOME_NET	10080:10081	SCAN Amanda client-version request
635	udp	$EXTERNAL_NET	any	$HOME_NET	49	SCAN XTACACS logout
636	udp	$EXTERNAL_NET	any	$HOME_NET	7	SCAN cybercop udp bomb
637	udp	$EXTERNAL_NET	any	$HOME_NET	any	SCAN Webtrends Scanner UDP Probe
1638	tcp	$EXTERNAL_NET	any	$HOME_NET	22	SCAN SSH Version map attempt
1917	udp	$EXTERNAL_NET	any	$HOME_NET	1900	SCAN UPnP service discover attempt
1918	icmp	$EXTERNAL_NET	any	$HOME_NET	any	SCAN SolarWinds IP scan attempt
1133	tcp	$EXTERNAL_NET	any	$HTTP_SERVERS	$HTTP_PORTS	SCAN cybercop os probe
8081	tcp	$EXTERNAL_NET	any	$HOME_NET	5000	SCAN UPnP service discover attempt

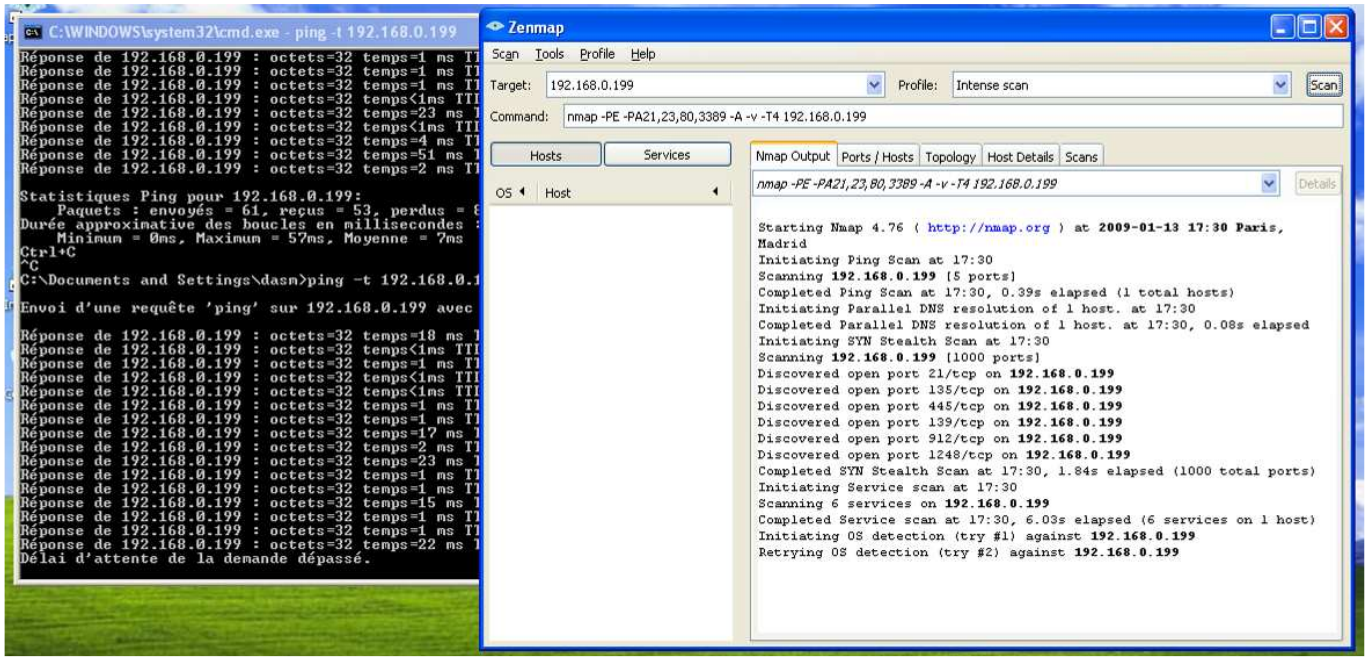
Nous activons et paramétrons notamment la règle « SCAN nmap XMAS » afin de pouvoir détecter un scan de port Nmap lancé depuis le LAN (interface d'écoute de SNORT, $HOME_NET) vers un hôte situé sur un réseau distant (interface WAN, $EXTERNAL_NET).

La configuration de test est désormais terminées, la machine de supervision peut d'hors et déjà consulter les alertes ainsi que la liste des IP bloquées (normalement vierge pour le moment ;):

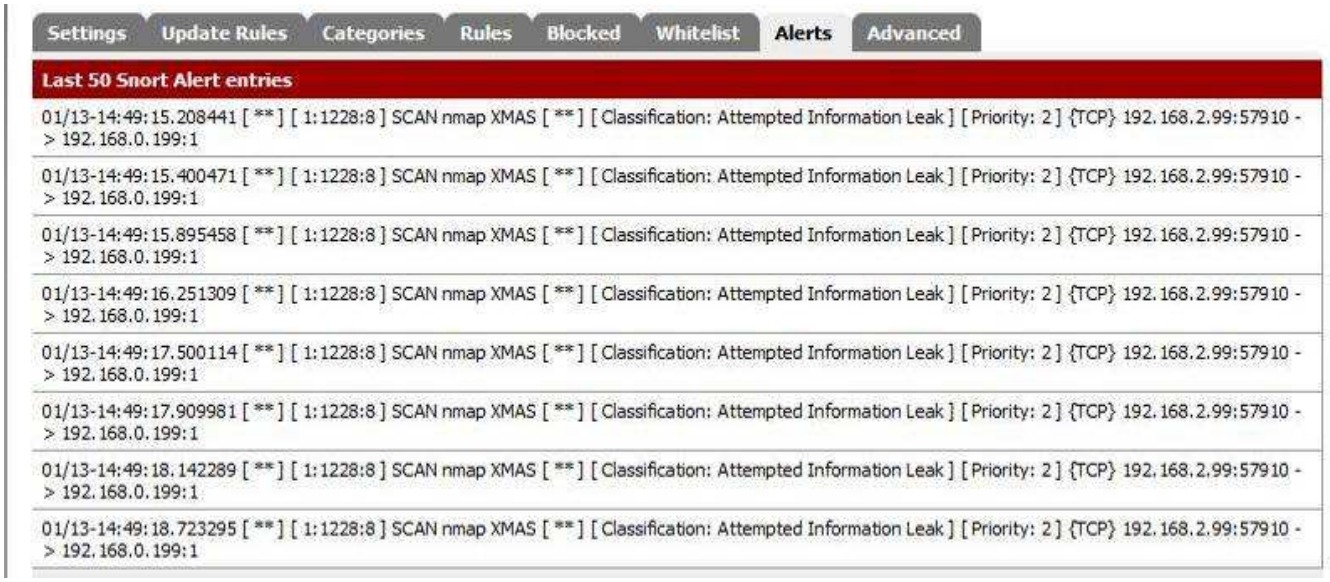


6.4 TEST DE LA SOLUTION

Le test repose sur le schéma présenté plus haut. Un attaquant va effectuer un scan de port Nmap sur un hôte distant. Pendant toute la durée du test, l'attaquant effectue en parallèle du scan de port un ping vers la victime, afin de vérifier en permanence la connectivité vers l'hôte et clairement mettre en avant le moment où il sera blacklisté par SNORT (attaque détecté ET contrée).



Une fois le scan de port lancé, la station de supervision peut très rapidement constater des alertes ainsi que l'IP 192.168.2.99 (notre attaquant !!) a été bloquée :



6.5 PRINCIPE DE FONCTIONNEMENT

Comme nous l'avons évoqué plus haut, une simple option à cocher permet d'octroyer à SNORT des fonctionnalités d'IPS en bloquant les IP suspectes. Pour ce faire, SNORT influence directement packet filter pour créer ou non des règles sur l'IP concernée.

Par défaut, packet filter bloque tout traffic, et créer des règles à chaque fois qu'un hôte désire ouvrir une session (à condition que les règles du firewall le permettent). Par exemple, dans la capture suivante, nous affichons les règles concernant l'hôte 192.168.2.99 qui n'est pas bloqué et qui ping l'hôte distant 192.168.0.199:

```
# pfctl -sa | grep 192.168.2.99
all tcp 192.168.2.99:37456 -> 192.168.0.88:57596 -> 192.168.0.199:33386       TIME_WAIT:TIME_WAIT
```

Comme expliqué, cet hôte remplissant toutes les conditions définies dans le firewall et n'étant pas bloqué par SNORT, une règle est créée afin de lui autoriser tout accès souhaité.

En revanche, la même commande ne retourne rien si l'hôte est bloqué par SNORT :

```
# pfctl -sa | grep 192.168.2.99
#
```

➔ Pas de règle donc trafic forcément bloqué par packet filter.

7 CLIENT/SERVEUR SSL : STUNNEL

7.1 INTRODUCTION

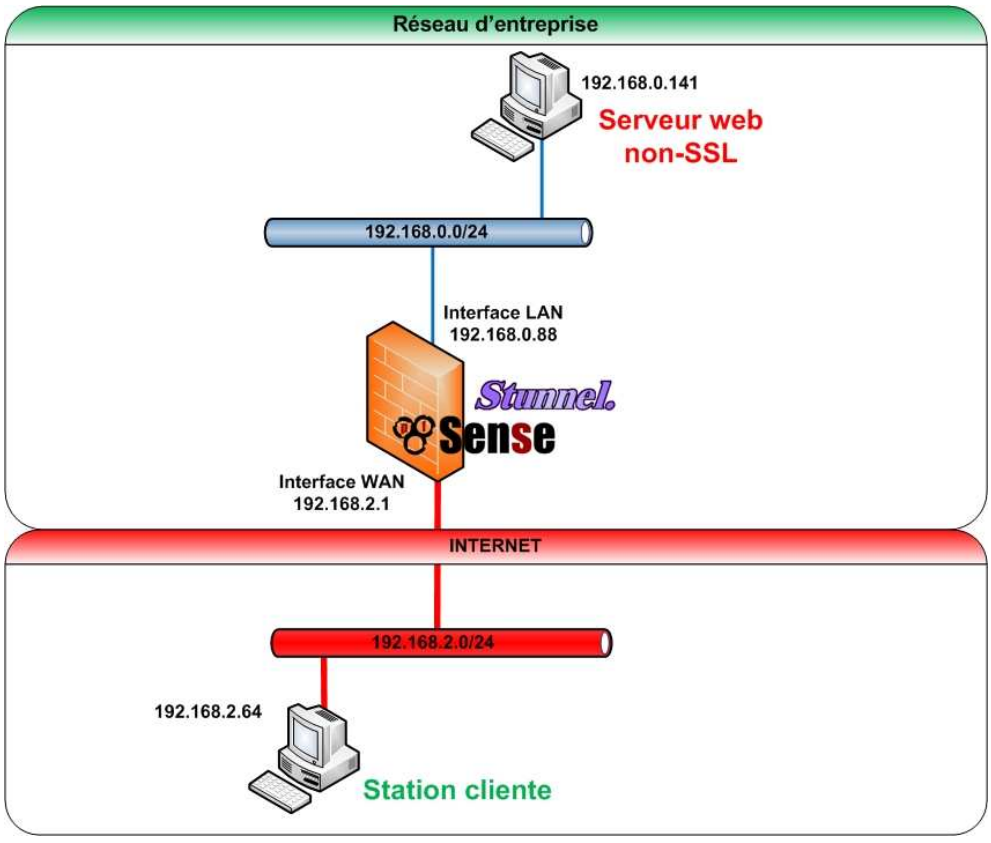
STunnel est un programme permettant de crypter des connexions TCP dans SSL. L'intérêt de cette solution est de pouvoir mettre en place des connexions sécurisées SSL pour des services ne le proposant pas initialement (POP, IMAP, LDAP…) sans avoir à toucher le code source ou la configuration de ces derniers.

Le programme sTunnel seul ne suffit pas pour mettre en place la solution, une bibliothèque SSL est indispensable pour compiler un tunnel SSL (dans notre cas, ce sera openSSL installé par défaut dans pfSense).

Ainsi, des clients et des serveurs ne permettant ni l'un ni l'autre de monter un tunnel SSL seront tout de même capables de sécuriser leurs échanges grâce à l'intégration de cette solution. Stunnel peut effectivement fonctionner en mode *client* ou en mode *serveur*.

7.2 MAQUETTE DE TEST

Afin de démontrer l'efficacité de sTunnel intégré à pfSense, nous imaginons la maquette suivante :



Afin de se rapprocher d'un cas réel, le réseau 192.168.2.0/24 représentera Internet, et le réseau 192.168.0.0/24 celui d'une entreprise voulant mettre à disposition du net un serveur WEB non SSL. Le but de l'exercice est de sécuriser via Stunnel le lien entre pfSense et la station cliente uniquement lorsque celle-ci désire accéder au serveur WEB de l'entreprise.

7.3 INSTALLATION ET CONFIGURATION DE STUNNEL

OpenSSL est indispensable mais déjà installé dans pfSense, la première étape sera donc l'installation du package sTunnel :

A ce moment, le menu de configuration de sTunnel est accessible dans l'onglet « service->stunnel » de pfSense. Cependant, nous déconseillons d'utiliser ce menu puisque les résultats obtenus et le fichier de configuration générés par pfSense ne se sont pas montrés concluants. Direction donc le fichier :

```
/usr/local/etc/stunnel/stunnel.conf
```

Mais avant de rentrer dans le vif du sujet, intéressons nous au fonctionnement de sTunnel.

D'après la maquette présentée, pfSense jouera le rôle de serveur Stunnel puisqu'il sera chargé d'intercepter les requêtes clientes (via une connexion cryptée SSL) et ensuite de rediriger les flux vers le serveur WEB. De ce fait, trois points sont à prévoir :

- Disposer de certificats valides
- Spécifier une adresse d'écoute sur le serveur, ainsi qu'un port d'écoute
- Spécifier une adresse et un port de redirection

Pour effectuer ce test, nous utiliserons les certificats d'essai fournis lors de l'installation de sTunnel. Nous allons maintenant détailler ligne par ligne le fichier stunnel.conf que nous injecterons dans notre pfSense :

```
; Nous indiquons le certificat à utiliser (ici, celui fourni par stunnel pour test)
cert = /usr/local/etc/stunnel/stunnel.pem

; Afin d'optimiser la sécurité de l'exécution du programme
chroot = /var/tmp/stunnel
pid = /stunnel.pid
setuid = stunnel
setgid = stunnel

; PfSense est serveur sTunnel, le mode client est donc désactivé
client = no

; Nous créons la règle WebServer
[WebServer]
; PfSense écoute et accepte les connexions SSL sur le port 6464
accept = 6464
; Redirection des connexions acceptées vers l'ip et le port du serveur web
connect = 192.168.0.141:80
TIMEOUTclose = 0
```

Nous n'avons plus qu'à sauvegarder la configuration et redémarrer stunnel. Pour tester le bon fonctionnement de notre stunnel, un client du WAN (192.168.2.64) va accéder au serveur web via SSL en rentrant dans son navigateur l'adresse d'écoute WAN de pfSense et le port adéquat, soit ici:

https://192.168.2.1:6464

La connexion est initialisée et accepté, l'utilisateur devra ici accepter le certificat proposé (pensez à générer et distribuer les votre en déploiement réel) ! Le client accède finalement au serveur WEB, tous les échanges sont encapsulés dans HTTPS.

Nous pouvons observer le bon déroulement de l'opération dans les logs de pfSense :

Jan 15 10:04:59	stunnel: LOG5[5733:675288832]: WebServer accepted connection from 192.168.2.64:51084
Jan 15 10:04:59	stunnel: LOG5[5733:675288832]: WebServer connected remote server from 192.168.0.88:31209

- ➔ La demande de connexion de notre client est acceptée
- ➔ pfSense nous redirige vers le serveur distant (192.168.0.141) depuis son interface LAN (192.168.0.88).

Pour finir, nous l'avons évoqué plus haut, sTunnel peut être configuré en client SSL dans le cas où ni le client ni le serveur pour un service donné ne sont compatibles SSL. Il suffit pour cela d'installer sTunnel sur le système client (windows, unix/linux), de spécifier que nous fonctionnons en mode client (client = yes) et d'indiquer les IPs et ports d'écoute/redirection.

8 PARTAGE DE LA BANDE PASSANTE : TRAFFIC SHAPER

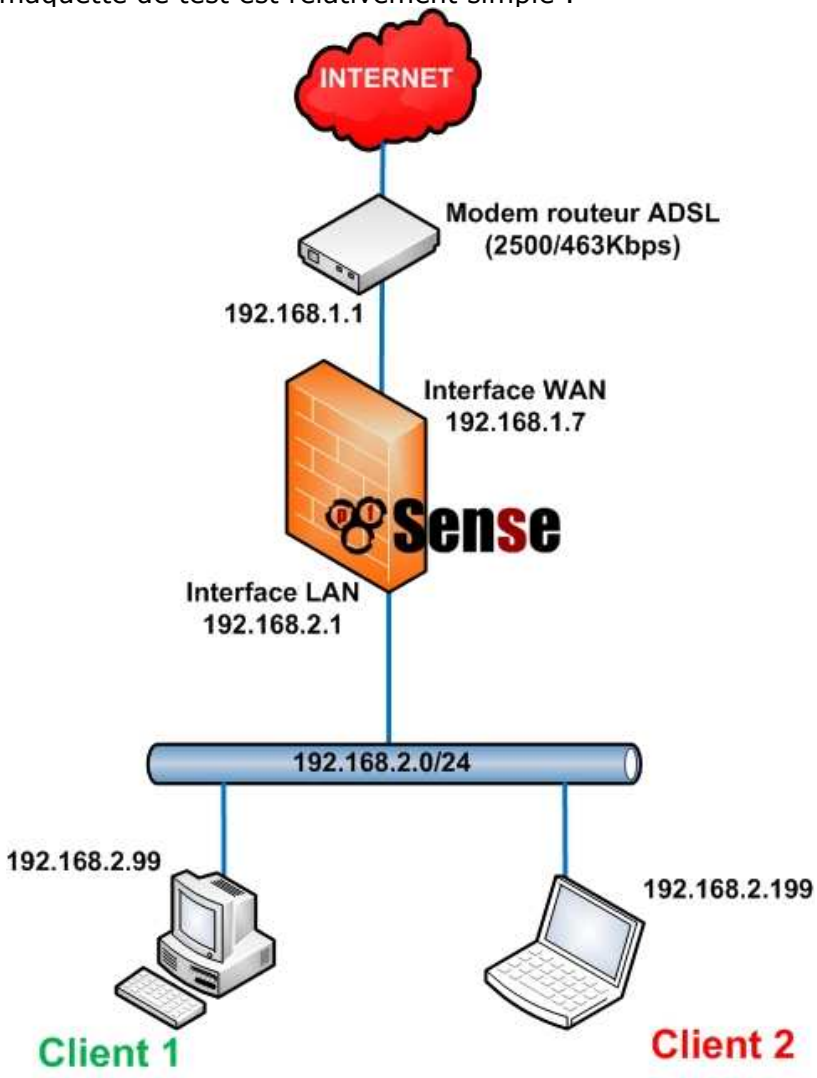
8.1 INTRODUCTION

La fonction « traffic shaping » de pfSense permet initialement d'optimiser la bande passante en attribuant des priorités aux différents flux du réseau. Par exemple, donner une meilleure priorité aux flux VOIP par rapport au reste du trafic afin d'optimiser les communications VOIP.

Nous allons voir comment mettre en place un autre aspect de la gestion de bande passante, à savoir comment la partager entre plusieurs hôtes/réseaux selon nos besoins.

8.2 MAQUETTE DE TEST

Pour ce chapitre, la maquette de test est relativement simple :



L'objectif va être de démontrer comment, à partir d'une connexion ADSL (2500Kbps down, 463 Kbps up), nous pouvons offrir une portion de bande passante différente à chacun nos deux clients, ou bien une bande passante limitée et partagée entre les deux clients.

Nous nous retrouverons donc dans deux cas de figure différents :

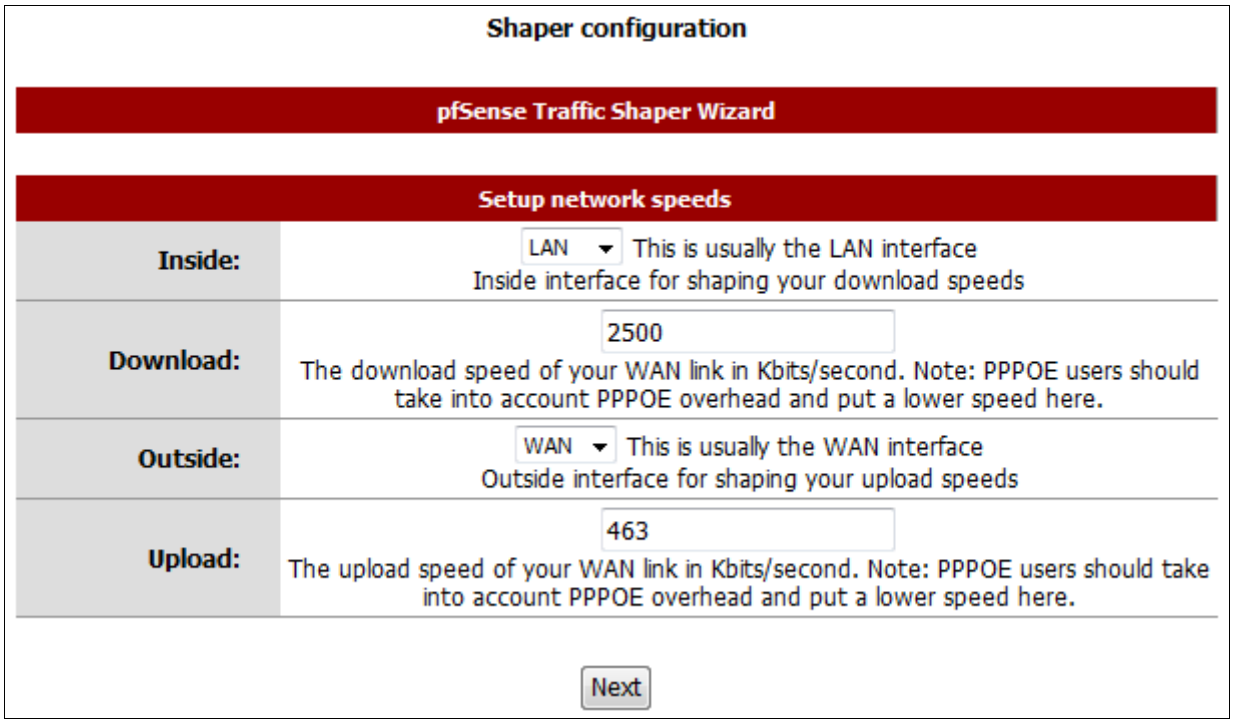
- Chacun des clients possèdera sa propre bande passante, par exemple proposer 40Ko/s en download pour le client 1 et 80Ko/s au client 2. Chaque portion de bande passante est réservée et n'influence pas l'autre.
- Une portion de bande passante est définie pour les deux clients, par exemple 80Ko/s en download qu'ils se partageront.

8.3 CONFIGURATION ET TEST DE LA SOLUTION

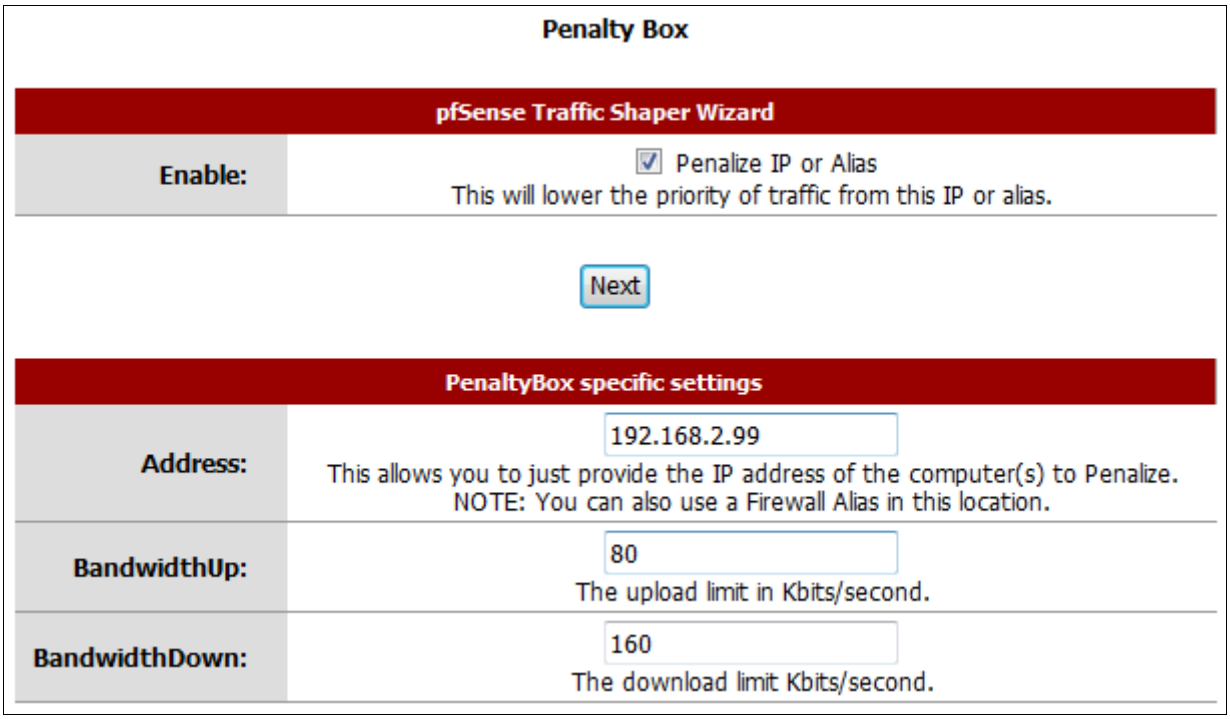
Nous allons détailler ici chaque étape de la configuration du traffic shaping de pfSense qui nous permettrons de mettre en œuvre les conditions présentées plus haut. Les tests seront réalisés au fil de la configuration afin de représenter au mieux les résultats de chaque élément configuré.

8.3.1 Configuration initiale via wizard

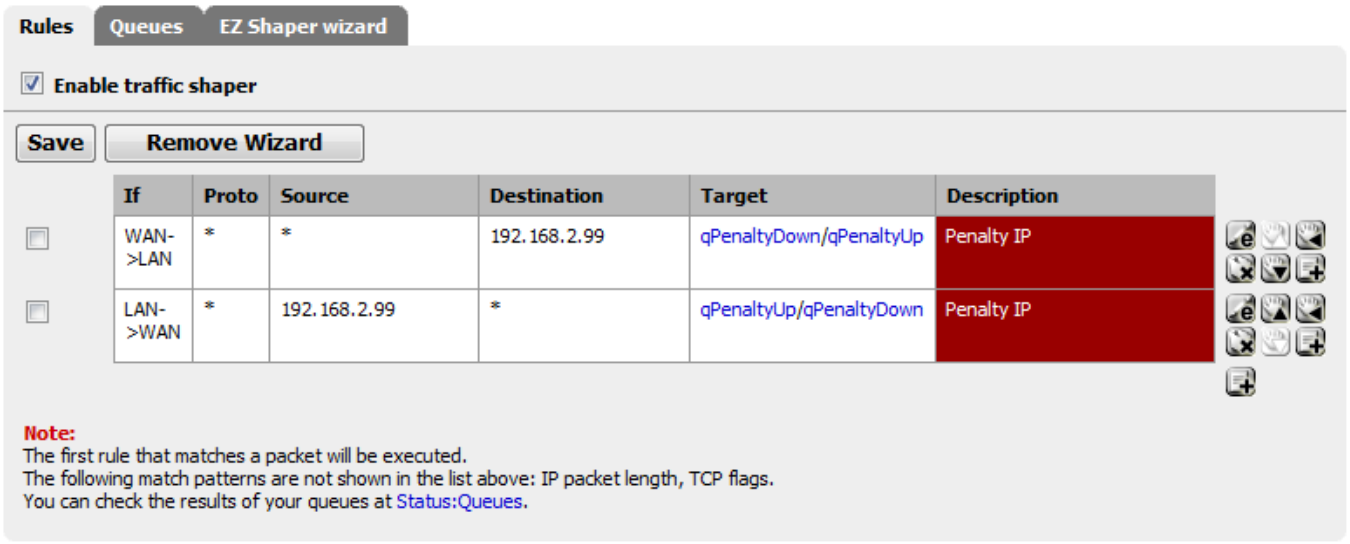
Pour commencer, nous conseillons de lancer et de suivre le « wizard » du traffic shaper, afin de rentrer les premiers éléments de configuration comme par exemple les caractéristiques de notre ligne ADSL :



Par la suite, le seul autre élément du wizard que nous configurons sera la « penalty box », qui va nous permettre de fixer des limitations de bande passante sur une IP, nous prendrons par exemple notre client 1, ip 192.168.2.99 :



Pour finir, cliquer sur suivant jusqu'à la fin du wizard. Désormais, le menu suivant sera accessible dans le traffic shaper :



8.3.2 Fonctionnement du traffic shaper

Avant d'aller plus loin dans la configuration, nous allons détailler le fonctionnement du traffic shaper de pfSense. Son fonctionnement repose sur deux éléments : les queues et les règles (des queues sont créées, puis des règles qui dépendent et fonctionnent d'après les queues).

Voici les queues que nous venons de créer automatiquement :

Flags	Priority	Default	Bandwidth	Name
	0	No	463 Kb	qwanRoot
	0	No	2500 Kb	qlanRoot
	1	Yes	1 %	qwandef
	1	Yes	1 %	qlandef
ACK	7	No	25 %	qwanacks
ACK	7	No	25 %	qlanacks
RED ECN	2	No	1 %	qPenaltyUp
RED ECN	2	No	1 %	qPenaltyDown

NB : tout ce qui fait référence au WAN concerne les flux montants (LAN->WAN), de même que ce qui fait référence au LAN concerne les flux descendants (WAN->LAN).

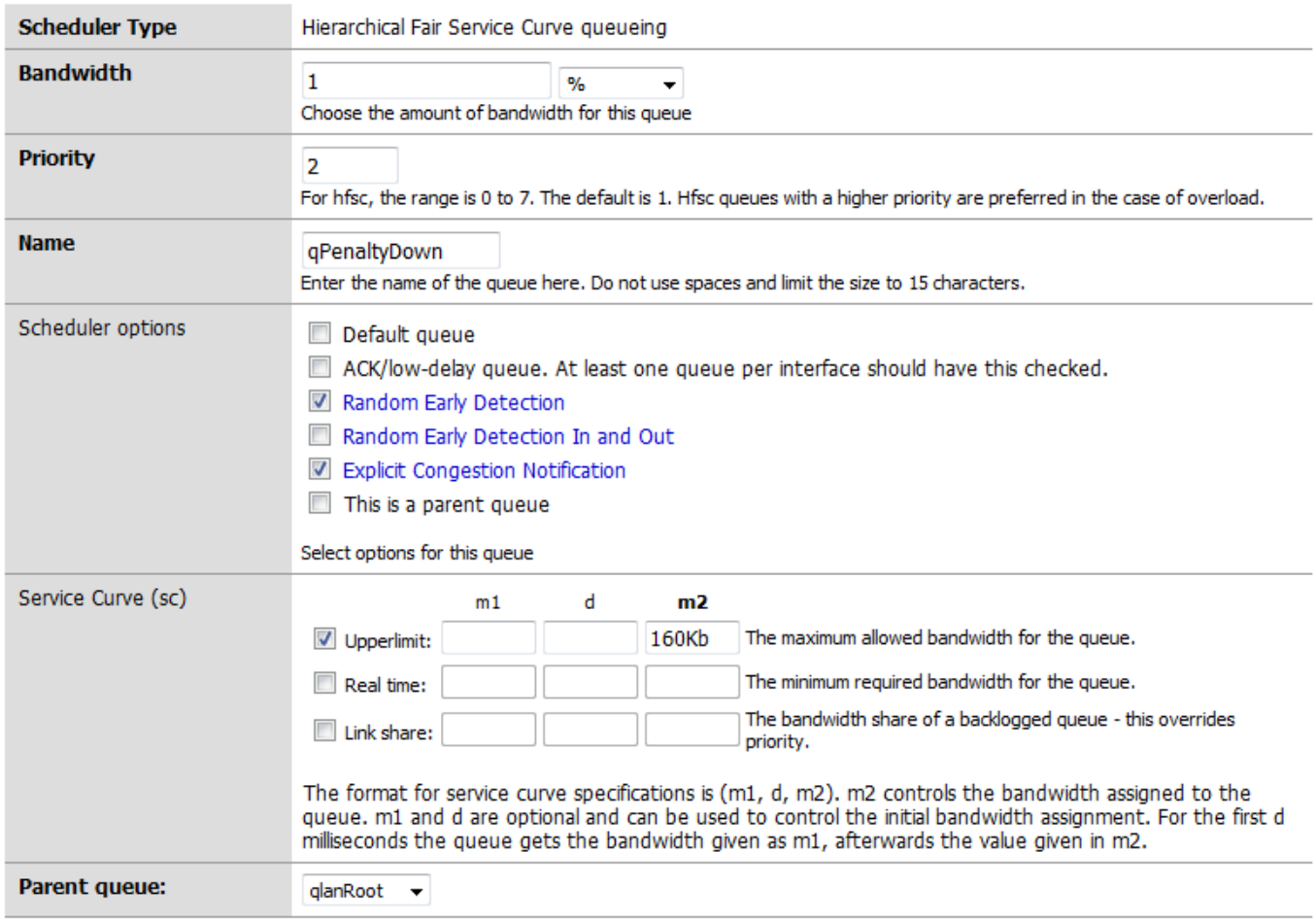
- qwanRoot et qlanRoot sont les queues dites « parentes » (à préciser dans les paramètres des queues), ce sont elles qui fixent les caractéristiques de la bande passante disponible initialement, soit ici 2500Kbps en down et 463Kbps en up (les limites de notre ligne ADSL). Toutes les autres queues seront définies comme « filles » de ces deux là.

- Qwandef et qlandef sont les queues par défaut (à préciser dans les paramètres des queues), c'est-à-dire que tout trafic ne correspondant pas à des règles spéciales dépendra de ces queues.

- Qwanacks et qlanacks sont les queues qui permettent de réserver suffisamment de bande passante au trafic de type « ack », ce qui permet de maintenir les sessions ouvertes ainsi que de bonnes conditions de download/upload.

- Pour finir, qPenaltyUp et qPenaltyDown sont les queues qui définissent les limitations sur notre client 1 (rentrées pendant le wizard).

qPenaltyUp et qPenaltyDown définissent donc des limitations de débits (dans notre cas, 160Kbps down, 80Kbps up, Cf. Wizard). Voici par exemple le contenu de la queue qPenaltyDown :



Nous constatons donc que :

- Cette queue bénéficie par défaut d'1% de la bande passante parente (ici, qlanRoot), que sa priorité est de 2 (sur une échelle de 0 à 7), et que la limite à ne pas dépasser en download sera donc 160Kbps.

Nous allons maintenant voir comment nos queues qPenaltyUp et qPenaltyDown agissent sur notre client 1, pour cela, direction les règles de notre traffic shaper :

If	Proto	Source	Destination	Target	Description
WAN->LAN	*	*	192.168.2.99	qPenaltyDown/qPenaltyUp	Penalty IP
LAN->WAN	*	192.168.2.99	*	qPenaltyUp/qPenaltyDown	Penalty IP

Deux règles ont été créées, une régissant le trafic de 192.168.2.99 dans le sens descendant, l'autre dans le sens montant. Nous observons bien la présence des queues concernées dans la colonne « target ».

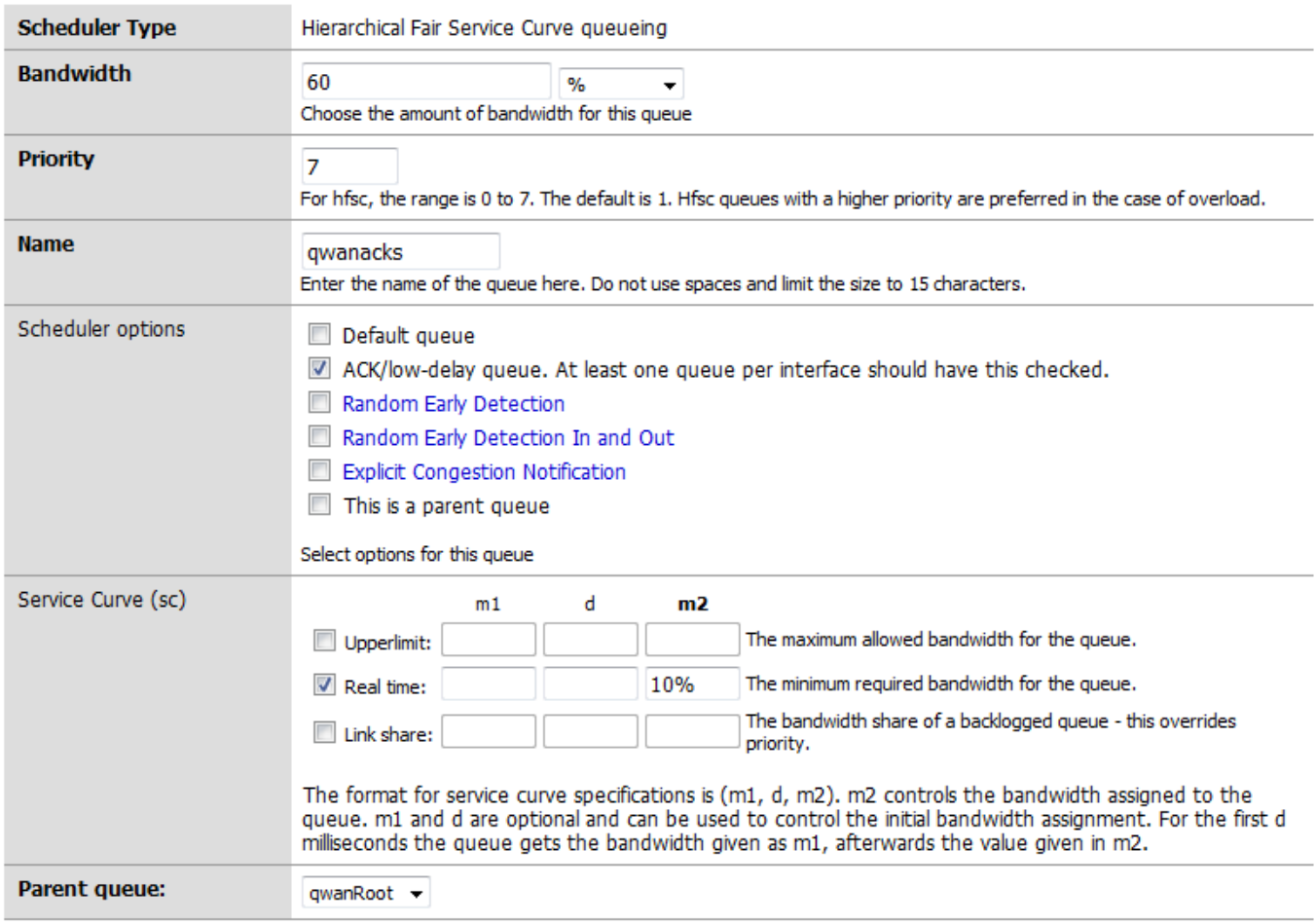
Pour finir sur le fonctionnement du traffic shaper pfSense, nous ajouterons que :

- Le traffic shaper repose sur les tables d'états (states) du firewall. Il est donc recommandé, à chaque modification de la configuration du traffic shaper, de réinitialiser les tables du firewall. Pour ce faire, rendez vous dans le menu « diagnostics->states->reset states » afin de vider les tables du firewall et réinitialiser toutes les connexions.
- La charge en temps réel de chaque queue est visible dans le menu « status->queues ».
- La somme de bande passante attribuée à chaque queue ne doit pas dépasser la valeur de la bande passante parente. Par ex : qpenaltyDown + qlanAcks + qlanDef ≤ qlanRoot.

8.3.3 Configuration avancée et tests

Nous avons vu le principe de fonctionnement des queues et des règles, nous allons maintenant pouvoir approfondir la configuration de celles-ci. Tous les paramètres que nous avons parcourus sont les paramètres par défaut, nous allons dans un premier temps les modifier afin de rendre tout ceci plus clair (en rapport avec notre maquette) et optimisé.

Par défaut, le wizard configure toutes les queues (ou presque) pour qu'elles utilisent 1% de la bande passante totale, ce qui n'est pas suffisant. Ceci est particulièrement le cas pour la queue qwanAck. En effet, lors d'un téléchargement, notre machine va envoyer des paquets « Ack » afin d'attester au serveur distant la bonne réception des paquets envoyés. Si la bande passante pour cette queue n'est pas suffisante, des paquets Ack pourraient être droppés automatiquement : le serveur considérera donc que les données n'ont pas été reçues et les renverra. Nous pouvons donc configurer cette queue pour qu'elle bénéficie de 60% de la bande passante totale, avec un minimum de 10% :



Nous pouvons conserver la configuration par défaut de la queue qlanacks, 25% de la bande passante totale dans le sens descendant est suffisant pour la réception de paquets d'acquittement.

Comme premier test, nous voulions que le client 1 n'ait droit qu'à 160Kbps de débit descendant. La queue qlanacks s'est vue réservée 25% soit 625Kbps. Nous pouvons donc configurer la queue qlandef pour qu'elle dispose de la bande passante restante soit : 2500-(160+625)= 1715Kbps.

Nous effectuons le même calcul concernant la queue qwandef, le résultat obtenu est 105Kbps.

Nous finissons par renommer nos queues pour que tout soit plus agréable à lire, nous obtenons ainsi les queues suivantes :

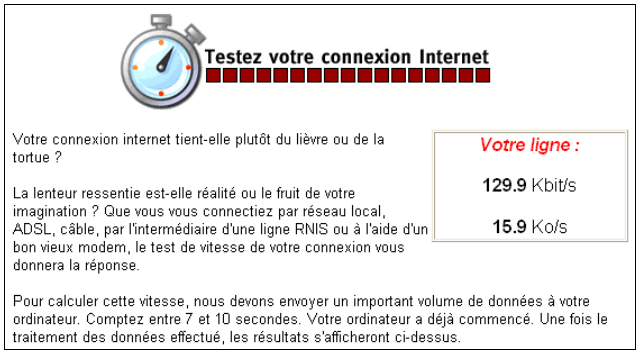
Flags	Priority	Default	Bandwidth	Name
	0	No	463 Kb	qwanRoot
	0	No	2500 Kb	qlanRoot
	1	Yes	105 Kb	qwandef
	1	Yes	1715 Kb	qlandef
ACK	7	No	60 %	qwanacks
ACK	7	No	25 %	qlanacks
RED ECN	2	No	80 Kb	client1Up
RED ECN	2	No	160 Kb	client1Down

Ainsi que les règles associées :

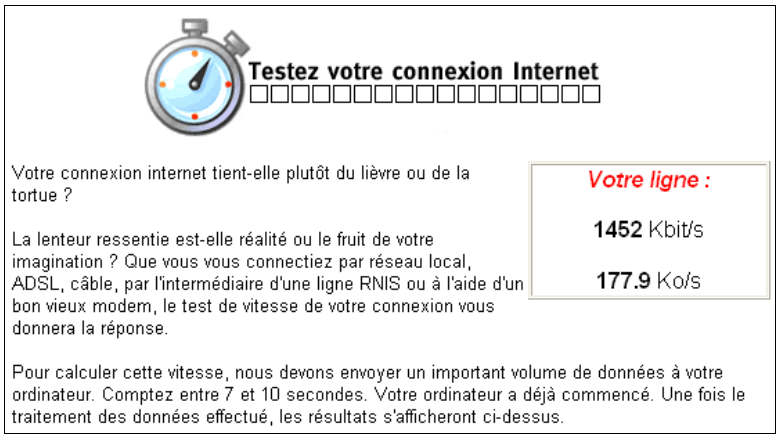
If	Proto	Source	Destination	Target	Description
WAN->LAN	*	*	192.168.2.99	client1Down/client1Up	limitations client 1 download
LAN->WAN	*	192.168.2.99	*	client1Up/client1Down	limitations client 1 upload

A partir de ce moment, notre client 1 sera limité à un débit descendant de 160Kbps (20Ko/s). Nous le vérifions d'une manière très simple, via le site zdnet.fr qui nous permet de calculer le débit descendant depuis une station.

Voici les résultats pour la station cliente 1 soumise à limitation :



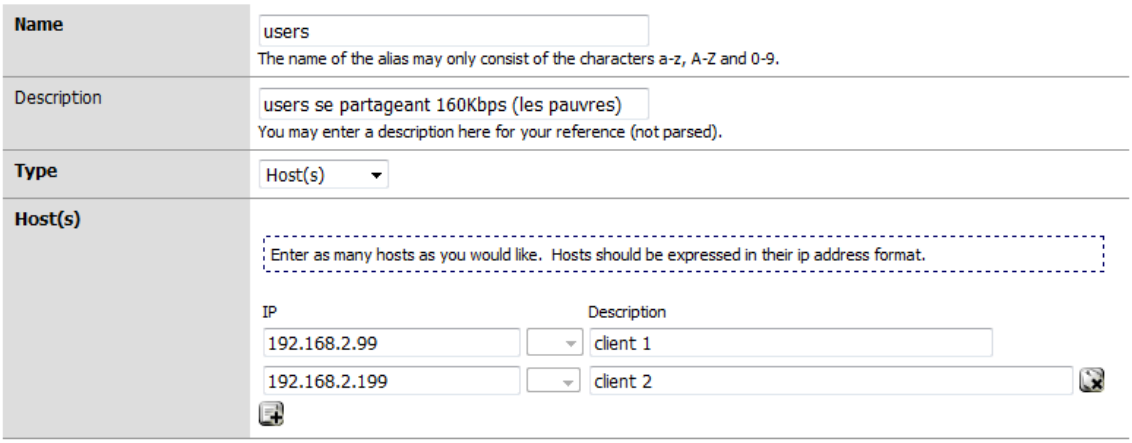
De même, voici le résultat du même test effectué depuis la station cliente 2 (192.168.2.199) non soumise à une règle particulière, et qui dépendra donc de la queue qlanDef (queue par défaut !) :



Dans les deux cas, les résultats concordent avec les configurations de chaque queue. Voici à titre indicatif les résultats obtenus depuis une des stations avant même de mettre en place le traffic shaper :

Nous venons de configurer les queues par défaut ainsi qu'une queue limitant le débit d'un hôte en particulier. Nous allons maintenant voir comment rajouter facilement un hôte dans la règle déjà établie, afin que les clients 1 et 2 se partagent la bande passante maximum allouée par les queues client1up et client1down (partage de 160kbps down et 80Kbps up).

Nous allons tout d'abord créer un « aliases » (firewall->aliases) configuré de la sorte :



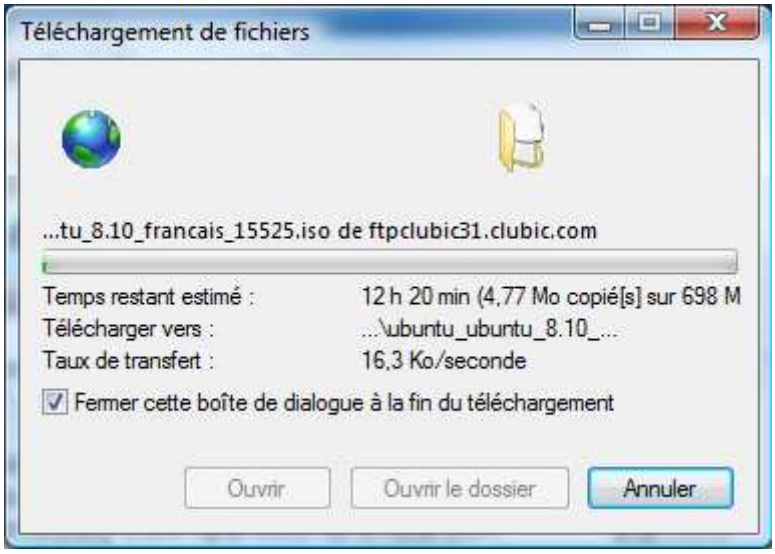
Cet alias peut pointer au choix sur plusieurs hôtes, plusieurs réseaux ou des ports. Dans notre cas, nous enregistrons les adresses de nos deux clients. Valider, l'alias est crée :

Name	Values	Description
users	192.168.2.99, 192.168.2.199	users se partageant 160Kbps (les pauvres)

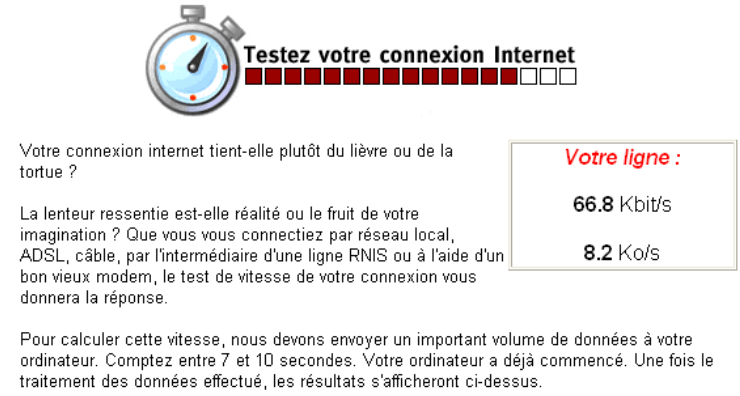
Pour finir, nous renseignons l'alias à la place de l'adresse précédente dans les règles du shaper :

If	Proto	Source	Destination	Target	Description
WAN->LAN	*	*	users	client1Down/client1Up	limitations 2 clients download
LAN->WAN	*	users	*	client1Up/client1Down	limitations 2 clients upload

Nous appliquons la nouvelle configuration du shaper, et effectuons quelques tests.
Notre premier hôte (192.168.2.199) lance un téléchargement via http :



En même temps, le second hôte exécute le même test de bande passante que précédemment :



➔ Une fois encore les résultats sont immédiats et en rapport avec nos attentes : les deux hôtes se partagent bien la portion de bande passante configurée dans nos queues.

Pour finir ce chapitre, nous allons voir comment attribuer une portion de bande passante indépendante à chacun de nos hôtes. Le principe consiste à créer un groupe de queues et de règles pour chaque utilisateur.

Notre station cliente 1 bénéficiera toujours de 160Kbps en download, nous allons faire en sorte que la station 2 bénéficie de 640Kbps.

Voici les queues que nous créons pour cela :

Flags	Priority	Default	Bandwidth	Name
	0	No	463 Kb	qwanRoot
	0	No	2500 Kb	qlanRoot
	1	Yes	85 Kb	qwandef
	1	Yes	1075 Kb	qlandef
ACK	7	No	60 %	qwanacks
ACK	7	No	25 %	qlanacks
RED ECN	3	No	40 Kb	client1Up
RED ECN	3	No	160 Kb	client1Down
RED ECN	2	No	60 Kb	client2up
RED ECN	2	No	640 Kb	client2down

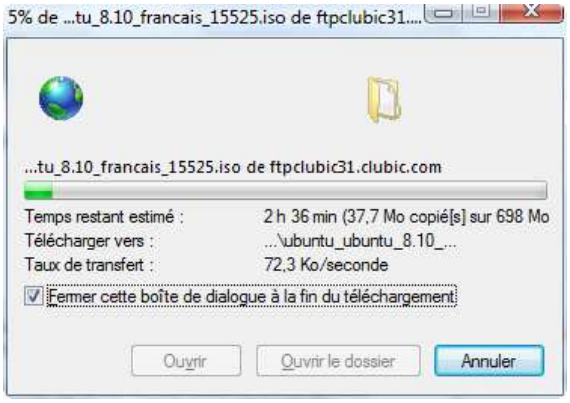
Ainsi, non content de bénéficier d'une meilleure bande passante disponible, le trafic du client 2 sera prioritaire sur celui du client 1 en cas de congestion.

Nous finissons par créer les règles adéquates :

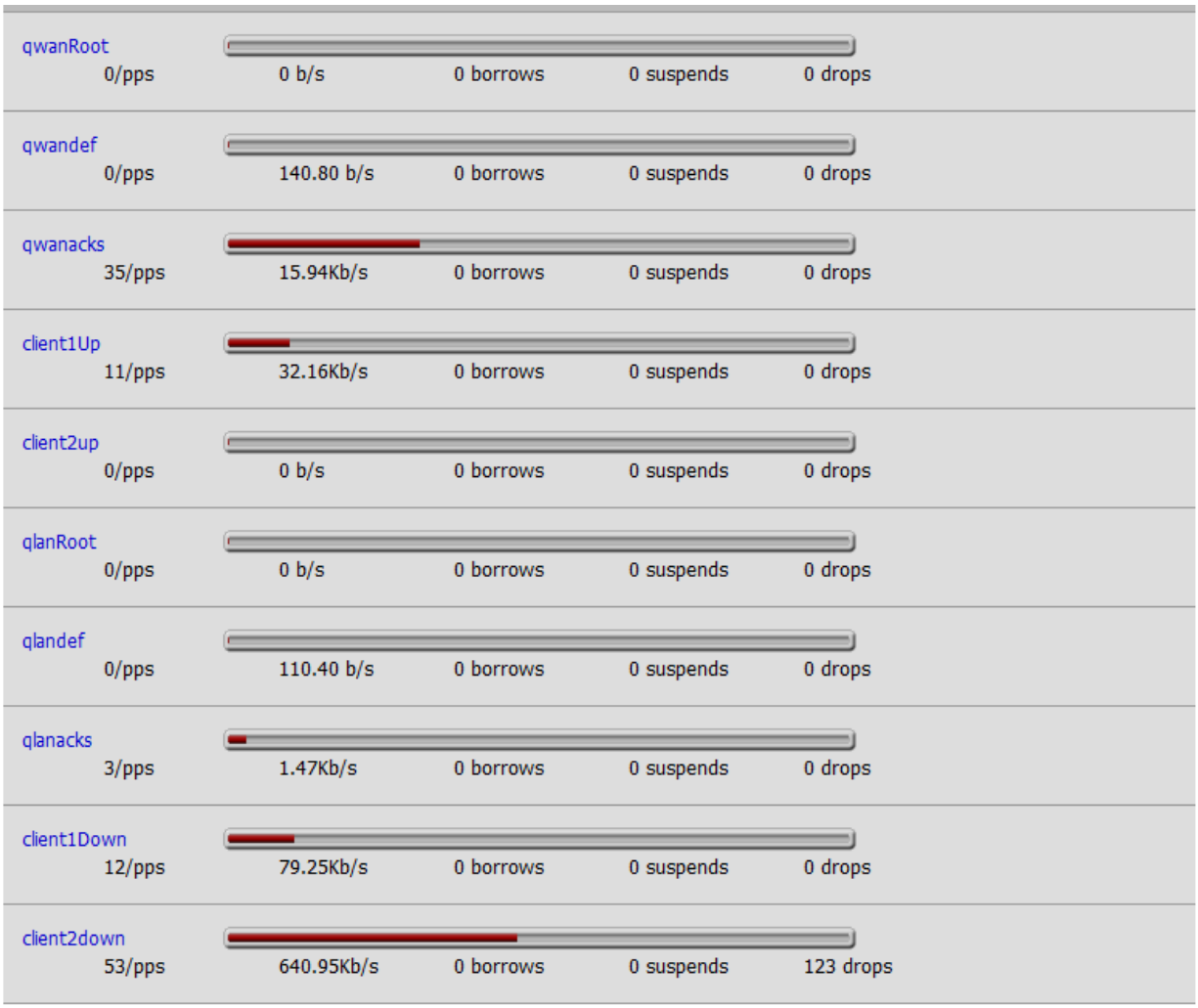
If	Proto	Source	Destination	Target	Description
WAN->LAN	*	*	192.168.2.99	client1Down/client1Up	limitations client 1 download
LAN->WAN	*	192.168.2.99	*	client1Up/client1Down	limitations client 1 upload
WAN->LAN	*	*	192.168.2.199	client2down/client2up	limitations client 2 download
LAN->WAN	*	192.168.2.199	*	client2up/client2down	limitations client 2 upload

Ainsi, le client 1 est bien limité à 160Kbps :

Alors qu'au même moment, le client 2 bénéficie de ses 640Kbps :



Comme nous l'évoquions plus haut, nous pouvons avoir une vue en temps réel sur la charge de chaque queue :



Cette vue est relativement intéressante puisqu'elle nous permet de contrôler que les débits configurés pour chaque queue sont bien respectés. Nous pouvons également avoir quelques informations supplémentaires sur chacune des queues (drop, suspends, borrows,…).

8.4 EXEMPLES D'APPLICATIONS

Comme dit précédemment, le shaper de pfSense permet initialement de rendre certain flux prioritaires sur d'autres. Par exemple la VOIP sera prioritaire sur le reste du trafic, quand le P2P sera le moins prioritaire de tous les flux. L'application que nous venons d'en faire, en partageant la bande passante (équitablement ou non) entre plusieurs entités, est une fonctionnalité particulièrement intéressante, notamment si nous nous trouvons dans l'un des deux cas suivants :

- Le partage équitable d'une ligne ADSL entre les différentes promotions d'une école (en l'occurrence, ce qui nous a amené à traiter cet aspect du shaper pfSense).

- Le partage d'une ligne xDSL entre les différentes entreprises d'une pépinière d'entreprises. Par pépinière nous entendons le fait qu'un bâtiment héberge plusieurs entreprises différentes et indépendantes, et que ce bâtiment ne possède qu'un unique accès xDSL à partager. Chacune des entreprises étant différente (en terme de nombre de poste et de besoins de bande passante), le partage ne sera pas forcément équitable, d'où l'intérêt du dernier point présenté !

9 SUPERVISION DE LA BANDE PASSANTE : NTOP

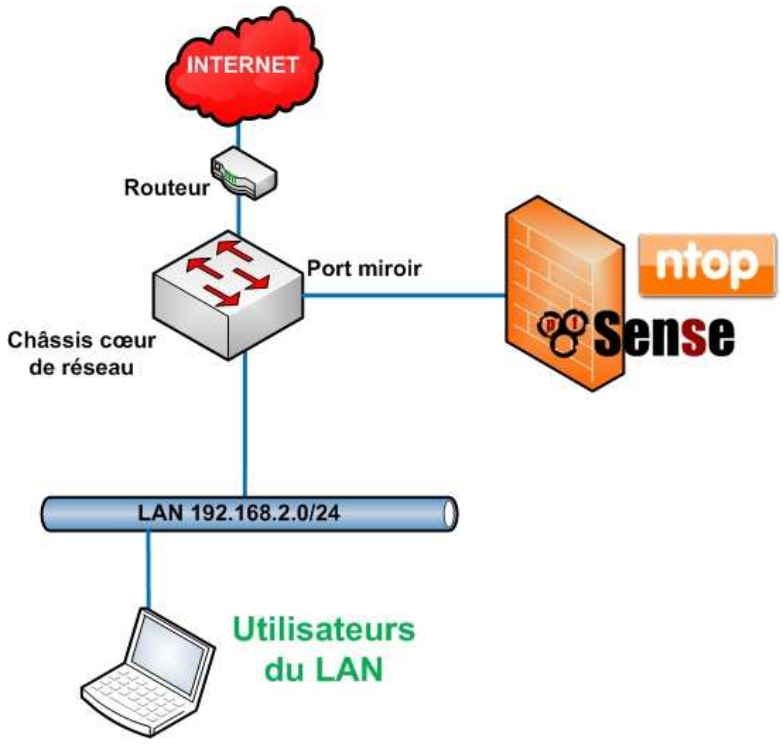
9.1 INTRODUCTION

Ntop est une sonde d'analyse du trafic réseau et nous permet ainsi d'avoir un œil sur l'utilisation qui est faite en temps réel de notre réseau. Nous pouvons également le qualifier de superviseur de bande passante, puisque nous pourrons afficher de manière détaillée un ensemble d'éléments tels que la bande passante moyenne utilisée par un hôte ou un réseau, les différents flux, leur type et leur sens (local->local, local->Remote…), et beaucoup plus encore.

Nous ne détaillerons pas ici l'ensemble des fonctions et éléments visualisables via Ntop (beaucoup trop nombreux), mais seulement les éléments qui nous semblent les plus intéressants pour superviser au mieux son réseau. De même, la fonction permettant à NTOP de recevoir des informations depuis une sonde NetFlow ne sera pas abordé…

9.2 MAQUETTE DE TEST

Typiquement, Ntop sera raccordé au cœur de votre réseau via un port miroir. Ce port miroir, aussi appelé port monitoring, effectue une réplication de l'ensemble du trafic transitant via l'élément actif sur lequel il est configuré (généralement un commutateur ou un châssis de cœur de réseau). Ainsi, l'ensemble des paquets entrants et sortants sera redirigé vers notre pfSense avec Ntop en écoute. Un port miroir se contente uniquement de dupliquer les paquets, ils ne sont en aucun cas remaniés, ce qui nous permet de conserver les adresses, ports, etc… d'origine. Voici ainsi la maquette déployée pour traiter ce chapitre :

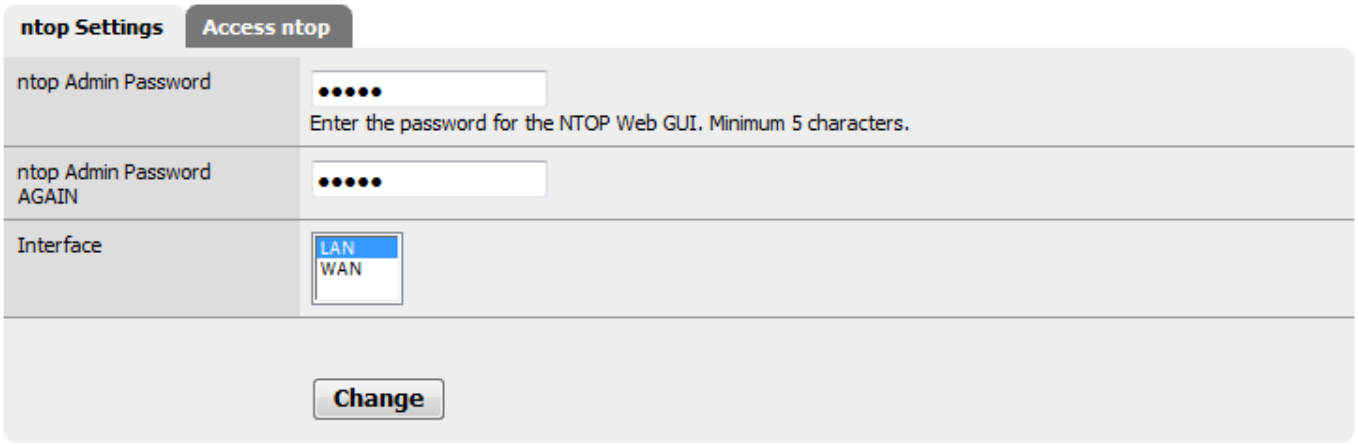


9.3 INSTALLATION ET CONFIGURATION

L'installation commence par le téléchargement et l'installation du package Ntop :

Package Name	Category	Package Info	Package Version	Description
ntop	Network Management	No info, check the forum	3.3.8	ntop is a network probe that shows network usage in a way similar to what top does for processes. In interactive mode, it displays the network status on the user's terminal. In Web mode it acts as a Web server, creating an HTML dump of the network status. It sports a NetFlow/sFlow emitter/collector, an HTTP-based client interface for creating ntop-centric monitoring applications, and RRD for persistently storing traffic statistics.

Une fois l'installation terminée, rendez-vous dans dans le menu « Diagnostics->ntop settings » pour initialiser ntop et lancer le service correspondant. Les paramètres disponibles ici sont maigres, et permettent seulement de configurer le mot de passe admin pour accéder à la configuration avancée de ntop, ainsi l'interface d'écoute :



Désormais Ntop est accessible via votre browser à l'adresse suivante : http://<@pfsense>:3000 (mais aussi en cliquant directement sur le bouton « access ntop » ci-dessus, ou encore via le menu pfSense « Diagnostics->ntop »).

En vous connectant à cette adresse, vous accéderez aux statistiques générales de votre réseau, affichant ainsi :

- De brèves informations concernant Ntop (interface d'écoute, uptime, etc…):

Network Interface(s)	**Name**	**Device**	**Type**	**Speed**	**Sampling Rate**	**MTU**	**Header**	**Address**
	le0	le0	Ethernet		0	1514	14	192.168.2.1
Local Domain Name	local							
Sampling Since	Wed Jan 21 14:44:13 2009 [40:44]							
Active End Nodes	171							

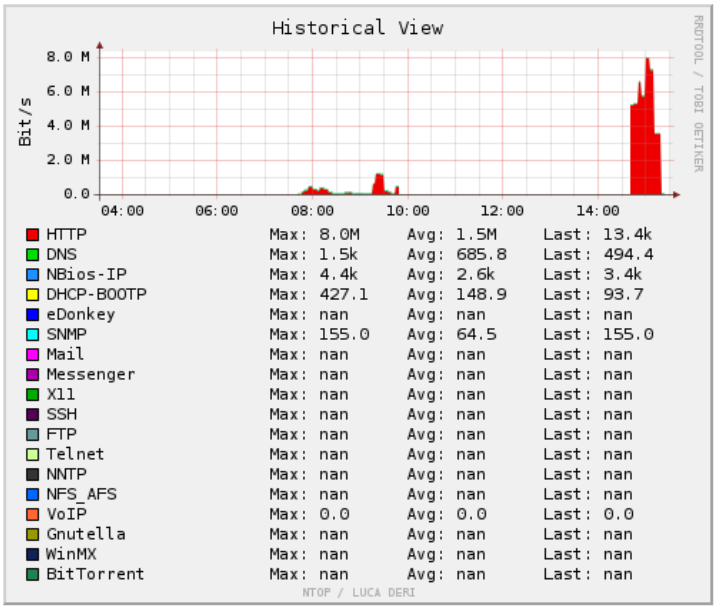
- Un rapport concernant le trafic sur l'interface d'écoute (paquets, trafic, ou la charge) :

Network Load	**Actual**	1.0 Mbit/s	201.5 Pkt/s
	Last Minute	1.0 Mbit/s	212.0 Pkt/s
	Last 5 Minutes	888.3 Kbit/s	178.1 Pkt/s
	Peak	10.4 Mbit/s	1380.8 Pkt/s
	Average	4.4 Mbit/s	609.0 Pkt/s

- La répartition totale du trafic par protocole :

Protocol	Data	Percentage			
IP	1.5 GBytes	99.8%	**TCP**	1.5 GBytes	99.9%
			UDP	1.6 MBytes	0%
			ICMP	39.0 KBytes	0%
			IGMP	5.6 KBytes	0%
			Other IP	270.9 KBytes	0%
(R)ARP	2.4 MBytes	0%			
STP	117.0 KBytes	0%			
Other	99.1 KBytes	0%			

- Ou encore un diagramme détaillé du trafic par services :



Sur la même page se trouve le menu principal de Ntop, dont nous détaillons le contenu :

- **Summary** — **Résumé de l'ensemble des informations NTOP**
  - Traffic — Affiche les éléments présentés précédemment
  - Hosts — Affiche les hôtes (locaux et distants) + infos basiques
  - Network load — Graphiques de la charge réseau à différentes périodes
  - Network flows — Informations basiques concernant les flux réseaux
- **All protocols** — **Informations concernant l'ensemble des protocoles**
  - Traffic — Données IN/OUT par hôte et par protocole de communication
  - Throughput — Débit (actuel, moyen et max) par hôte
  - Activity — Activités des hôtes (en % du trafic total) sur les 24H dernières
- **IP** — **Informations concernant TCP/IP uniquement**
  - Summary
    - Traffic — Données IN/OUT par hôte et par protocole de TCP/IP
    - Multicast — Statistiques multicast par hôte
    - Internet Domain — Volume de données in/out par domaine internet
    - Networks — Volume de données in/out par réseau
    - ASs — Liste des systèmes BGP autonomes traversés par le trafic
    - Host clusters — Statistiques pour tous les clusters d'hôtes
    - Distribution — Répartition du trafic (local, local->remote, rem->local)
  - Traffic directions
    - Local to local — Informations concernant les flux locaux
    - Local to Remote — Informations concernant le sens de flux local->distant
    - Remote to local — Informations concernant le sens de flux distant->local
    - Remote to Remote — Informations concernant les flux distants
  - Local
    - Ports used — Ports utilisés par hôte et par service
    - Active TCP/UDP sessions — Sessions TCP/UDP actives
    - Host fingerprint — Affiche l'OS des hôtes détectés
    - Host characterization — Affiche le type d'équipement pour chaque IP détectée
    - Network traffic map — Dessine une carte du réseau
    - Local Matrix — Affiche une matrice des flux locaux

- **Utils** — **Pour 'dumper' des données, et afficher les logs**
- **Plugins** — **Donne accès aux différents plugins NTOP**
- **Admin** — **Menu d'administration avancée de NTOP**

NB : Toutes les données collectées et archivée pour créer les historiques NTOP sont stockées dans les RRD (Round-Robin Databases). Vous pouvez modifier la manière dont ces données sont récupérées et stockées dans le menu « Plugins->Round-Robin databases->configure ».

NB2 : Les clusters d'hôtes sont des regroupements de plusieurs hôtes sous un nom (équivalent d'alias). Ceci nous permet d'afficher les statistiques sur un groupe d'utilisateurs donnés au lieu des informations individuelles. Nous pouvons le configurer dans le menu « admin->configure->preferences ».

Pour finir, nous ne détaillerons pas la configuration même de NTOP, qui reste relativement simple et relève plus de la customisation personnelle tant l'outil tel qu'installé est déjà entièrement exploitable. Dans tous les cas, le menu « admin » vous offrira toutes les options nécessaires pour personnaliser votre NTOP.

9.4 SCENARIOS D'UTILISATION DE NTOP

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

9.4.1 Quels hôtes consomment le plus de bande passante Internet ?

Des lenteurs ont été constatées pour tout accès à Internet, que ce soit pour du download ou de l'upload, et nous désirons contrôler l'utilisation que fait chaque hôte de notre connexion à Internet. Nous allons donc afficher un « top 10 » des hôtes les plus gourmands en bande passante Internet. Pour ce faire :

1. Sélectionner all protocols -> traffic
2. Dans 'hosts' choisir 'Local Only'
3. Dans 'data', choisir au choix 'received' ou 'sent'
4. Et enfin le VLAN concerné ou la totalité du réseau

Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	IPsec	(R)ARP	AppleTalk	NetBios	GRE	IPv6	STP	IPsec	OSPF	IGMP
dams-pc		13.5 MBytes	91.7 %	13.5 MBytes	14.8 KBytes	0	0	0	0	0	1.2 KBytes	0	0	0	0	0	0	0	0
192.168.2.1		1.1 MBytes	7.3 %	1.1 MBytes	0	0	0	0	0	0	1.6 KBytes	0	0	0	0	0	0	0	0
01:80:C2:00:00:00		102.6 KBytes	0.7 %	0	0	0	0	0	0	0	0	0	0	0	0	102.6 KBytes	0	0	0
01:40:0D:55:00:00		48.4 KBytes	0.3 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
00:0C:29:D2:FB:5F		460	0.0 %	0	0	0	0	0	0	0	460	0	0	0	0	0	0	0	0

Nous affichons ainsi l'ensemble des hôtes et les quantités de données reçues et/ou envoyées. Il ne reste plus qu'à cliquer sur 'data' pour afficher les plus gros consommateurs en tête de liste !

NB : Dans chaque fenêtre NTOP de ce type, en cliquant sur le nom ou l'adresse d'un hôte, vous pourrez accéder à toutes ses statistiques détaillées.

9.4.2 Quels sites les plus gros consommateurs de bande passante visitent-ils ?

Nous allons maintenant nous assurer que notre top 10 des consommateurs de bande passante, l'utilise bien à des fins professionnelles et non pas perverses et obscures… >:-D

Pour cela, rien de plus facile puisqu'il suffit de cliquer le nom ou l'IP de l'hôte voulu. Nous n'avons plus qu'à descendre la page affichée jusqu'aux tableaux « Last contacted peers » et « TCP/UDP Service/port Usage » afin de constater quels sites web ont été consultez, les quantités de données envoyées ou émises pour chacun d'eux, ainsi que pour chaque service Internet :

Last Contacted Peers

Sent To	IP Address
224.0.0.252	224.0.0.252
00:0C:29:D2:FB:55	
192.168.0.17	192.168.0.17
207.46.109.58	207.46.109.58
80.10.246.129	80.10.246.129
pop.mail.yahoo.fr	217.12.10.63
g.microsoft.com	207.68.179.201
Total Contacts	292

Received From	IP Address
www.google-analytics.com	209.85.173.127
csi.gstatic.com	72.14.221.102
00:0C:29:D2:FB:55	
192.168.0.17	192.168.0.17
207.46.109.58	207.46.109.58
80.10.246.129	80.10.246.129
pop.mail.yahoo.fr	217.12.10.63
g.microsoft.com	207.68.179.201
Total Contacts	192

TCP/UDP Service/Port Usage

IP Service	Port	# Client Sess.	Last Client Peer	# Server Sess.	Last Server Peer
domain	53	130/10.8 KBytes	80.10.246.129		
http	80	3383/3.4 MBytes	207.46.109.58		
pop3	110	99/26.6 KBytes	pop.mail.yahoo.fr		
snmp	161	74/6.1 KBytes	192.168.0.17		
https	443	70/55.1 KBytes	urs.microsoft.com		

9.4.3 Quels sites reçoivent/émettent le plus de trafic depuis/vers mon entreprise ?

Suivant le même ordre d'idée que précédemment, nous allons vérifier quels sites web reçoivent le plus de donnée depuis notre réseau local. En effet, il pourrait être intéressant de contrôler les sites les plus souvent sollicités afin d'affiner notre blacklist SquidGuard par exemple… Pour cela :

1. Sélectionner all protocols -> traffic
2. Dans 'hosts' choisir 'remote only'
3. Dans 'data' choisir 'received only'

Nous sommes ainsi en mesure d'afficher les sites qui ont reçu le plus de requêtes/datas depuis notre entreprise :

Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	IPsec	(R)ARP	AppleTalk	NetBios	GRE	IPv6	STP	IPsec	OSPF
192.168.0.88		3.4 MBytes	64.6 %	3.3 MBytes	119.1 KBytes	36.2 KBytes	0	0	0	0	46	0	0	0	0	0	0	0
192.168.100.200		823.9 KBytes	15.2 %	823.9 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0	0
224.0.0.18		317.5 KBytes	5.9 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
239.255.255.250		225.5 KBytes	4.2 %	0	225.5 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0
exiaserver [NetBIOS]		203.8 KBytes	3.8 %	0	203.5 KBytes	0	0	0	0	0	322	0	0	0	0	0	0	0
207.46.109.58		161.3 KBytes	3.0 %	161.3 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0	0
224.0.0.252		74.2 KBytes	1.4 %	0	74.2 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.0.254		36.3 KBytes	0.7 %	0	0	36.2 KBytes	0	0	0	0	138	0	0	0	0	0	0	0
www.google.fr		16.3 KBytes	0.3 %	16.3 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0	0
clients1.google.com		11.8 KBytes	0.2 %	11.8 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ows.messenger.msn.com		11.0 KBytes	0.2 %	11.0 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.0.17		10.9 KBytes	0.2 %	0	10.1 KBytes	0	0	0	0	0	782	0	0	0	0	0	0	0
urs.microsoft.com		6.9 KBytes	0.1 %	6.9 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0	0
view.atdmt.com		3.6 KBytes	0.1 %	3.6 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0	0
rad.msn.com		2.9 KBytes	0.1 %	2.9 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0	0
spe.atdmt.com		2.5 KBytes	0.0 %	2.5 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0	0

De la même manière, nous pouvons afficher les sites qui envoient le plus de données vers notre réseau local. Il suffit pour cela de changer 'received only' par 'sent only' dans le menu 'data' :

Host	Domain	Data ⇩		TCP	UDP	ICMP	ICMPv6	DLC	IPX	IPsec	(R)ARP	AppleTalk	NetBios	GRE	IPv6	STP	IPsec	OSPF
192.168.100.200		14.7 MBytes	88.5 %	14.7 MBytes	3.4 KBytes	0	0	0	0	0	92	0	0	0	0	0	0	0
192.168.0.88		759.7 KBytes	4.5 %	473.1 KBytes	244.0 KBytes	41.2 KBytes	0	0	0	0	1.4 KBytes	0	0	0	0	0	0	0
192.168.0.246		360.3 KBytes	2.1 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.0.40		262.6 KBytes	1.5 %	0	262.6 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0
207.46.109.58		194.9 KBytes	1.1 %	194.9 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0	0
exiaserver [NetBIOS]		121.7 KBytes	0.7 %	0	121.7 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.0.207		56.7 KBytes	0.3 %	0	56.7 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.0.254		41.2 KBytes	0.2 %	0	0	41.2 KBytes	0	0	0	0	0	0	0	0	0	0	0	0
urs.microsoft.com		25.2 KBytes	0.1 %	25.2 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0	0
toth [NetBIOS]		21.0 KBytes	0.1 %	0	20.4 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0
fulgore [NetBIOS]		17.4 KBytes	0.1 %	0	17.4 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0
pponzio [NetBIOS]		15.9 KBytes	0.1 %	0	15.9 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.0.17		12.8 KBytes	0.1 %	0	12.7 KBytes	0	0	0	0	0	46	0	0	0	0	0	0	0

9.4.4 Quels hôtes s'échangent le plus de données ?

Nous avons la possibilité d'afficher une matrice des flux locaux, idéal afin de constater les quantités de données échangées entre différents hôtes (fonctionne uniquement avec des hôtes locaux du même domaine de broadcast). Nous y accédons en cliquant sur « IP->Local->local matrix » :

IP Subnet Traffic Matrix

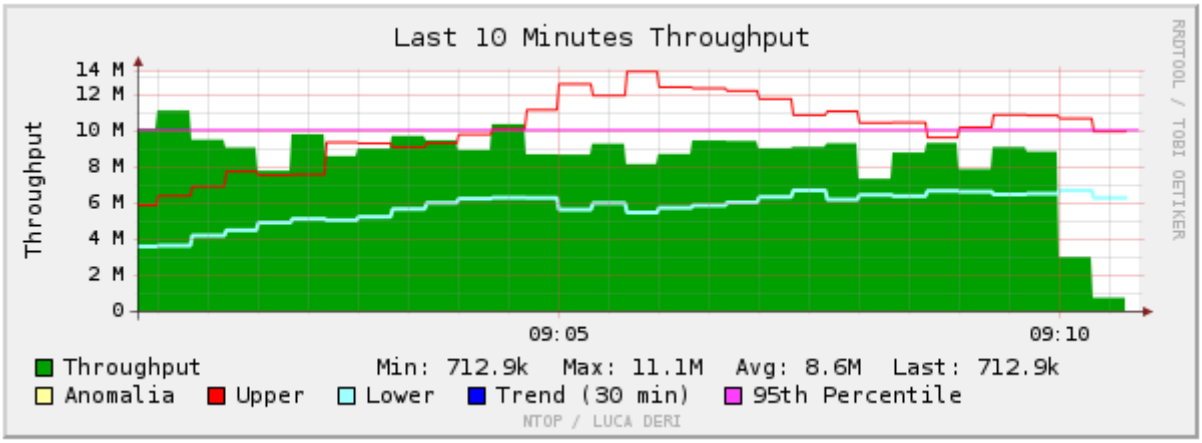
From \ To	192.168.2.199	224.0.0.252	pfsense
192.168.2.199		13.0 KBytes	11.9 MBytes
224.0.0.252	13.0 KBytes		
pfsense	11.9 MBytes		

9.4.5 Quelle est la charge de mon réseau ?

Vous désirez afficher la charge de votre réseau sur les 10 dernières minutes, ou bien encore constater à quelle heure de la journée votre réseau est le plus utilisé ? Nous nous rendons pour cela dans le menu « summary->network load » qui nous permet de détailler via des graphiques la charge du réseau pour :

- Les 10 dernières minutes
- La dernière heure
- La journée en cours
- Le mois en cours

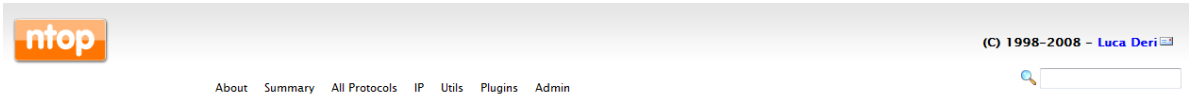
Voici à titre d'exemple le graphique pour les dix dernières minutes d'utilisation :



Cet exemple fait apparaître les différentes informations que peut nous afficher le graphique :
La charge moyenne (throughput), les pics hauts (upper) et bas (lower), et un pallier représentant les 95% d'utilisation pour situer le reste de la charge.

9.4.6 Quel type d'équipement correspond à chacun de mes hôtes ?

Nous avons vu qu'il était très facile d'afficher une liste des différents hôtes de notre réseau. Nous allons voir comment les identifier très clairement. Ains, nous saurons exactement quel hôte est serveur DHCP, imprimante, commutateur, passerelle, ou autre. Nous nous rendons dans le menu « IP->local->host characterization » :



Local Hosts Characterization

Host	Unhealthy Host	L2 Switch Bridge	Gateway	VoIP Host	Printer	NTP/DNS Server	SMTP/POP/IMAP Server	Directory/FTP/HTTP Server	DHCP/WINS Server	DHCP Client	P2P
192.168.0.115	X										
192.168.0.62	X										
192.168.0.203	X										
192.168.0.58	X										
192.168.0.145	X										
192.168.0.151	X										
192.168.0.109	X										
192.168.100.100	X										
192.168.0.17	X										
192.168.0.92	X										
192.168.0.121	X										
192.168.0.55	X										
192.168.0.142	X										
192.168.0.70	X										
192.168.0.245	X										
192.168.0.50	X										
192.168.0.135	X										
192.168.0.46	X										
192.168.0.123	X										
192.168.0.126	X										
192.168.0.120	X										
192.168.0.201	X										
192.168.0.199	X										
192.168.0.134	X										
192.168.0.165	X										
192.168.1.20	X										
192.168.0.71	X										
192.168.0.96	X										
192.168.0.63	X										
192.168.0.44	X										
00:09:B7:26:15:85 (vlan 3)		X	X								
192.168.0.77	X										
192.168.0.104	X										
192.168.0.98	X										
0.0.0.0	X										
192.168.0.10	X										
192.168.0.29	X										
192.168.2.199	X										
192.168.0.254	X										
pfsense	X		X					X			
192.168.0.125	X										
192.168.0.54	X										
0.0.0.0	X										
192.168.0.143	X										
192.168.0.69	X										
192.168.0.152	X										
192.168.0.66	X										
192.168.0.150	X										
192.168.0.85	X										
192.168.0.112	X										
192.168.0.80	X										
192.168.0.60	X										
192.168.0.102	X										
192.168.0.90	X										
192.168.0.116	X										
192.168.0.103	X										
192.168.0.107	X										
Total	56 [90.3 %]	1	2				1				

Report created on Fri Jan 23 09:20:41 2009 [ntop uptime: 58:27]
Generated by ntop v.3.3.8 [i386-unknown-freebsd7.1]
© 1998-2008 by Luca Deri, built: Dec 4 2008 15:19:59.
Listening on [le0] for all packets (i.e. without a filtering expression)
Web reports include only interface "le0"

CONCLUSION

Une conclusion voudrait que le travail soit achevé, or nous venons d'initier un document poussé à évoluer. En effet vous avez sûrement remarqué que certains services proposés par PfSense ne sont pas traités. En cela nous espérons notre démarche sera largement suivie et le tutorial complété.

Plus globalement nous sommes heureux d'avoir pu contribuer à la communauté en lui proposant une première version de tutorial.

L'administration réseau est un travail compliqué. Le métier veut que l'on doive souvent maîtriser différentes technologies et les faire travailler ensembles. La tâche se complique encore si l'administration et la configuration de tout cela se fait manuellement. Des questions fusent : Est-ce que ces technologies fonctionnent ensembles ? Ne vais-je pas trop perdre de temps à administrer telle ou telle technologie ? etc.

En ce sens nous avons vérifié à travers ce document que PfSense répond à ces interrogations. Cet Outil est en effet un gestionnaire central d'outils réseaux. On peut ainsi faire travailler ensemble un pare feu, un routeur, un serveur VPN, un Proxy, un outil de détection d'attaque réseau, un système de Failover, etc. Le tout sur un seul et même Serveur. On peut par exemple créer très facilement des « Backups » pour ne pas se retrouver avec un seul point névralgique dans notre réseau… Bref nous pensons que PfSense est voué à exister et se développer.

Nous avons mis en place et testé certains services (les principaux pour être précis) de PfSense. Tous ces outils cohabitent parfaitement ensemble dans PfSense, il ne manquait plus qu'à les documenter en Français, c'est à présent chose faite.

CE QU'IL RESTE A FAIRE

Au 01/02/2009

- Créer la partie SQUID /SQUIDGuard
- Ajouter la partie de CCNET publiée sur http://forum.pfsense.org/index.php?topic=13551.0
- ???