Université de Limoges

Initiation et mise en application du firewall pfSense

Loïc Laforet

Dernière modification : 30 juin 2013

Table des matières

Version	Date	Note / Description
1.1	À planifier	– SSH keys RSA – Services DHCP - paramètres avancés – CARP / Redondance de charge – Taffic-shapping (qos) – Bridge d'interfaces – VLAN – Service et maintenance v2
1.0	30 juin 2013	– installation – configuration initiale – services essentiels – vpn ipsec site-to-site – configurations avancées – service et maintenance v1

TABLE 1 – Historique des versions

Chapitre I

Préambule

PfSense est un système d'exploitation à part entière, open source, utilisé pour mettre en oeuvre un pare-feu, un routeur ou une solution permettant la fourniture d'autres services réseaux. **PfSense** est une distribution FreeBSD [1] personnalisée, et basée initialement sur le projet **m0n0wall**, distribution de pare-feu puissant mais léger. **PfSense** s'appuie sur le principe de base de **m0n0wall** et reprend la plupart de ses fonctions, en prenant soin de mieux les faire cohabiter, de les sécuriser, de les stabiliser, tout en favorisant la compatibilité du système afin d'y ajouter une variété d'autres services liés essentiellement aux réseaux.

Ce document couvre les paramètres de base et nécessaires pour la quasi totalité des déploiements de **pfSense**, qu'il s'agisse d'un *simple* pare-feu (nous verrons ensemble qu'il n'est pas si aisé de déployer ce rôle), d'un routeur voire d'un point d'accès sans fil.

Une fois **pfSense** installé et configuré selon les bonnes pratiques de ce guide ou des différents sites Internet (et communautés actives sur ce sujet), vous bénéficierez d'un pare-feu et/ou d'un routeur entièrement opérationnel.

À son niveau le plus élémentaire, un **pfSense** peut être utilisé pour remplacer le routeur d'un réseau domestique et pour fournir des fonctionnalités supplémentaires. Dans des configurations plus complexes, **pfSense** peut être déployé pour établir un tunnel chiffré et sécurisé entre deux sites et/ou pour un client distant, pour établir un équilibrage de charge réseau sur une batterie de serveurs Web, ou façonner et hiérarchiser le trafic réseau pour ne citer que quelques exemples. Il y a littéralement une centaine de façons de configurer et déployer un firewall **pfSense**.

Une fois **pfSense** installé, il existe deux façons d'accéder au système d'exploitation : par le protocole SSH et par l'Interface Web. Par l'accès SSH, le firewall **pfSense** vous proposera le même menu système que celui visualisé lors de la fin du processus d'installation de la distribution, et présent par défaut lorsque la machine est allumée.

Nous n'utiliserons pas dans ce document l'administration du firewall par l'accès **SSH**, étant donné que la totalité des fonctions d'administration sont disponibles par l'interface d'administration Web.

I Pré-requis

Nous nous basons dans ce document sur une infrastructure virtuelle sous l'applicatif propriétaire **VMware** [2] et sous son produit gratuit *Esxi 5.1*. Comme l'illustre le schéma I.1, nous utiliserons quatre *vlan* [3] pour scinder

1. http ://www.freebsd.org
2. http ://www.vmware.com
3. Virtual Local Area Network - cf. standard IEEE 802.1Q

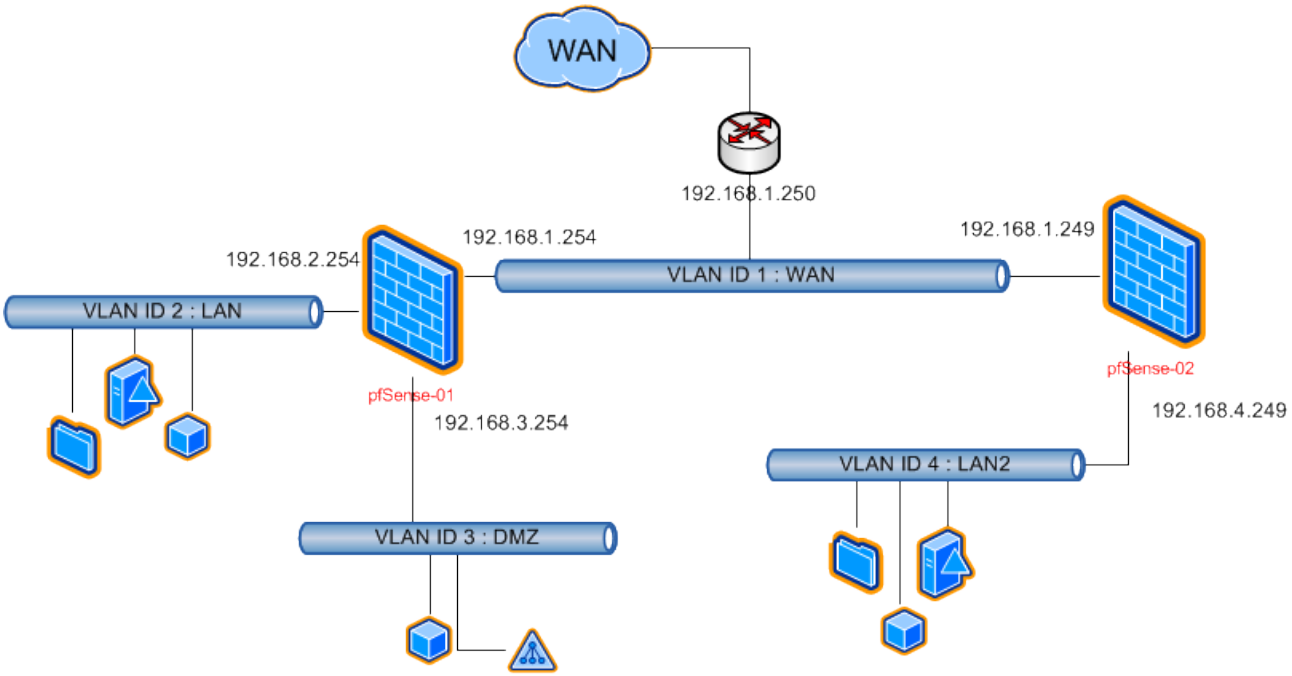

FIGURE I.1 – Schéma de l'infrastructure de R&D

les différents réseaux que nous serons amenés à utiliser pour les mises en application.

Pour mettre en oeuvre cette infrastructure virtuelle, il est nécessaire d'acheminer les différents réseaux virtuels (*vlan*) au serveur physique *Esxi*. Il est donc nécessaire, pour une infrastructure virtuelle de type **VMware**, d'ajouter des *Virtual Machines Port Group* pour chaque *VLAN*.

Le schéma I.2 illustre la gestion des réseaux sur un *Esxi* pour l'infrastructure illustrée ci-dessus.

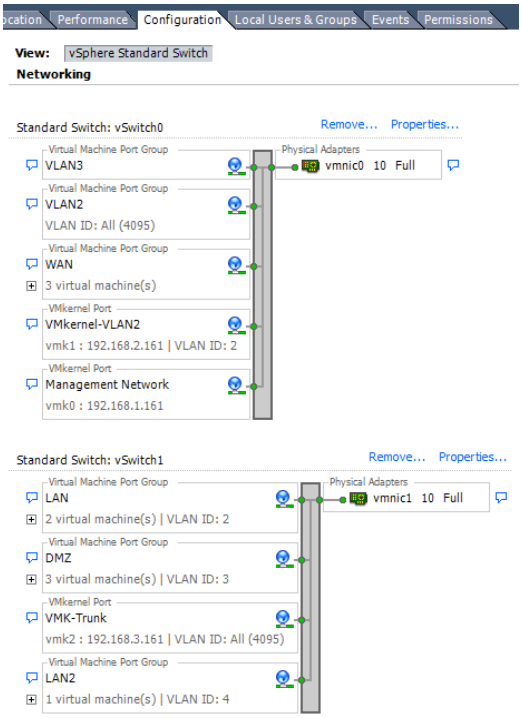

FIGURE I.2 – Esxi : gestion des réseaux

Il est indispensable que les interfaces du ou des firewall (en dehors du réseau `WAN`) ne soient pas connectées sur le même réseau physique ou virtuel. Nous considérons enfin que le routeur, répondant à l'adresse IP `192.168.1.250`, ne gère et ne fournit aucun autre rôle.

II Installation du pfSense-01

Après avoir téléchargé [4] la dernière version stable de **pfSense**, version `2.0.3` à l'écriture de ce document, il est nécessaire d'installer la distribution sur une machine (virtuelle dans ce document).

Lors du lancement de la machine virtuelle, un premier écran nous invite à sélectionner le mode de *boot* :

– **choisir l'option [1]**, celle par défaut ;

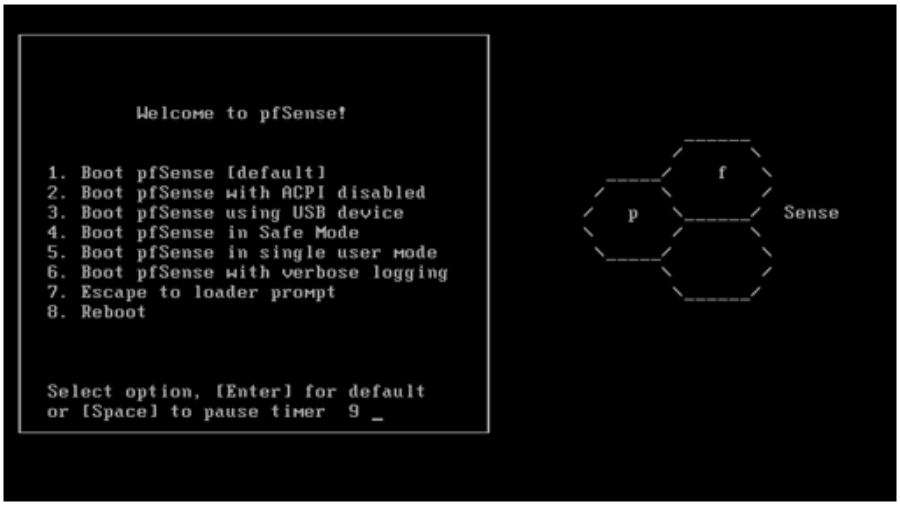

FIGURE I.3 – pfSense-installation : phase de démarrage

Pendant la phase de démarrage, **pfSense** va vérifier l'ensemble des ressources dont il dispose. En fonction des paramètres techniques choisis lors de la génération de la machine virtuelle, il se peut que **pfSense** ne parvienne pas à détecter certaines ressources. Les éléments les plus sensibles sont le disque dur et les interfaces réseaux (NIC [5]). Vous pouvez vous inspirer du schéma I.4-**Machine virtuelle : compatibilité du matériel virtuel** en page 8, indiquant des références de matériels virtuels compatibles avec la distribution **pfSense**.

4. http ://www.pfsense.org/mirror.php ?section=downloads
5. Network Interface Card

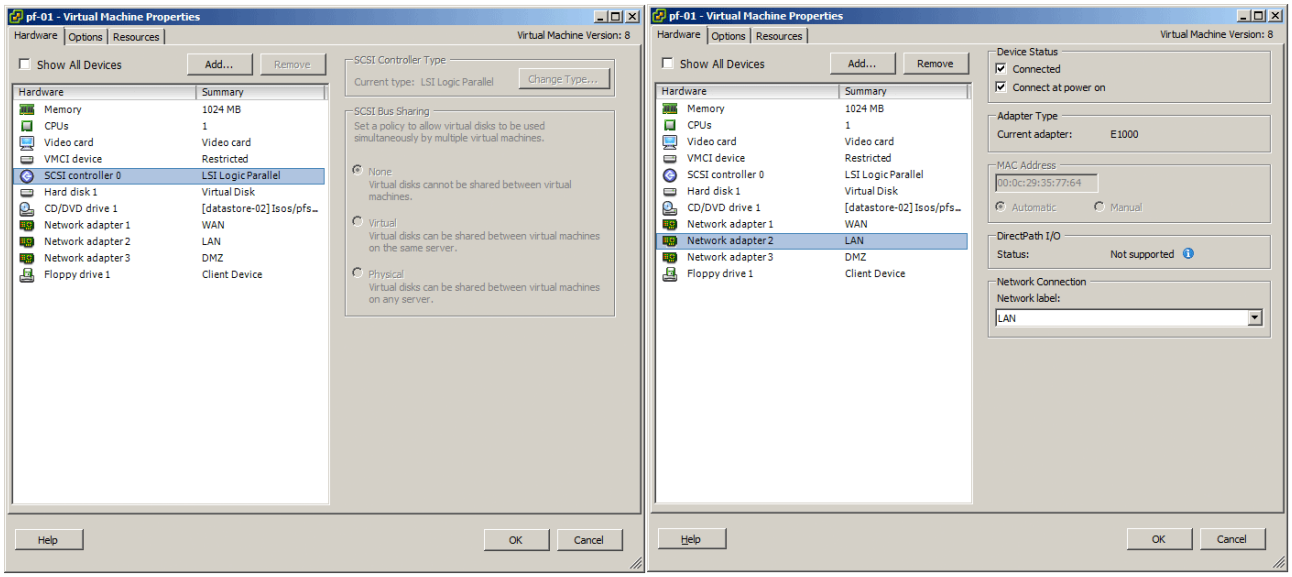

FIGURE I.4 – Machine virtuelle : compatibilité du matériel virtuel

Si **pfSense** identifie les ressources matérielles compatibles, il vous invite à sélectionner le mode de démarrage de la distribution. Deux choix s'offrent à nous : le mode *live CD* et le mode *Installer*. Le premier permet de charger en mémoire **pfSense**, de configurer le firewall et les services associés comme vous le souhaitez, et de les utiliser de manière totalement opérationnels. Étant chargé en mémoire, il est important de ne pas redémarrer la machine sinon tous vos paramètres disparaîtront. Nous sélectionnerons ici le choix numéro **deux**, afin d'installer l'applicatif sur le disque dur virtuel.

– **Appuyer** sur la **touche [I]** ;

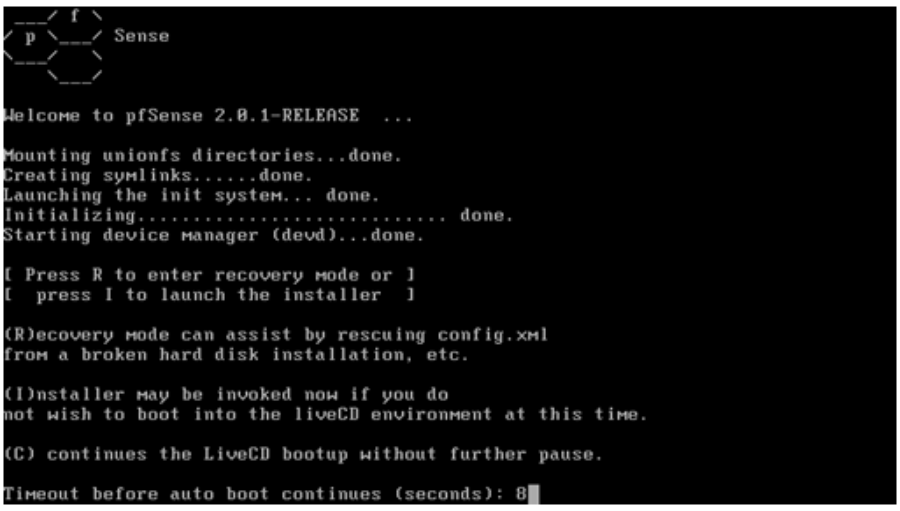

FIGURE I.5 – pfSense-installation : mode de démarrage

– **Sélectionner** le choix **[Accept these Settings]** ;

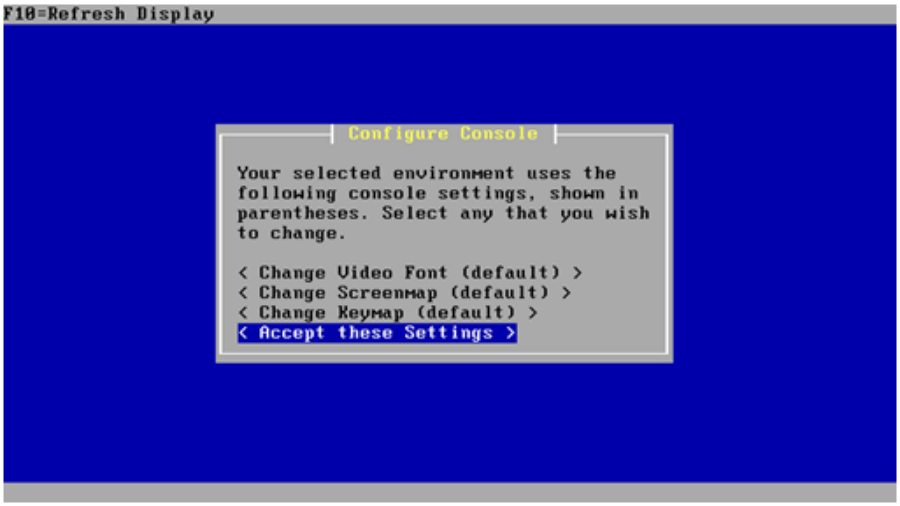

FIGURE I.6 – pfSense-installation : paramétrage de la résolution et du clavier

– **Sélectionner** le choix **[Quick/Easy Install]** ;

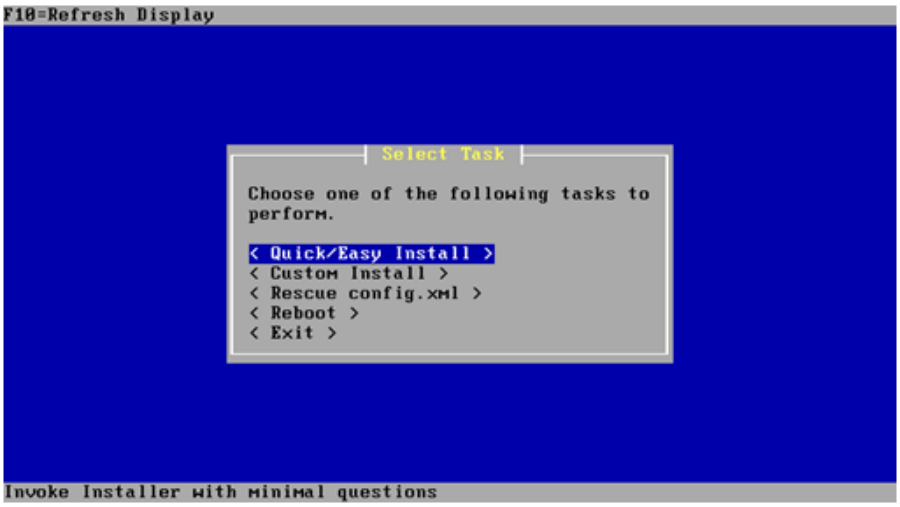

FIGURE I.7 – pfSense-installation : validation de l'installation de pfSense

– **Sélectionner** le choix **[OK]** pour installer la distribution sur le disque dur virtuel (cf. figure I.8) ;

– **Sélectionner** le choix numéro 1 **[Symmetric multiprocessing kernel ...]** (cf. figure I.9) ;

– **Rédémarrer** la machine en sélectionnant **[Reboot]** ;

Une fois l'installation terminée, la distribution redémarre pour prendre en compte l'ensemble des éléments précédemment installés. Nous verrons dans la prochaine section le paramétrage des interfaces réseaux (NIC).

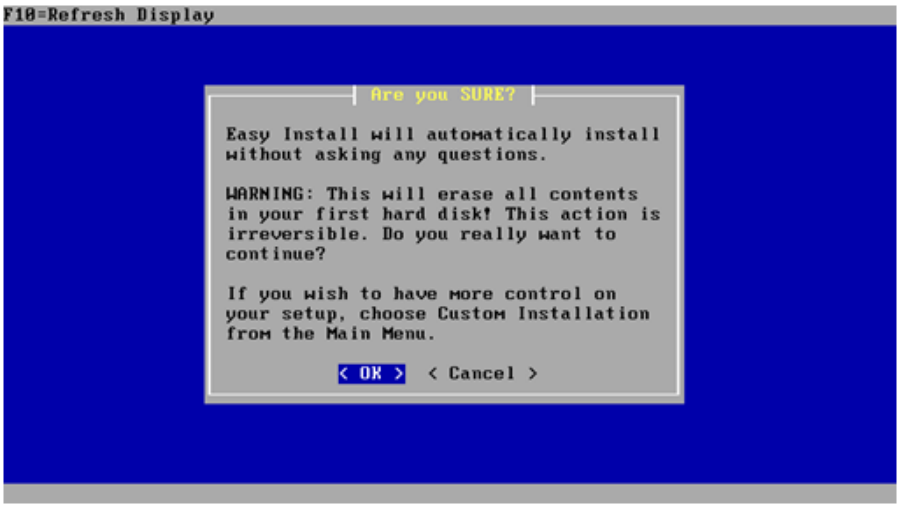

FIGURE I.8 – pfSense-installation : confirmation de l'installation de pfSense

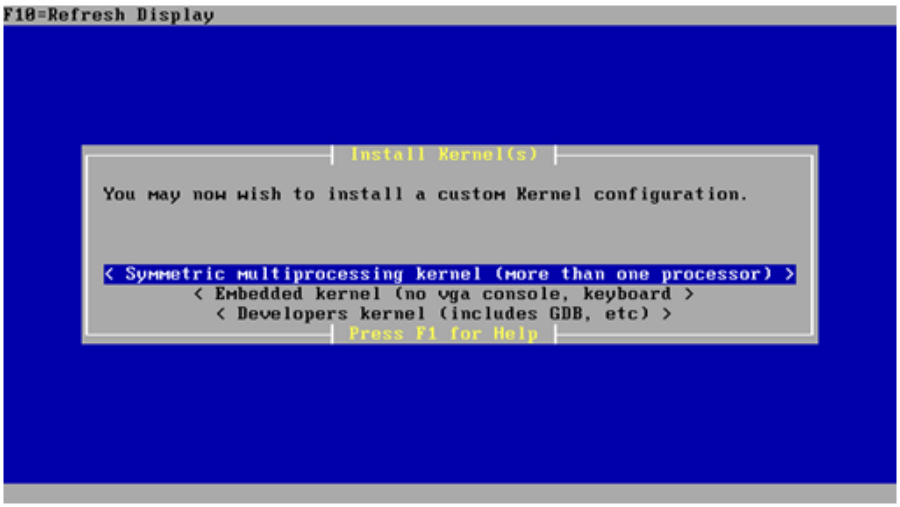

FIGURE I.9 – pfSense-installation : choix d'une configuration du kernel

III Gestion des interfaces

La première étape de configuration demandée par l'installateur de **pfSense** concerne le paramétrage des interfaces réseaux. Comme le montre la figure I.4-**Machine virtuelle : compatibilité du matériel virtuel** en page 8, trois interfaces réseaux virtuelles sont connectées à la machine virtuelle. Nous avons ici fait le choix d'ajouter ces *NICs* afin d'acheminer les trois réseaux préalablement paramétrés sur notre serveur de machines virtuelles Esxi (cf. III-**Gestion des interfaces**, page 11).

La première étape concerne l'identification des interfaces réseaux. Il est en effet important de faire correspondre les interfaces virtuelles (ou physiques) de notre machine virtuelle avec les interfaces réseaux détectées par **pfSense** (nommées *emXX dans le cadre d'une NIC VMware de type E1000*.

> `Astuce :` **pfSense** affiche le status d'une carte réseau et renvoie en console son état (connecté/déconnecté). Ainsi, il suffit de déconnecter une à une les cartes réseaux (filaires dans le cadre d'une carte réseau physique, déconnecter virtuellement[a] le câble dans le cadre d'une NIC virtuelle) pour visualiser son nom par le firewall.
>
> a. Depuis les propriétés d'une machine virtuelle, sélectionner la carte réseau à identifier, puis cliquer déconnecter la carte virtuelle

> `Remarque :` Deux choix s'offrent à l'adminitrateur concernant la gestion de *vlans*. Le premier consiste, comme décrit dans ce document, à gérer les *vlans* (ou lire et enlever les *tags - quatre octets*) par le serveur VMware. L'autre choix consiste à indiquer à l'Esxi d'interpréter les *vlans* mais de conserver les *tags* lorsqu'il les achemine aux NICs des machines virtuelles. Si l'administrateur opte pour le choix numéro deux, il sera nécessaire de répondre **[oui]** à la gestion des vlans par **pfSense**. Nous disposerons ainsi d'une inteface virtuelle supplémentaire pour chaque vlan associé. Elle seront gérées comme une interface physique par **pfSense**, à la manière d'une patte `LAN, WAN, DMZ` ...

– **Répondre** **[n]** à la gestion des vlans (cf. I.10, page 12) ;

Une fois les interfaces identifées, nous pouvons désormais les assigner à celles détectées par **pfSense**. Pour cela, il suffit de répondre aux questions posées par l'installateur du firewall. La première interface que **pfSense** souhaite identifier concerne la patte `WAN`, comme le montre la figure I.11.

Dans l'exemple illustré par les figures ci-après I.11, I.12 et I.13 situées à la page 12, nous avons les correspondances suivantes :

1. **WAN** -> `em0`
2. **LAN** -> `em1`
3. **OPT** -> `em2`

pfSense ne nous propose pas pour le moment de nommer notre interface `DMZ`. Il nomme toutes les interfaces supplémentaires `OPTX`. Nous utiliserons l'interface web de management pour modifier le nom de cette interface.

– **Valider** par la touche **[Entrée]** pour sortir du menu de configuration des `NICs` ;

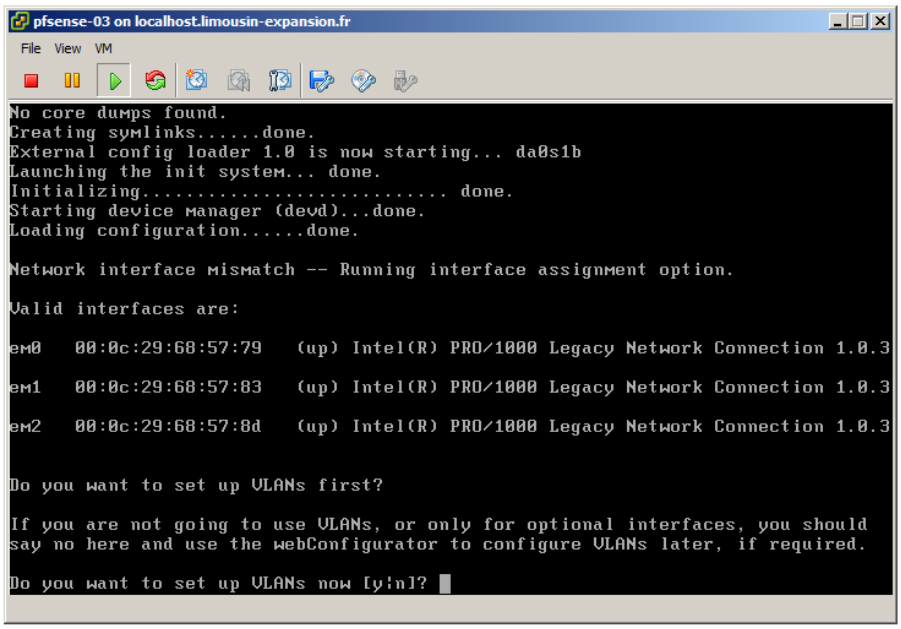

FIGURE I.10 – pfSense : assignation des interfaces réseaux

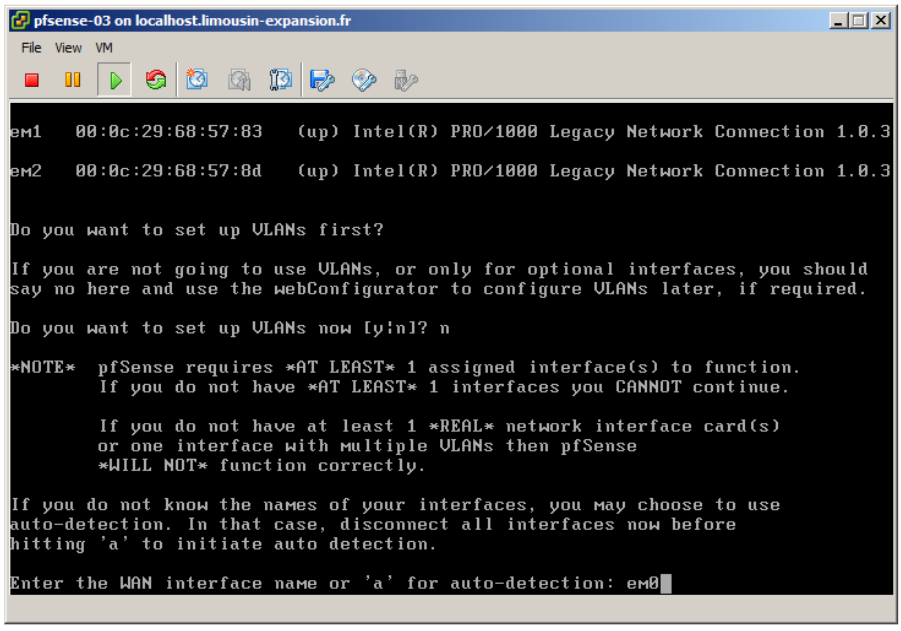

FIGURE I.11 – pfSense : assignation de l'interface WAN

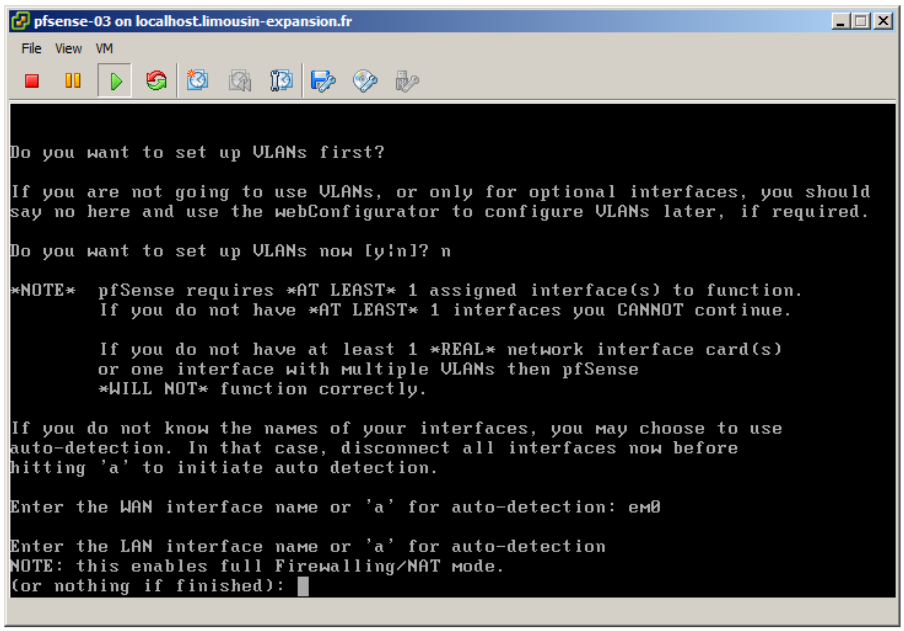

FIGURE I.12 – pfSense : assignation de l'interface LAN

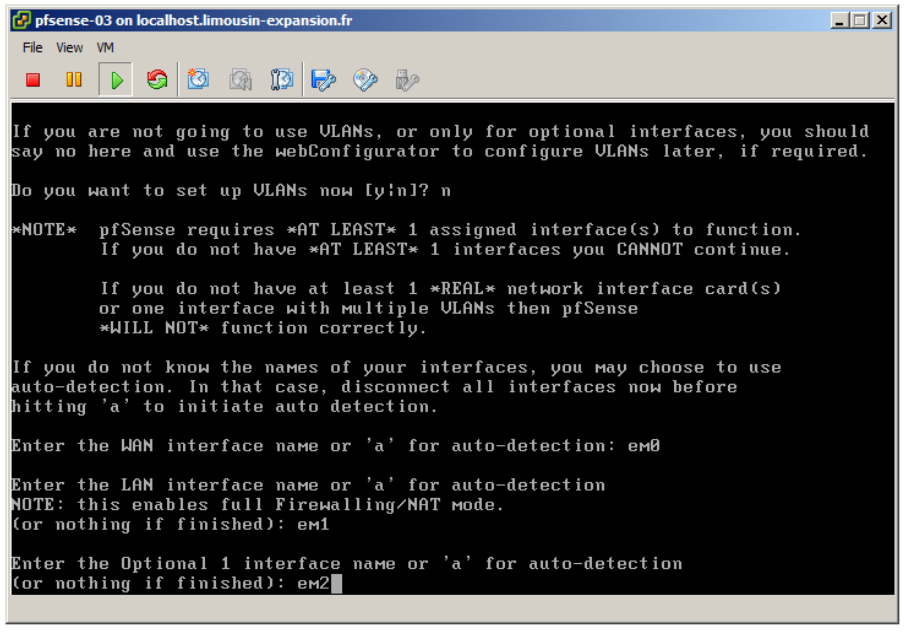

FIGURE I.13 – pfSense : assignation de l'interface OPT

– **Valider** la prise en compte des paramètres fournis par la touche **[y]** ;

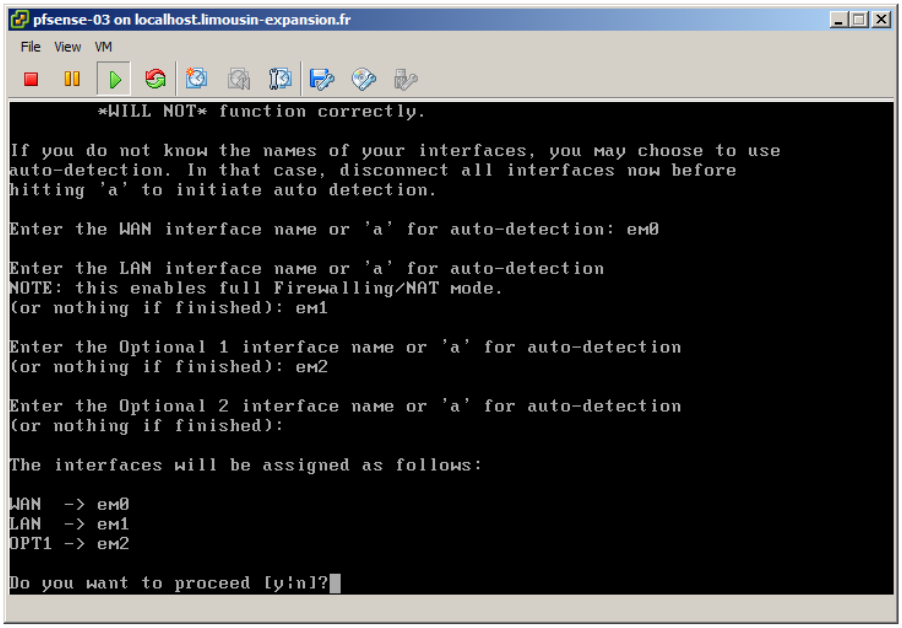

FIGURE I.14 – pfSense : validation de l'installation

L'installation du firewall **pfSense** est terminée. Nous retrouvons un menu d'administration et un récapitulatif de la configuration des `NICs` (cf. figure I.15).

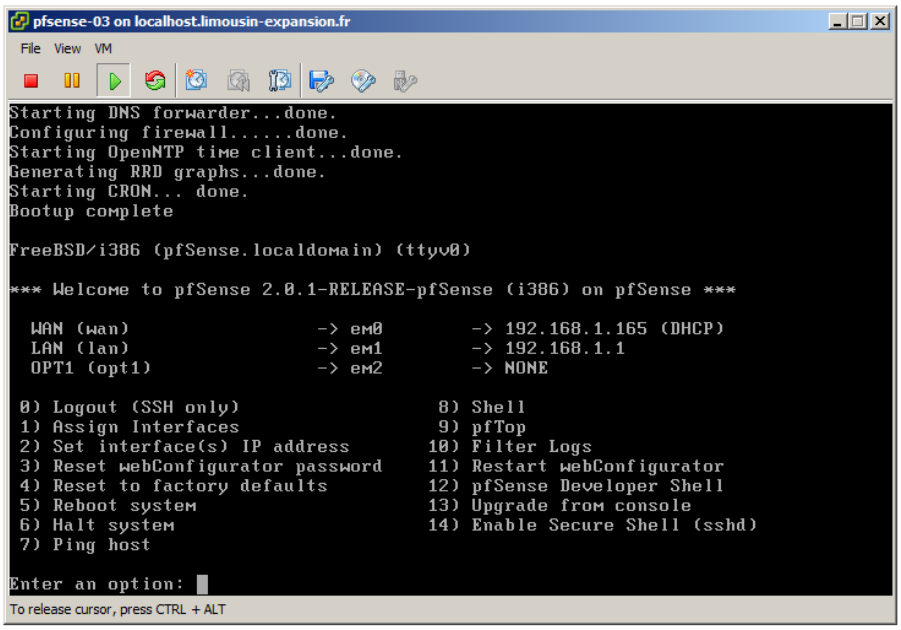

FIGURE I.15 – pfSense : installation terminée

On s'aperçoit que les interfaces `WAN` et `LAN` sont paramétrées dans le même sous réseau. En effet, d'une part le réseau dans lequel cette mise en pratique est effectuée dispose d'un serveur DHCP sur le routeur situé dans le `vlan 1 : WAN` (cf. I.1 page 6, et d'autre part **pfSense** attribue par défaut l'adresse IP `192.168.1.1` à sa patte `LAN`.

Afin d'administrer le **pfSense** par son interface `LAN`, nous devons changer son adresse IP par la console

d'administration.

Ajustez les paramètres réseaux en fonction de votre besoin.

- **Sélectionner** le choix **[2) Set interfaces IP address]** ;
- **Sélectionner** le choix **[2) LAN]** pour sélectionner l'interface correspondante au réseau local ;
- **Saisir** l'adresse IP `192.168.2.254` pour notre exemple ;
- **Saisir** le masque de sous réseau sous la forme CIDR[6] `24` pour notre exemple ;
- **Répondre oui** à la demande d'activation d'un service `DHCP` ;
- **Saisir l'adresse de début et de fin** de la plage du service `DHCP` ;
- Enfin, **Répondre oui** lorsque pfSense vous demande de revenir à un protocol `http` pour accéder à l'interface d'administration ;
- Pour terminer, **Cliquer** sur **[Entrée** pour revenir à la console d'administration ;

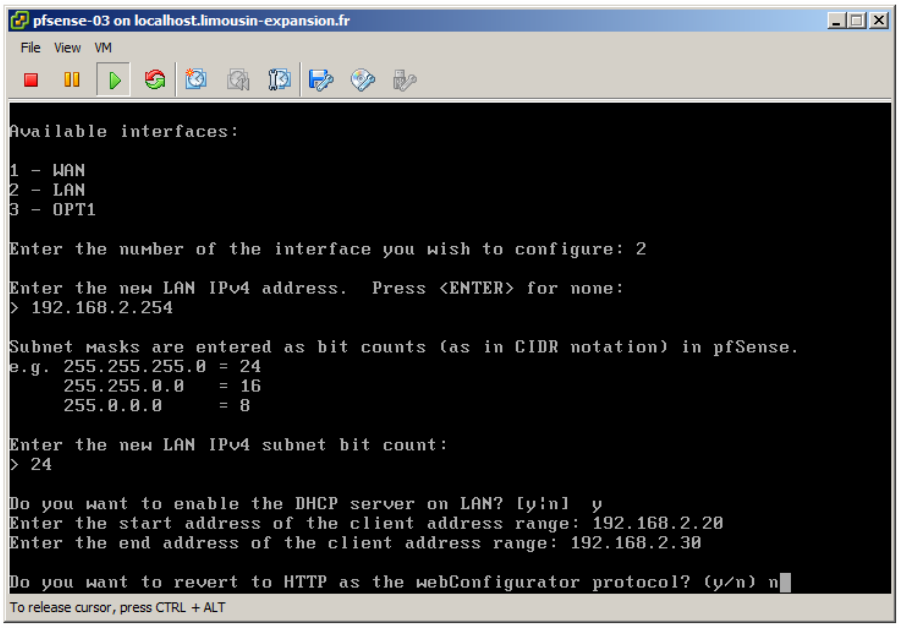

FIGURE I.16 – pfSense : configuration de l'interface LAN

6. Classless Inter-Domain Routing

Chapitre II

Configuration initiale

I Application des paramètres de base

La première étape concerne la connexion à l'interface d'administration. Par défaut, et en fonction des choix réalisés lors de la dernière phase d'installation du firewall, **pfSense** est accessible en `http(s)` à l'aide du couple *login/mot de passe* suivant :

- Nom d'utilisateur : admin
- Mot de passe : pfsense

Nous allons ici paramétrer la base de la configuration de notre firewall. Ces paramètres sont regroupés dans le menu **[System]**.

1. Menu System

À l'aide des directives accessibles depuis le menu **System | General Setup**[1] :

1. **Nommer** le nom du firewall par la directive hostname : *pfSense-01* ;
2. **Indiquer** ensuite le domaine du firewall par la directive domain : `mondomaine.tld;`
3. **Indiquer** l'adresse du ou des serveurs DNS de votre réseau : `192.168.1.250;`
4. **Ajuster** le fuseau horaire à l'aide du menu déroulant Time zone : `Europe/Paris;`
5. **Valider** les changements par le bouton **Save** ;

> `Remarque :` L'option Allow DNS server list to be overridden by DHCP/PPP on WAN garantit que toutes les requêtes DNS qui ne pourraient être résolues en interne sont transmises et résolues par les serveurs DNS externes fournis par votre FAI.

1. Adapter ici les informations en fonction de vos besoins

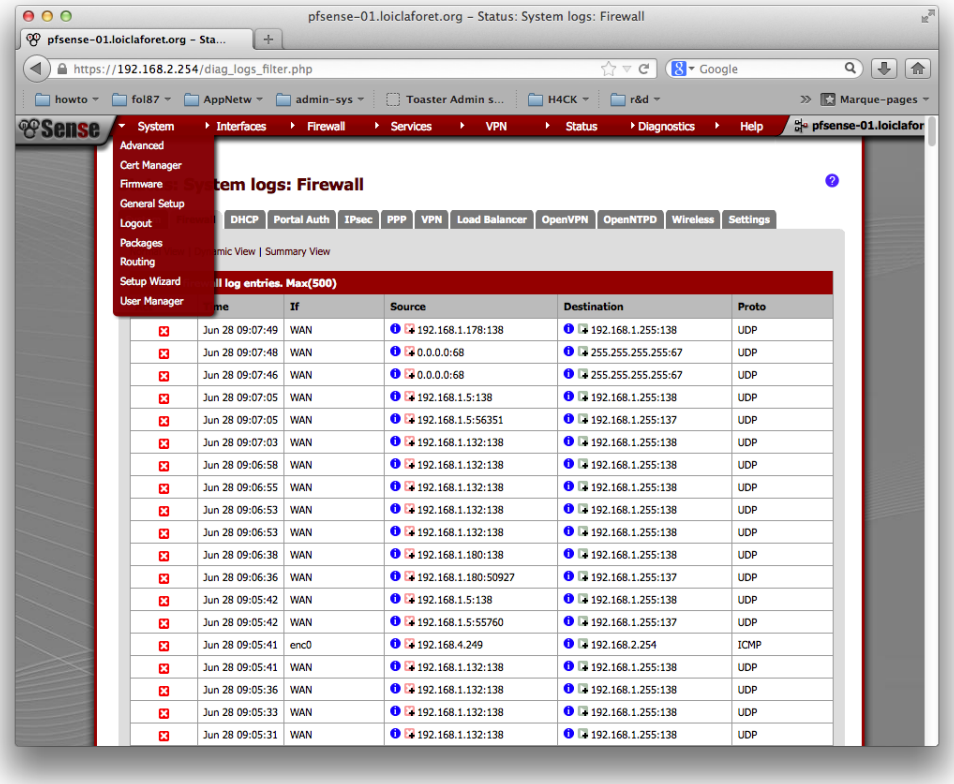

FIGURE II.1 – Menu System

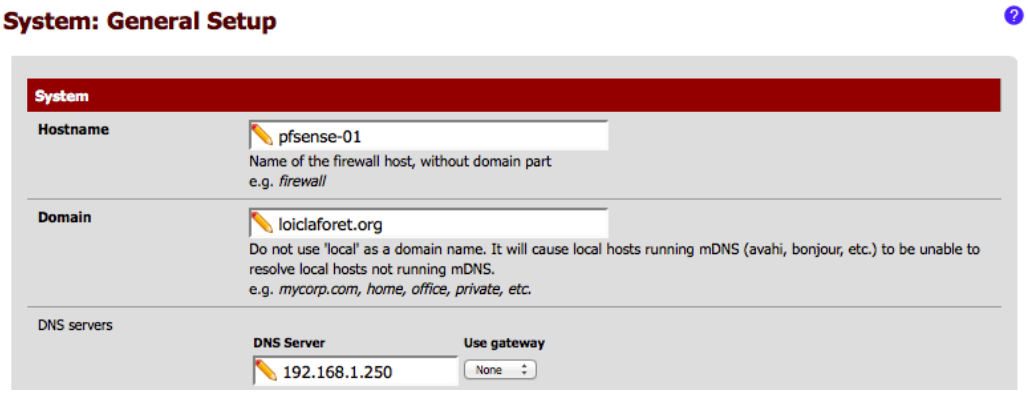

FIGURE II.2 – Menu System : general setup

Nous nous rendons maintenant dans le menu **System | Advanced** afin de basculer sur un protocole chiffré pour accéder au **pfSense**. Il est en effet préférable d'utiliser un protocole chiffré de manière générale, et indispensable lorsqu'il s'agit d'accéder à l'interface d'administration d'un firewall.

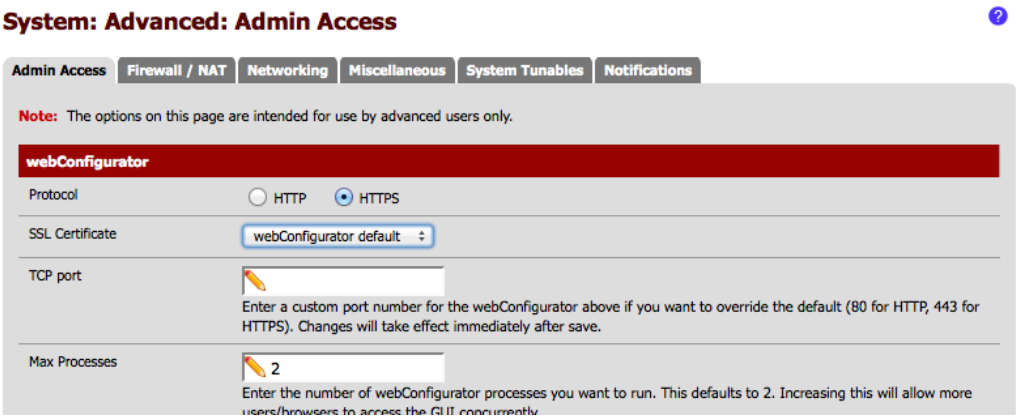

FIGURE II.3 – Menu System Advanced : activation du protocole https

Après l'activation du protocole `https`, l'interface d'administration se recharge automatiquement et bascule sur le protocole chiffré.

a. Activation de SSH

`SSH` est un protocole réseau qui permet d'établir une communication chiffrée entre deux appareils. L'activation de `SSH` permet un accès sécurisé à la console de **pfSense** à distance, comme si vous étiez physiquement devant la console.

- **Cliquer** sur **System | Advanced | Secure Shell** ;
- **Cocher** la case **Enable Secure Shell** ;
- Il est obligatoire de s'authentifier lors de l'établissement d'une connexion au service `SSH` de **pfSense**. Utiliser les login/mot de passe habituels.

> `Remarque :`
> Le fait de cocher **Disable password login for Secure Shell** permet d'activer la fonction d'authentification par clé privée RSA à la place du simple login/password. (non décrit dans cette version)

b. Bonnes pratiques

Voici une liste (non exhaustive) des bonnes pratiques à appliquer lors de l'installation d'un firewall **pfSense**.

- Toujours sélectionner un accès par le protocole `HTTPS` ;
- Se créer éventuellement un certificat sur mesure et spécifique au serveur ;
- Désactiver la redirection automatique (WebGUI Redirect), pour forcer le `HTTPS`, et ne pas répondre sur le HTTP ;
- Désactiver l'option Anti-lockout **une fois** que toutes les règles de firewall seront convenablement écrites ;
- Conserver la règle DNS Rebinding Checks ainsi que HTTP_REFERER ;

– Si souhaité, possibilité d'activer l'accès par SSH en préférant un accès via une clé RSA ;
– Sauvegarder la configuration à chaque changement, conserver un versionning ...

Nous allons maintenant configurer l'interface `WAN` de notre firewall, pour permettre à nos utilisateurs situés dans le `LAN` d'accéder à Internet.

2. Menu Interfaces

Nous avons vu lors de la phase de configuration des NICs que **pfSense**, comme n'importe quel autre système d'exploitation, référence chacune de ses interfaces réseaux NIC par une valeur unique (par exemple : fxp0, em0, em1, et ainsi de suite). Cette référence unique, régulièrement associée au pilote de la ressource matérielle, est utilisée pour simplifier, pour nous humains, l'identification des interfaces réseaux, plutôt que l'adresse MAC associée (00 :0c :29 :68 :57).

L'interface `WAN` est le lien avec le monde extérieur. Il est nécessaire ici de disposer des éléments nécessaires pour permettre à l'interface de joindre le réseau Internet. Pour modifier ces paramètres :

– **Cliquer** sur **Interfaces | WAN** ;
– **Changer** le type de l'interface en `static` ;
– **Laisser** inchangées les directives MAC Address, MTU, MSS et Private Network ;
– **Ajuster** l'adresse IP et le masque de sous réseau : `192.168.1.254/24` ;
– **Créer** à l'aide du lien add a new one la gateway correspondante au routeur de votre réseau : `192.168.1.250` ;
– **Valider** les changements par le bouton **Save** ;

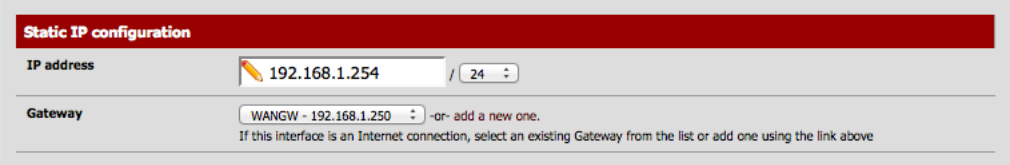

FIGURE II.4 – Menu Interfaces : configuration de l'interface WAN

L'exemple que nous avons réalisé est typique de beaucoup d'environnements. En plaçant notre firewall comme la seule machine possédant un accès direct à Internet, nous sécurisons notre environnement en établissant un contrôle complet sur le trafic qui circule dans et sort de nos réseaux. Tout le trafic doit passer à travers notre **pfSense** et ainsi respecter nos règles de firewall.

La connexion Internet étant normalement établie, nous pouvons vérifier l'état de l'interface `WAN`, en sélectionnant le menu **Status | Interfaces** (cf. figure II.5).

Nous avons, lors de la phase d'installation du **pfSense** paramétré l'adresse IP de l'interface `LAN`. Si ce n'est pas le cas, modifier les paramètres en reprenant les éléments décrits par la figure I.16, page 15.

Penchons nous sur l'interface nommée `OPT1`. Ce réseau *en option* créé par nos soins lors de la génération de la machine virtuelle et lors de la phase d'installation du **pfSense** est communément appelé une `DMZ` [2]. L'idée est tirée du concept militaire d'une zone démilitarisée, dans laquelle une partie du trafic est explicitement autorisée à passer et une partie du trafic ne l'est pas. L'idée est donc que cette partie du réseau soit entièrement contrôlée mais surtout isolée des autres réseaux.

Lorsqu'il est appliqué à des réseaux informatiques, un réseau DMZ suit ce modèle :
– *Trafic Internet | <- DMZ <- LAN trafic*

2. Zone démilitarisée

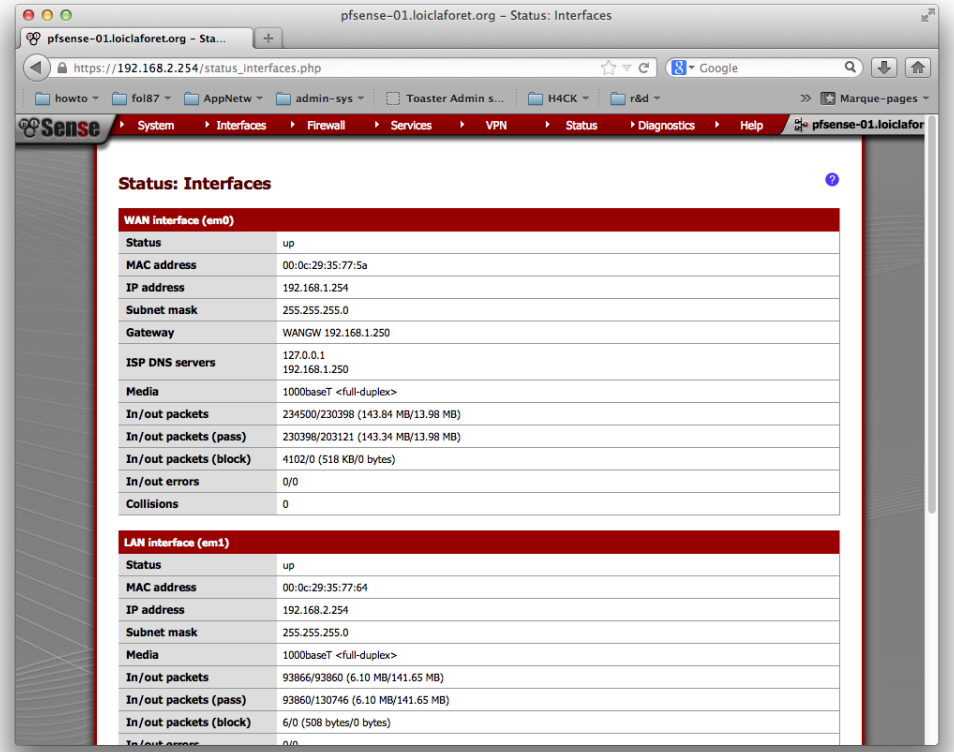

FIGURE II.5 – Menu Status : interface WAN

Le trafic Internet non sécurisé est autorisé à entrer dans la zone démilitarisée, pour accéder à un serveur web par exemple. Le trafic depuis le `LAN` peut entrer dans la `DMZ`, afin d'accéder au serveur web également. Toutefois, la clé réside dans la dernière règle : le trafic de la `DMZ` **n'est pas autorisé à entrer** dans le réseau local `LAN`.

Le zone `DMZ` est donc un réseau *moins sécurisé*, où nous allons explicitement permettre certains accès par l'ouverture de ports par exemple. La condition pour configurer une `DMZ` est de disposer d'une interface réseau.

Nous allons donc ici configurer l'interface `OPT1` en tant que `DMZ` :

- **Cliquer** sur **Interfaces | OPT1** pour sélectionner l'interface ;
- **Cliquer** sur **Enable** pour l'activer ;
- **Nommer** l'interface à l'aide de la directive Description : `DMZ` ;
- **Changer** le type de l'interface en `static` ;
- **Ajuster** l'adresse IP et le masque de sous réseau : `192.168.3.254/24` ;
- **Laisser** vide les champs et choix Gateway, Block Private networks et Block bogon networks [3] ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;

3. Permet de bloquer les adresses IP privées, et les adresses IP sources reservées ou non attribuées par l'IANA

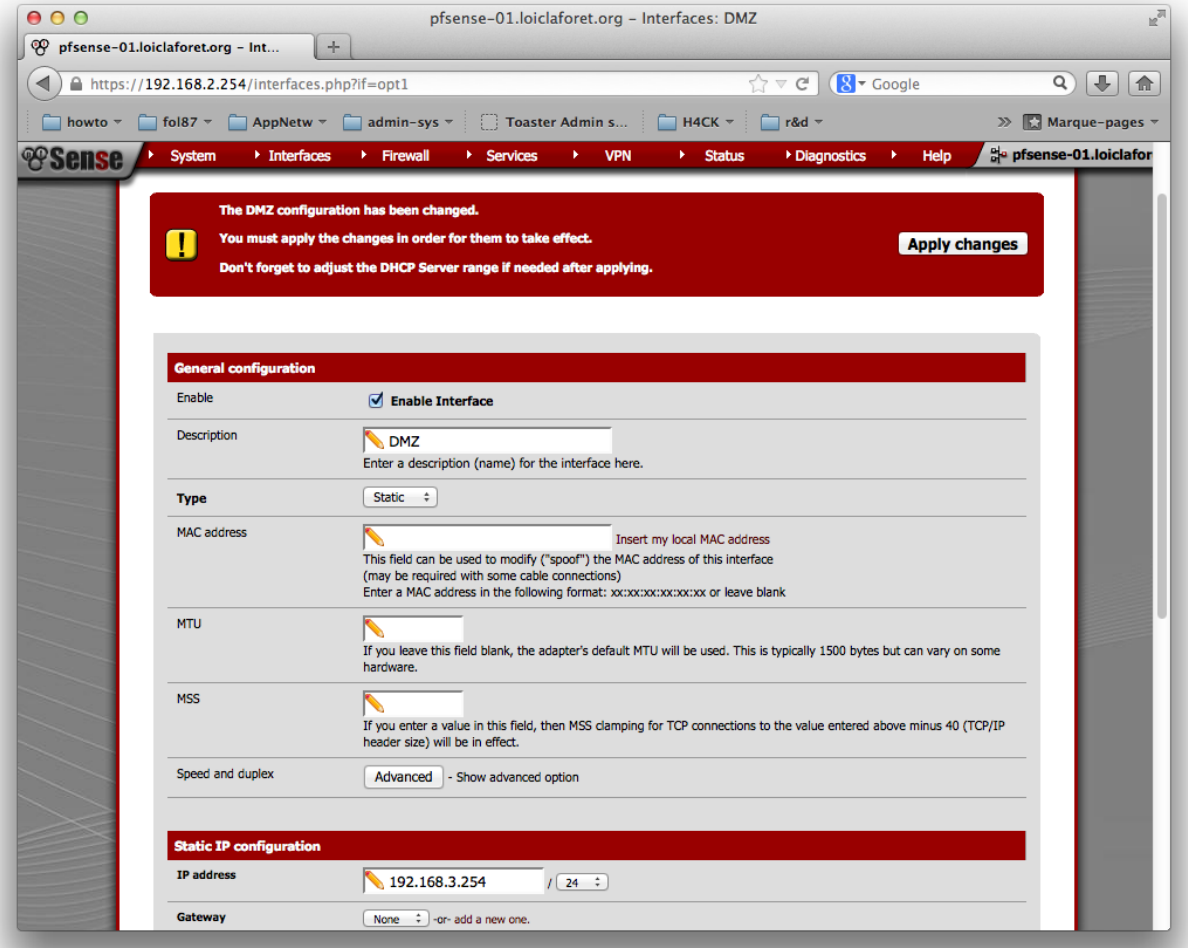

FIGURE II.6 – Menu Interfaces : configuration d'une DMZ

3. Mise à jour

Il est possible de mettre à jour le firmware de pfSense automatiquement depuis son interface web. Cette procédure permet de s'abstenir de réaliser une surveillance accrue des correctifs de sécurité par exemple.

La configuration de la mise à jour automatique s'effectue par le menu **System | Firmware | Updater Settings** ;

- Depuis le menu déroulant, **sélectionner** la version du pfSense déployé ;
- **Valider** les changements par le bouton **Save** ;

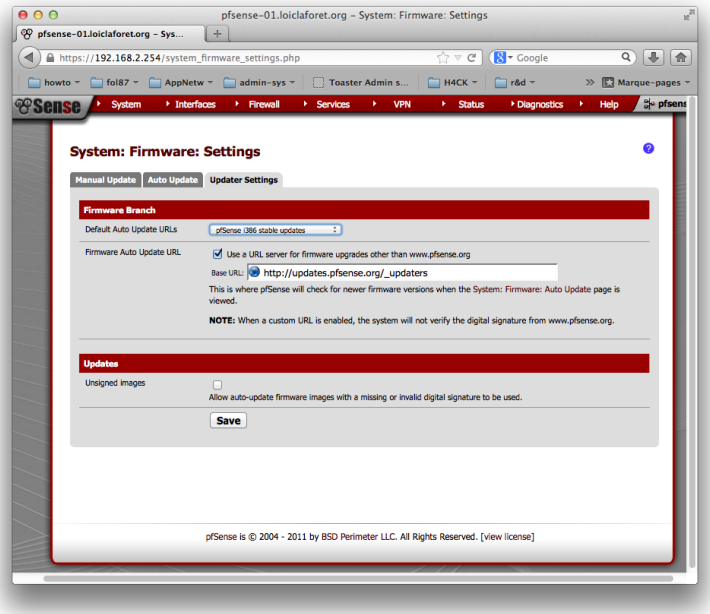

FIGURE II.7 – Menu System : mise à jour du firmware

Il est possible de visualiser le status du firmware depuis la page d'accueil, appelé `Dashboard` par **pfSense**.

FIGURE II.8 – Dashboard : status du firmware

Passons dans le vif du sujet et attaquons les services de base fournis par **pfSense**.

4. Sauvegarde et Restauration

pfSense fournit la possibilité de sauvegarder tout ou partie de sa configuration. Comme l'illustre la figure II.9 il est possible d'extraire au format *xml* la totalité de la configuration du firewall, plugins compris.

- **Cliquer** sur le bouton **Download configuration** et **Enregistrer** le fichier sur une ressource locale ou réseau ;
- **Cliquer** sur parcourir, **sélectionner** le fichiers de configuration et **cliquer** sur le bouton **Restore configuration** pour effectuer une restauration du firewall ;

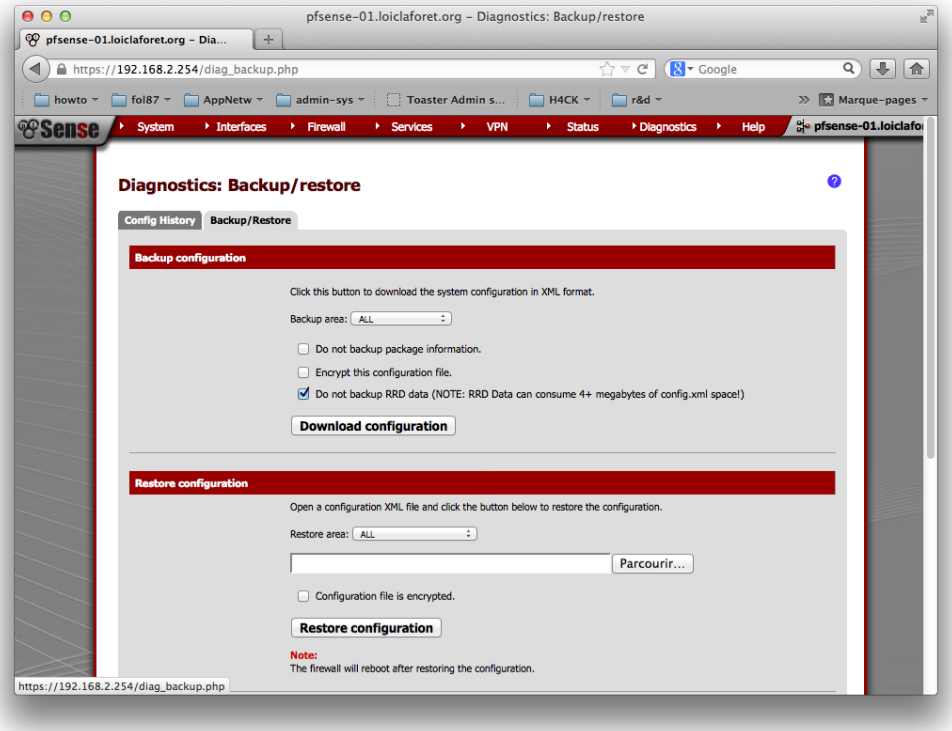

FIGURE II.9 – Menu Diagnostics : backup / restore

Chapitre III

Services fondamentaux

Après l'installation de **pfSense** et les différentes étapes de configurations initiales du chapitre précédent, nous possédons désormais une structure de base de notre système exploitable.

Nous sommes ainsi prêts à commencer à configurer les services réseaux fondamentaux que notre **pfSense** fournira.

I Configuration du DHCP serveur

Nous l'avons vu lors de l'installation du firewall, **PfSense** peut jouer le rôle de serveur `DHCP`, mais uniquement pour les interfaces configurées à l'aide d'une adresse IP statique.

Pour activer le service `DHCP` :

- **Cliquer** sur **Services** | **DHCP Server** pour accéder à l'interface d'administration du service ;
- **pfSense** nous propose alors de sélectionner l'interface sur laquelle nous souhaitons activer le service `DHCP`. Il est donc possible d'activer un service `DHCP` par interface physique et/ou virtuelle ;
- **Sélectionner** l'interface **LAN** ;
- Nous retrouvons les éléments pré-configurés lors l'installation du firewall ;
- Si vous n'avez pas réalisé cette opération lors de l'installation, ou si vous souhaitez configurer le service pour une autre interface :
- **Cliquer** sur la case **Enable DHCP on XXX Interface** ;
- **Spécifier** l'étendue de votre service `DHCP` par l'intermédiaire des 2 directives range : `192.168.2.10` et `192.168.2.20` - prenez soin de respecter le réseau sur lequel votre interface est paramétrée ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;
- Tester l'opération connectant un équipement dans le réseau correspondant à l'interface `LAN` par exemple ;

1. Configuration d'une réservation d'adresse

De manière simplifiée, un serveur DHCP répond à une demande d'un client en lui fournissant la première adresse IP de sa plage disponible. Il est ainsi très probable que le client recevra une adresse IP différente à chaque requête. Pour garantir au client la même adresse IP, **pfSense** propose de créer un *mapping* (correspondace) entre l'adresse MAC du client et une adresse IP statique. Pour effectuer cette opération :

- **Cliquer** sur le **[symbole +]** situé en bas de la page de configuration du service DHCP ;
- **Renseigner** l'adresse MAC de l'équipement ;
- **Renseigner** éventuellement l'adresse IP souhaitée, en dehors de l'étendue préalablement définie ;
- **Saisir** un nom de machine et une description ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;
- Pour tester l'opération, **forcer** le renouvellement du bail de votre équipement ;

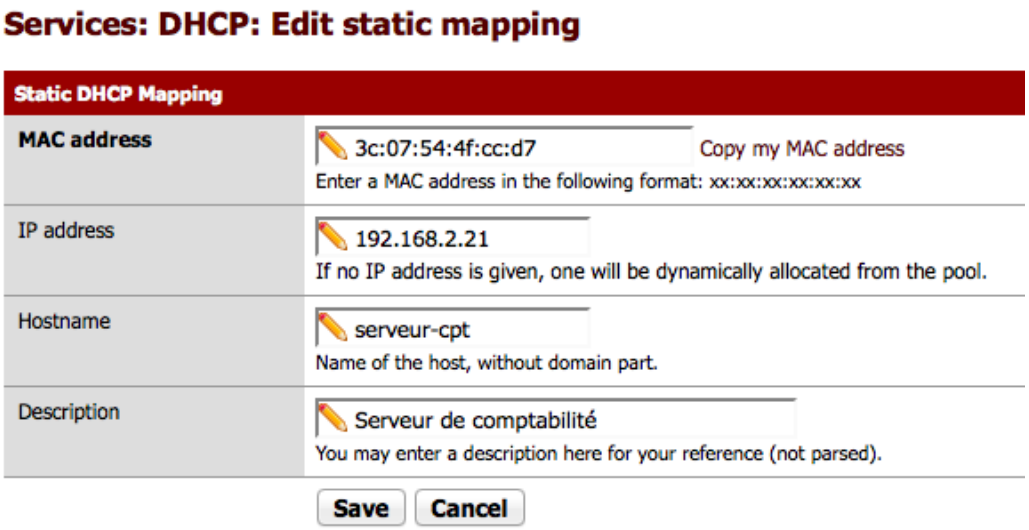

FIGURE III.1 – Service DHCP : Réservation d'adresse pour un équipement

Les autres options possibles sont :

Deny Unknown Clients :

L'activation de cette option permet de s'assurer que seuls les clients possédant explicitement un mappage statique sur le service DHCP recevront une adresse IP. Toutes les requêtes DHCP des clients non référencés seront ignorées.

DNS Servers :

Permet de spécifier un ou plusieurs serveur DNS lors de l'attribution des baux aux clients DHCP. Si le champ est laissé vide, **pfSense** attribuera automatiquement les serveurs DNS en fonction de :

1. si le DNS Forwarder est activé, l'adresse IP de l'interface sera utilisée en tant que serveur DNS.
2. Si le DNS Forwarder n'est pas activé, alors ce seront les serveurs DNS spécifiés dans la configuration générale de **pfSense** qui seront spécifiés.

Gateway :

De manière systématique, c'est l'adresse IP de l'interface de pfSense qui est spécifiée comme gateway aux clients. Dans des configurations inhabituelles, il est possible de forcer une autre gateway.

Domain Name :

C'est le domain name spécifié dans la configuration générale de **pfSense** qui est spécifié ici. Il est également possible de modifier le domaine de recherche préféré des clients en modifiant cette directive.

2. Configuration du DHCP relai

Le `relai DHCP` est une alternative au serveur `DHCP` décrit à la section I. Le service `relai DHCP` permet de spécifier un serveur DHCP existant pour tout ou partie des interfaces gérées par **pfSense**. Si vous exploitez et maintenez un serveur `DHCP` sur votre réseau local, vous ne souhaiterez certainement pas basculer ce service sur votre firewall. Le service `DHCP relai` fournit ainsi la possiblité pour chaque interface de votre choix de spécifier le serveur `DHCP` existant. **pfSense** transfèrera ainsi toutes les requêtes des clients depuis les interfaces spécifiées vers le serveur existant (cf. III.2).

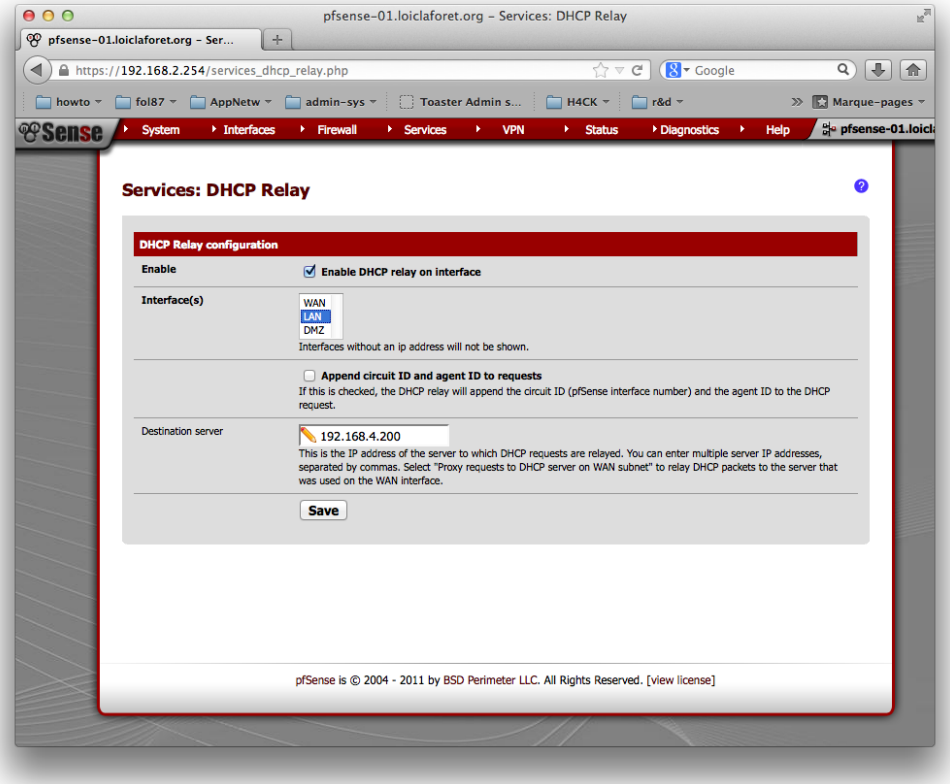

FIGURE III.2 – Service DHCP Relay : Configuration du relai DHCP

II Spécifier des serveurs DNS

Concernant la résolution des noms `DNS`, la plupart des environnements s'appuient sur les serveurs `DNS` fournis par le fournisseur d'accès Internet via leur connexion `WAN`. Par défaut, aucun serveur `DNS` n'est défini sur **pfSense** l'option Allow DNS server list to be overridden by DHCP/PPP on WAN est cochée dans le menu **System | General Setup**.

Toutefois, il est possible de spécifier manuellement les serveurs DNS ainsi :

- **Accéder** au menu **System | General Setup** ;
- La section `DNS` contient les paramètres suivant :
  - **Renseigner** l'adresse IP du serveur `DNS` ;
  - **Décocher** l'option Allow DNS server list to be overridden by DHCP/PPP on WAN ;
- **Sauvegarder** les changements ;

– **Appliquer** si besoin ;

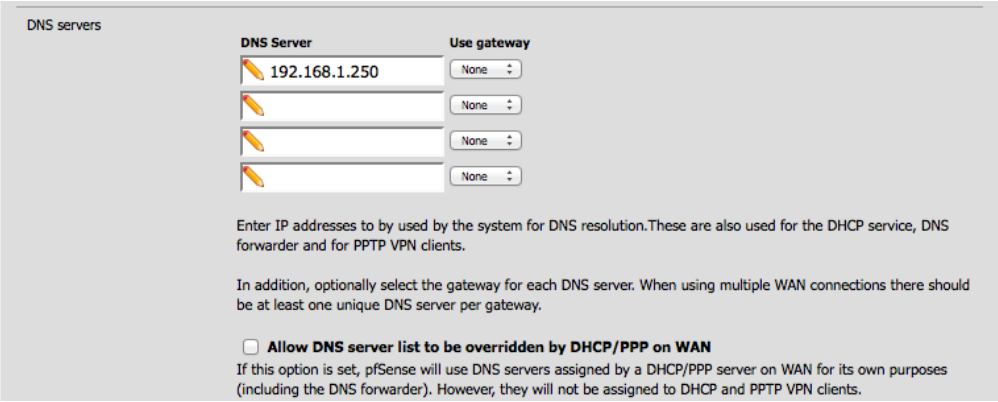

FIGURE III.3 – Menu System : spécifier un serveur DNS

III Activer le DNS forwarder

Le **DNS forwarder** de **pfSense** permet de résoudre les requêtes DNS des clients DHCP (mappés ou non) ainsi que des entrées DNS saisies manuellement. Le **DNS forwarder** permet également de renvoyer les requêtes DNS des clients pour un domaine particulier.

– **Accéder** au menu **Services | DNS Forwarder | Enable DNS Forwarder** ;
– Si l'option **Register DHCP leases in DNS Forwarder** est active, toutes les entrées présentes dans le *lease* du serveur seront joignables directement par le service **DNS Forwarder** ;
– Si l'option **Register DHCP static mappings in DNS Forwarder** est active toutes les correspondances *adresses MAC - adresses IP* présentes dans la configuration du service DHCP seront joignables directement par le service **DNS Forwarder** ;
– Il est possible d'ajouter une entrée de type *poste* ou *domaine* directement par l'intermédiaire des **boutons +**, en bas de la page. L'ajout d'entrées dans ces sections aura pour effet de *bypasser* la résolution de nom habituelle pour leur résolution ;
– **Sauvegarder** les changements ;
– **Appliquer** si besoin ;

Chapitre IV

Configuration générale

La fonctionnalité de base de n'importe quel firewall implique la création de règles de sécurité et des redirections de ports, et **pfSense** n'échappe pas à la règle. L'ensemble de ces fonctionnalités de base, et quelques autres ont été regroupées dans le menu **Firewall** de l'interface web de **pfSense**.

Ce chapitre décrit comment configurer ces règles et les caractéristiques qui leur sont associées.

I Les alias

Un pré-requis avant d'entrer dans le vif du sujet des règles de firewalling concerne l'utilisation *d'Alias*. Nous allons créer ces alias pour créer des objets (variables) que nous utiliserons lors de la génération des règles, `NAT port-forwarding` ... Ce service facilitera la manipulation et l'écriture des règles.

Les alias améliorent ainsi la lecture des règles et permettent de regrouper des adresses IP, des ports, des réseaux ou encore des `URL`. Leur utilisation nous évitera, par exemple, pour un protocole donné, d'avoir à écrire une règle pour chaque port dans le cas de ports non consécutifs.

Cela nous permettra de réaliser une seule modification d'un groupe de port ou d'hôtes par exempe, et celle-ci sera répercutée automatiquement sur l'ensemble des règles faisant appel à l'alias.

On voit ici l'intérêt de préparer convenablement le terrain lors du déploiement d'une telle solution. L'audit ou la construction d'un cahier des charges précis est un réel atout lors du déploiement d'un firewall.

> `Attention :`
> Les caractères spéciaux comme le `trait d'union "-"` ne sont pas autorisés.

- **Se rendre** dans le menu **Firewall** | **Alias** ;
- **Cliquer** sur le **bouton +** ;
- **Saisir** le nom de l'alias à créer ;
- **Indiquer** une description du type et du contenu de l'alias ;
- **Spécifier** le type de l'alias (hôte(s), port(s), réseau(x)), URL ou URL Table) ;
- **Ajouter** à l'aide du **bouton +** la ou les entrées correspondantes à l'alias ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;

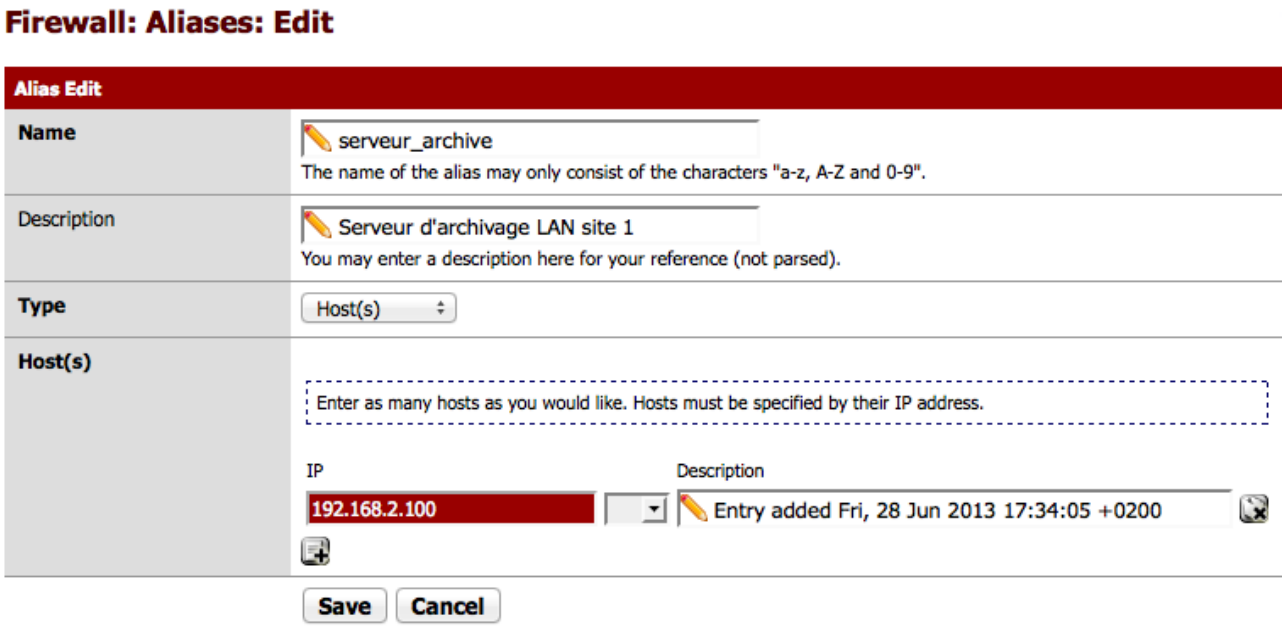

FIGURE IV.1 – Firewall Aliases : Création d'un alias

`Remarque :`
La sélection du type d'alias **URL Table** vous permet de créer un alias détenant une `URL` unique pointant vers une liste d'adresses. Cela peut être particulièrement utile lorsque vous avez besoin d'importer une liste importante d'adresses IP ou de sous-réseaux.

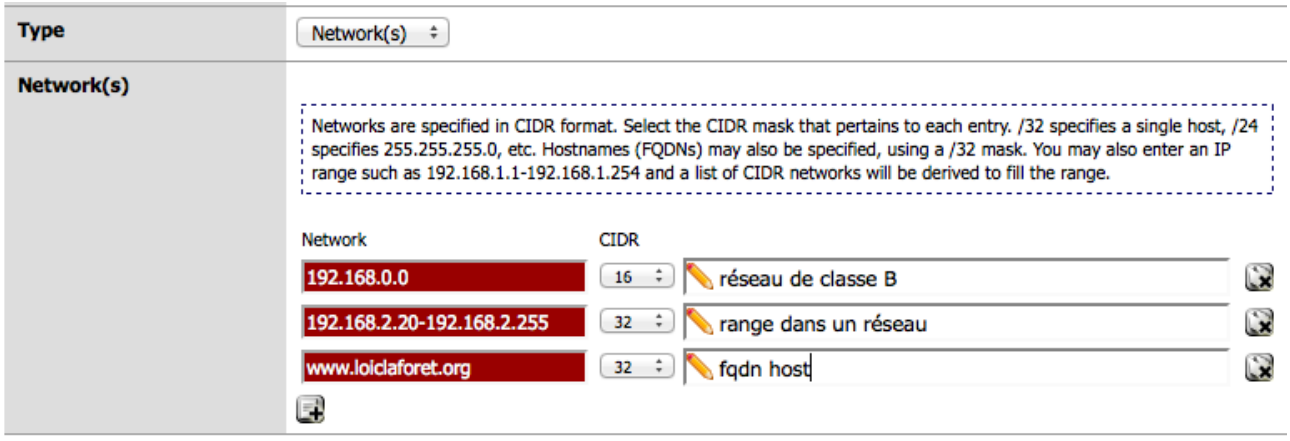

FIGURE IV.2 – Firewall Aliases : Création d'un alias de type réseau

La figure IV.6 illustre les possibilités offertes par pfSense pour administrer les alias.

- le **bouton +** permet d'ajouter une entrée ;
- le **bouton e** permet d'éditer une entrée ;
- le **bouton x** permet de supprimer une entrée ;
- le **bouton flèche vers le haut** permet, lorsqu'une règle est sélectionnée, de modifier le rang dans la liste ;

Vous retrouverez ce principe pour l'ensemble des éléments (règles notamment) administrés par **pfSense**.

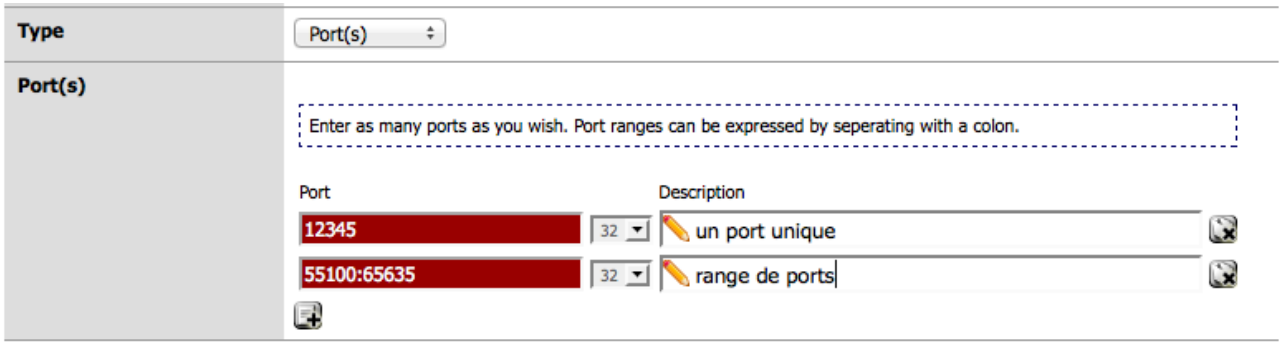

FIGURE IV.3 – Firewall Aliases : Création d'un alias de type port

FIGURE IV.4 – Firewall Aliases : Création d'un alias de type url

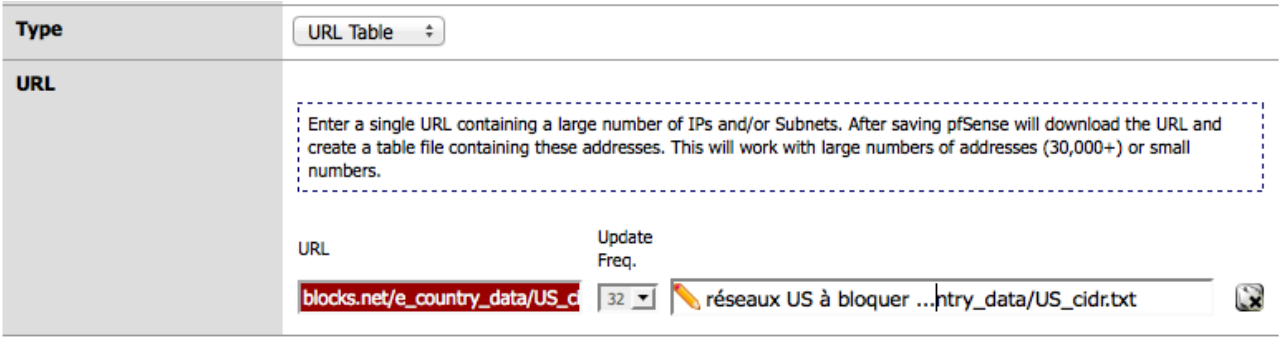

FIGURE IV.5 – Firewall Aliases : Création d'un alias de type url table

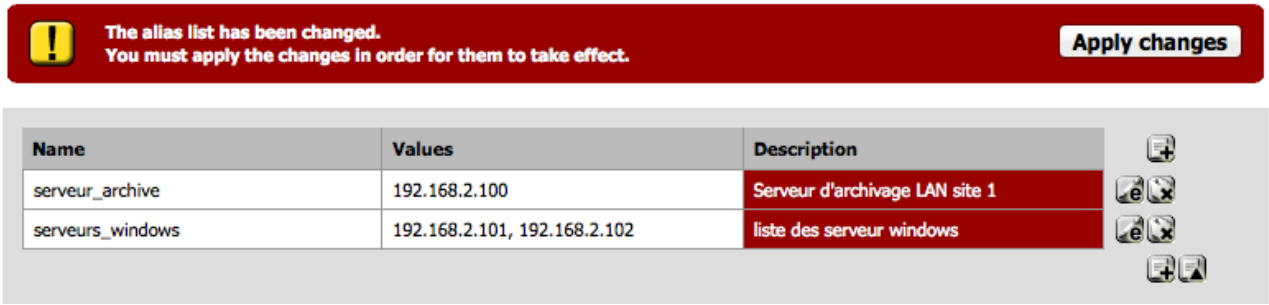

FIGURE IV.6 – Firewall Aliases : Administration des alias

II Création d'une règle de NATP / port forwarding

La complexité des règles de redirection de port (NATP[1]) peut varier considérablement. Chaque aspect d'une règle est détaillé dans la section suivante. Pour l'exemple, voici un scénario typique : nous allons créer une redirection de port afin de transférer toutes les requêtes Web entrantes sur le protocole `HTTP` vers un hôte préalablement configuré comme serveur web.

- **Se rendre** dans le menu **Firewall | NAT** ;
- **Cliquer** sur le **Port Forward** ;
- **Cliquer** sur le **bouton +** ;
- **Sélectionner** dans la directive Destination port range le protocole `HTTP` dans les deux listes déroulantes (*from* et *to*) ;
- **Indiquer** l'adresse IP ou l'alias correspondant à un serveur Web par la directive Redirect target IP : `192.168.2.159`, ou `serveur_web` ;
- **Sélectionner** pour la directive Redirect target port le protocole `HTTP` dans la liste déroulante ;
- **Ajouter** une description ;
- **Laisser** les choix par défaut pour les listes use system default et Filter rule association ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;

Le symbole situé à gauche de la règle de **Port Forward** nouvellement créé indique que cette règle est liée à une autre règle. Pour visualiser la règle correspondante, il suffit d'afficher les règles de firewalling par le menu **Firewall | Rules | WAN**.

1. Network Address and Port Tranlation

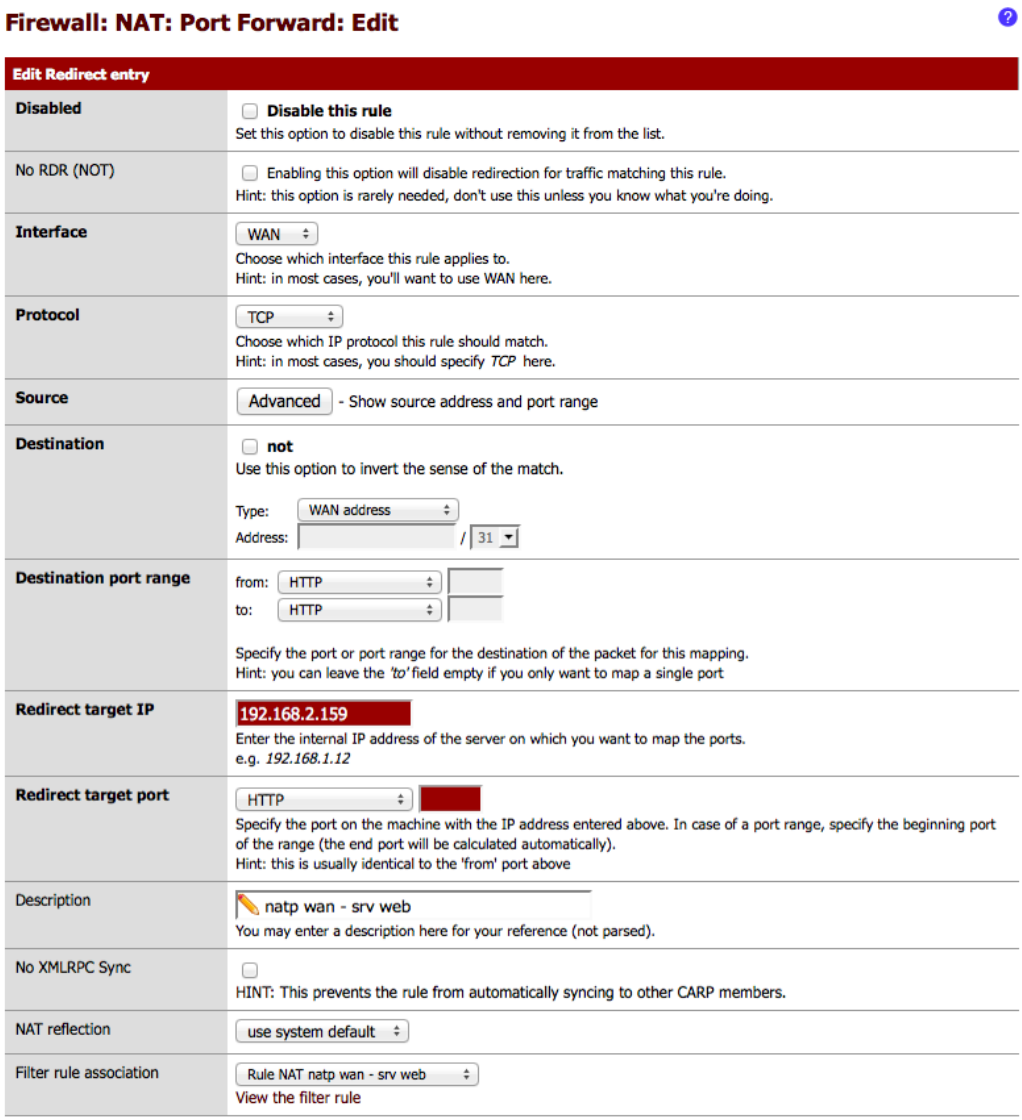

FIGURE IV.7 – Firewall NATP : Création d'une redirection d'un port

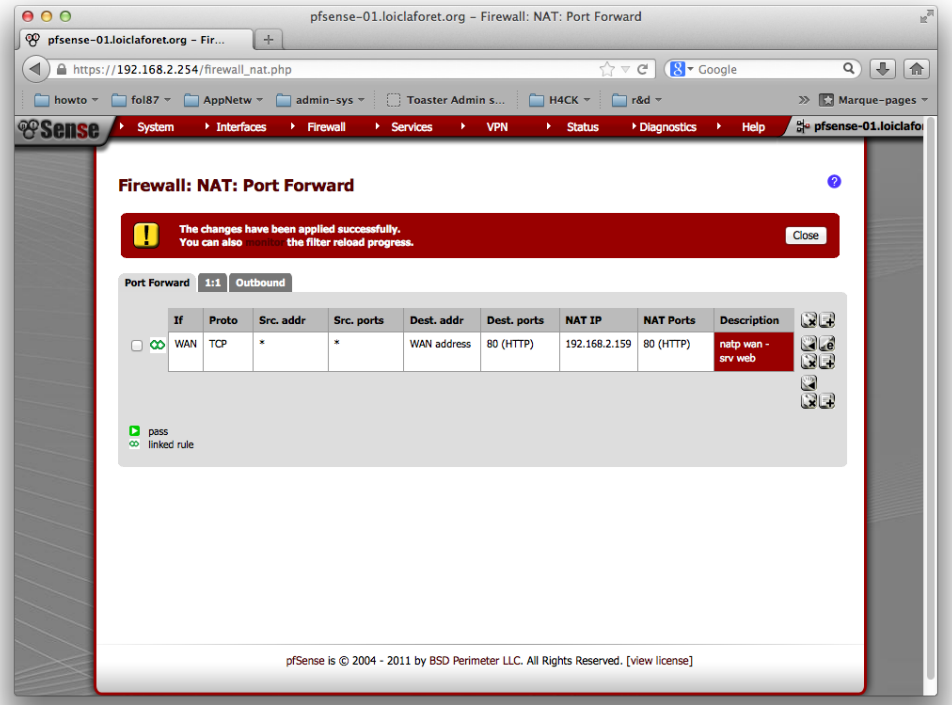

FIGURE IV.8 – Firewall NATP : Rendu d'une redirection d'un port

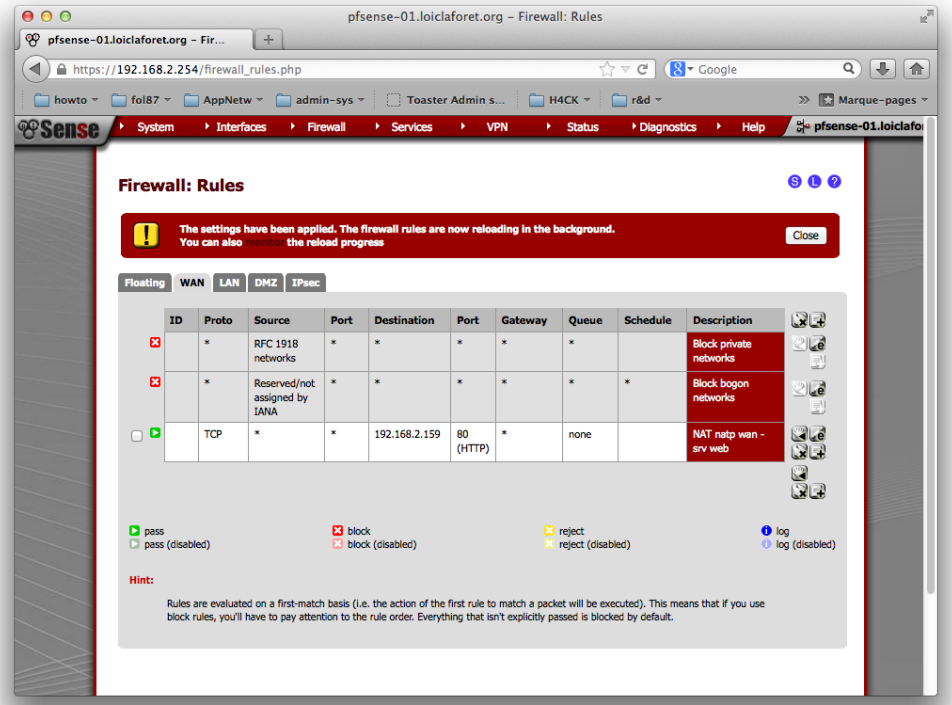

FIGURE IV.9 – Firewall NATP : règle de firewall associée à une redirection de port

Les règles de NAT peuvent être configurés à l'aide d'une variété d'options, dont voici un rapide descriptif pour chaque élément :

Disabled :

Active ou désactive la règle de NAT.

No RDR (NOT) :

L'activation de l'option permet de désactiver la redirection du trafic.

Interface :

Spécifie l'interface sur laquelle la règle NAT se base (généralement l'interface `WAN`).

Protocol :

Indique le protocole de la règle `NAT`. Généralement nous retrouvons `TCP`, `UDP ou TCP/UDP` , mais nous pouvons également choisir GRE [2] et ESP [3].

Source :

La source est généralement laissée à la valeur par défaut **All**, mais il est possible de spécifier une adresse ou un réseau source spécifique.

Source port range :

Généralement, la plage de port source est laissée à la valeur par défaut à **All** mais il est possible de spécifier les ports si nécessaire.

Destination :

Le plus souvent, la destination est laissée à la valeur par défaut de l'adresse `WAN`, (adresse IP publique), mais une alternative peut être choisie si nécessaire.

Destination port range :

C'est le port utilisé lors de la requête générée par les clients. Dans notre exemple, nous souhaitons fournir un accès vers un serveur Web, nous avons ainsi spécifié le protocole `HTTP`, présent parmi la liste des ports les plus courants. Il est cependant possible de spécifier le port de notre choix. N'oubliez pas l'utilisation d'un alias lors de la désignation des règles de NATP.

Redirect target IP :

Nous spécifions ici l'adresse IP de l'ordinateur cible sur lequel nous souhaitons rediriger le trafic.

Redirect target port :

Il s'agit du port correspondant au service fourni par l'ordinateur spécifié ci-dessus.

Description :

La description fournie ici sera copiée dans les règles de firewall (précédée de la mention `NAT`) générées de manière automatique. C'est également un aide mémoire lorsque nous devons gérer un nombre important de règles de type NATP.

No XMLRPC Sync :

L'activation de cette option peut restreindre la propagation lors de l'utilisation de firewall redondants utilisant `CARP`.

NAT reflection :

Le système l'utilise par défaut, mais elle peut être désactivée selon le règlement, si nécessaire.

Filter rule association :

Ajoute une règle de firewall automatiquement lors de la génération d'une règle de NAT.

2. Generic Routing Encapsulation
3. Encapsulating Security Payload, RFC 2406

III Création des règles de firewall

Comme nous venons de le voir dans la section précédente, une première règle de firewall a été générée lors de la création de la règle de NAT (cf. section II, page 31). Cette règle de firewall est nécessaire pour autoriser le trafic web transmis par la translation de port. Nous aurions d'ailleurs pu la générer manuellement sans passer par son automatisation. Nous aurions donc procédé ainsi :

- **Se rendre** dans le menu **Firewall** | **Rules** ;
- **Cliquer** sur l'onglet **WAN** ;
- **Cliquer** sur le **bouton +** ;
- **Sélectionner** l'action **pass** pour autoriser le trafic ;
- **Sélectionner** l'interface `WAN` ;
- **Spécifier** le protocole **TCP** ;
- **Sélectionner** **Any** pour la directive Source ;
- **Sélectionner** **Any** pour la directive Source Port Range ;
- **Saisir** l'adresse IP ou l'alias du serveur dans le formulaire Destination ;
- **Spécifier** le port web `HTTP` dans Destination Port Range ;
- **Saisir** une description de la règle dans Description ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;

Pour compléter la construction d'une règle de firewalling, nous retrouvons :

Action :

1. L'action **Block** jette les paquets alors l'option **Reject** retourne le paquet à l'envoyeur ;
2. L'option disabled

Disabled :

Permet de désactiver la règle sans la supprimer. Equivalant au petit triangle vert disponible lors de la vue générale accessible par le menu **Firewall** | **Rules**.

Interface :

Permet de sélectionner l'interface sur laquelle la règle s'applique.

Protocol :

Spécifie le type de protocole, qui peut varier en fonction du trafic de la règle.

Source :

Correspond à l'adresse ip ou réseau générateur de la requête. **Any** la plupart du temps mais peut être affinée.

Source Port Range :

Correspond aux ports sources de la requête **Any** la plupart du temps mais peut être affinée.

Destination :

Désigne généralement l'alias (ou l'adresse IP) correspondant au serveur devant traiter la requête.

Destination Port Range :

Désigne en général le port spécifique utilisé par le service hébergé par le serveur de destination.

Log :

Permet d'enregistrer la trace de tout le trafic correspondant à la règle.

Description :

Permet de fournir une description.

Remarque :
Lors de la génération d'une règle, il est important de se rappeler que la plage de ports sources est systématiquement placée sur le choix **Any**. Lorsque l'on interroge un site web, notre requête part vers le port 80 du serveur que nous souhaitons attaquer, mais c'est bien notre équipement qui décide du port à ouvrir côté client. Ce port correspond au port source, un port finalement en constante évolution et très difficilement indentifiable. Ainsi, dans 99% des cas, nous ne pourrons pas spécifier la plage de port source du trafic de nos règles.

Le firewall est la fonction principale de **pfSense**. Les règles de filtrage sont évaluées sur la base de la première correspondance. Dès qu'un paquet correspond à une règle celui-ci est filtré. Les règles les plus permissives doivent donc être placées en bas de la liste. **pfSense** est un firewall à gestion d'état (*stateful*) : il autorise le trafic depuis l'interface sur laquelle le trafic est généré. Ainsi lorsqu'une connexion est initiée, à la suite d'une correspondance réussie avec une règle autorisant explicitement le trafic, une entrée est ajoutée dans la table de gestion d'état (*state table*[4]). Le trafic retour est alors automatiquement autorisé par le firewall quelque soit le type de trafic (TCP, ICMP ...).

1. Changer l'ordre des règles

Comme nous l'avons évoqué, les règles de **pfSense** sont toujours évaluées de haut en bas. Si la première règle correspond à un trafic, elle est exécutée et le reste des règles sont évincées. La logique nous pousse donc à placer des règles très précises en haut de la liste, et les règles *plus génériques* en bas.

Pour réorganiser une règle, il faut la sélectionner, puis cliquer sur le symbole *main+flèche* situé à l'endroit où l'on souhaite déplacer la règle.

2. Dupliquer une règle

Parmi les options pratiques liées à la gestion des règles par **pfSense**, nous retrouvons la possibilité de dupliquer une règle par la création d'une règle existante. Il suffit alors de cliquer sur le **bouton +** situé à droite de la règle que nous souhaitons dupliquer. **pfSense** ouvre alors le formulaire de création de règle avec le contenu de la règle précédemment copiée. Il suffit de modifier les éléments souhaités, puis de sauvegarder la nouvelle règle.

3. Options avancées

Des options avancées existent lors de la création des règles. Il est ainsi possible de spécifier des éléments liés à la couche sept du modèle OSI, par exemple en limitant l'accès à Internet si le poste client possède un système d'exploitation Windows. Des éléments techniques complexes comme l'analyse des protocoles et des flags associés ...

Ces options ne sont pas décrites dans cette première version du document. N'hésitez pas à consulter les références section **??**, page **??** pour réaliser des recherches sur ces fonctionnalités avancées.

4. Menu Diagnostics | Show states

IV Création d'un planning

Les plannings permettent de préciser des périodes d'activation des règles. Ils sont principalement utilisés avec les règles de firewall. Si une règle de firewall spécifie un calendrier, la règle est activée uniquement pendant cette période.

- **Se rendre** dans le menu **Firewall | Schedules** ;
- **Saisir** le nom du calendrier ;
- **Saisir** une description pour le calendrier ;
- **Spécifier** les jours et la tranche horaire correspondant au calendrier ;
- **Valider** les changements par le bouton **Save** ;
- **Éditer** une règle et dans ses paramètres avancés, **spécifier** le calendrier nouvellement créé ;

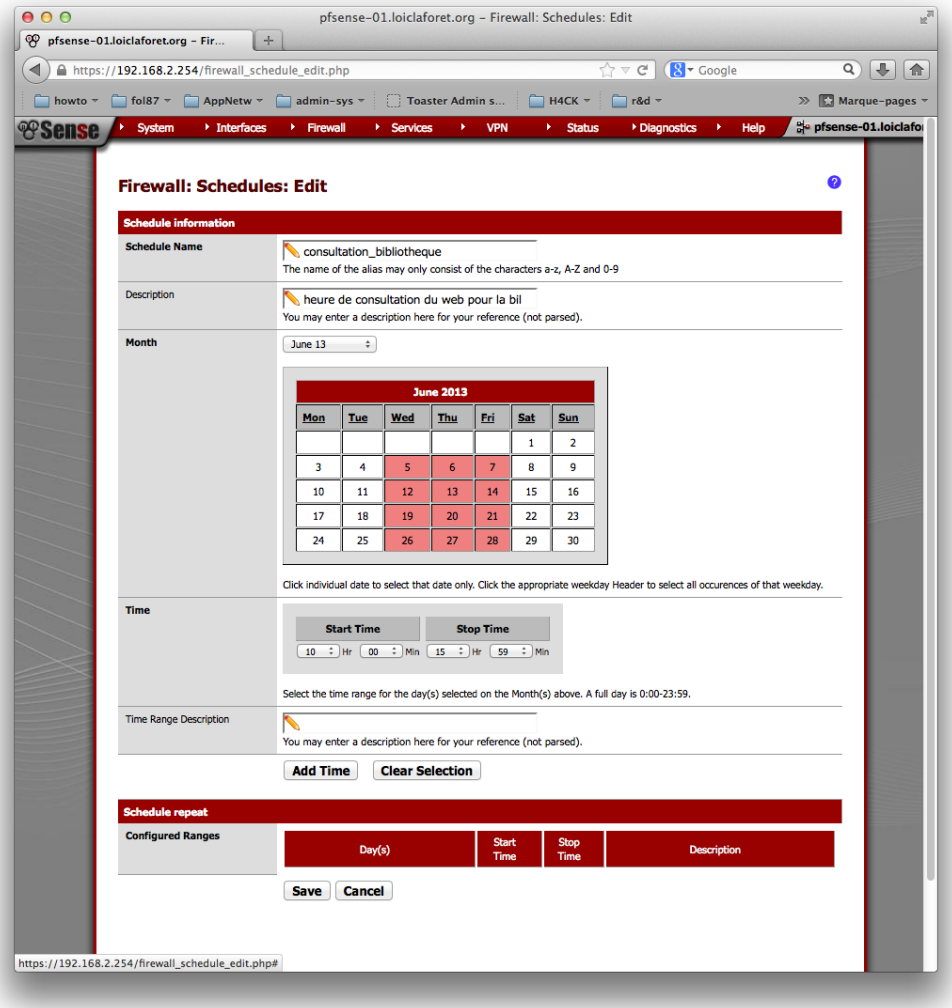

FIGURE IV.10 – Firewall Schedules : ajout d'un calendrier

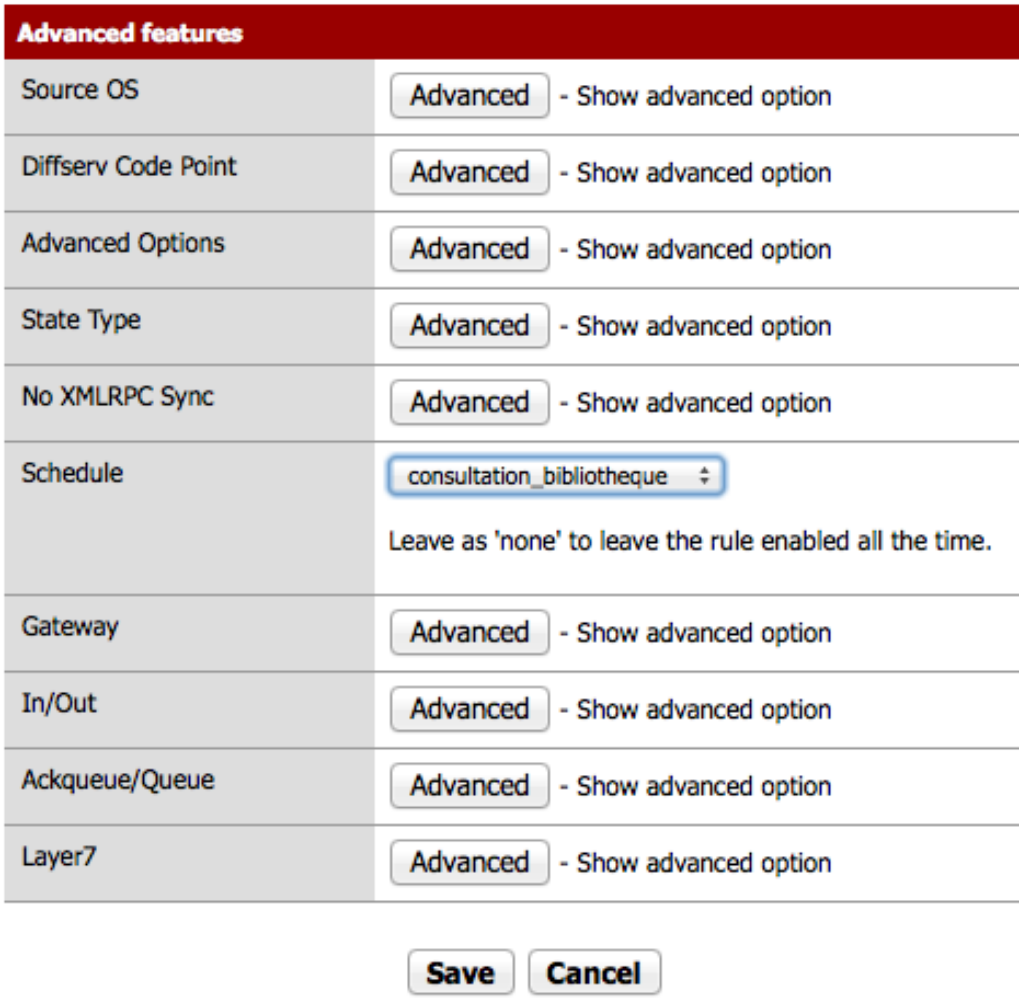

FIGURE IV.11 – Firewall Rules : ajout d'un calendrier

V Accès réseau à distance (RDP)

Le but de cette section est de décrire un processus complet de mise en oeuvre, du DHCP en passant par l'alias, le NAT et la règle de firewall ... L'exemple se base ici sur la mise en place d'un accès vers un serveur Windows utilisant le service `RDP`. Nous devons donc fournir la possibilité à n'importe quel poste relié à Internet d'accéder et d'ouvrir une session sur le serveur `RDP`.

1. **Connecter** un poste dans le réseau local ;
2. **Accéder** au menu **Status | DHCP Lease**, et **cliquer** sur le **bouton +** nommé Add a static mapping for this MAC addres
3. **Saisir** l'adresse IP : `192.168.2.100` ;
4. S'assurer que le service DNS Forwarder est correctement configuré pour automatiquement résoudre les mapping DHCP (menu **Services | DNS Forwarder**) ;

Status: DHCP leases

IP address	MAC address	Hostname	Start	End	Online	Lease Type
192.168.2.11	00:50:56:8c:12:fb	VCENTER-LL	2013/06/28 23:11:55	2013/06/29 01:11:55	online	active

FIGURE IV.12 – Status DHCP Leases : Mapping d'un poste à une adresse IP

General DNS Forwarder Options	
Enable	☑ **Enable DNS forwarder**
DHCP Registration	☐ **Register DHCP leases in DNS forwarder** If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.
Static DHCP	☑ **Register DHCP static mappings in DNS forwarder** If this option is set, then DHCP static mappings will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.

FIGURE IV.13 – Services DNS forwarder : Résolution des static mapping

1. **Se rendre** dans le menu **Firewall | Schedules** ;
2. **Créer** un nouveau calendrier basé sur les heures et jours ouvrés ;
3. **Créer** une règle de `NAT` depuis le menu **Firewall | NAT** permettant de transférer les requêtes acheminées de notre interface WAN vers notre serveur Windows ;
4. **Désactiver** pour cette règle la création automatique de la règle de firewalling correspondante ;
5. **Créer** enfin la règle de firewalling autorisant le trafic `RDP` depuis Internet vers le serveur Windows ;
6. **Sauvegarder** les changements par le bouton **Save** ;
7. **Valider** les changements par le bouton **Apply changes** ;

Chapitre V

Virtual Private Networking

Les réseaux privés virtuels (VPN) sont la pierre angulaire des systèmes informatiques actuels. Une connexion VPN permet par exemple à un utilisateur distant de se connecter en toute sécurité au réseau et accéder à des ressources comme s'il était présent et connecté localement. Il existe une multitude de services VPN, et pfSense en propose quatre nativement.

1. **OpenVPN** [1] est doucement en train de devenir le standard des protocoles VPN (non intégré nativement sous Windows) ;
2. **IPSec** est plus complexe mais reste un standard très populaire sur Internet
3. **PPTP** et **L2TP** sont souvent remplacés par les deux alternatives mentionnées ci-dessus, mais leur utilisation reste encore très répandue. L'avantage est qu'ils sont quasiment intégrés dans la plupart des systèmes d'exploitation.

I Création d'un tunnel VPN IPsec

IPSec est souvent la méthode préférée pour monter des tunnels site à site (par opposition aux clients mobiles). Un scénario typique consiste à créer une connexion sécurisée permanente entre deux sites distants, la maison mère et une filiale par exemple.

Le principe est plutôt simple, on crée une configuration particulière sur chacun des deux sites par l'intermédiaire de firewall **pfSense**, ou d'autres appliances (cisco, sonicwall...), afin qu'ils puissent établir entre eux un tunnel chiffré sur le réseau Internet. Dans l'exemple qui va suivre, nous utiliserons deux pfSense basés sur le même réseau de classe C privé, mais la démarche reste lorsque l'on souhaite joindre un site distant (cf. schéma I.1, page 6).

Nous allons ici tenter de monter un tunnel VPN entre le `pfSense-01`, installer à la section II-**Installation du pfSense-01**, page 7 et un `pfSense-02` que nous devons installer.

Dans un premier temps, passons à la configuration du `pfSense-01`.

1. http ://www.openvpn.org

1. Préparation du site 1 - pfSense-01

> `Remarque :`
> Les réseaux interconnectés par le tunnel VPN doivent impérativement utilier des réseaux différents (adresse de réseau). Donc si deux VLAN distincts tous deux répartis sur des sites différents utilisent le réseau `10.87.1.0/24`, le VPN ne fonctionnera pas.

Le fonctionnement d'un tunnel IPsec site à site fonctionne en deux phases, paramétrées également de manières distinctes par **pfSense**. Pour la première phase :

- **Se rendre** dans le menu **VPN** | **IPsec** ;
- **Cliquer** sur le **bouton +** ;
- **Spécifier** la gateway du site distant : `192.168.1.249` ;
- **Indiquer** une description : `tunnel site 1 to site 2` ;
- **Spécifier Mutual PSK** pour la méthode d'authentification ;
- **Choisir aggressive** pour la méthode de négociation ;
- **Sélectionner My IP address** comme identificateur ;
- **Spécifier Peer IP address** pour Peer identifier ;
- **Choisir** `votrecledechiffrementdevotrechoix` pour la clé chiffrement partagée (sera également à fournir sur le site 2) ;
- **Laisser Default** pour Policy Generation ;
- **Laisser Default** pour Proposal Checking ;
- **Choisir 3DES** comme Alorithme de chiffrement ;
- **Laisser SHA1** comme algorithme pour le hash ;
- **Choisir 2** pour le DH Key Group ;
- **Spécifier 28800** secondes pour pour la durée de vie de la phase 1 ;
- **Laisser** par défaut les valeurs des options avancées ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;

Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description
WAN 192.168.1.249	aggressive	3DES	SHA1	tunnel site 1 to site 2
+ - Show 1 Phase-2 entries				

FIGURE V.1 – VPN IPsec : récapitulatif du site 1 - phase 1

Pour la seconde, qui correspond aux réseaux que vous souhaitez faire communiquer :

- **Se rendre** dans le menu **VPN** | **IPsec** | **phase 1 - tunnel site 1 to site 2** ;
- **Cliquer** sur le **bouton +** pour ajouter une phase 2 à notre tunnel VPN ;
- **Laisser** le **Mode** sur Tunnel ;
- **Choisir** le **LAN SubnetMode** pour la directive Local Network ;
- **Choisir Network** et `192.168.4.0/24` pour la directive Remote Network (cf. schéma I.1, page 6) ;
- **Indiquer** une description : `accès vers LAN site 2` ;
- **Choisir ESP** pour le protocole ;

- **Choisir** uniquement **3DES** comme Alorithme de chiffrement ;
- **Choisir** uniquement **SHA1** comme algorithme pour le hash ;
- **Désactiver** le PFS key Group ;
- **Augmenter** à **86400** secondes pour pour la durée de vie de la phase 2 ;
- **Spécifier** la gateway du LAN2 du site 2 dans Automatically ping host ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;

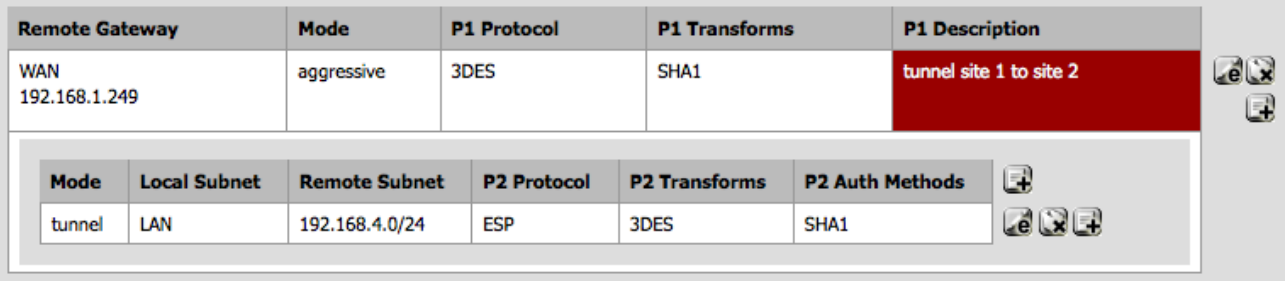

FIGURE V.2 – VPN IPsec : récapitulatif du site 1 - phase 2

Cette phase terminée, nous pouvons passer à l'installation d'un `pfSense-02`.

2. Préparation du site 2 - pfSense-02

Afin de reproduire l'infrastructure décrite par le schéma schéma I.1, page 6), nous devons réaliser l'installation d'un second **pfSense** pour monter convenablement notre tunnel VPN IPsec.

L'installation du **pfSense** reste identique à l'installation du `pfSense-01`, en dehors des adresses IP côté WAN et LAN. La figure V.3 illustre la console d'administration de la seconde machine virtuelle hébergeant notre firewall `pfSense-02`.

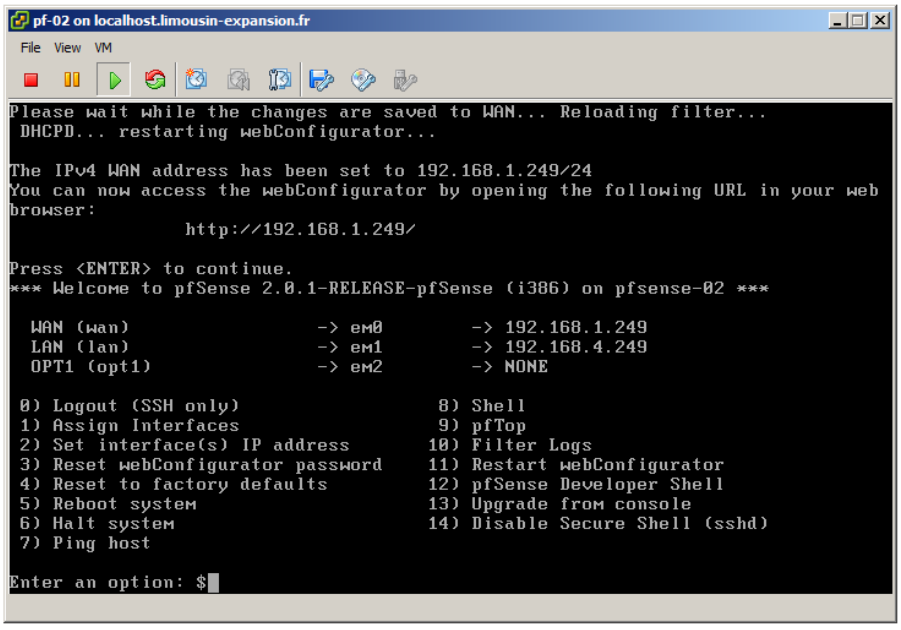

FIGURE V.3 – Machine virtuelle pfSense 2 - site 2

Nous pouvons modifier le thème du `pfSense-02` afin d'identifier plus simplement le firewall sur lequel nous accédons. Pour cela :

- **Se rendre** dans le menu **System | General Setup** ;
- **Sélectionner** un autre thème que celui déployé par défaut dans la section Theme ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;

Finaliser la configuration en reprenant si besoin les éléments décrits dans les chapitres I et II, respectivement situés aux pages 5 et 16.

Reprenons le fil de cette section, et préparons la configuration des phases 1 et 2 de notre tunnel VPN IPsec du site 2. Nous suivons la même procédure décrite dans la section 1. page 41 :

> Attention :
> Nous sommes ici sur le `pfSense-02`.

- **Se rendre** dans le menu **VPN | IPsec** ;
- **Cliquer** sur le **bouton +** ;
- **Spécifier** la gateway du site distant : `192.168.1.254` ;
- **Indiquer** une description : `tunnel site 2 to site 1` ;
- **Spécifier Mutual PSK** pour la méthode d'authentification ;
- **Choisir aggressive** pour la méthode de négociation ;
- **Sélectionner My IP address** comme identificateur ;
- **Spécifier Peer IP address** pour Peer identifier ;
- **Resaisir** la même clé que sur le site 1 : `votrecledechiffrementdevotrechoix` pour la clé chiffrement partagée ;
- **Laisser Default** pour Policy Generation ;
- **Laisser Default** pour Proposal Checking ;
- **Choisir 3DES** comme Alorithme de chiffrement ;
- **Laisser SHA1** comme algorithme pour le hash ;
- **Choisir 2** pour le DH Key Group ;
- **Spécifier 28800** secondes pour pour la durée de vie de la phase 1 ;
- **Laisser** par défaut les valeurs des options avancées ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;

La phase 1 étant terminée, nous passons à la phase 2 :

- **Se rendre** dans le menu **VPN | IPsec | phase 1 - tunnel site 2 to site 1** ;
- **Cliquer** sur le **bouton +** pour ajouter une phase 2 à notre tunnel VPN ;
- **Laisser** le **Mode** sur Tunnel ;
- **Choisir** le **LAN SubnetMode** pour la directive Local Network ;
- **Choisir Network** et `192.168.2.0/24` pour la directive Remote Network (cf. schéma I.1, page 6) ;
- **Indiquer** une description : `accès vers LAN site 1` ;
- **Choisir ESP** pour le protocole ;
- **Choisir** uniquement **3DES** comme Alorithme de chiffrement ;
- **Choisir** uniquement **SHA1** comme algorithme pour le hash ;
- **Désactiver** le PFS key Group ;
- **Augmenter** à **86400** secondes pour pour la durée de vie de la phase 2 ;
- **Spécifier** la gateway du LAN1 du site 1 dans Automatically ping host ;

– **Valider** les changements par le bouton **Save** ;
– **Cliquer** sur le bouton **Apply changes** ;

Pour vérifier le fonctionnement de notre tunnel VPN, nous nous rendons dans le menu **Status** | **IPsec**, sur chacun des deux firewall.

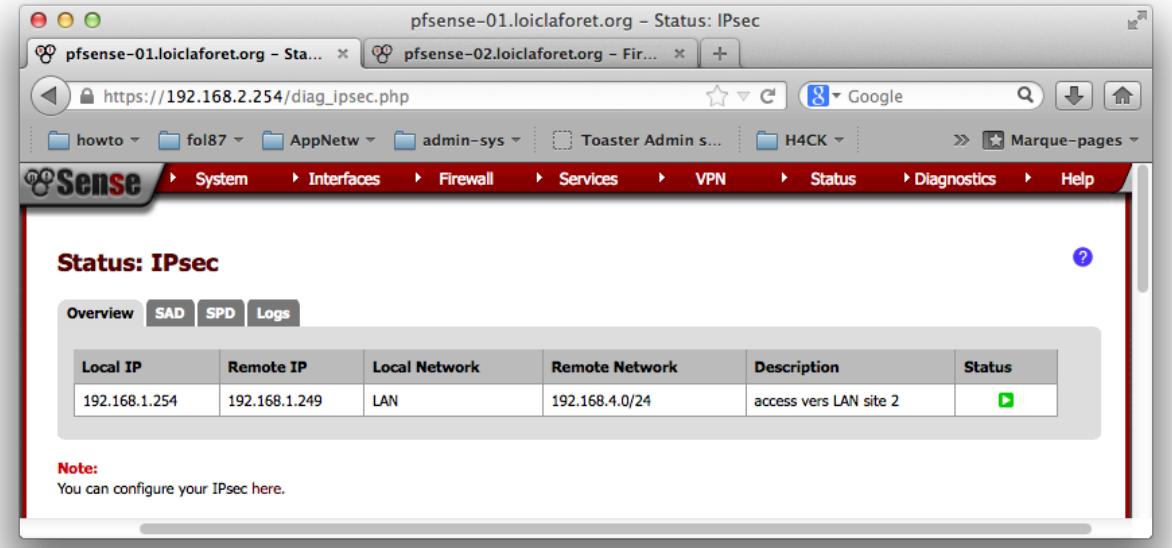

FIGURE V.4 – VPN IPsec : pfSense-01

FIGURE V.5 – VPN IPsec : pfSense-02

On s'apperçoit que le tunnel est convenablement monté. On peut également vérifier les différentes phases

suivies par nos deux **pfSense** lors de l'établissement de notre tunnel IPsec.

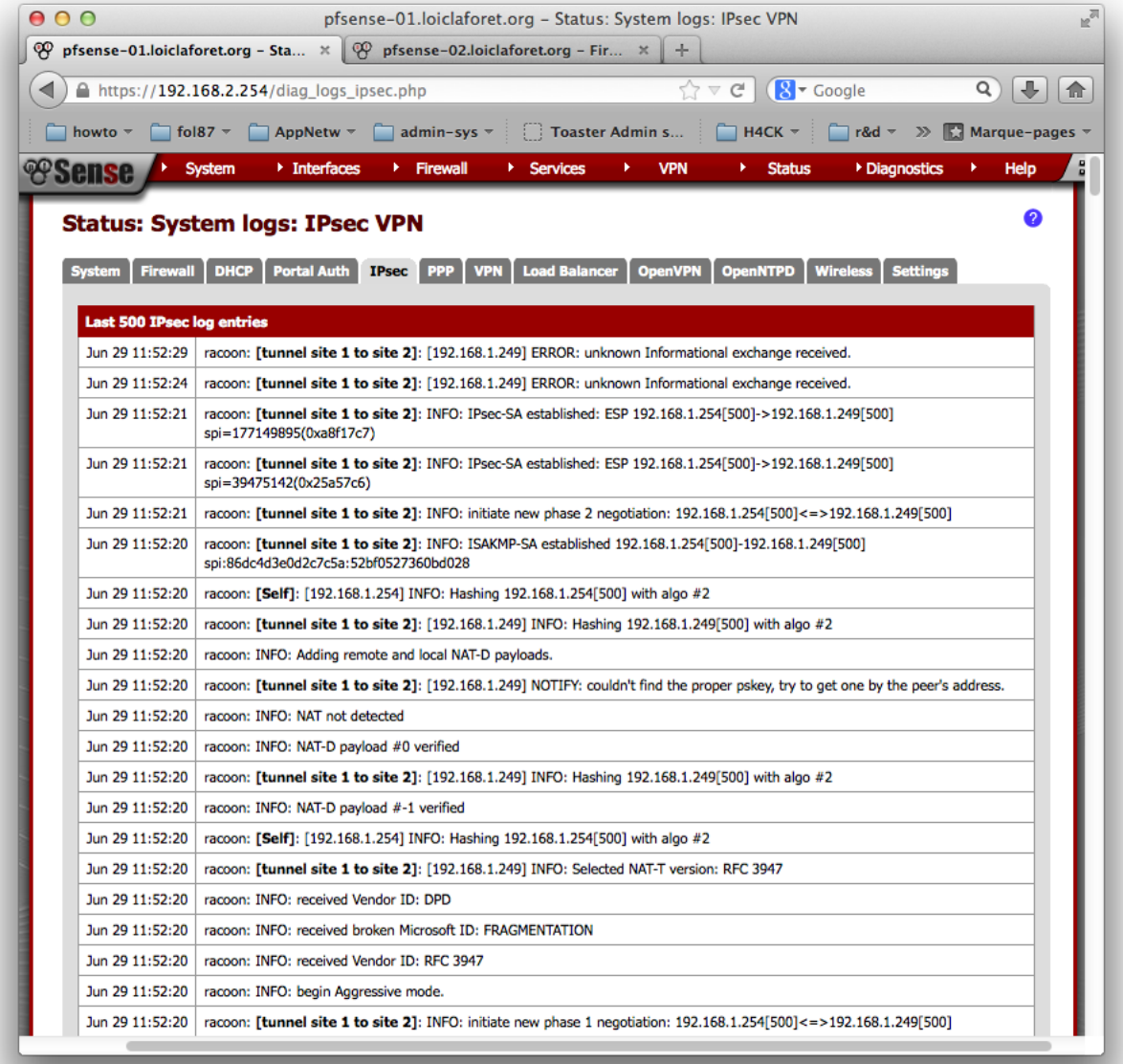

FIGURE V.6 – VPN IPsec : logs liés à l'établissement d'un tunnel

Ceci fait, nous devons maintenant faire en sorte d'utiliser ce tunnel VPN pour permettre une véritable interconnexion de nos réseaux entre les sites 1 et 2. Si nous connectons un client sur le réseau LAN1, et que nous souhaitons joindre par une requête ICMP la patte LAN du `pfSense-02`, nous nous apercevons que le trafic n'est pas autorisé. C'est le principe même de tous les firewall. Tout trafic non explicitement autorisé est bloqué. Le trafic transitant dans le tunnel VPN ne fait pas exception. Cela nous convient plutôt bien car il n'est pas envisageable d'autoriser tout type de trafic dans le tunnel VPN IPsec.

Nous avons vu lors du chapitre III – `Création des règles de firewall à la page` à la page 35 qu'une des particularités du firewall pfSense concernait sa gestion des tables d'état (*stateful*). Nous allons nous en rendre compte ici.

Connectons un client dans le `LAN1`, donc derrière le firewall `pfSense-01`, et tentons de joindre la gate-

way du pfSense-02.

```
MacBook-Pro-de-Loic:~ loiclaforet$ ping 192.168.4.249
PING 192.168.4.249 (192.168.4.249): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
--- 192.168.4.249 ping statistics ---
5 packets transmitted, 0 packets received, 100.0% packet loss
MacBook-Pro-de-Loic:~ loiclaforet$
```

Pour régler ce problème, et autoriser le trafic ICMP entre les réseaux LAN1 et LAN2, nous allons explicitement mentionner sur notre pfSense-02 le fait que le trafic ICMP est autorisé à entrer depuis le réseau LAN1 vers le réseau LAN2. Commencer par créer un alias du réseau du site 1 sur le pfSense-02.

- **Se rendre**, depuis le firewall pfSense-02, dans le menu **Firewall | Rules | IPsec** ;
- **Cliquer** sur le **bouton +** pour ajouter une règle ;
- **Choisir Pass** pour l'action ;
- **Laisser** la règle active ;
- **Laisser** l'interface IPsec ;
- **Choisir** le protocole **ICMP** ;
- **Choisir** tous les protocoles de type ICMP ;
- **Sélectionner** le choix **Single host or alias** et saisir l'alias LAN_SITE_1 pour la source ;
- **Sélectionner** le choix **LAN subnet** pour la destination ;
- **Cocher** l'option de log pour garder une trace du trafic dans les logs du firewall ;
- **Ajouter** une description sur le rôle de cette règle ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;

Après un temps de compilation des règles par le pfSense-02, on s'apperçoit que le trafic ICMP est désormais autorisé. Le trafic est autorisé à entrer sur l'interface IPSEC du pfSense-02 depuis le LAN1.Si vous réalisez le test inverse, en réalisant une requête ICMP depuis le LAN2 derrière le **pfSense-02** vers une machine du LAN1 du site 1, la requête sera naturellement rejetée car le pfSense-01 ne possède pas explicitement de règle autorisant le trafic à entrer sur l'interface IPsec depuis le réseau LAN2.

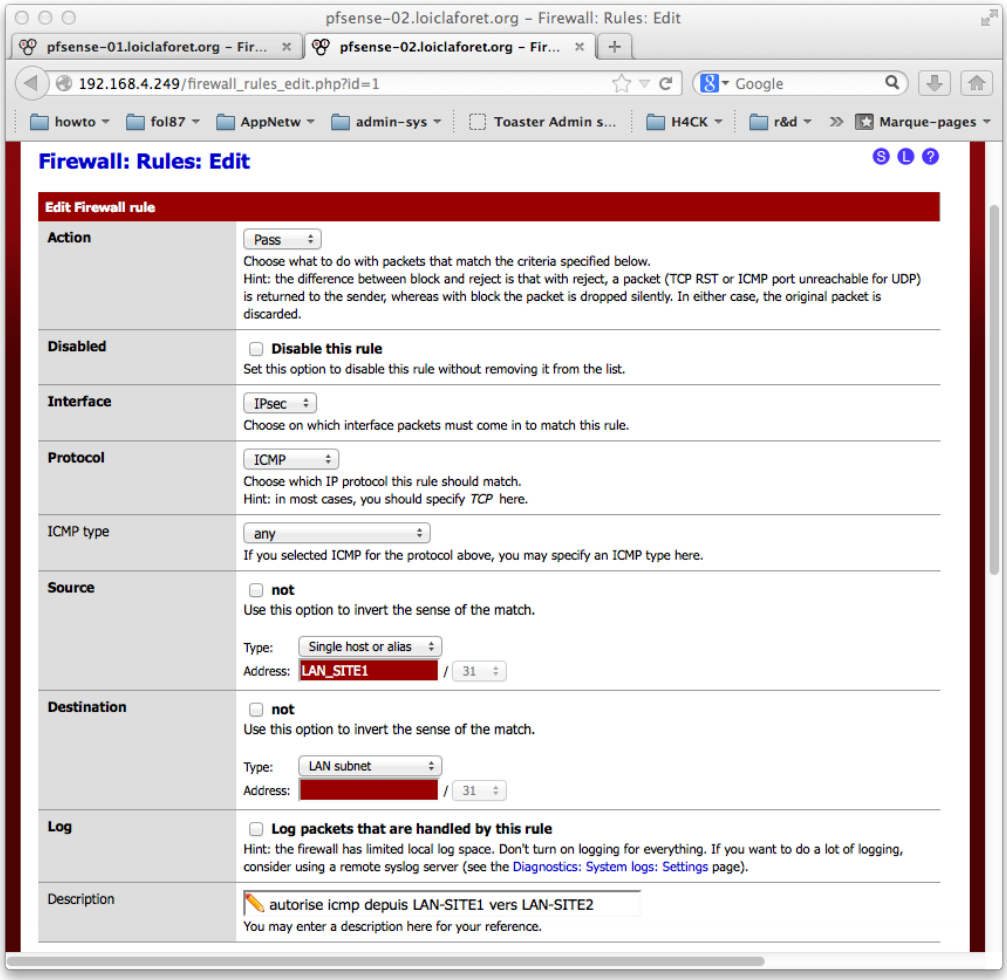

FIGURE V.7 – Firewall Rules : ajout d'une règle pour le protocole ICMP

Chapitre VI

Configurations avancées

Les sections suivantes couvrent des fonctions réseaux avancées que l'on trouve habituellement dans les entreprises. Chacune de ces caractéristiques est disponible dans la dernière version de **pfSense**.

I Configuration d'un NAT Outbound et d'un NAT

Une règle de NAT outbound définit comment le trafic doit sortir du firewall. C'est un concept quelque peu complexe à saisir car dans la plupart des configurations pour lesquelles nous installons des firewall, nous ne nous préoccupons généralement pas de la manière dont les paquets réseaux sont redirigés lorsqu'ils sortent du firewall.

Cette section tentera de décrire comment utiliser une règle NAT Outbound pour résoudre un scénario commun qui implique un *NATING* d'une machine possédant plusieurs interfaces. Nous supposerons ici que nous avons un serveur avec deux interfaces LAN et DMZ, que notre firewall **pfSense** protège.

En utilisant une règle de port forwarding, nous transmettons convenablement les requêtes HTTP vers le serveur sur son interface DMZ. Cependant, lorsque nous tentons de transmettre des requêtes SSH sur l'interface LAN du serveur, le trafic arrive correctement mais tente de répondre via son interface DMZ.

Le firewall interprête ce trafic comme une possible attaque et bloque ce trafic. La solution ici consiste à traiter les requêtes SSH en utilisant une règle NAT outbound couplé avec un NAT 1 :1, comme décrit dans la section **??**. Il est également possible d'utiliser cette fonctionnalité pour forcer un VLAN à sortir par une adresse IP publique spécifique.

- **Se rendre** dans le menu **Firewall | Virtual IP** ;
- **Cliquer** sur le **bouton +** pour ajouter une nouvelle IP virtuelle ;
- **Sélectionner** le type **Proxy ARP** ;
- **Sélectionner** l'interface **WAN** ;
- **Sélectionner** **Single Address** comme type IP address et spécifier l'adresse IP publique de votre FAI ;
- **Ajouter** une description sur le rôle de cette IP virtuelle ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;

On force ici le fait que le serveur doit nous répondre sur son interface LAN lorsque l'on interroge son service SSH.

- **Se rendre** dans le menu **Firewall | NAT** ;
- **Cliquer** sur l'onglet **Outbound** ;

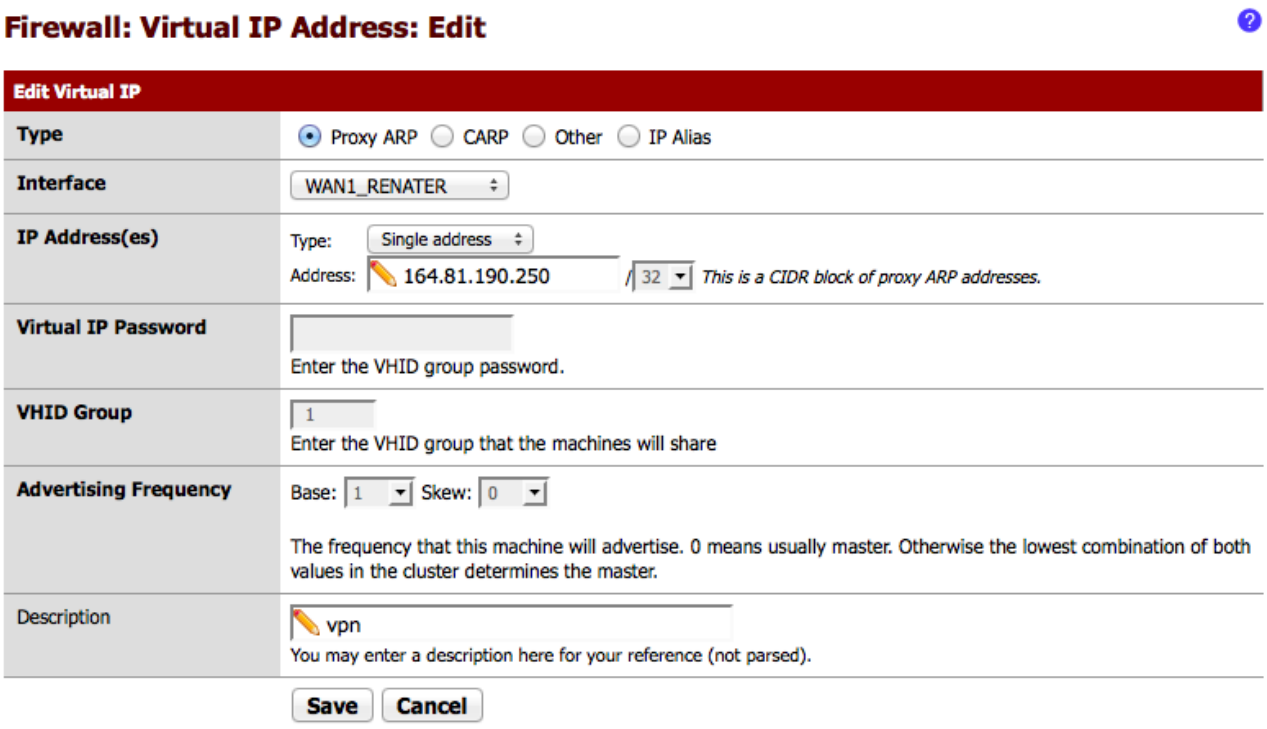

FIGURE VI.1 – Firewall Virtuals IP : création d'une IP Virtuelle

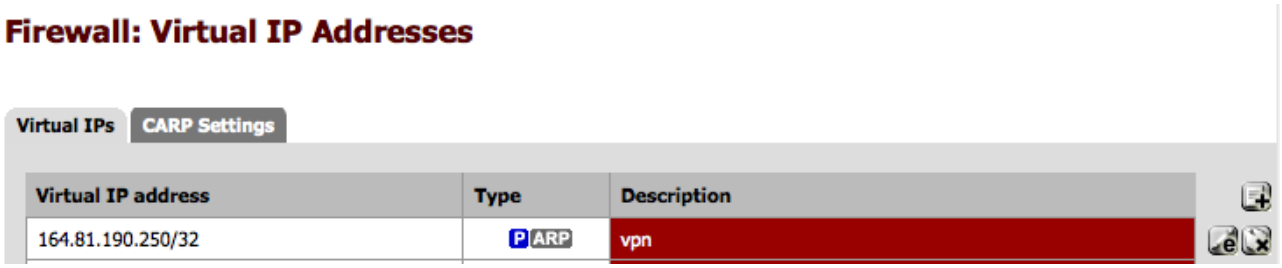

FIGURE VI.2 – Firewall Virtuals IP : vue générale

- **Sélectionner** l'option **Automatic outbound NAT rule generation (IPsec passthrough included)** ;
- **Cliquer** sur le **bouton +** pour ajouter une nouvelle règle de NAT outbound ;
- **Sélectionner** l'interface **LAN** ;
- **Sélectionner** **Any** comme Source ;
- **Spécifier** une destination correspondant à l'adresse IP du serveur côté LAN ;
- **Laisser** la directive Translation sur le choix **Interface address**, et **spécifier** le port `22` pour le protocole SSH ;
- **Ajouter** une description sur le rôle de cette règle de NAT outbound ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;

> Attention :
> L'opération de basculement par l'option **Automatic outbound NAT rule generation (IPsec passthrough included)** est une opération visiblement irréversible, ou en tout cas pouvant poser certaines difficultés. Pour vos tests, n'hésitez pas à réaliser un snapshot de votre machine virtuelle avant d'activer cette fonction.

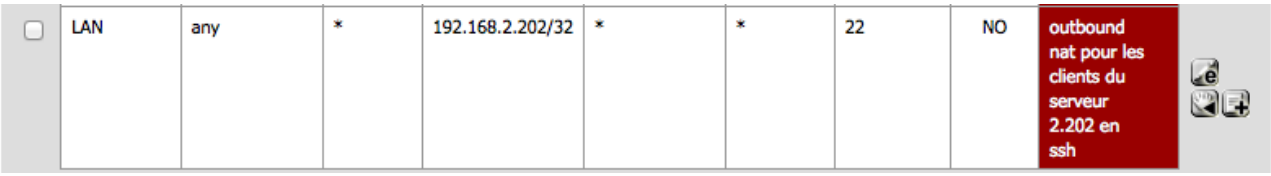

FIGURE VI.3 – Firewall NAT Outbound : vue générale

Ajoutons le NAT permettant l'accès à notre serveur Web par notre interface WAN.

- **Se rendre** dans le menu **Firewall** | **NAT** ;
- **Cliquer** sur l'onglet **1 :1** ;
- **Cliquer** sur le **bouton +** pour ajouter une nouvelle règle de NAT ;
- **Sélectionner** l'interface **WAN** ;
- **Saisir** l'adresse IP publique dans la directive External subnet IP ;
- **Saisir** l'adresse IP privée du serveur par la directive Internal IP et Single Host ;
- **Ajouter** une description sur le rôle de cette règle de NAT outbound ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;

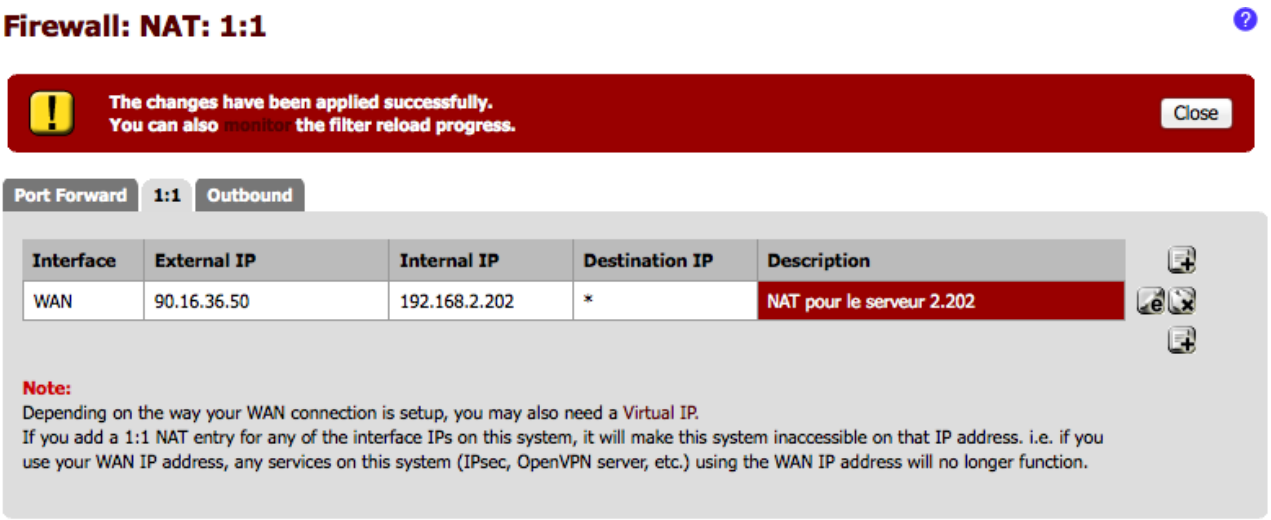

FIGURE VI.4 – Firewall NAT 1 :1 : vue générale

Il nous reste l'autorisation du trafic par l'ajout d'une règle de firewalling.

- **Se rendre** dans le menu **Firewall** | **Rules** ;
- **Cliquer** sur l'onglet **WAN** ;
- **Cliquer** sur le **bouton +** pour ajouter une nouvelle règle de firewalling ;
- **Sélectionner** **Any** pour la directive Source ;

- **Sélectionner** **Any** pour la directive Source port range ;
- **Sélectionner** **Single Host or Alias** pour la Destination et **spécifier** l'adresse IP privée du serveur ;
- **Spécifier** le port **SSH** pour la directive Destination port range ;
- **Ajouter** une description sur le rôle de cette règle de firewalling ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;

FIGURE VI.5 – Firewall Rules : vue générale

La règle de NAT outbound que nous avons explicitement créé force pfSense à directement acheminer le trafic sortant par l'interface LAN de notre serveur. Cela permet au trafic SSH de trouver son chemin retour, ce qui n'était préalablement pas le cas car la passerelle par défaut du serveur est configuré pour son interface DMZ.

II Création d'une gateway

On ne trouve normalement qu'une seule gateway sur un réseau. Mais pour des besoins spécifiques comme de l'équilibrage de charge, ou plus simplement des besoins particuliers de routage, il est nécessaire de passer par la création de passerelles supplémentaires. Leurs créations reste simple :

- **Se rendre** dans le menu **System | Routing** ;
- **Cliquer** sur l'onglet **Gateways** ;
- **Cliquer** sur le **bouton +** pour ajouter une nouvelle règle passerelle ;
- **Sélectionner** l'interface sur laquelle la gateway doit être active ;
- **Sélectionner** le nom de la passerelle ;
- **Sélectionner** l'adresse IP de la passerelle ;
- **Sélectionner** éventuellement une adresse de **monitoring** ;
- **Ajouter** une description ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;

III Création d'une route statique

Les routes statiques sont utilisées pour rendre interconnectables des réseaux ne l'étant pas par défaut par l'interface WAN, mais par l'intermédiaire d'un autre routeur (ou noeud réseau).

La création d'une route statique suit le même procédé, qui commence à vous être familier :

- **Se rendre** dans le menu **System | Routing** ;
- **Cliquer** sur l'onglet **Routes** ;
- **Cliquer** sur le **bouton +** pour ajouter une nouvelle route ;
- **Spécifier** le réseau de destination et son masque de sous réseau correspondant au format CIDR ;
- **Sélectionner** la passerelle à utiliser pour joindre ce nouveau réseau ;
- **Ajouter** une description sur le rôle de cette route ;
- **Valider** les changements par le bouton **Save** ;

– **Cliquer** sur le bouton **Apply changes** ;

IV Création d'un portail captif

Un portail captif est un système permettant d'intercepter toutes les requêtes d'un client. Le but est d'authentifier les utilisateurs d'un réseau en les renvoyant vers une page prévue à cet effet - d'où le nom portail captif. Ces services sont communément utilisés dans les hotspots, hotels ... Dans d'autres scénarios, les portails captifs sont utilisés pour l'authentification des utilisateurs sur un réseau filaire ou pour forcer l'accord d'un contrat ou charte d'usage du moyen mis à disposition.

Au cours de cette section, nous verrons comment configurer **pfSense** pour qu'il remplisse le rôle de portail captif avec authentification, bloquant ainsi les utilisateurs depuis notre zone `DMZ`.

– **Se rendre** dans le menu **Services** | **Portal captive** ;
– **Cocher** la case **Enable captive portal** ;
– **Sélectionner** l'interface sur laquelle vous souhaitez que pfSense force l'interception des requêtes des utilisateurs : `DMZ` pour l'exemple ;
– **Spécifier** la directive Idle Timeout à `10 minutes` ;
– **Spécifier** la directive Hard Timeout à `60 minutes` ;
– **Spécifier** la directive Enable logout popup window pour que les utilsiateurs puissent se déconnecter lors de la fermeture du popup ;
– **Sélectionner** **Local User Manager / Vouchers** pour gérer l'authentification des utilisateurs ;

> `Remarque :`
> Nous avons utilisé ici la base locale des utilisateurs du système **pfSense**. Il est conseillé, lors de la mise en production d'une telle solution de coupler le portail captif à un serveur **Radius** (**freeradius** par exemple) par l'ajout du plugin dédié ou de manière externalisée.

– **Se rendre** dans le menu **System** | **User Manager** ;
– **Cliquer** sur l'onglet **User** ;
– **Cliquer** sur le **bouton +** pour ajouter une nouvelle entrée ;
– **Indiquer** le login de l'utilisateur ;
– **Indiquer** le mot de passe de l'utilisateur et **confirmer-le** ;
– **Indiquer** les nom/prénom de l'utilisateur ;
– **Ajouter** une description sur le rôle de cette route ;
– **Valider** les changements par le bouton **Save** ;
– **Cliquer** sur le bouton **Apply changes** ;

> `Remarque :`
> Dans l'exemple, nous ajoutons le service de portail captif sur l'interface DMZ, qui ne possède pas encore de règle particulière. Ajoutez une règle permettant la sortie vers le HTTP et le DNS au minimum pour pouvoir convenablement tester le portail captif.

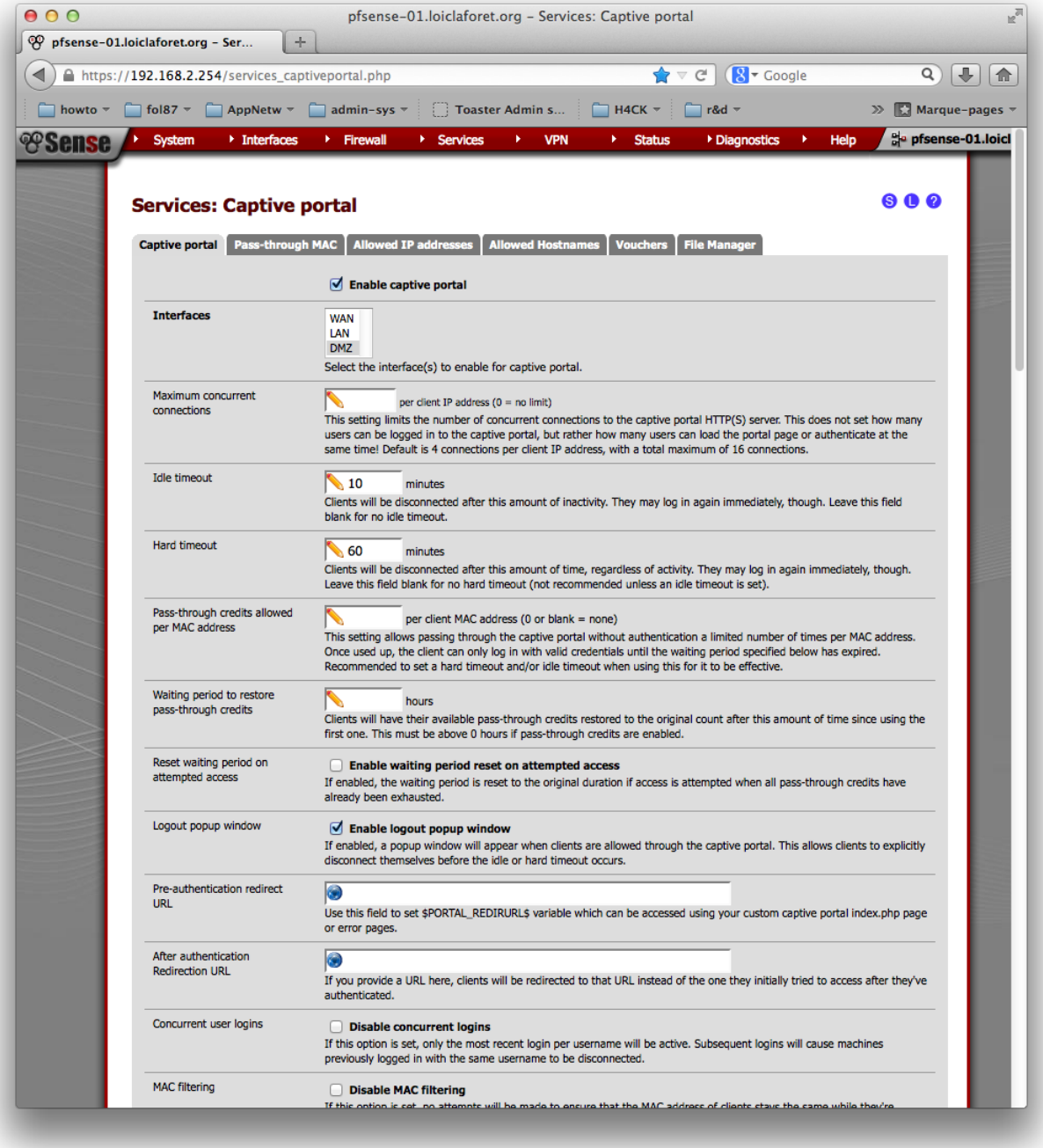

FIGURE VI.6 – Service Portal captive : création d'un portail captif

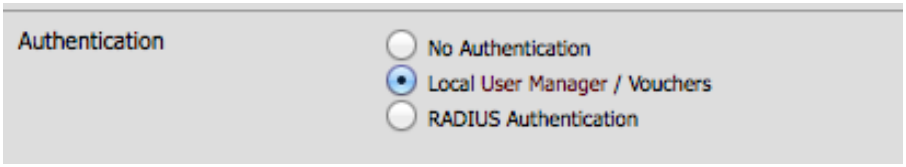

FIGURE VI.7 – Service Portal captive : gestion de l'authentification

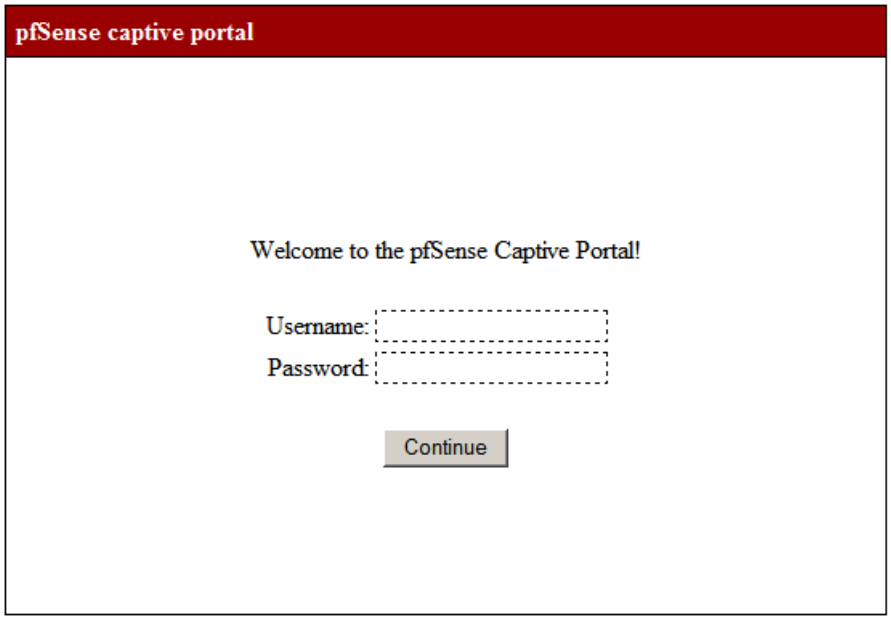

FIGURE VI.8 – Service Portal captive : interception

V Configuration du proxy Squid-SquidGuard

Comme nous l'avons mentionné dans de l'introduction de ce document, **pfSense** permet l'ajout de packages ou plugins. Ces éléments permettent ainsi d'ajouter des fonctionnalités à notre firewall. Nous allons dans cette section ajouter les packages nécessaires pour ajouter un rôle de proxy à notre **pfSense**, par l'intermédiaire du couple **Squid** et **SquidGuard**. Ce dernier permettra l'ajout d'une fonctionnalité de filtrage de contenu au proxy **Squid**.

1. Installation des packages

La première étape consiste à ajouter les plugins **Squid** et **SquidGuard**, par l'intermédiaire du menu dédié à la gestion des packages.

> Remarque :
> Dans la liste des paquets disponibles apparaît la version 3 de **Squid** en beta. Elle n'a pas encore été basculée en stable, donc nous restons sur la dernière version valide : `2.7.9`.
> Dans cet environnement de test, vous pouvez aisément tester les évolutions de la version 3 de **Squid** en prenant soin de réaliser un snapshot de votre VM au préalable par exemple.

- **Se rendre** dans le menu **System | Packages** ;
- **Sélectionner** l'onglet **Available Packages** ;
- **Sélectionner** dans la liste le package **Squid** pour le télécharger et l'installer par l'intermédiaire du **bouton +** ;
- **Valider** l'opération ;
- **Effectuer** la même opération pour le package **SquidGuard** ;

pfSense affiche alors le déroulement de l'installation des packages. Le processus automatique passe par le

téléchargement du paquet, l'extraction et l'installation de ce dernier. Le temps nécessaire au déploiement varie en fonction de la bande passante et des ressources mémoires et processeur allouées à la machine virtuelle.

squid	Network	Stable 2.7.9 pkg v.4.3.3 platform: 2	No info, check the forum	High performance web proxy cache.
squid3	Network	beta 3.1.20 pkg 2.0.6 platform: 2.0	Package Info	High performance web proxy cache. It combines squid as a proxy server with it's capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant.
squid3-dev	Network	beta 3.3.5 pkg 2.1.2 platform: 2.0	Package Info	High performance web proxy cache. It combines squid as a proxy server with it's capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, ssl filtering and antivirus integration via i-cap
squidGuard	Network Management	Beta 1.4_4 pkg v.1.9.5 platform: 1.1	No info, check the forum	High perfomance web proxy URL filter. Requires proxy Squid 2.x package.

FIGURE VI.9 – System Packages : listes des paquets Squid disponibles

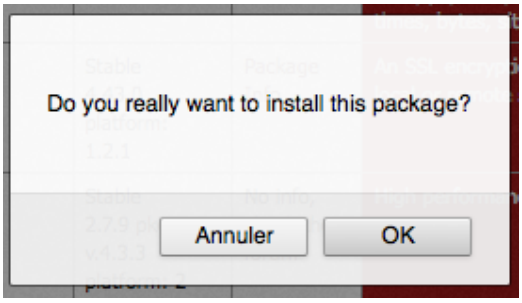

FIGURE VI.10 – System Packages : confirmation de l'installation d'un paquet

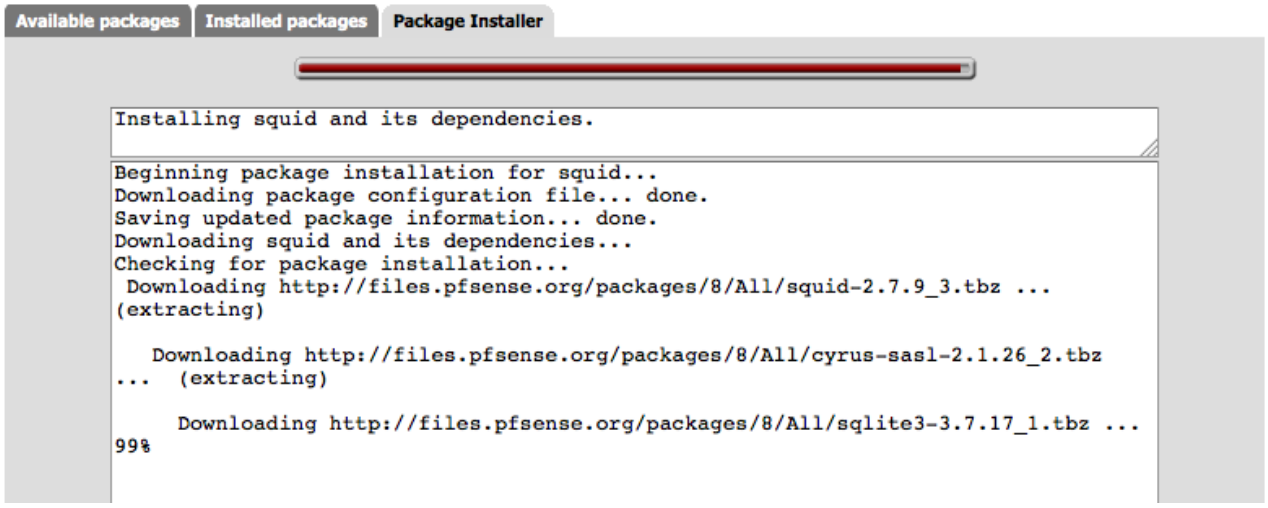

FIGURE VI.11 – System Packages : processus d'installation automatique d'un paquet

```
Beginning package installation for squid...
```

```
Downloading package configuration file... done.
Saving updated package information... done.
Downloading squid and its dependencies...
Checking for package installation...
 Downloading http://files.pfsense.org/packages/8/All/libwww-5.4.0_4.tbz ...  (extracting)
Loading package configuration... done.
Configuring package components...
Additional files... done.
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Executing custom_php_resync_config_command()...done.
Custom commands...
Executing custom_php_install_command()...done.
Executing custom_php_resync_config_command()...done.
Menu items... done.
Integrated Tab items... done.
Services... done.
Writing configuration... done.

Installation completed.  Please check to make sure that the package is configured from
the respective menu then start the package.
```

Pour vérifier l'installation des packages, nous nous rendons dans le menu **Services** pour vérifier la présence du nouveau service **Proxy Server**

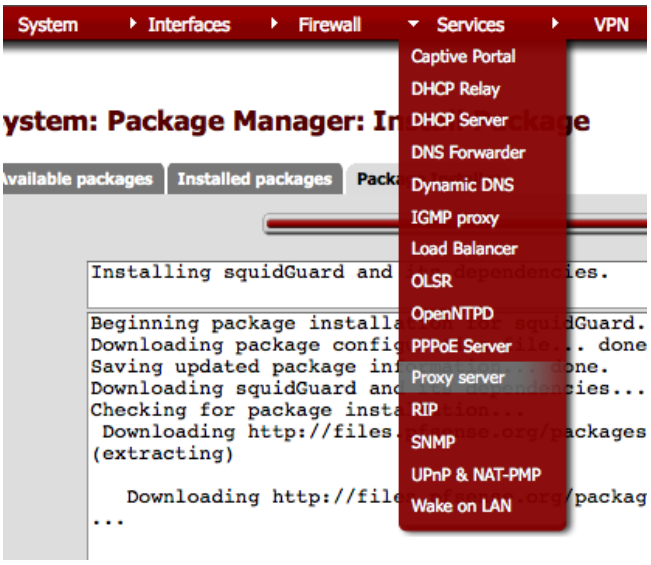

FIGURE VI.12 – Services Proxy Server : Menu

2. Configuration de Squid

À la fin de l'installation du paquet, nous pouvons nous lancer dans la configuration du service. Si vous souhaitez des informations sur le fonctionnement et les possibilités techniques offertes par l'applicatif **Squid**,

n'hésitez pas à consulter le site des développeurs http://www.squid-cache.org.

La première étape consiste à sélectionner l'interface sur laquelle nous allons appliquer le service **Squid**. Nous allons donc ici associer le service sur la patte LAN de notre **pfSense**.

> Remarque :
> Dans l'exemple qui va suivre, nous allons procéder au déploiement d'un Squid *transparent*. Il existe en effet deux façons d'installer ce proxy. Le principe est ici assez simple à comprendre : les utilisateurs passeront par le proxy lorsqu'ils navigueront sur Internet, et ce de manière transparente pour eux. Nous utiliserons une fonctionnalité de pfSense que nous avons vu dans le chapitre IV.II.**Création d'une règle de NATP / port forwarding** à la page 31, pour forcer le trafic web des clients à passer par le proxy **Squid** afin d'être mis en cache, analyer et filtrer par **SquidGuard** ... Vous pouvez donc choisir de laisser l'option **Transparent proxy** désactivée, et tenter de réaliser les règles de NAT manuellement.

- **Se rendre** dans le menu **Services** | **Proxy Server** ;
- **Sélectionner** l'interface **LAN** ;
- **Cocher** l'option Allow users on interface pour ajouter le réseau correspondant à l'interface LAN ;
- **Cocher** Enable logging (en fonction de la taille du disque de votre **pfSense**) ;
- **Spécifier** 7 jours pour la directive Log rotate ;
- **Spécifier** 3128 pour la directive Proxy port ;
- **Valider** les changements par le bouton **Save** ;
- **Sélectionner** l'onglet **Cache Mgmt** ;
- **Spécifier** 2000 Mb pour la directive Hard disk cache size ;
- **Valider** les changements par le bouton **Save** ;
- **Sélectionner** l'onglet **Access Control** ;
- **Ajouter** au besoin d'autres réseaux à autoriser ;
- **Cliquer** sur le bouton **Save** ;
- **Se rendre** dans le menu **Services** | **Proxy Filter** pour accéder à la configuration de **SquidGuard** ;
- **Cliquer** sur **Enable** pour activer le service puis sur le bouton **Apply** ;
- **Cliquer** sur **Enable GUI log** pius sur **Enable log** ;
- **Saisir** l'adresse http://www.shallalist.de/Downloads/shallalist.tar.gz dans la directive Blacklist URL ;
- **Cliquer** sur le bouton **Save** en base de page ;
- **Sélectionner** l'onglet **Blacklist** ;
- **Saisir** la liste http://www.shallalist.de/Downloads/shallalist.tar.gz (celle de Toulouse pose problème ...) ;
- **Cliquer** sur le bouton **Save** ;
- **Se rendre** sur l'onglet **Common Access Control List (ACL)** ;
- **Régler** pour chaque catégorie le contenu à bloquer ou autoriser ;
- **Cliquer** sur le bouton **Save** ;

Le statut des services est disponible par le menu **Status** | **Services**.

Voici les logs remontés par Squid lors d'une navigatoin d'un client.

```
MacBook-Pro-de-Loic:~ loiclaforet$ ssh admin@192.168.2.254
Password:
```

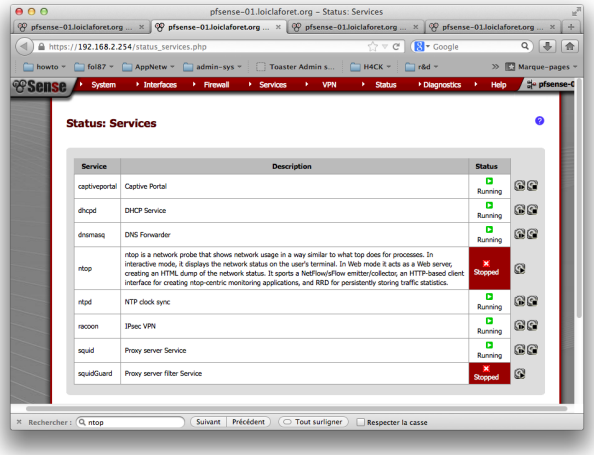

FIGURE VI.13 – Status Services : vue générale

```
*** Welcome to pfSense 2.0.1-RELEASE-pfSense (i386) on pfsense-01 ***

  WAN  (wan)                -> em0        -> 192.168.1.254
  LAN  (lan)                -> em1        -> 192.168.2.254
  DMZ  (opt1)               -> em2        -> 192.168.3.254

 0) Logout (SSH only)                  8) Shell
 1) Assign Interfaces                  9) pfTop
 2) Set interface(s) IP address       10) Filter Logs
 3) Reset webConfigurator password    11) Restart webConfigurator
 4) Reset to factory defaults         12) pfSense Developer Shell
 5) Reboot system                     13) Upgrade from console
 6) Halt system                       14) Disable Secure Shell (sshd)
 7) Ping host

Enter an option: 8

[admin@pfsense-01.loiclaforet.org]/root(1): tail -f /var/squid/logs/access.log
1372595727.314   2793 192.168.2.12 TCP_MISS/200 28229 GET http://www.free.fr/im/2010/focu
1372595727.326      0 192.168.2.12 TCP_MISS/504 1356 GET http://www.free.fr/im/2010/leftr
1372595727.693   8538 192.168.2.12 TCP_MISS/200 69797 GET http://www.free.fr/im/temp/vds
1372595727.704      0 192.168.2.12 TCP_MISS/504 1346 GET http://www.free.fr/im/global/hd
1372595728.135   3422 192.168.2.12 TCP_MISS/200 22771 GET http://www.free.fr/im/2010/foc
```

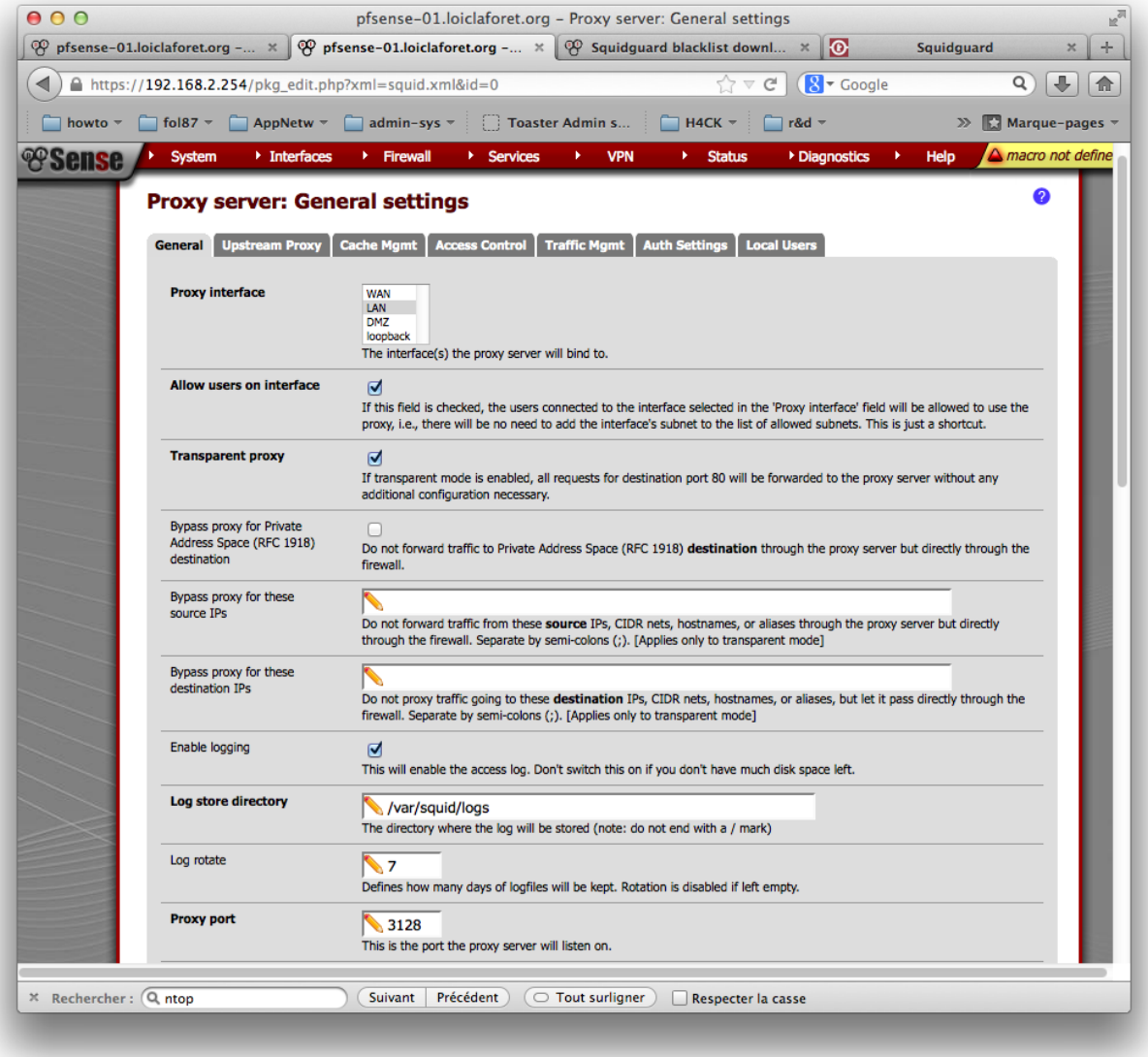

FIGURE VI.14 – Services Squid : configuration

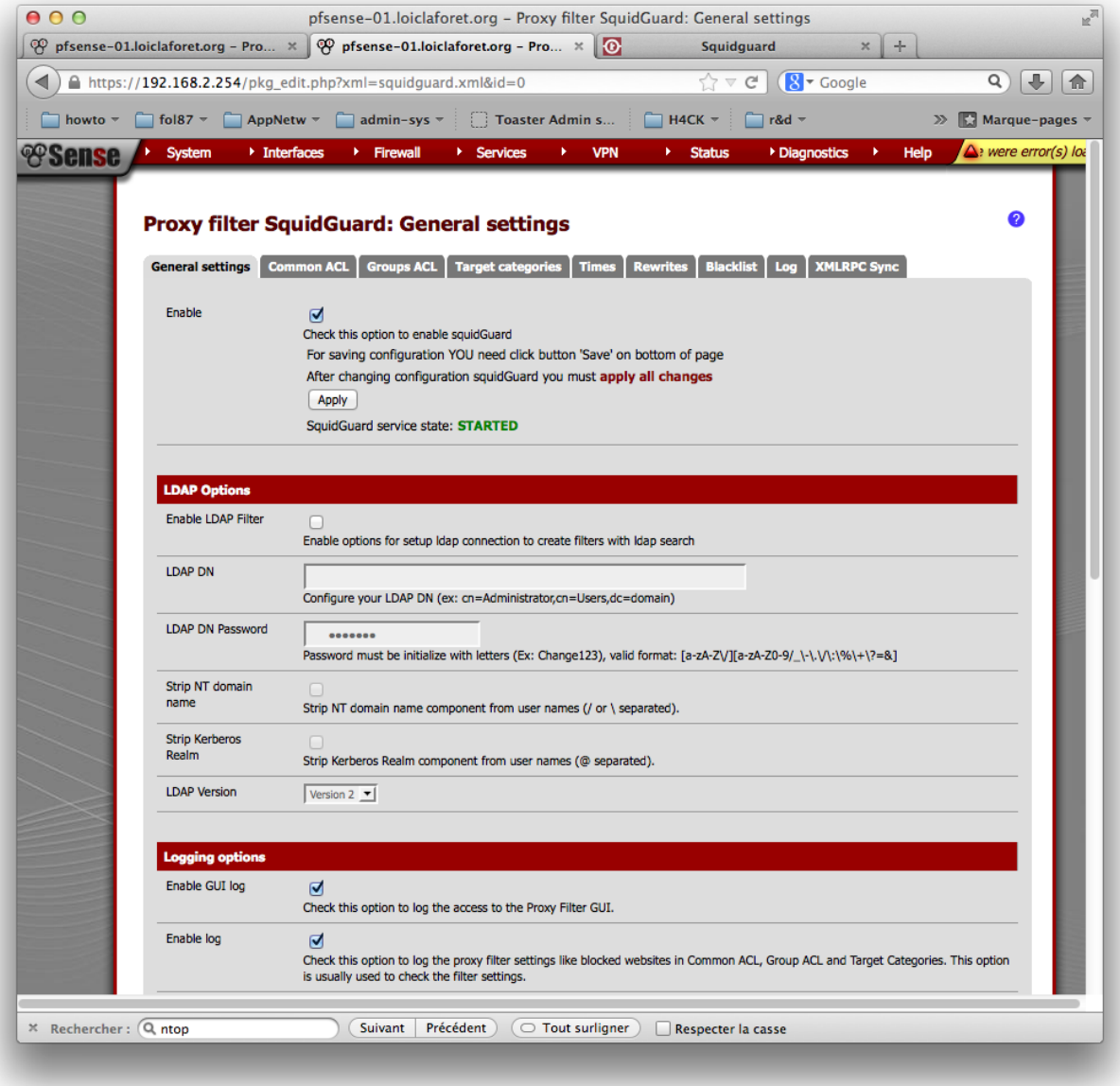

FIGURE VI.15 – Services SquidGuard : configuration

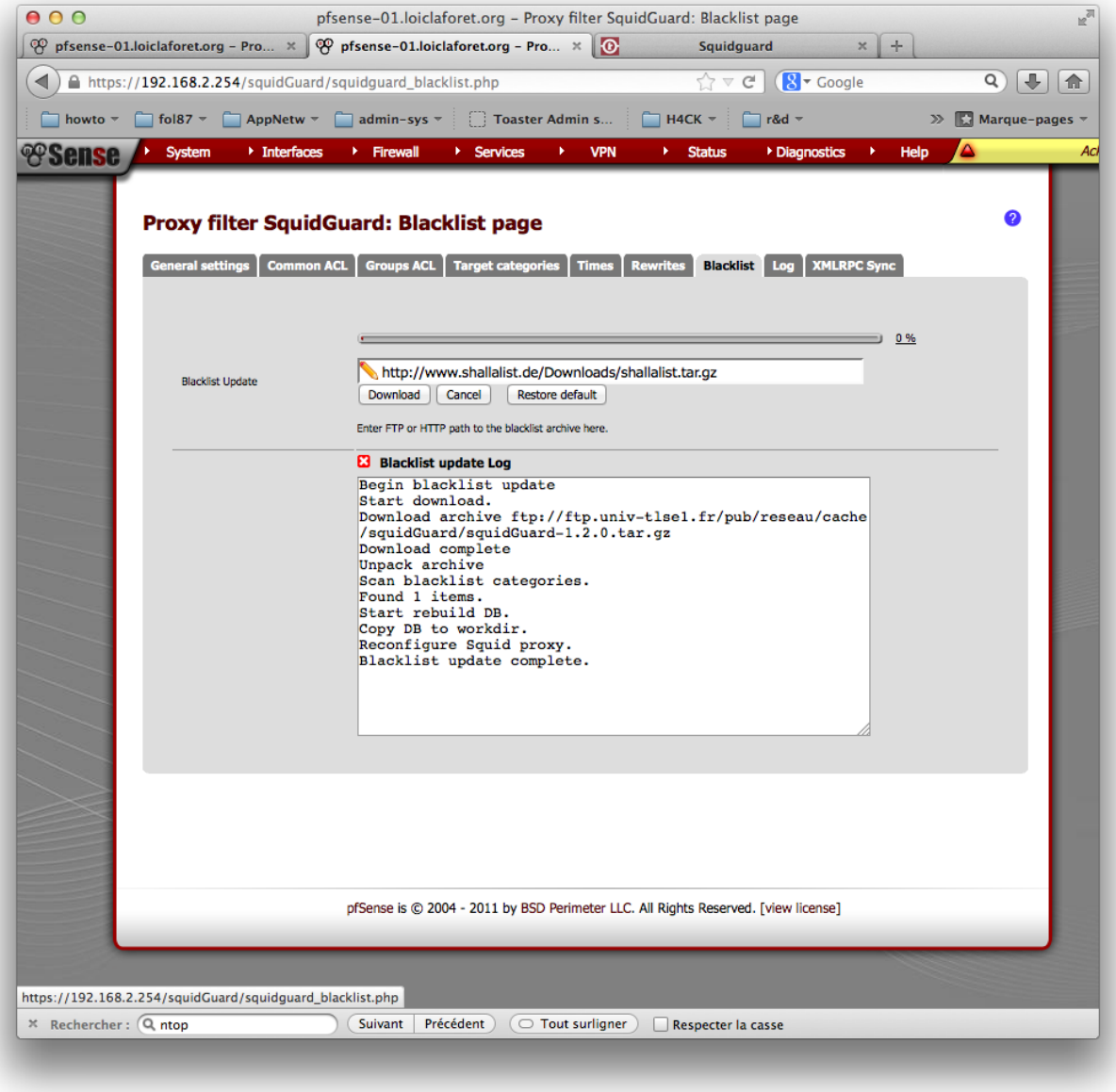

FIGURE VI.16 – Services SquidGuard : configuration d'une blacklist

Chapitre VII

Services et maintenance

pfSense offre une multitude de services réseaux et de fonctionnalités. Ce chapitre expose les services dédiés à la maintenance de notre firewall. N'hésitez pas à utiliser les commandes **ping** et **traceroute** qui permettent de réaliser des diagnostiques essentiels lors de l'implémentation d'un firewall et présentes dans l'interface Web de **pfSense**.

La première étape de ce chapitre est consacrée à l'utilisation d'un serveur syslog pour centraliser les logs de nos équipements.

I Centralisation des logs - Syslog

Idéal pour débugger une situation ou pour mieux comprendre un comportement **pfSense** log et centralise l'ensemble de ses journaux système et services dans le menu **Status | System logs** :

FIGURE VII.1 – Status System Logs : vue générale

Nous allons dans un premier temps paramétrer cette fonctionnalité pour faciliter la consultation des logs, pour afficher plus que la valeur par défaut (50). Nous allons également rediriger l'ensemble des journaux de **pfSense** vers un serveur **Syslog-ng** hébergé par une `Debian`. Ceci nous permettra de réaliser des filtres et tris beaucoup plus précis que par la simple interface de consultation proposée par **pfSense**.

- **Se rendre** dans le menu **Status | System Logs | Setting** ;
- **Cocher** la case permettant de changer l'ordre d'apparence des logs de **pfSense** ;
- **Ajouter** quelques lignes supplémentaires à l'affichage des logs proposés par **pfSense** ;
- **Cocher** l'activation d'un serveur syslog et **spécifier** l'adresse de ce dernier ;
- **Cocher** la case **Everything** ;
- **Valider** les changements par le bouton **Save** ;
- **Cliquer** sur le bouton **Apply changes** ;

Il est nécessaire ensuite de spécifier au service **syslog-ng** (installable par un `apt-get install` l'autorisation et la gestion des logs de notre firewall `pfSense-01`.

```
root@srvm-deb:~# nano /etc/syslog-ng/syslog-ng.conf
# LL
source s_net { udp (); };

destination df_pfsense01 { file("/var/log/pfsense/pfsense01.log"); };
filter f_pfsense01 { host( "192.168.2.254" ); };
log { source ( s_net ); filter( f_pfsense01 ); destination ( df_pfsense01 ); };

root@srvm-deb:~# /etc/init.d/syslog-ng restart
root@srvm-deb:~# netstat -tupwan
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Adresse locale      Adresse distante    Etat        PID/Prg
tcp        0      0 0.0.0.0:22          0.0.0.0:*           LISTEN      12993/sshd
tcp        0      0 192.168.2.253:22    192.168.2.12:56875  ESTABLISHED 14008/0
tcp6       0      0 :::22               :::*                LISTEN      12993/sshd
udp        0      0 0.0.0.0:514         0.0.0.0:*                       13636/syslog-ng
root@srvm-deb:~#
```

Nous éditons dans un premier temps le fichier de configuration de l'application **syslog-ng**, puis nous redémarrons le service pour prendre en compte nos modifications. La commande **netstat** suivante permet de vérifier le bon fonctionnement de notre modification.

Nous pouvons alors visualiser les logs remontés par le firewall en affichant le contenu du fichier correspondant :

```
root@srvm-deb:~# tail -f /var/log/pfsense/pfsense01.log
Jun 29 16:08:18 192.168.2.254 pf: 00:00:00.088355 rule 21/0(match): block in on em0:
Jun 29 16:08:18 192.168.2.254 pf:     192.168.1.178.138 > 192.168.1.255.138: NBT UDP
Jun 29 16:08:24 192.168.2.254 pf: 00:00:06.004151 rule 21/0(match): block in on em0:
Jun 29 16:08:24 192.168.2.254 pf:     192.168.1.132.65428 > 192.168.1.255.8612: UDP,
Jun 29 16:08:24 192.168.2.254 pf: 00:00:00.000109 rule 21/0(match): block in on em0:
Jun 29 16:08:24 192.168.2.254 pf:     192.168.1.132.62724 > 224.0.0.1.8612: UDP, leng
Jun 29 16:08:31 192.168.2.254 pf: 00:00:07.048120 rule 21/0(match): block in on em0:
Jun 29 16:08:31 192.168.2.254 pf:     192.168.1.132.56348 > 192.168.1.255.8612: UDP,
Jun 29 16:08:31 192.168.2.254 pf: 00:00:00.000010 rule 21/0(match): block in on em0:
Jun 29 16:08:31 192.168.2.254 pf:     192.168.1.132.64256 > 224.0.0.1.8612: UDP, len
Jun 29 16:08:36 192.168.2.254 pf: 00:00:04.956236 rule 21/0(match): block in on em0:
Jun 29 16:08:36 192.168.2.254 pf:     192.168.1.178.137 > 192.168.1.255.137: NBT UDP
Jun 29 16:08:37 192.168.2.254 pf: 00:00:00.739306 rule 21/0(match): block in on em0:
^C
root@srvm-deb:~#
```

Il est alors possible d'extraire ces logs dans une base de données mysql, ou faire des scripts à l'aide des commandes **sed, grep** pour analyser en profondeur ces logs et favoriser la pro-activité de la gestion de notre firewall.

Chapitre VIII

Travaux Pratiques

Le présent chapitre propose une mise en application par des exercices basés sur les différents éléments vus jusqu'à présent dans ce document.

I Installation d'un pfSense et configuration de la base du système

Objectifs :

+ Savoir installer un pfSense ;
+ Savoir identifier et configurer les interfaces d'un pfSense ;
+ Connaître et savoir mettre en application les éléments essentiels d'un firewall ;

Durée : 60 minutes ;

- **Créer** un firewall **pfSense** possédant 3 interfaces réseaux ;
- **Nommer** le firewall à l'aide de vos initiales ainsi : `pf-01-XX` ;
- **Paramétrer** les interfaces `LAN` et `WAN`, en respectant les instructions données par l'animateur ;
- **Ajouter** une interface `DMZ`, en respectant les instructions données par l'animateur ;
- **Modifier** les éléments de base du firewall (mot de passe admin, sécurisation de l'accès, accès ssh, mise à l'heure, firmware, sortie sur Internet ...) ;

II Configure les services fondamentaux pour gérer une infrastructure

Objectifs :

+ Savoir installer et configurer un service DHCP ;
+ Savoir paramétrer les différentes fonction de pfSense liées au service DNS ;

Durée : 30 minutes ;

- **Ajouter** une plage d'adresse dédiée à votre service DHCP sur votre interface `LAN` ;
- **Ajouter** une plage d'adresse dédiée à votre service DHCP sur votre interface `DMZ` ;

- **Forcer** votre service DHCP à fournir l'adresse IP DNS de votre firewall, ou celle d'un serveur DNS externe ;
- **Paramétrer** le service DHCP relai si vous possédez un serveur DHCP existant ;
- **Paramétrer** une ou plusieurs entrées *DNS Forwarding* pour *bypasser* la résolution habituelle réalisée par votre service DNS ;

III Configure les éléments essentiels à la sécurité des firewall pfSense

Objectifs :

+ Savoir utiliser les alias ;

+ Savoir paramétrer et gérer les règles de firewalling ;

+ Savoir paramétrer une règle de *port forwarding* ;

+ Savoir utiliser les plannings ;

Durée : 45 minutes ;

- **Ajouter**, en fonction des instructions données par l'animateur, l'ensemble des alias que vous jugez utile pour gérer l'ensemble de votre infrastructure (réseaux, hôtes, ports) ;
- **Configurer** les règles de firewalling essentielles pour sécuriser le trafic de l'interface LAN vers la WAN et LAN vers la DMZ ;
- **Configurer** les règles de firewalling essentielles pour sécuriser le trafic de l'interface DMZ vers le WAN et le WAN vers la DMZ ;
- **Ajouter** les règles de *port forwarding* nécessaires pour que les serveurs situés dans la DMZ soient accessibles par le WAN ;
- **Ajouter** deux plannings aux règles de firewalling préalablement déployées, l'une pour le LAN aux horaires de bureaux, et l'autre pour la DMZ uniquement les jours de semaine 24/24 ;

IV Interconnecter deux sites distants par un tunnel VPN IPsec

Objectifs :

+ Savoir paramétrer et gérer un tunnel VPN IPsec ;

Durée : 45 minutes ;

- **Créer**, en fonction des instructions données par l'animateur, les éléments nécessaires pour interconnecter 2 pfSense par le biais d'un tunnel IPsec ;
- **Configurer** les règles de firewalling nécessaires pour limiter uniquement le trafic nécessaire entre les deux sites ;
- **Configurer** un planning limitant l'accès du site 1 au site 2 tous les jours aux horaires de bureaux sauf entre 12h et 14h ;

V Ajouter des services avancés au firewall pfSense

Objectifs :

+ Savoir configurer une règle de NAT outbound ;
+ Savoir configurer un NAT 1 :1 ;
+ Comprendre l'utilisation des IP virtuelles ;
+ Savoir ajouter une route statique ;
+ Savoir ajouter une passerelle supplémentaire ;
+ Savoir configurer et gérer un portail captif ;
+ Savoir configurer et administrer un proxy de type Squid ;

Durée : 90 minutes ;

- **Créer** le paramétrage nécessaire pour permettre à un serveur d'une DMZ de répondre par sa deuxième interface LAN sur le protocole SSH ;
- **Paramétrer** votre **pfSense** pour rendre accessible le serveur www, situé dans la DMZ, par l'intermédiaire de l'adresse IP publique, et ce pour les ports 21, 22, 80, 443, 10000 ;
- **Ajouter** la route statique nécessaire pour joindre un réseau supplémentaire (à définir avec l'animateur) ;
- **Créer** un portail captif sur une interface supplémentaire, sinon sur la patte DMZ ;
- **Configurer** les services Squid et SquidGuard au pfSense, afin qu'il filtre l'ensemble du trafic de vos interfaces LAN* ;
- **Ajouter** au **dashboard** les graphiques liés aux trafics des différentes interfaces de **pfSense** ;

VI Déploiement d'une infrastructure complète en binôme

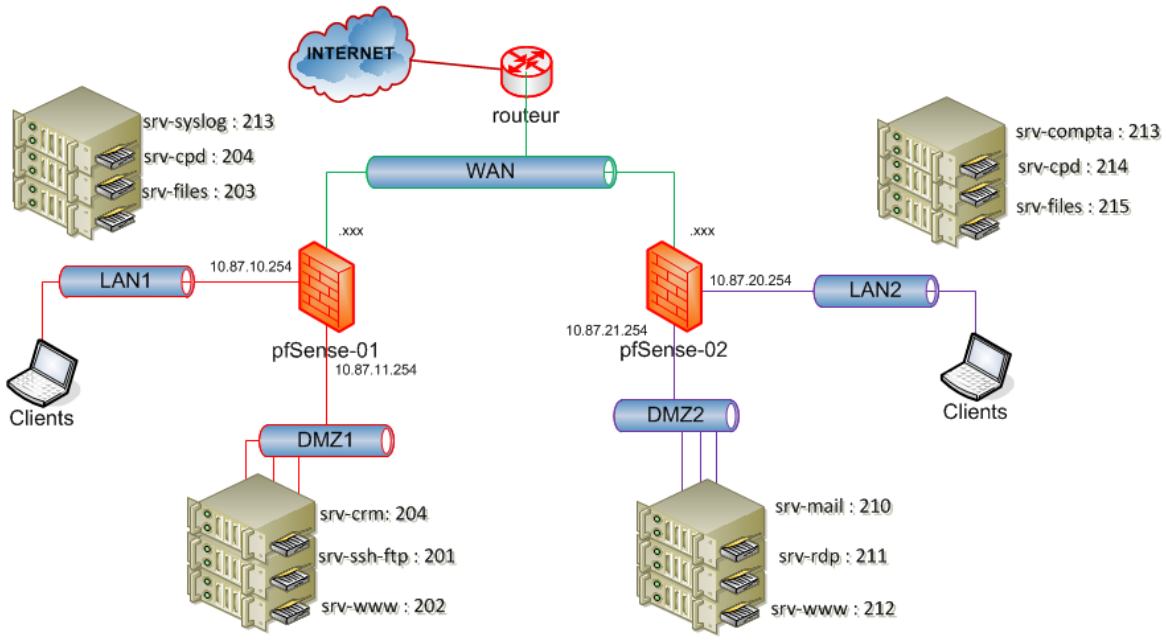

FIGURE VIII.1 – TP : Schéma d'infrastructure

Chapitre IX

Bibliographie

Table des figures

Bibliographie

[1] http://fr.wikipedia.org/wiki/Accueil

[2] http://pfsense.org/

[3] http://forum.pfsense.org/

[4] http://www.howtoforge.com

[5] http://www.google.fr

[6] *[Guide de mise en oeuvre de pfSense v2]* - drTIC / Lycees et CFA de l'enseignement agricole

[7] *[pfSense Cookbook]* - M. Williamson / Packt 2011

Index