# Présentation de pfsense

|  |  |
| --- | --- |
| How to Install and Configure pfSense on X86-64bit Win10 Mini PC? - Latest  open tech from seeed studio | pfsense est une distribution logicielle permettant de réaliser une passerelle réseau à partir d'un serveur x86.  Il date de 2004 à partir d’un fork de m0n0wall par Chris Buechler et Scott Ullrich. |

Très fréquemment rencontré dans les PME et les petites structures, pfsense offre une solution complète de routage, filtrage, VPN et partage de connexion. Il est basé sur pf, et intègre un grand nombre de composants tiers : serveur DHCP/DNS, serveur de temps, proxy web, monitoring...   
La configuration se fait entièrement via une interface web.

pfsense est disponible sous licence BSD. Un support officiel est proposé par la société *Netgate*.

pfsense peut être installé sur un simple ordinateur personnel comme sur un serveur.   
Basé sur PF (*packet filter*), comme *iptables* sur GNU/Linux, il est réputé pour sa fiabilité.

Après une installation en mode console, il s'administre ensuite simplement depuis une interface web et gère nativement les VLAN (802.1q).

## Focntionalités

pfsense ne fait pas seulement un pare-feu, il offre également toute une panoplie de services réseaux.

* **Pare-feu**  
  Le pare-feu est celui de *FreeBSD*, à savoir **PacketFilter**.
* **Table d'état**  
  La table d'état (*State table*) contient les informations sur les connexions réseaux.   
  Cela permet d'avoir un aperçu des connexions et surtout de créer des règles comme par exemple sur le nombre de connexion maximum pour un hôte.
* **Translation d'adresses réseaux** (NAT)  
  Permet de joindre un réseau privé vers l'extérieur.
* **VPN**  
  Permet la création de VPN IPsec, OpenVPN ou PPTP.
* **Serveur DHCP**.
* **Serveur DNS et DNS dynamiques**.
* **Portail Captif**.
* **Redondance et équilibrage de charge**.
* **Graphes pour la charge système et réseaux**
* …

Des logiciels complémentaires s'installent grâce à un système d’ajout.   
Ces derniers sont configurés pour s'intégrer à l'interface web.

Comme exemple d’ajout on trouve *squid* (comme serveur mandataire Web) et FreeRADIUS.

Le nombre d’ajout augmente régulièrement.

Il est aussi possible d'installer d'autres paquets que ceux proposés par l'interface, en ligne de commande.

# Environnement de travail

|  |  |
| --- | --- |
| Scénario 01 | Scénario 02 |
| Mise en place avec deux (2) machines virtuelles | **Mise en place avec trois (3) machines virtuelles** |
| MV 01 Système d’exploitation (SE) pfsense Interfaces réseau 2   (1 *Bridged* ou *NAT*  et 1*Segment LAN*) Processeur 1 Mémoire vive 512 Mo   (1Go recommandé) Autres paramètres Défaut | MV 01 Système d’exploitation (SE) **pfsense** Interfaces réseau **2**   (1 *Bridged* ou *NAT*  et 1 *Segment LAN*) Processeur **1** Mémoire vive **512 Mo**   (1Go recommandé) Autres paramètres **Défaut** |
| MV 02 Système d’exploitation (SE) SE avec   interface graphique   (Linux ou Windows) Interface réseau 1  (*Segment LAN*)  Client DHCP Processeur Selon le SE Mémoire Selon le SE | **MV 02** Système d’exploitation (SE) **SE avec   interface graphique** (Linux ou Windows)Interface réseau **1** (*Segment LAN*)  **Client DHCP** Processeur **Selon le SE** Mémoire **Selon le SE** |
|  | **MV 03** Système d’exploitation (SE) **SE CLI** (Linux)   avec Apache2 et vsFTPd installés Interface réseau **1**  (*Segment LAN*)  **Client DHCP** Processeur **Selon le SE** Mémoire **Selon le SE** |

# Installation de pfsense

pfsense est un pare-feu à état (*statefull firewall*) basé sur FreeBSD.   
En plus de sa puissance et flexibilité, la distribution inclut beaucoup de fonctionnalités.

|  |  |
| --- | --- |
| **Téléchargement de l’image iSO** | |
| Image ISO | Site du téléchargement <https://www.pfsense.org/download/> |
|  | Sélection de l’image à télécharger … |

|  |  |
| --- | --- |
| **Préparation de la machine virtuelle** | |
| Paramètres de la machine virtuelle  Mémoire vive 1 Go  Processeur(s) 1  Interfaces réseau   * Interface 1 Bridged Interface vers le  Réseau Externe * Interface 2 Segment LAN Interface vers le  Réseau interne * Interface 3 Segment LAN Interface vers le  Réseau périphérique   Remarque … Il est possible pour le moment de ne pas ajouter l’interface 3 Il sera possible de l’ajouter plus tard  Autre paramètres Par défaut  Remarque … On peut choisir le segment LAN présent par défaut ou en ajouter un |  |

|  |  |
| --- | --- |
| Étapes d’installation | |
| Étape 01 Démarrage  de la machine virtuelle  Au démarrage de la machine virtuelle, on laisse aller le démarrage  Aucune intervention à ce moment … |  |
|  |  |
| Étape 02 Installation de base  de pfsense  Acceptation du contrat d’utilisation  Il faut accepter la licence (Accept) de pfsense |  |
| Étape 02 Installation de base  de pfsense  Options d’installation  Quelques options sont disponibles …   * Installation sur disque dur de la machine virtuelle  (Install) ; * Démarrage de l’invite de commande de secours (Rescue Shell) ; * Réparation du système à l’aide d’un fichier de sauvegarde  (Recover config.xml) |  |
| Étape 02 Installation de base  de pfsense  Choix de la langue pour le clavier |  |
| Étape 02 Installation de base  de pfsense  Choix du partitionnement du disque   * Utilisation du BIOS (Auto (UFS) BIOS) ; * Utilisation du UEFI (Auto (UFS) UEFI) ; * Choix manuel (Manual) ; * Choix à l’aide de l’invite de commande  (Shell) ; * Choix d’une partition ZFS (Auto (ZFS)) | ­­­­­­­­­­­­­­­­- |
| Étape 02 Installation de base  de pfsense  Finalisation de l’installation  Il est possible cette étape de compléter l’installation à l’aide de l’invite de commandes  On redémarre pfsense pour compléter les paramètres  pfsense devrait redémarrer à partir du disque dur |  |
| Étape 02 Installation de base  de pfsense  On redémarre pfsense pour compléter les paramètres  pfsense devrait redémarrer à partir du disque dur |  |

|  |  |
| --- | --- |
| Paramètres de base pfsense | |
| Étape 01 Configuration des interfaces  À partir de l’invite de commande (menu de base) …  Assignation des interfaces  pfsense a identifié deux interfaces … WAN (em0)  LAN (em1)  Option 1 Assign interface(s) VLAN -> n (Pas de VLAN) WAN -> em0 LAN -> em1 OPT1 -> em2 \*  Option 2 Set interface(s) IP address pfsense a attribué par défaut les adresses suivantes … WAN -> DHCPv4 et DHCPv6 LAN -> 192.168.100.1 \*\*  Il est possible de les modifier au besoin | **Paramètres suggérés pour service DHCP** … Départ … 192.168.100.100/24 Fin … 192.168.100.200/24  **\*** L’interface OPT1 sera éventuellement désignée comme l’interface vers la DMZ  **\*\***  Il est important de désigner un réseau privé autre que celui de son réseau afin d’éviter les conflits |

|  |  |
| --- | --- |
| Vérification de la connectivité | |
| Étape 01 Mise en place  de la machine virtuelle | Voici les caractéristiques de la MV …   * La MV doit comporter un système d’exploitation graphique  (Windows ou Linux) ; * Pour la configuration de la MV, il est important que l’interface réseau soit sur le même segment de réseau que pfsense (Segment LAN – em1) ; * La MV doit être configuré comme cliente DHCP. pfsense devrait lui attribuer sa configuration IP à l’aide du protocole DHCP ; * Il faudra redémarrer la MV au besoin. |
| Étape 02 Configuration des interfaces  La MV a-t-elle obtenu sa configuration IP ? \*  La MV est-elle capable de rejoindre *pfsense* ?  La MV est-elle capable de pinger le serveur Web du collège ?  \* Si la MV n’a pas obtenu sa configuration IP, il faut, dans la console de gestion de pfsense, s’assurer que le service DHCP est en fonction  Pour ce faire, il faut suivre les étapes de l’option 2 – Set interface(s) Ip address et suivre les instructions pour la définition du service DHCP |  |
| Étape 03 Accès à Internet | On démarre un fureteur (*browser*) et on entre l’URL suivante … <http://www.cmaisonneuve.qc.ca>  La page d’accueil du site Web du collège devrait s’afficher |

|  |  |
| --- | --- |
| Étape 04 Accès à pfsense  à l’aide de l’interface Web | pfsense est un pare-feu qui peut être entièrement configuré par une interface web. Cette interface est, par défaut, accessible uniquement à partir d’un segment LAN du réseau. Autrement dit, il n’est pas possible d’y accéder à partir d’internet.  Toutefois, il est toujours possible de modifier l’accès de l’externe en désactivant le pare-feu à partir du menu Shell. Ceci n’est pas conseillé.  On démarre un fureteur (*browser*) et on entre l’URL suivante … <http://192.168.100.1> (adresse de l’interface interne par défaut)  Pour se connecter à l'interface graphique …  Nom d'usager … admin  Mot de passe … pfsense |
| Écran d’accueil de *pfsense* | |



|  |
| --- |
| Configuration de base |
| Étape 01 Modification du mot de passe de l’administrateur  À l’ouverture de la console de gestion (*dashboard*) de *pfsense*, on est invité à modifier le mot de passe de l’administrateur du système.  System -> User -> Manager -> Users -> Edit |
|  |

|  |
| --- |
| Étape 02 Modification de la console de gestion (*dashboard*)  Il est possible d’ajouter des widgets en cliquant sur le + en haut de la page. |
|  |

|  |
| --- |
| Étape 03 Tour d’horizon  Le menu au haut de la console de gestion donne accès aux ifférentes focntionnalités de pfsense. |
| Description du Menu   * System Paramètres de configuration du système * Interfaces Gestion des interfaces réseau * Firewall Configuration du pare-feu Aliases, NAT, Rules, … * Services DHCP, DNS, NTP, SNMP, … * VPN Configuration des divers VPN * Status États des différents services * Diagnostics Outils de résolution de problèmes * Help Aide pour l’utilisation et la configuration   Les trois premiers menus seront les plus utilisés  Afin de revenir rapidement à la console de gestion (dashboard), ou puet cliquer sur l’icône . |

|  |
| --- |
| Paramètres du pare-feu |
| Étape 01 Création d’alias  Pour pfsense un alias est utilisé pour associer ou regrouper des éléments sous un nom commun.  Ce nom est utilisable dans certaines zones, lors de la création de règles par exemple Un alias (ou groupe) peut être constitués de ports, d'adresses IP ou de réseaux.  Ces éléments, de différentes natures, ne peuvent pas être mélangés au sein d'un même alias.  Création d’un alias pour un hôte  Firewall -> Aliases    Slectionner le bouton Add …    Les choix possibles sont …    Les alias simplifient, entre autres, la gestion des règles.  Notion importante …  Pour donner suite à la plupart des modifications effectuée avec pfsense, il faudra, de manière globale, confirmer les modifications … |

|  |
| --- |
| Paramètres du pare-feu |
| Étape 02 Création de règles  Création d’une règle …  Firewall -> Rules  Il existe trois types de règle …   * Règles Flotantes ; * Règles WAN (trafic provenant du réseau externe – internet) ; * Règles LAN (trafic provenant du réseau interne)     Pour le trafic provenant du réseau externe (WAN) deux règles sont définies par défaut. Ces deux règles, comme leurs descritions l’indiquent, sont pour bloquer les paquets …   * ayant comme source des adresses IP privées (RFC 1918)  et * ayant des adresses sources impossibles appelés bogon (comme 0.0.0.0 et 169.254.0.0).     Pour le trafic provenant du réseau interne (lAN) trois règles sont définies par défaut. Ces trois règles, comme leurs descritions l’indiquent, sont pour autoriser les paquets …   * en direction de l’interface de gestion (webconfigurator) de pfsense ; * en direction de l’extérieur IPv4 (connexions ESTABLISHED ou RELATED)  afin que le pare-feu autorise rle retour  et * en direction de l’extérieur IPv6 (connexions ESTABLISHED ou RELATED)  afin que le pare-feu autoriser le retour.     Les règles de pare-feu flottantes présentent plusieurs avantages distincts par rapport aux règles non flottantes …   * Elles peuvent s'appliquer à plusieurs interfaces à la fois.  Cela nous évite d'avoir à faire des copies de règles essentiellement identiques sur différentes interfaces, et est pratique dans un certain nombre de situations dans lesquelles on souhaite qu'une règle soit en vigueur sur plusieurs interfaces ; * Considérant que les règles de pare-feu classiques ne sont invoquées lorsque les paquets laissent une interface, flottante des règles de pare-feu peut être invoqué lorsque le trafic entre une interface (LAN), lorsqu'il quitte une interface (WAN), ou les deux sens.   .  Exemple de création d’une première règle Bloquer les connexion Telnet du réseau interne vers le réseau interne …  Les étapes sont …   * On sélectionne l’interface interne (LAN) ; * On clique sur le bouton Add ;       Les options sont …   * Action  On définit l’action qu’effectue la règle (Pass, Block ou Reject) ; * Disabled On peut créer une règle et la mettre en fonction ultérieurement ; * Destination port range On précise le protocole de destination ; * Log   On veut journaliser lorsque la règle est appliquée ;   * Description On donne une description.   On confirme la création.  Remarque … Les actions possibles sont …   * Block  Détruit le paquet sans retour vers la source ; * Reject Un retour est effectué vers la source disant qu’il est refusé ; * Pass Accepte le paquet.     Positionnement des règles Lecture des règles, une par une  Les règles sont séquentielles, c’est-à-dire qu’elles sont lues dans l’ordre, l’une après l’autre.  Si un paquet est l’objet d’une règle qui le concerne, acceptation ou refus, la lecture s’arrête.  C’est pour cette raison que les règles les plus globales doivent être placées à la fin, alors que les règles les plus fines, elles, doivent être placées au début. Le risque majeur est qu’une règle globale englobe justement une règle plus fine qui ne sera jamais lue.  Ce qu'il est permis de faire avec un pare-feu traditionnel est donc de lire l’en-tête d’un paquet.  C’est un peu comme lire le titre d’un livre, mais sans avoir accès à son contenu.  Dans cet exemple, la règle qui bloque Telnet est positionnée avant les règles plus globales (*Default allow LAN*).  Notion importante … Encore une fois il vaut valider la création de la règle. |

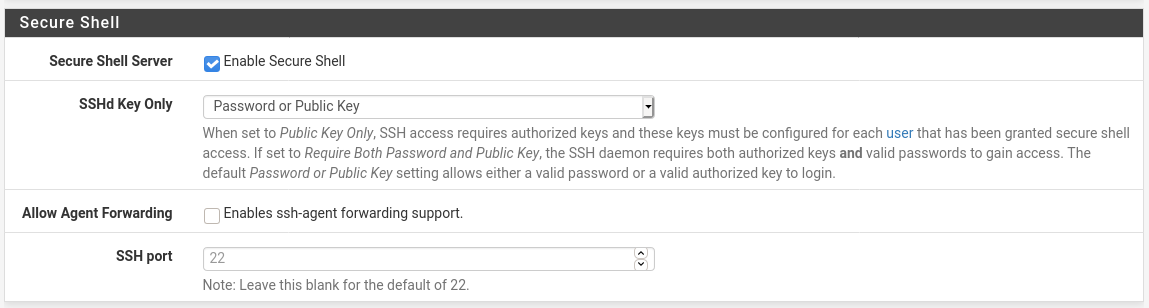
# Pour aller plus loin …

## Connexion à l’aide de SSH

Il est possible de se connecter à l’interface en ligne de commande de pfsense.

Pour ce faire …

À l’aide de l’interface graphique …  
**System -> Advanced - > Admin Access**



À l’aide de l’interface texte …

**Option 14 – Enable Secure shell (sshd)  
SSH is currently enabled (disabled). Would you like to disabled (enabled) [y/n] ?**

Il est ensuite possible de se connecter en tant qu’admin à l’aide du protocole SSH

## Désactivation du pare-feu

Un administrateur peut (très temporairement) désactiver les règles de pare-feu en utilisant la console ou SSH.

**Avertissement** …  
Cela désactive complètement pfce qui désactive les règles de pare-feu et NAT.   
Si le réseau géré par ce pare-feu repose sur NAT pour fonctionner, ce que la plupart font, l'exécution de cette commande interrompra la connectivité du LAN à Internet.

Pour désactiver le pare-feu, on se connecte à la console ou à l’aide de ssh et on sélectionne l'option 8 pour démarrer un shell …  
**>> pfctl -d**

Cette commande désactivera le pare-feu, y compris toutes les fonctions NAT.   
L'accès à l'interface graphique est désormais possible de n'importe où, au moins pendant quelques minutes ou jusqu'à ce qu'un processus sur le pare-feu provoque le rechargement du jeu de règles (ce qui correspond à presque toutes les actions d'enregistrement de page ou d'application des modifications).

Une fois que l'administrateur a ajusté les règles et retrouvé l'accès nécessaire, on réactive le pare-feu …  
**>> pfctl -e**

## Ajout de règles avec easyrule

L’utilitaire easyRule peut être utilisé depuis l'interface graphique ou encore depuis la ligne de commande afin d’ajouter rapidement des règles de pare-feu.

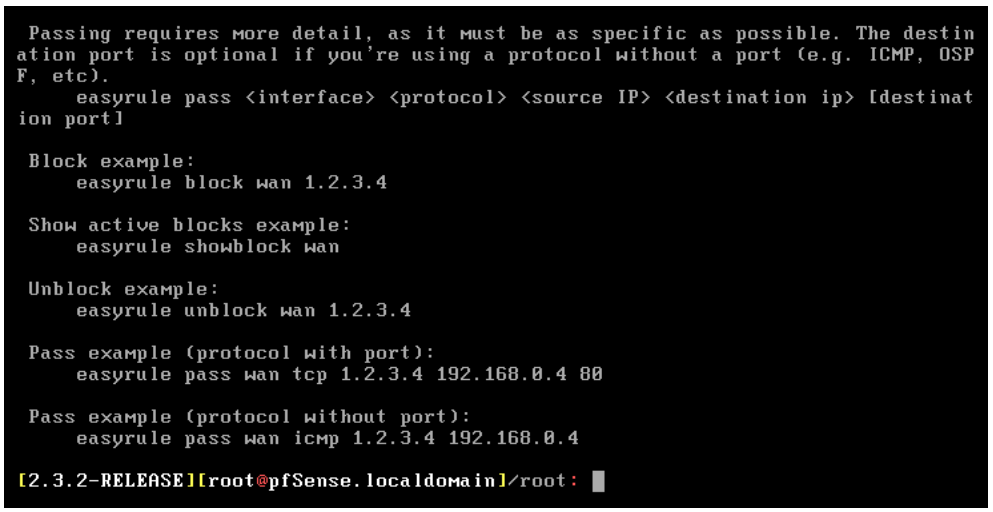
Depuis la console, on active l’interface de commande à l’aide de l’**option 8 Shell** ou à l’aide de la console SSH.

**>>** **easyrule block <interface> <IP source>  
>> easyrule pass <interface> <protocole> <IP source> <IP dest.> [port dest.]**

**Exemples** …

**>> easyrule block wan 1.2.3.4  
>> easyrule pass wan tcp 1.2.3.4 192.168.100.4 80   
>> easyrule pass wan icmp 1.2.3.4 192.168.100.4**

**Remarque** …  
Tout comme à l’aide de l’interface graphique, le pare-feu doit redémarrer afin de tenir compte des nouvelles règles.  
Si on a désactivé le pare-feu, il sera automatiquement réactivé.



Normalement, l'interface Web n'est accessible que depuis l'interface LAN de gestion (ou LAN par défaut).

Si, pour une raison quelconque, on est verrouillé ou on a besoin d'accéder à partir d'une adresse IP différente à l’aide de l'interface WAN, il est possible d’utiliser la ligne de commande easyrule afin d’ajouter temporairement une règle qui donne un accès depuis une adresse IP distante.

La commande suivante ajoute une règle de pare-feu, permettant le trafic TCP sur le port 443 à partir de l'adresse IP 206.167.44.10 vers l'adresse IP WAN sur 10.80.240.100 …  
**>> easyrule pass wan tcp 206.167.44.10 10.80.240.100 443**

Il est également possible d’autoriser l'accès SSH et configurer un port distant …  
(ssh -L localport:remoteip:remoteport remoteip)  
**>> easyrule pass wan tcp 206.167.44.100 10.80.240.100 22**

## Sauvegarde et restauration de la base de données pfsense

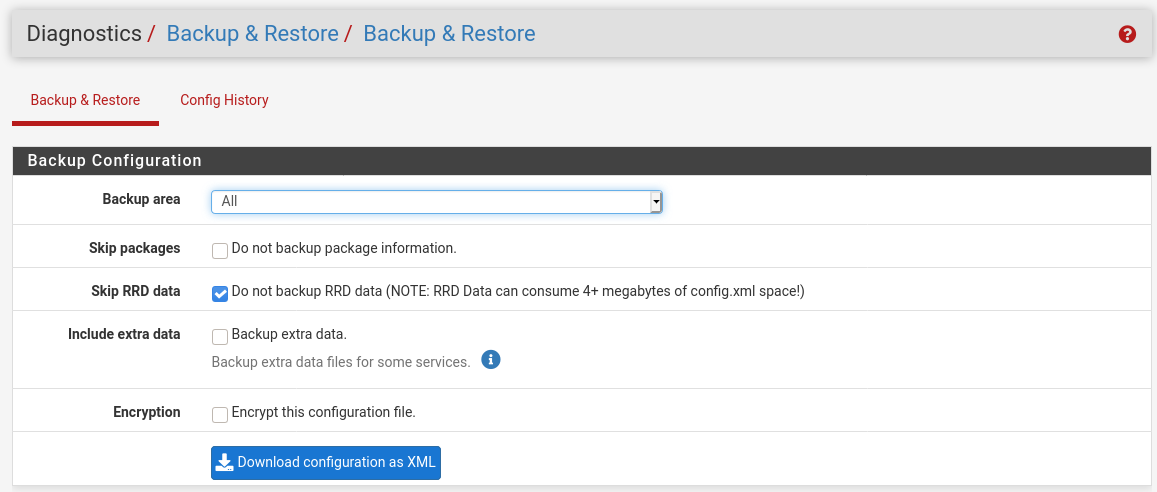
Il est toujours une bonne idée de sauvegarder la configuration de pfsense dans un fichier que l’on pourra déposer dans un lieu sécure.

En cas de défaillance de pfsense, il sera toujours possible de remonter facilement le pare-feu et ses services.

Faire une sauvegarde dans l'interface graphique est simple …

**Diagnostics -> Backup & Restore**

On définit les options souhaitées …

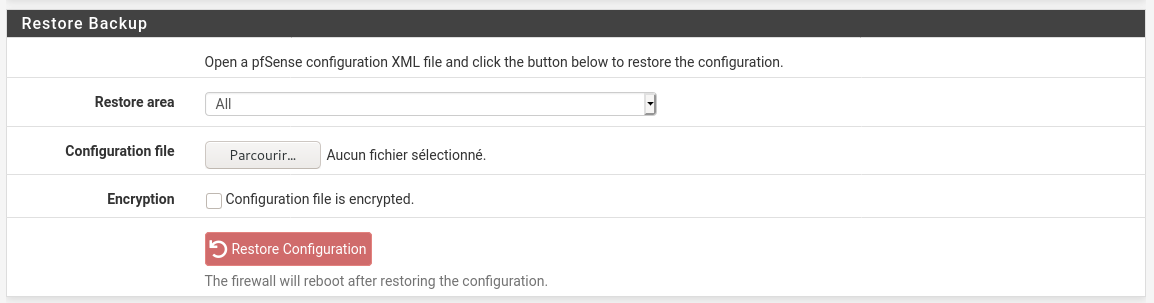


On clique sur **Download configuration as XML** pour démarrer le téléchargement.

Pour récupérer un fichier au format XML pour retrouver une configuration précédente …

**Diagnostics -> Backup & Restore**

On définit les options souhaitées …



On clique sur **Restore Configuration** pour démarrer la restauration.  
Comme indiqué, pfsense devrait redémarrer.

## Création d’un alias

Les alias fournissent un degré de séparation entre les règles de pare-feu/NAT et les valeurs qui peuvent changer à l'avenir, telles que les adresses IP, les réseaux et les ports.   
L'utilisation d'alias autant que possible facilite grandement la gestion des règles de pare-feu.

Pour ajouter un alias …  
**Firewall -> Aliases -> Add**

Un alias est un espace réservé pour les informations qui peuvent changer. Par exemple, on peut avoir une imprimante dont l'adresse IP est 192.168.100.150.   
En créant un alias pour cette adresse IP, on peut ensuite créer des règles de pare-feu et NAT qui font référence à l'imprimante sans avoir à changer toutes les règles si l'adresse IP de l'imprimante change.   
Si l'adresse IP change, il suffit de changer l'alias.

Lors de la création d'un alias, on peut choisir différents types …

* **Hôte(s)**  
  Cette option permet de spécifier une ou plusieurs adresses IP ou noms d'hôte.   
  Les noms d'hôte seront périodiquement résolus à nouveau ;
* **Réseau(x)**  
  On peut spécifier un réseau en spécifiant la partie réseau d'une adresse IP et le CIDR   
  (par exemple, 192.168.100.0/24) ;
* **Port(s)**  
  On peut spécifier un port ou une étendue des ports   
  (le premier et le dernier port doivent être séparés par deux points) ;
* **URL (IP)**  
  Il est possible de spécifier une ou plusieurs URL qui, à leur tour pointe sur des listes de texte d'adresses IP ;
* **URL (ports)**  
  On peut spécifier une ou plusieurs URL qui, à leur tour, pointe sur des listes de texte de ports ;
* **Table d'URL (IP)**  
  Similaire à URL (IP), on ne peut toutefois spécifier qu’une seule URL et la liste de texte chargée sera actualisée à un intervalle de son choix ;
* **Table URL (ports)**  
  Similaire à URL (ports), on ne peut toutefois spécifier qu’une seule URL et la liste de texte chargée sera actualisée à un intervalle de son choix.

### Utilisation d’un alias

On peut généralement utiliser un alias où que l’on est autorisé à entrer quel que soit le type de l'alias.   
Par exemple, si un alias fait référence à une adresse IP et que le champ que l’on saisit nécessite un nom d'hôte ou une adresse IP, il sera possible d’utiliser l'alias.  
On sera en mesure de dire si c'est le cas, car si on commence à saisir l'alias et que les alias sont autorisés dans le champ, la fonctionnalité de saisie semi-automatique de pfSense devrait faire apparaître tous les alias valides.

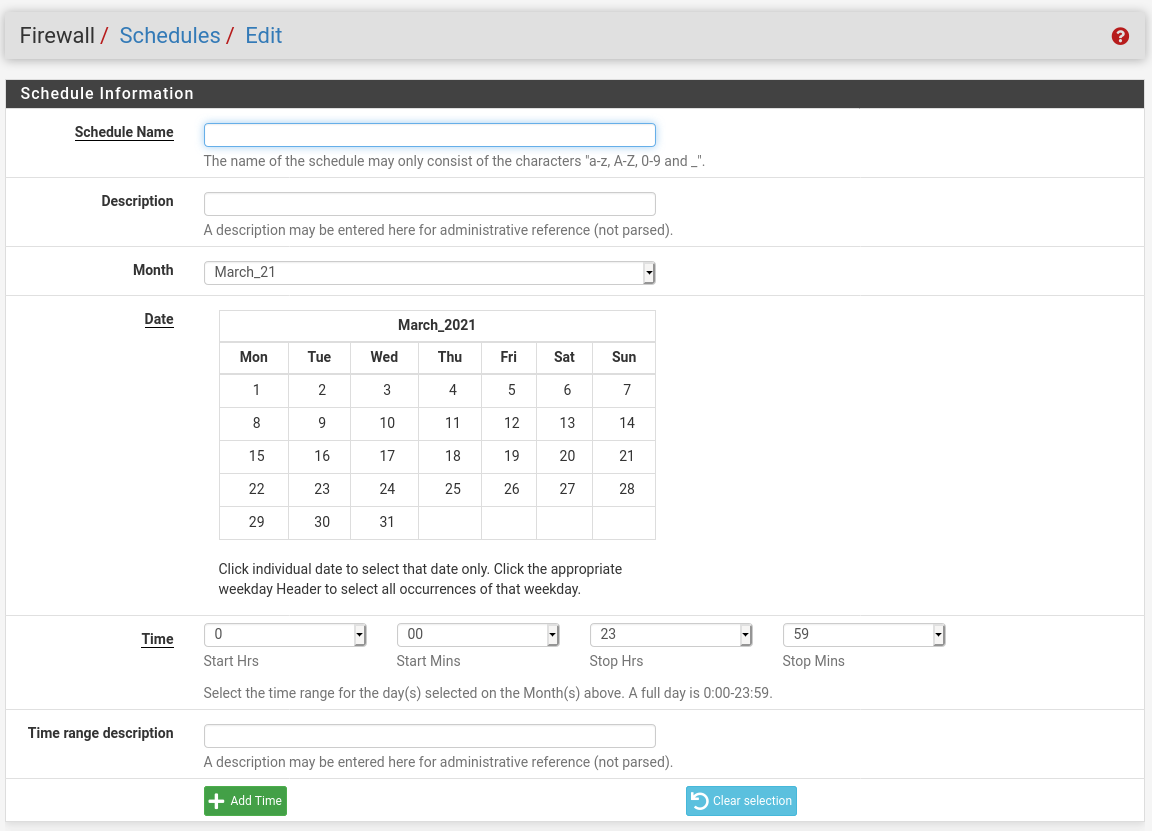
## Définition d'un calendrier de règles de pare-feu

Les horaires nous permettent de contrôler le moment où les règles de pare-feu sont activées.   
Ils sont principalement utilisés avec les règles de pare-feu, mais leur conception générique leur permet d'être utilisés avec de nombreuses fonctionnalités pfSense.

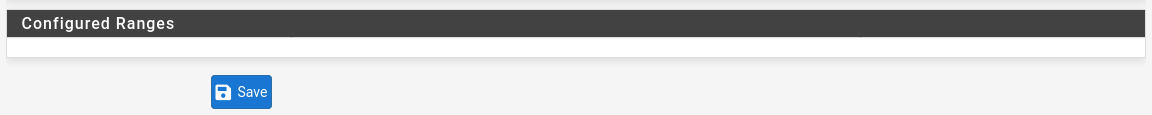
Si une règle de pare-feu spécifie une planification, la règle ne sera activée que pendant ces heures.

Pour créer une planification afin qu’une règle ne soit activée que pendant les heures de travail (9 h 00-17 h 00) …  
**Firewall -> Schedules.-> Add**

* Sur la page d’édition d’un calendrier, on entre un nom dans le champ Schedule Name ;
* On entre une brève description dans le champ Description ;
* Sur le calendrier, on sélectionne chacun des en-têtes de colonne pour les jours de la semaine   
  (lun, mar, mer, jeu, ven) pour sélectionner tous les jours de la semaine.
* On sélectionne le moment de la journée où les règles de pare-feu seront activées  
  (9h00 comme heure de début et 17h00 comme heure de fin) ;
* Il est possible de saisir une brève description de la plage horaire ;
* On sélectionne Add Time.  
  La plage horaire est maintenant ajoutée à la section Configured Ranges ;



* On sauvegarde le tout.



Les fonctionnalités associées à une planification ne seront actives que pendant la planification spécifiée.   
On doit par la suite associer une règle de pare-feu à l'entrée de planification.

**Firewall -> Rules** ; **Onglet LAN** pour afficher les règles du pare-feu LAN ;  
**Icône d'édition** (le crayon) sur une règle ;  
**Page d'édition de la règle** de pare-feu, **Display Advanced** ;  
**Advanced Options**, **Schedule** et on sélectionne le calendrier ;  
On sauvegarde **Save** ;  
**Apply Changes** pour recharger les règles du pare-feu.