

PFSense

Installation et

Configuration

Debian 11.2.0

23 MARS

Simplon

Créé par : Delcourt Gaspard



SIMPLON
.co

Table des matières

Installation.....	3
Matériels	3
Réseau	4
Accès http depuis le Client	5
La redirection du NAT	6
Le Pare-Feu et ses règles	7
La Topologie du Réseau.....	8

Installation

Sous VMWare, commencez par monter votre ISO puis lancer l'installation.
(Choisissez bien votre image).

ISO : <https://www.pfsense.org/download/>

Dans le cadre de notre Brief, nous aurons besoin :

- Une VM PFSense
- Une VM Debian 11.2.0 pour le serveur WEB
- Une VM Debian 11.2.0 pour le client

Matériels

Les VM seront ainsi configurer :

PFSense : 1 Processeur / 2G de RAM / 20G de stockage / 3 cartes réseaux

Serveur WEB : 2 Processeurs / 4G de RAM / 50G de stockage / 1 carte réseau

Client : 2 Processeurs / 2G de RAM / 40G de stockage / 1 carte réseau

Réseau

Pour le réseau, la configuration sera la suivante :

- **PFSense : Carte réseau WAN : 192.168.116.10/24**
 - Pas de DHCP
 - Passerelle de votre Routeur
- **PFSense : Carte réseau LAN : Lan Segment 1**
 - Pas de DHCP
 - IP Fixe : 192.168.1.10/24
 - Pas de passerelle
- **PFSense : Carte réseau DMZ : Lan Segment 2**
 - Pas de DHCP
 - IP Fixe : 10.10.10.10/24
 - Pas de passerelle

- **ServeurWeb : Carte Réseau**
 - Lan Segment 2
 - IP Fixe 10.10.10.20/24
 - DNS : 10.10.10.10
 - Passerelle : 10.10.10.10

- **Client : Carte Réseau**
 - Lan Segment 1
 - IP Fixe 192.168.1.20/24
 - DNS : 192.168.1.10
 - Passerelle : 192.168.1.10

Il se peut que vous ne voyiez pas la carte réseau DMZ (EPT1 par défaut).

Dans ce cas, pas de soucis, vous l'activerez par la suite à partir du navigateur du client.

Accès http depuis le Client

Depuis votre Client, lancer un navigateur de votre choix puis entrer l'adresse suivante : <http://192.168.1.10/>

Vous allez arriver sur l'interface web de PFSense (Si cela ne fonctionne pas, vérifier vos paramètres réseau)

Les identifiants de connexion par défaut sont :

- admin
- pfsense

Une fois sur la page suivez les instructions et modifier votre mot de passe, veillez à décocher l'option suivantes :

Block RFC1918 Private Networks*

RFC1918 Networks	
<input checked="" type="checkbox"/> Block RFC1918 Private Networks	<input type="checkbox"/> Block private networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Cette option pourrait vous bloquer quand vous faites de la virtualisation.

L'interface ici utilisé est en Français, pour la mettre en Français, rendez-vous dans la section « Settings » puis « general » puis dans localisation modifier la langue.

Une fois sur votre interface web, diriger vous vers « Interface » puis « affectations ».

Ici vous pourrez non seulement renommez vos interfaces mais également les activer, si votre DMZ n'était pas active vous pourriez l'activer en cliquant sur son nom puis en la paramétrant.

La redirection du NAT

Dans l'onglet Pare-feu et « NAT » dirigez votre WAN vers votre DMZ, de sorte à ce que les connexions entrantes passent dans votre DMZ.

Vous aurez à faire 2 redirections : HTTP et HTTPS.

Interface : WAN

Protocole : TCP

Destination : WAN address

Plage de port de destination : HTTPS

IP de redirection de cible : Hôte unitaire => 10.10.10.20

Port de redirection cible : HTTPS

Faites de même pour le http.

Le Pare-Feu et ses règles

Avant toutes manipulation, le pare-feu est totalement ouvert.

Vous pourrez, en fonction de la carte choisies autoriser ou non certaines actions interne ou externe.

Pare-feu / Règles / Modifier ☰ 📄 📄 ?

Modifier la règle de Pare-Feu

Action
Choisissez que faire des paquets qui correspondent aux critères ci-dessous.
Aide : La différence entre bloquer et rejeter est qu'avec 'Rejeter', un paquet (TCP, RST ou ICMP port unreachable pour UDP) est retourné à l'expéditeur, alors qu'avec 'Bloquer', le paquet est supprimé silencieusement. Dans tous les cas, le paquet est supprimé.

Désactivé Désactiver cette règle
Choisissez cette option pour désactiver cette règle sans la supprimer de la liste.

Interface
Choisissez l'interface d'où les paquets doivent provenir pour correspondre à cette règle.

Famille d'adresse
Choisissez la version du protocole IP à laquelle cette règle s'applique.

Protocole Les protocoles varient en fonction du port que vous voulez autoriser

Choisissez quel protocole IP cette règle devrait correspondre.

Source

Source Invert match /

La source correspond à l'endroit depuis lequel la requête est émise

[Afficher les options avancées](#)

La **plage de ports source** d'une connexion est généralement aléatoire et presque jamais égale au port de destination. Dans la plupart des cas, ce paramètre doit rester à sa valeur par défaut, any.

Destination

Destination Invert match /

Plage de port de destination
De Personnalisé(e) À Personnalisé(e)

Spécifiez le port destination ou la plage de port pour cette règle. Le champ « A » peut rester vide seulement si le filtre est sur un seul port.

Options additionnelles

Journalise Journaliser les paquets gérés par cette règle
Suggestion : Le pare-feu a un espace de journalisation limité. N'activez pas la journalisation de tout. Si vous faites beaucoup de journalisation considérez l'utilisation d'un serveur syslog distant (voir la page [Statut: Journaux système](#) : Paramètres).

Description

Une description est proposée ici pour aider l'administrateur. Un maximum de 52 caractères sera utilisé dans l'ensemble de règles et affiché dans le journal du pare-feu.

Options Avancées [Afficher les options avancées](#)

La Destination correspond à l'endroit depuis lequel la requête est reçue La plage de port de destination correspond au port que vous voulez autoriser ou refuser La description peut être très utile pour classer vos règles

[Enregistrer](#)

La Topologie du Réseau

