jmy37
GitHub : https://github.com/jmy37/infrathome

GUIDE D'INSTALLATION	
Pare-feu PFSense	
Infr@home_GUI-INST_01-Firewall	
Version 1.1	**Date d'application : 09/12/2020**
Projet/SI : Infr@home	

1. HISTORIQUE DES MODIFICATIONS

Version	Date	Auteur	Objet de la modification
1.0	20/10/2020	jmy37	Création du document
1.1	09/12/2020	jmy37	Ajout du serveur NTP (titre 5.4)

Tableau 1 : Historique des modifications

2. RÉFÉRENCES

2.1. Table des matières

2.2. Liste des tableaux

2.3. Liste des figures

3. PRÉAMBULE

Ce document décrit l'installation, l'exploitation et la résolution de pannes associées au composant « Pare-feu » de la solution « Infr@home ».

3.1. Le projet PFSense

PFSense est une solution de pare-feu s'appuyant sur le système d'exploitation FreeBSD. Le suivi du projet est assuré par la société Netgate. Le site https://www.pfsense.org/ met à disposition le téléchargement des sources et de nombreuses documentations relatives au projet.

3.2. Configuration requise

La configuration minimale[1] (trafic non-chiffré à 100Mo/s) pour PFSense est définie dans le Tableau 2.

Composant	Serveur virtuel	Serveur physique
Processeur	1 cœur	600MHz
Mémoire vive	512Mio	512Mio
Stockage	4Go	4Go
Réseau	Au moins une par réseau soutenu	Au moins une par réseau physique

Tableau 2 : Configuration requise pour PFSense

Les performances requises peuvent être affinées en fonction des fonctionnalités à activer. Le détail des calculs est donné sur le site de PFSense[2].

Il est ensuite nécessaire de récupérer la dernière image ISO de PFSense depuis le site de l'éditeur, en architecture x64 : https://www.pfsense.org/download/.

L'installation peut alors commencer.

[1] https://docs.netgate.com/pfsense/en/latest/book/hardware/minimum-hardware-requirements.html
[2] https://docs.netgate.com/pfsense/en/latest/book/hardware/hardware-sizing-guidance.html#feature-considerations

4. INSTALLATION

Une fois la machine virtuelle créée, démarrer sur le DVD à jour. Laisser le système se lancer avec les options par défaut. Ensuite, suivre l'assistant d'installation :

- Accepter les conditions d'utilisation
- Lancer l'installeur avec une disposition de clavier « *fr.kbd* »
- Choisir le partitionnement par défaut
- Ne pas ouvrir de shell à la fin de l'installation
- Redémarrer

Une fois le serveur redémarré, il est nécessaire de lui attribuer ses adresses IP :

- Choisir « *2* » pour assigner une adresse IP
- Choisir le numéro de l'adresse IP
- Saisir l'adresse IP souhaitée
- Saisir le masque désiré

La suite de la configuration se fait ensuite par l'interface web.

- Se connecter à l'aide des identifiants par défaut (admin|pfsense)
- Lancer l'assistant de configuration initiale
- Choisir le nom d'hôte, le nom de domaine et les serveurs DNS
- Choisir un serveur NTP et un fuseau horaire (« *Europe/Paris* »)
- Définir la configuration de l'interface WAN
- Définir la configuration de l'interface LAN
- Définir le mot de passe d'administration
- Recharger PFSense
- Accéder à « *System/Package Manager* »
- Accéder à « *Available Package* »
    - Installer les additions invitées (uniquement pour un hyperviseur VMware) : « *Open-VM-Tools* »

5. EXPLOITATION

Plusieurs méthodes existent pour créer des règles. Une méthode flexible consiste à créer des alias, et à configurer les règles pour ces alias.

5.1. Alias

La configuration des alias se réalise depuis « *Firewall/Aliases* ».

Une politique de nommage des alias peut être « ALIAS_<TYPE>_<FUNCTION>.

- Créer un nouvel alias
- Lui définir un nom et une description
- Configurer un alias de type « *Host* »
  - Définir une adresse ou un FQDN par hôte à intégrer à l'alias
  - Définir une description par hôte à intégrer à l'alias
- Configurer un alias de type « *Network* »
  - Définir une adresse réseau ou une plage d'adresses dans un réseau par réseau à intégrer à l'alias (séparation par un tiret)
  - Choisir le masque de sous-réseau par réseau à intégrer à l'alias
  - Ajouter une description par réseau à intégrer à l'alias
- Configurer un alias de type « Ports »
  - Définir un numéro de port ou une plage de ports à intégrer à l'alias (séparation par un pipe)
  - Ajouter une description par port à intégrer à l'alias

Les alias de type URL permettent d'importer des fichiers contenant jusqu'à 3000 entrées pour un même alias, ou bien des tables qui seront relues régulièrement, pouvant contenir plus de 30000 entrées.

5.2. Règles de pare-feu

Comme pour n'importe quel pare-feu, les règles s'appliquent dans l'ordre dans lequel elles sont indiquées, et le traitement s'arrête à la première règle rencontrée.

Par défaut, un paquet entrant va d'abord se voir appliquer les règles de filtrage de son interface d'arrivée, puis les règles flottantes seront appliquées. Si aucune de ces règles ne correspond à la définition du paquet, il sera alors supprimé.

Cependant, il est possible de créer des règles flottantes prioritaires, en cochant la case « *Quick* ». Ces règles flottantes sont également les seules à pouvoir s'appliquer à plusieurs interfaces en une seule fois.

Les logs systèmes permettent de consulter l'activité, et par conséquent de réaliser de la recherche de panne.

5.3. Passerelle

Les passerelles permettent de joindre les réseaux non-directement connectés au pare-feu.

- Accéder à « *System/Routing* »
- Créer une passerelle ou un groupe de passerelle
- Définir une passerelle par défaut
- Créer des routes statiques si nécessaire

5.4. Serveur NTP

5.4.1. Configuration du serveur

Cette partie doit être réalisée sur chaque serveur destiné à devenir un serveur NTP.

- Accéder à « *System/General Setup* »
- S'assurer qu'un serveur NTP au moins (4 à 5 recommandé) soit renseigné
- Sauvegarder
- Accéder à la page d'accueil du pare-feu
- Vérifier sur le widget « *NTP Status* » qu'une synchronisation soit bien effective, tel que prévu sur la Figure 1)
- Accéder à « *Services/NTP* »
- Sélectionner les interfaces pour lesquelles le pare-feu sera un serveur NTP
- Renseigner les serveurs NTP de référence
- Sauvegarder

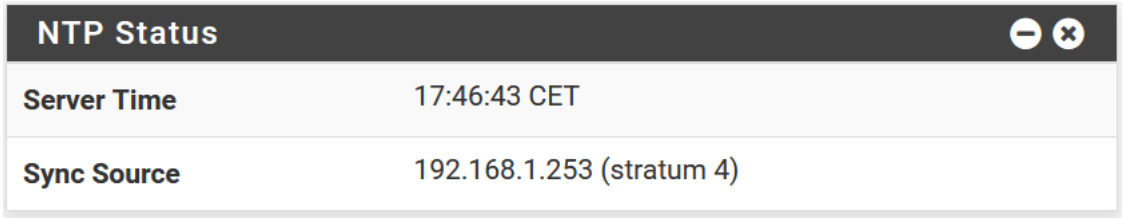


Figure 1 : Synchronisation avec un serveur NTP en amont

5.4.2. Configuration sur un client CentOS 8

La configuration peut facilement être testée depuis un serveur CentOS 8, qui exploite le client « *chrony* ».

- Supprimer toutes les lignes de serveurs du fichier de configuration chrony
- Ajouter les lignes des pares-feux
- Redémarrer chrony
- Vérifier la synchronisation effective

```
sed -i '/^server /d' /etc/chrony.conf

sed -i -- 's+# These servers were defined in the installation:+# These servers
were defined in the installation:\nserver 172.16.20.252 iburst\nserver
172.16.20.253 iburst+g' /etc/chrony.conf

systemctl restart chronyd

chronyc sources
210 Number of sources = 2
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^* vlsfwlacs01                   4   6   377     4    -98us[ -148us] +/-   56ms
^+ vlsfwlacs02                   4   6   377     3   +195us[ +195us] +/-   56ms
```

6. ANNEXES

6.1. Mise en place d'un serveur de secours

6.1.1. Installation

Une fois la machine virtuelle créée, démarrer sur le DVD à jour. Laisser le système se lancer avec les options par défaut. Ensuite, suivre l'assistant d'installation :

- Accepter les conditions d'utilisation
- Lancer l'installeur avec une disposition de clavier « *fr.kbd* »
- Choisir le partitionnement par défaut
- Ne pas ouvrir de shell à la fin de l'installation
- Redémarrer

Une fois le serveur redémarré, il est nécessaire de lui attribuer ses adresses IP :

- Choisir « *2* » pour assigner une adresse IP
- Choisir le numéro de l'adresse IP
- Saisir l'adresse IP souhaitée
- Saisir le masque désiré

La suite de la configuration se fait ensuite par l'interface web.

- Se connecter à l'aide des identifiants par défaut (admin|pfsense)
- Lancer l'assistant de configuration initiale
- Choisir le nom d'hôte, le nom de domaine et les serveurs DNS
- Choisir un serveur NTP et un fuseau horaire (« *Europe/Paris* »)
- Définir la configuration de l'interface WAN
- Définir la configuration de l'interface LAN
- Définir le mot de passe d'administration
- Recharger PFSense

6.1.2. Création de VIP (nécessaire pour chaque réseau soutenu)

Afin de procéder à la synchronisation des paramètres, depuis le premier serveur PFSense :

- Se connecter à l'interface Web
- Accéder à « *Firewall\Virtual IPs* »
- Ajouter une VIP
- Choisir le type « *CARP* », l'interface concernée et définir l'adresse qui sera utilisée par les postes clients
- Définir un mot de passe unique et robuste, qui sera renseigné également sur le second serveur
- Choisir la valeur « *Skew* » comme priorité : plus la valeur sera basse, plus le serveur sera prioritaire pour traiter les demandes

Cette création de VIP doit être réalisée pour chaque VLAN.

Si Hyper-V est utilisé, la fonctionnalité avancée d'usurpation d'adresse MAC doit être activée : le pare-feu va utiliser une adresse MAC différente pour chaque VIP, qui sera elle-même différente de celles des interfaces physiques.

6.1.3. VIP et NAT

Par défaut, les VIP sont disponibles, mais non-utilisées pour le NAT. Il faut donc forcer les instances PFSense à faire suivre le trafic sur les VIP (la règle n'a besoin d'être créée que sur le pare-feu primaire).

- Se connecter à l'interface Web
- Accéder à « *Firewall\NAT* »
- Dans l'onglet « *Outbound* », cocher la case « *Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)* »
- Ajouter une règle avec le format suivant du Tableau 3

Paramètre	Valeur
Disabled	Non
Do not NAT	Non
Interface	DMZ
Famille d'adresses	IPv4
Protocole	Tous
Source	Adresses réseaux soutenues
Destination	Toutes
Translation	CARP VIP DMZ
Pas de synchro XMLRPC	Désactivé

Tableau 3 : Configuration de la haute disponibilité pour le NAT

Dans le cadre de l'utilisation du serveur DHCP, ne pas oublier de mettre à jour la passerelle ainsi que l'adresse du serveur DHCP de secours dans la configuration du service DHCP.

Dans le cadre de l'utilisation du VPN, l'interface d'écoute doit être modifiée elle aussi, que ce soit pour OpenVPN ou pour des VPN IPsec.

6.1.4. Synchronisation des configurations et des états

Par défaut, la communication n'est pas autorisée entre les pares-feux.

- Se connecter à l'interface Web
- Accéder à « *Firewall\Rules* »
- Créer une règle provisoire sur le pare-feu secondaire permettant tout le trafic sur l'interface de synchronisation (cette règle disparaitra si la suite de la configuration est correctement réalisée)
- Créer une règle sur l'interface de synchronisation dédiée du pare-feu primaire permettant la synchronisation des configurations, conformément au Tableau 4

Paramètre	Valeur
Action	Pass
Désactivée	Non
Interface	FIREWALL_HA
Famille d'adresses	IPv4
Protocole	TCP
Type de source	Single host or alias
Adresse source	ALIAS_IP_FW_FIREWALL_HA
Type de destination	Single host or alias
Adresse de destination	ALIAS_IP_FW_FIREWALL_HA
Port de destination	HTTPS (443)
Logs	Désactivé
Description	Allow configuration synchronization

Tableau 4 : Règle de pare-feu - synchronisation de configurations

- Créer une règle sur l'interface de synchronisation dédiée du pare-feu primaire permettant la synchronisation des états, conformément au Tableau 5

Paramètre	Valeur
Action	Pass
Désactivée	Non
Interface	FIREWALL_HA
Famille d'adresses	IPv4
Protocole	PFSYNC
Type de source	Single host or alias
Adresse source	ALIAS_IP_FW_FIREWALL_HA
Type de destination	Single host or alias
Adresse de destination	ALIAS_IP_FW_FIREWALL_HA
Logs	Désactivé
Description	Allow state synchronization

Tableau 5 : Règle de pare-feu - synchronisation d'états

- Créer une règle sur l'interface de synchronisation dédiée du pare-feu primaire permettant la supervision et le diagnostic, conformément au Tableau 6

Paramètre	Valeur
Action	Pass
Désactivée	Non
Interface	FIREWALL_HA
Famille d'adresses	IPv4
Protocole	ICMP (echo request)
Type de source	Single host or alias
Adresse source	ALIAS_IP_FW_FIREWALL_HA
Type de destination	Single host or alias
Adresse de destination	ALIAS_IP_FW_FIREWALL_HA
Logs	Désactivé
Description	Allow ICMP echo for Diagnostics

Tableau 6 : Règle de pare-feu - diagnostic et supervision

- Appliquer les règles

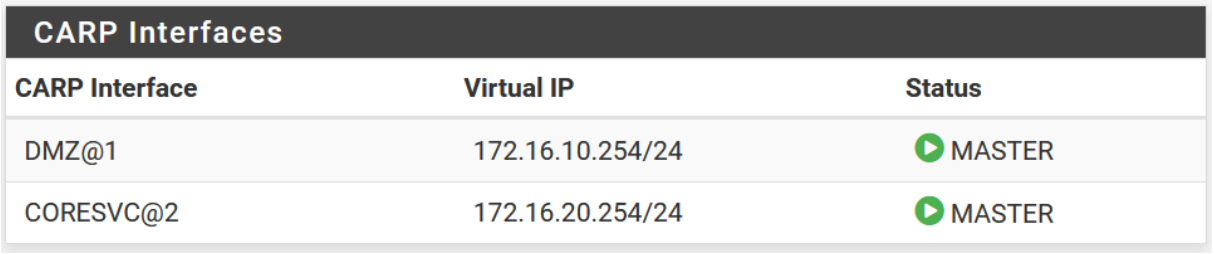
6.1.5. Activation de la haute disponibilité et du transfert de configurations

La dernière étape consiste à activer la haute-disponibilité et le transfert de configurations entre les deux serveurs (sur les deux serveurs).

- Se connecter à l'interface Web
- Accéder à « *System\High Avail. Sync* »
- Activer la synchronisation de statut
- Choisir l'interface de synchronisation dédiée
- Saisir l'adresse IP de l'autre serveur
- Compléter la partie relative à la synchronisation XMLRPC : adresse IP de l'autre serveur, nom d'utilisateur et mot de passe du compte d'administration Web du serveur de secours (ne rien compléter sur le serveur secondaire) et cocher toutes les cases

6.1.6. Vérification

Le statut des adresses virtuelles apparaît sur chaque pare-feu, sous « *Status/CARP* ». Il doit ressembler à la Figure 2



CARP Interfaces

CARP Interface	Virtual IP	Status
DMZ@1	172.16.10.254/24	MASTER
CORESVC@2	172.16.20.254/24	MASTER

Figure 2 : Statut des VIP CARP