Installation de Pfsense



Rémi RENARD

Date : 12/12/2023

CFA UTEC Emerainville

Table des matières

Table des matières	2
A quoi sert un pare-feu ?	3
Installation de base de pfSense (sur une VM)	4
Configuration des Interfaces	9
Mise en place de liste de blockage	11
Mise à jour Pfsense	15

3

utec*

A quoi sert un pare-feu ?

PfSense est un *pare-feu open source faisant également fonction de routeur* appartenant à Rubicon Communications et Netgate. Il est basé sur le système d'exploitation FreeBSD issu de la famille d'Unix

Un pare-feu, aussi nommé firewall, est un système de sécurité *(matériel ou logiciel)* qui va définir et contrôler les flux de données qui sont autorisés à entrer et sortir de votre réseau. Votre modem fournit par votre fournisseur d'accès à internet est un firewall matériel par exemple. Avec peu de fonction certes, mais c'est tout de même un firewall.

On dit globalement d'un firewall qu'il « applique la politique de sécurité de l'entreprise » grâce à des règles d'actions pour le trafic réseau. Pour simplifier, il va en fait accepter seulement les types de communications définies dans des règles et rejeter tout ce qui n'est pas explicitement autorisé.



4

Installation de base de pfSense (sur une VM)

Au niveau de la configuration de la VM pfsense, elle est assez légère (réalisé sous VMWare Workstation) :

- Devices	
📰 Memory	1 GB
Processors	2
🔚 Hard Disk (SCSI)	20 GB
💿 CD/DVD (IDE)	Using file E:\ISO\
🔁 Network Adapter	NAT
🗣 Network Adapter 2	Custom (VMnet3)
🚭 USB Controller	Present
් Sound Card	Auto detect
Display	Auto detect

En revanche, pfsense agissant comme un routeur, <u>il est impératif d'avoir au moins 2 cartes réseaux,</u> <u>sur 2 réseaux différents</u> : le réseau WAN (*Internet*) et le réseau LAN (*local*). La première carte va correspondre à l'interface WAN de pfsense, **elle a été positionnée en NAT** et **la seconde** sera l'interface LAN, elle est ici positionnée dans un réseau privé (*vmnet3*).Nous utiliserons également une 3eme carte qui servira de DMZ.

Commençons tout de suite par **installer pfsense**. Après avoir insérer l'ISO de pfsense dans VM dédiée, vous pouvez démarrer la machine. Le setup va démarrer automatiquement après quelques secondes .





Le setup va vous demander de **partitionner le disque** de stockage de la machine. Avec les touches fléchées de votre clavier, allez sur **« Auto (UFS) » et appuyez sur Entrée**.

- Partitioning Ном would you like to partition your disk?
Auto (2FS) Guided Root-on-ZFS Futo (UFS) Guided UFS Disk Setup Manual Manual Disk Setup (experts) Shell Open a shell and partition by hand
Cancel>

Vous pouvez confirmer que vous voulez utiliser le disque entier pour installer le système d'exploitation, pour cela, placez vous sur **« Entire Disk » et appuyez sur Entrée**.



Ici je reste simplement sur « MBR DOS Partitions » et appuyez sur Entrée pour valider.

FreeBSD Installer Hould (da0) share Using curre	Partition Scheme Select a partition scheme for this volume: APM Apple Partition Map BSD BSD Labels GPT GUID Partition Table BZ DDS Partitions C DK] [Cancel]
Bootable on most x86 sy	istems

L'installer propose un découpage sur le disque 0 (*nommé ici da0*), je n'ai pas besoin de modifier la proposition faites, placez vous sur **« Finish »** et appuyez sur Entrée.

FreeBSD Installer	
Partition Editor Please review the disk setup. When complete, press the Finish button. Iddl 20 GB MBR da0s1 20 GB BSD da0s1a 19 GB freebsd-ufs / da0s1b 1.0 GB freebsd-swap none	
[Create] [Delete] [Modify] [Revert] [Auto] [Finish]	

Un ultime avertissement sur le fait que le disque sera effacé pour faire face au système d'exploitation de pfsense. Placez vous sur « **Commit** » et appuyez sur Entrée.



Au démarrage, pfsense va se lancer, tester et configurer les services dont il a besoin.

Starting device Manager (devd)2023-08-14T16:36:43.739744+00:00 - php-fpm 372
∕rc.linkup: DHCP Client not running on wan (eм0), reconfiguring dhclient.
2023-08-14T16:36:43.768898+00:00 - php-fpm 371 /rc.linkup: Ignoring link eve
nt during boot sequence.
done.
Loading configurationdone.
Updating configurationMigrating System Memory RRD file to new format
. done .
Checking config backups consistencydone.
Setting up extended sysctlsdone.
Setting timezonedone.
Configuring loopback interfacedone.
Starting syslogdone.
Setting up interfaces microcodedone.
Configuring loopback interfacedone.
Configuring LAN interfacedone.
Configuring WAN interfacedone.
Configuring CARP settingsdone.
Syncing OpenVPN settingsdone.
Configuring firewalldone.
Starting PFLOGdone.
Setting up gateway monitorsdone.
Setting up static routesdone.
Setting up DNSs
Starting DNS Resolver

Une fois que le démarrage est finalisé, vous aurez la vue suivante sur la machine :

Starting CRON done. pfSense 2.7.1-RELEASE amd64 20231115-: Bootup complete	1786
FreeBSD/amd64 (pfSense.home.arpa) (tty	(804
VMware Virtual Machine - Netgate Devic	ce ID: 56fc4367196452a50762
*** Welcome to pfSense 2.7.1-RELEASE	(amd64) on pfSense ***
WAN (wan) -> le0 -> v4/l LAN (lan) -> le1 -> v4: OPT1 (opt1) -> le2 ->	DHCP4: 10.17.5.44/24 172.16.0.252/24
0) Logout (SSH only) 1) Assign Interfaces 2) Set interface(s) IP address 3) Reset webConfigurator password 4) Reset to factory defaults 5) Reboot system 6) Halt system	9) pfTop 10) Filter Logs 11) Restart неbConfigurator 12) PHP shell + pfSense tools 13) Update from console 14) Enable Secure Shell (sshd) 15) Restore recent configuration
7) Ping host 8) Shell	16) Restart PHP-FPM
Enter an option:	

Configuration des Interfaces

L'interface « WAN » obtient une adresse IP grâce au DHCP de l'école. Nous voulons changer l'adresse IP « LAN » pour quelle corresponde a notre réseau local. Donc nous allons tapez 2 puis encore 2 pour choisir l'interface LAN.



Nous ne voulons pas que l'adresse soit celle donnée par le DHCP, donc nous mettons "n" (pour non) et nous saisissons l'adresse que nous souhaitons pour la suite. Ensuite, le masque (en CIDR, donc 24 pour 255.255.255.0).

```
Available interfaces:
1 - WAN (le0 - dhcp)
2 - LAN (le1 - static)
3 - OPT1 (le2)
Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.30.253
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
255.255.0.0 = 16
     255.0.0.0
                    = 8
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

Pour la suite dans la configuration de l'interface nous répondons non partout ou juste entrer

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press (ENTER) for none:
Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press (ENTER) for none:
Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading filter...
DHCPD...
The IPv4 LAN address has been set to 192.168.30.253/24
You can now access the webConfigurator by opening the following URL in your web
browser:
http://192.168.30.253/
Press (ENTER) to continue.
```

Pour accéder à l'interface graphique de pfSense, il vous suffit d'entrer l'adresse IP de la carte LAN dans le navigateur de votre choix. N'oubliez pas d'aligner l'adresse IP de votre machine physique sur le même réseau que celui de la carte LAN.

État / Tableau de b	ord		+ 0
Informations système	100	Netgate Services And Support	00
Nom	pfSense.home.arpa	Contract type Community Sunport	
Utilisateur	admin@192.168.30.60 (Local Database)	Community Support Only	
Système	VMware Virtual Machine ID de l'appareil Netgate: 56fc4367196452a50762	NETGATE AND pfSense COMMUNITY SUPPORT RESOURCE	CES
BIOS	Fournisseur:Phoenix Technologies LTD Version:6.00 Date de sortie:Thu Nov 12 2020	If you purchased your plSense gateway firewall appliance from Netgate elected Community Support at the point of sale or installed rdSanse of	and on your own
Version	2.7.1-PRELASE (end64) Basé sur Wed Kor 15 18 06:00 CET 2023 FriesBD 14.0-CURRENT Version 2.7.2 est disponible Informations sur la version mises à jour à Sat Jan 20 12:30:32 CET 2024 6	hardnare, you have access to various community support resources. The NETGATE RESOURCE LIBRARY. You also may upgrade to a heighte Global Technical Assistance Cente Support subscription. Were always on Our team is staffed 24:07:055 commetted to developing enterprise relax, workdive support at a price per more than competitive when compared to others in our space.	This includes f (TAC) ind ind is
Type de CPU	AMD Ryzen 5 5600H with Radeon Graphics 2 CPUs: 2 package(e) x 1 core(e) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No	Upgrade Your Support Community Support Resource Netgate Global Support FAQ Official pHsense Training by Ne Netgate Professional Services Visit Netgate.com	s tgate
Encryption matérielle	Inactive		
Noyau PTI	Désactivé	If you decide to purchase a Netgate Global TAC Support subscription MUST have your Netgate Device ID (NDI) from your firewall in orde	n, you er to
MDS Mitigation	Inactive	validate support for this unit. Write down your NDI and store it in a sa	afe place.
Durée de fonctionnement	01 Hour 56 Minutes 07 Seconds	ruu can purchase TAC supports nere.	
Date/Heure actuels	Sat Jan 20 14:25:40 CET 2024		Ø
Serveur(s) DNS	• 127.0.0.1 • 192.168.1.1	Interfaces	100
Dernière modification de la configuration	Sat Jan 20 14:22:50 CET 2024	ALAN Autoselect 192.168.30.253	
Taille de la table d'état			

Mise en place de liste de blockage

Nous allons voir comment mettre en place une liste de blocage qui permet de refuser l'accès à certains sites web, en fonction des catégories telles que le téléchargement illégal, les sites d'achats, les sites pour adultes, etc.

Pour cela, nous pouvons la créer ou utiliser une déjà prête élaborée par d'autres personnes ayant recensé ces sites. Afin de mettre en place ces listes de blocage, nous devons installer plusieurs packages. Sans ces paquets, il nous sera impossible d'imposer des restrictions grâce à ces listes.

Dans mon cas, je vais mettre en place la blacklist de Toulouse. Pour ce faire, nous devons installer les paquets en accédant à "Système / Gestionnaire de paquets".

Une fois dans le gestionnaire, nous devons accéder à "Available Packages" et installer les paquets Squid, SquidGuard et Lightsquid. Nous pouvons rechercher ces paquets en utilisant le terme "squid". En l'absence de l'un de ces paquets, il nous sera impossible de mettre en place notre filtrage par rapport à nos sites web.

	€, Syste on	m • Interfaces • Firewall • Services • VPN • Status • Diagnostics • Help •	6
System	/ Pacl	kage Manager / Available Packages	0
Installed Pac	kages A	vailable Packages	
Search			Θ
Search terr	m	squid Both Search Diclear	
		Enter a search string or *nix regular expression to search package names and descriptions.	
Packages	5		
Name	Version	Description	
Lightsquid	3.0.6_4	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	🕂 Install
		Package Dependencies: % lighttpd-1.4.47_1 % lightsquid-1.8_5	
biupa	0.4.42_1	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.	🕂 Install
		Package Dependencies: Squidclamav-6.16 Squid_radius_auth-1.10 Squid-3.5.27 C-icap-modules-0.4.5	
squidGuard	1.16.4	High performance web proxy URL filter.	+ Install
			100

Pour chaque installation une demande de confirmation d'installation nous ai demander.

COMMUNITY EDITION	¢
System / Package Manager / Package Installer	0
Installed Packages Available Packages Package Installer	
Confirmation Required to install package pfSense-pkg-squidGuard.	
Confirm	

Pour chaque installation, nous avons l'avancement, il est important de ne pas fermer la page, si non l'installation échou.

Please wait while the installation of This may take several minutes. Do	pfSense-pkg-squidGuard completes. tot leave or refresh the page!	
Installed Packages Available Pack	ages Package Installer	
Package Installation		
<pre>>>> Installing pfSense-pkg-s Updating pfSense-core reposi pfSense-core repository is w</pre>	nuidGuard ory catalogue) to date.	
Updating pfSense repository pfSense repository is up to All repositories are up to d	atalogue late.	

Une fois les paquets installer, nous allons pouvoir installer notre blacklist, pour cela, nous devons

aller dans "Services / SquidGuard Proxy Filter".

Nous devons activer la blacklist et nous devons mettre le lien de notre blackliste, ce qui nous permet de la mettre à jour facilement en cas de mise à jour de celle-ci

Blacklist options	
Blacklist	Check this option to enable blacklist Do NOT enable this on NanoBSD installs!
Blacklist proxy	
	Blacklist upload proxy - enter here, or leave blank. Format: host:[port login:pass] . Default proxy port 1080. Example: "192.168.0.1:8080 user:pass"
Blacklist URL	p://dsi.ut-capitole.fr/black ists/download/blacklists_for_pfsense.tar.gz
	Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz).

Lien de la blacklist : http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

Ce n'est pas la seul blackliste existante, mais elle comprend beaucoup de site.

Maintenant, nous devons nous rendre dans "Système / Géneral / Blacklist", puis la télécharger

Blacklist Updat	e					
) % http://dei.ut.com	vitala fr/blacklints/da	walood/blocklists	for pfranca tar at			
inch://usi.uc.uab	noie.11/biackiists/do	writeddy blacknata_	_ioi_preense.tai.gz			
t and a local		and the second				
Sownload S	Cancel O Restor	e Default				
inter FTP or HTTP n	ath to the blacklist a	rchive here.				
and a second p	and to the blackhort a					
O plaatiliat						
🛛 Blacklist up	pdate Log					
Blacklist up	pdate Log					
Blacklist up Begin blacklist up	pdate Log					
Begin blacklist up Start download. Download archive h	pdate Log pdate nttp://dsi.ut-capit	ole.fr/blacklist	s/download			
Begin blacklist up Start download. Download archive h /blackliste_for_pf	pdate Log pdate http://dsi.ut-capit faense.tar.yz	ple.fr/blacklist.	s/download			
Blacklist up Begin blacklist up Start download. Download archive h blacklists_for_pf Download complete	pdate Log pdate http://dsi.ut-capit faense.tar.gz	ole.fr/blacklist	s/download			
Begin blacklist up Start download. Download archive h /blacklists_for pp Download complete Unpack archive	pdate Log pdate http://dsi.ut-capit foense.tar.gz	ole.fr/blacklist	s/download			
Blacklist up Begin blacklist up Start download. Download archive h /blacklists_for_pf Download complete Unpack archive Scan blacklist cat	pdate Log pdate http://dsi.ut-capit foemse.tar.gz regories.	ole.fr/blacklist	s/download			
C Blacklist up Start download. Download archive b Ohlacklist for pf Download complete Unpack archive Scan blacklist cat Found 50 items.	pdate Log pdate http://dsi.ut-capit fsense.tar.gz tegories.	ole.fr/blacklist.	s/download			
Blacklist up Begin blacklist up Start download. Download archive F /blacklists_for_pf Download complete Unpack archive Scan blacklist cat Start rebuild DS. Start rebuild DS.	pdate Log pdate http://dsi.ut-capit coense.tar.gz tegories.	ble.fr/blacklist	s/download			
C Blacklist up Begin blacklist up Start download. Download archive P blacklists_for pf Download complete Mupack archive Scan blacklist cat Found 58 items. Scart rebuild DB. Copy DB to workdin Economic Scut Coll	pdate Log pdate http://dsi.ut-capit foense.tar.gz regories. r. provv	ole.fr/blacklist	s/download			
Blacklist up Start download. Download archive F /blacklist_for pr Download complete Unpack archive Soan Dlacklist cat Found 58 items. Start rebuild DB. Start rebuild DB. Backlist worksin Reconfigure Squid Dacklist unders	pdate Log pdate http://dsi.ut-capit fsense.tar.gz tegories. c. proxy. opplate	ole.fr/blacklist	s/download			
Blacklist up Begin blacklist up Start download. Download archive F /blacklists_for_pf Download complete /blacklists_for_pf Download complete /blacklist_graph Start rebuild DB. Copy DB to workdis Blacklist update	pdate Log pdate http://dsi.ut-capit fsense.tar.gz tegories. r. proxy. complete.	ole.fr/blacklist	s/download			
© Blacklist up Begin blacklist up Start download. Download archive P bhlacklists_for pf Download complete Unpack archive Soan blacklist cat Found 58 items. Start rebuild DB. Copy DB to workdin Reconfigure Squid Blacklist update of	pdate Log pdate http://dsi.ut-capit foense.tar.gz tegories. r. proky. complete.	ole.fr/blacklist	s/download			
Blacklist up Begin blacklist up Start download. Download archive P /blacklist_for pp Download complete Unpack archive Scan blacklist complete Start rebuild DS. Copy DB to workdin Reconfigure Squid Blacklist update o	pdate Log pdate http://ddi.ut-capit foense.tar.gz tegories. r. proxy. complete.	ole.fr/blacklist	s/download			

Un avancement du téléchargement est fait et la base de données ajoute les éléments de la liste

IMUNITY EDITION	aus + Diagnostics +	ныр 🗸	
Package / SquidGuard / Blacklists			0
Seneral settings Common ACL Groups ACL Target categories Times Rev	writes Blacklist Lo	og XMLRPC Sync	
Blacklist Update			
Blacklist DB rebuild progress			
1 %			
L Download O Cancel D Restore Default			
Download Cancel Restore Default Enter FTP or HTTP path to the blacklist archive here			
Download Cancel Crestore Default Enter FTP or HTTP path to the blacklist archive here.			
Download Cancel Restore Default Enter FTP or HTTP path to the blacklist archive here. Blacklist update Log			
Download Cancel Restore Default Enter FTP or HTTP path to the blacklist archive here. Blacklist update Log Begin blacklist update			
Download Cancel Restore Default Enter FTP or HTTP path to the blacklist archive here. Blacklist update Log Begin blacklist update Start download.			
Download Cancel Restore Default Enter FTP or HTTP path to the blacklist archive here. Blacklist update Log Begin blacklist update Start download. Download archive http://dsi.ut-capitole.fr/blacklists/download /blacklists for pfaense.tar.oz			
Download Cancel Cancel			
Download Cancel Restore Default Enter FTP or HTTP path to the blacklist archive here. Blacklist update Log Begin blacklist update Start download. Download archive http://dsi.ut-capitole.fr/blacklists/download /blacklists_for_pfsense.tar.gz Download complete Unpack archive			
Download Cancel Restore Default Enter FTP or HTTP path to the blacklist archive here. Blacklist update Log Begin blacklist update Start download. Download archive http://dsi.ut-capitole.fr/blacklists/download /blacklists_for_pfsense.tar.gz Download complete Unpack archive Scan blacklist categories.			
Download Cancel Restore Default Enter FTP or HTTP path to the blacklist archive here. Blacklist update Log Begin blacklist update Start download. Download archive http://dsi.ut-capitole.fr/blacklists/download /blacklist_for_pfsense.tar.gz Download complete Unpack archive Scan blacklist categories. Found St items.			_

Une fois notre blackliste télécharger et ajouter, nous devons nous rendre dans "Services /

SquidGuard Proxy Filter" et activer le service SquidGuard si il ne l'est pas

eral Options	(
En	Able Check to Important: The Save To activa	his option to enab Please set up at lo button at the b ite squidGuard o	le squidGuard. east one category on thi lottom of this page i configuration chang	e 'Target Cate must be cliv es, the App	gories' tab befo cked to save Iy button mu	ore enabling. Se configuratio ist be clicke e	ee this link f n change: d.	or details. S.

On verifie que notre paquet squidGuard soit bien actif

Mise à jour Pfsense

Les mises à jour sont importantes, tant au niveau des fonctionnalités que de la sécurité. La mise à jour de PFSENSE est facile à effectuer. Pour cela, nous devons nous connecter au panneau de contrôle, et sur le tableau de bord, nous trouvons la version actuelle. Comme on peut le constater, la version 2.7.2 est disponible, et nous pouvons donc la mettre à jour en cliquant sur le bouton 'Confirmer'

Système / Mettre	à jour / Mise à jour système	0
Mise à jour système F	Paramètres de mise à jour	
Confirmation requise	pour mettre à jour le système pfSense.	
Version	Current Stable Release (2.7.2) Veuillez sélectionner la version à partir de laquelle mettre à jour le système. L'utilisation de la version de développement est à vos risques et périls!	
Système de base actuel	2.7.1	
Dernier système de base	2.7.2	
Confirmer la mise à jour	✓ Confirmer	

Puis l'installation se fait, mais on ne doit ni quitter ni fermer cette page car la mise à jour va s'arrêter

et risque de planter PFSENSE.

Système / Mettre à jour / Mise à jour système	0
Veuillez patienter pendant que la mise à jour se termine. Cela peut prendre plusieurs minutes. Ne quittez pas et ne rafraîchissez pas la page !	
Mise à jour système Paramètres de mise à jour	
Mise à jour du système	
isc-dhcp44-relay: 4.4.3P1_3 -> 4.4.3P1_4 [pfSense]	
openvor: 2.6.7 -> 2.6.8 1 [ofSense]	
pfSense: 2.7.1 -> 2.7.2 [pfSense]	
pfSense-base: 2.7.1 -> 2.7.2 [pfSense-core]	
pfSense-boot: 2.7.1 -> 2.7.2 [pfSense-core]	
pfSense-default-config: 2.7.1 -> 2.7.2 [pfSense]	
program with the program of the prog	
strongswan: 5.9.11_2 -> 5.9.11_3 [pfSense]	
Number of packages to be upgraded: 11	

Nous avons un message qui nous informe que la mise à jour est fini et que PFSENSE doit redémarrer.

Système / Mettre	e à jour / Mise à jour système	0
Upgrade will continue after	the system restarts. Please do not reset or power off.	
Mise à jour système	Paramètres de mise à jour	
	Redémarrage La page se rechargera automatiquement dans 70 secondes	
Mise à jour du systèr	me	
<pre>>>> Updating repositori Updating pfSense-core r Fetching meta.conf: . c Fetching packagesite.pk Processing entries: . c pfSense-core repository Updating pfSense reposi Fetching meta.conf: . c Fetching mata.conf: . c Fetching packagesite.pk Processing entries: La mise à jour à l</pre>	<pre>es metadata 'epository catalogue Jone (g: , done Jone / update completed. 4 packages processed. itory catalogue Jone (g: done bien été faite.</pre>	
Système / Mettre	e à jour / Mise à jour système	0
Mise à jour système	Paramètres de mise à jour	
Confirmation requise	pour mettre à jour le système pfSense.	
Version	Current Stable Release (2.7.2)	

Version	Current Stable Release (2.7.2)
	Veuillez sélectionner la version à partir de laquelle mettre à jour le système. L'utilisation de la version de développement est à vos risques et périls!
Système de base actuel	2.7.2
Dernier système de base	2.7.2
État	À jour.