## FIREWALL PFSENSE BTS – SIO 2 / SISR



## **Clément Paccard**

22/01/2024

# TABLE DES MATIERES

FII	REWALL PFSENSE	3
Intr	oduction	3
1-	Installer PFsense	.5
2-	Configurer PFsense	6
3-	Réglage PFsense	.8
Α.	SSH/HTTPS	8
Β.	Ajouter une passerelle	10
C.	Ajouter une route	11
4-	Portail Captif	12
COI	NCLUSION	15

## FIREWALL PFSENSE

#### INTRODUCTION

Cette procédure montre comment installer et paramétrer un Pare-feu PFsense.

Précédemment nous avions configurer deux Routeur sur Windows serveur, un serveur DHCP avec basculement et un serveur DNS pour que les PC de différents réseaux puissent communiquer entre eux et avec internet en recevant une configuration IP complète et puissent résoudre les noms.



Le pare-feu, ou Firewall, joue un rôle crucial dans la sécurité des réseaux informatiques. Il agit comme une barrière protectrice en contrôlant et en filtrant le trafic réseau, autorisant ainsi uniquement les communications autorisées tout en bloquant les activités non autorisées. L'implémentation d'un pare-feu est essentielle pour renforcer la sécurité d'un réseau en surveillant le flux de données entrant et sortant.

PFsense, une solution open-source de pare-feu et de routeur, offre une virtualisation pratique pour mettre en œuvre des politiques de sécurité avancées. Cette solution permet de définir des règles de filtrage du trafic, de gérer l'accès aux ressources réseau, et de protéger les systèmes contre les menaces potentielles.

Le fonctionnement d'un pare-feu repose sur des règles configurées par l'administrateur réseau. Ces règles déterminent quels types de trafic sont autorisés ou bloqués, en fonction de critères tels que l'adresse IP source, l'adresse IP de destination, le port, etc. PFsense offre une interface conviviale pour la configuration de ces règles, facilitant ainsi la gestion des politiques de sécurité.

Dans notre cas, le pare-feu PFsense sera déployé en tant que machine virtuelle, assurant ainsi la protection du réseau. Des règles spécifiques seront définies pour contrôler le trafic entrant et sortant, renforçant ainsi la sécurité globale de l'environnement réseau.

L'adresse IP respective de chaque instance PFsense sera configurée, et des règles spécifiques seront établies pour garantir une protection efficace contre les menaces potentielles. La virtualisation de PFsense offre une solution agile et évolutive pour répondre aux besoins changeants de sécurité réseau.

Nous allons créer également 3 LAN supplémentaires :

- LAN 0 : 192.168.10.0/27
- DMZ: 172.16.0.0/12
- WIFI : 10.0.0.0/8

#### **1-INSTALLER PFSENSE**

Pour commencer il faut créer une nouvelle machine virtuelle avec l'ISO de PFsense. En démarrant la VM nous avons quelques menus à passer et/ou configurer :

Sélectionner Install avec les flèches puis appuyer sur entrer (Ok)

Welcome to pfSense!	Welcome
<mark>Install</mark> Rescue Shell Recover config.×Ml	<mark>Install pfSense</mark> Launch a shell for rescue operations Recover config.xml from a previous install
<u> </u>	<mark>OK &gt;</mark> <cancel></cancel>

Sélectionner Install avec les flèches puis appuyer sur entrer (Ok) puis sélectionner stripe avec les flèches puis appuyer sur entrer (Ok)

>>> Install	Proceed with Installation
Pool Type∕Disks:	stripe: Ø disks
Rescan Devices	*
Disk Info	*
Роо1 Наме	pfSense
Force 4K Sectors?	YES
Encrypt Disks?	NO
Partition Scheme	GPT (BIOS)
Swap Size	1g
1 Mirror Swap?	NÖ
	NO

Select Virtual Device type:						
stripe	Stripe - No Redundancy					
Mirror	Mirror – n-Way Mirroring					
raid10	RAID 1+0 - n x 2-Way Mirrors					
raidz1	RAID-Z1 - Single Redundant RAID					
raidz2	RAID-Z2 - Double Redundant RAID					
raidz3	RAID-23 - Triple Redundant RAID					
L						
	(Cancel)					
rp	ress arrous TAB or ENTED1					

Ne pas oublier de cocher la case [] à l'aide de la barre d'espace puis enter et enter encore.

ZFS Configuration	ZFS Configuration stripe: Not enough disks selected. (0 < 1 minimum)
[*] 1a0 VMware, VMware Virtual S	Change Selection> < Cancel > [Press arrows, TAB or ENTER]
< Dk > < Back >	

Ici on confirme avec enter puis une fois PF installé on redémarre.



#### **2-CONFIGURER PFSENSE**

Nous allons commencer par configurer les interfaces avec leurs IP respectives.

- WAN : DHCP
- LAN 0 : 192.168.10.30
- DMZ : 172.16.255.254
- WIFI: 10.255.255.254

Pour ce faire il faut aller dans le menu 1 de PFsense :

You can now access the webConfigurator by opening the following URL in your web browser: http://10.255.255.254/ Press {ENTER} to continue. WMware Virtual Machine - Netgate Device ID: 405cd3d4625b9270859c \*\*\*\* Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense \*\*\* WAN (wan) -> em1 -> v4/DHCP4: 192.168.1.100/24 LAN (lan) -> em1 -> v4/DHCP4: 192.168.1.100/24 LAN (lan) -> em4 -> v4: 192.168.10.30/27 OPT1 (opt1) -> em3 -> v4: 10.255.255.254/12 OPT2 (opt2) -> em3 -> v4: 10.255.255.254/12 0PT2 (opt2) -> em3 -> v4: 10.255.255.254/8 0) Logout (SSH only) 9) pfTop 1) Assign Interfaces 10 Filter Logs 3) Reset webConfigurator password 4) Reset to factory defaults 13 Update from console 13) Update from console 14) Restore recent Scholl (sshd) 15) Restore recent configuration 16) Restart PHP-FPM 10) Shell Enter an option:

Ici on attribue le nom des interfaces (em0, em1...) grâce à leur adresse MAC.

eM2 00:0c:29:b1:7b:79 (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper) 00:0c:29:b1:7b:83 (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
Do ULANs need to be set up first? If VLANs will not be used, or only for optional interfaces, it is typical to say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y!n]? n
If the names of the interfaces are not known, auto-detection can be used instead. To use auto-detection, please disconnect all interfaces before pressing 'a' to begin the process.
Enter the WAN interface name or 'a' for auto-detection (eM0 eM1 eM2 eM3 or a): eM3
Enter the LAN interface name or 'a' for auto-detection NOTE: this enables full Firewalling/NAT mode. (eM0 eM1 eM2 a or nothing if finished): eM0
Enter the Optional 1 interface name or 'a' for auto-detection (eM1 eM2 a or nothing if finished): eM2
Enter the Optional 2 interface name or 'a' for auto-detection Ensuite dans le menu 2 on peut attribuer les IP des interfaces avec leur nom.

WAN (wan)         -> em1         -> vo           LAN (lan)         -> em8         -> vo           DM2 (opt1)         -> em3         -> vo           WIFI (opt2)         -> em2         -> vo	4/DHCP4: 192.168.170.135/24 4: 192.168.10.30/27 4: 172.31.255.254/12 4: 10.255.255.254/8
<ul> <li>Ø) Logout (SSH only)</li> <li>1) Assign Interfaces</li> <li>2) Set interface(s) IP address</li> <li>3) Reset webConfigurator password</li> <li>4) Reset to factory defaults</li> <li>5) Reboot system</li> <li>6) Halt system</li> <li>7) Ping host</li> <li>8) Shell</li> </ul>	9) pfTop 10) Filter Logs 11) Restart webConfigurator 12) PHP shell + pfSense tools 13) Update from console 14) Disable Secure Shell (sshd) 15) Restore recent configuration 16) Restart PHP-FPM
Enter an option: 2	
Available interfaces:	
1 - WAN (em1 - dhcp, dhcp6) 2 - LAN (em0 - static) 3 - DM2 (em3 - static) 4 - WIFI (em2 - static)	
Enter the number of the interface y	ou wish to configure:

En premier on choisit DHCP ou non sur IPv4/IPv6, si on choisit de ne pas être en DHCP on renseigne ensuite l'IP et masque de l'interface.



On peut ensuite on peut se connecter à l'interface web depuis le LAN 0 en renseignant l'adresse de l'interface LAN : 192.168.10.30

#### **3-REGLAGE PFSENSE**

## A.SSH/HTTPS

Pour commencer on va activer le SSH et l'HTTPS sur l'interface WEB.

Pour ce faire aller dans System  $\rightarrow$  Advenced

A Non sécurisé   https://192.168.10.30/system_advar	iced_admin.php		as A 🗘 🕻
	System - Interf	aces - Firewall - Services - VPN - Status - Diagnostics - Help - 🕻	<b>→</b>
System /	Advanced Certificates General Setup	nin Access 🕹	
Admin Acces	<ul> <li>High Availability</li> <li>Package Manager</li> </ul>	Networking Miscellaneous System Tunables Notifications	_
webConfig	Register Routing	HTTPS (SSL/TLS)	
SSL/TLS	Setup Wizard Update User Manager	jurator default (652536ca4d3a2)  known to be incompatible with use for HTTPS are not included in this list.	
	Logout (admin) Enter a cu after save	stom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately	
Max	Processes 2 Enter the r concurrent	umber of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI lly.	
WebG	UI redirect Disable	webConfigurator redirect rule	

## Cocher HTTPS (SSL/TLS)

Non sécurisé   https://192.168.10.3	30/system_advanced_admin.pl	p	аљ	A* 🔄 🗘
	The changes have been app One momentredirecting to	ied successfully. https://192.168.10.30/system_advanced_admin.php in 20 seconds.	×	
	Admin Access Firewa	l & NAT Networking Miscellaneous System Tunables Notifications		
	webConfigurator		-	
	Protocol	OHTTP ® HTT(Mr (SSL/TLS)		
		No Certificates have been defined. A certificate is required before SSL/TLS can be enabled. Create or Import a Certificate.		
	SSL/TLS Certificate	webConfigurator default (652536ca4d3a2)		
		Certificates known to be incompatible with use for HTTPS are not included in this list.		
	TCP port			
		Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immed after save.	liately	
	Max Processes	2		
		Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.		
	WebGUI redirect	Disable webConfigurator redirect rule		

## Renseigner le port TCP 443

Non sécurisé   https://192.168.10.30/system_advanced_admin	.php				aå A <sup>N</sup>	ជ
COMMUNITY EDITION System	n → Interfaces → Firewall → S	Services - VPN -	Status - Diagnostics -	Help 🗸 🐥	2 🕞	
System / Advar	ced / Admin Access				0	
Admin Access Fire	wall & NAT Networking Miscellar	neous System Tunables	Notifications			
webConfigurator	OHTTR			(2)		
SSL/TLS Certificate	webConfigurator default (652536ca4d	13a2) vith use for HTTPS are not inc	Iluded in this list.			
TCP port	443 [h] Entered custom port number for the web after save.	oConfigurator above to overric	¢ le the default (80 for HTTP, 443	for HTTPS). Changes will take effect imm	nediately	
Max Processes	2 Enter the number of webConfigurator pr concurrently.	rocesses to run. This defaults	to 2. Increasing this will allow	more users/browsers to access the GUI		
WebGUI redirect	Disable webConfigurator redirect rul	e 			1. akra k	

Puis dans la rubrique Secure Shell cocher Enable Secure Shell

A Non sécurisé   https://192.168.10	0.30/system_advanced_admin.ph	np ai	ь A <sup>h</sup>	☆	C(D
		nost name.			
	Secure Shell		1		
	Secure Shell Server	Inable Specure Shell			
	SSHd Key Only	Password or Public Key			
		When set to <i>Public Key Only</i> , SSH access requires subhorzed logs and these keys must be configured for such user that has been granted succes shell access. If set to <i>Require Both Password and Public Key</i> , the SSH daemon requires both authorized keys <b>and</b> valid pasewords to gain access. The default <i>Password or Public Key</i> setting allows either a valid password or a valid authorized keys to login.			
	Allow Agent Forwarding	Enables ssh-agent forwarding support.			
	SSH port	22			
		Note: Leave this blank for the default of 22.			
	Login Protection				
	Threshold	30			
		Block attackers when their cumulative attack score exceeds threshold. Most attacks have a score of 10.			
	Blocktime	120			
		Block attackers for initially blocktime seconds after exceeding threshold. Subsequent blocks increase by a factor of 1.5.			
		Attacks are unblocked at random intervals, so actual block times will be longer.			
	Detection time	1800			
		n the start of a transmission of the start o			

## **B. AJOUTER UNE PASSERELLE**

Il faut ajouter la passerelle R1 (192.168.10.29) pour que le routage puisse se faire par la suite.

Aller dans System/Routing/Gateways puis cliquer sur Add si elle n'existe pas, ou modifier (le crayon) si elle existe déjà.

atew	ays	Static Routes	Gateway Groups					
atev	/ays							
		Name	Default	Interface	Gateway	Monitor IP	Description	Actions
	$\odot$	WAN_DHCP6		WAN			Interface WAN_DHCP6 Gateway	Ø 🖸
	$\odot$	WAN_DHCP	Default (IPv4)	WAN	192.168.170.2	192.168.170.2	Interface WAN_DHCP Gateway	/0
1.	$\odot$	Vers_LAN0		LAN	192.168.10.29	192.168.10.29	Route vers LAN0	∥□⊘亩
								Save + Add
Defau	lt gat	eway						
Def	ult gat	eway IPv4	WAN_DHCP			~		
		Se	elect a gateway or failow	er gateway grou	p to use as the defau	ilt gateway.		
Def	ult gat	eway IPv6	None			~		
		Se	elect a gateway or failow	er gateway grou	p to use as the defau	It gateway.		

Puis ici on renseigne les informations, l'interface concernée, le nom et l'IP de la passerelle.

Edit Gateway					
Disabled	Disable this gateway				
	Set this option to disable this gateway without removing it from the list.				
Interface	LAN				
	Choose which interface this gateway applies to.				
Address Family	IPv4 ¥				
	Choose the Internet Protocol this gateway uses.				
Name	Vers_LANO				
	Gateway name				
Gateway	192.168.10.29				
	Gateway IP address				
Gateway Monitoring	Disable Gateway Monitoring				
	This will consider this gateway as always being up.				
Gateway Action	ay Action 🛛 Disable Gateway Monitoring Action				
	No action will be taken on gateway events. The gateway is always considered up.				
Monitor IP					
	Enter an alternative address here to be used to monitor the link. This is used for the quality RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).				
Static route	Do not add static route for gateway monitor IP address via the chosen interface				
	By default the firewall adds static routes for gateway monitor IP addresses to ensure traffic to the monitor IP address leaves via the correct interface. Enabling this checkbox overrides that behavior.				
Force state	🗌 Mark Gateway as Down				
	This will force this gateway to be considered down.				
State Killing on Gateway	Use global behavior (default)				
Failure	Controls the state killing behavior when this specific gateway goes down. Killing states for specific down gateways only affects states created by				
	policy routing rules and reply-to, has no effect if gateway monitoring of its action are disabled of if the gateway is forced down, may not have any effect on dynamic gateways during a link loss event.				
Description	Route vers LAN0				
	A description may be entered here for reference (not parsed).				
	Copley Advanced				
	B Save				

## **C. AJOUTER UNE ROUTE**

Ici nous allons ajouter des routes pour renseigner le chemin vers les LAN1/LAN2/LAN3. Pour ce faire aller dans System/Routing/Static Routes et ajouter ici les trois routes en cliquant sur Add.

On renseigne l'adresse réseau de destination, la passerelle à utiliser (ici R2 configuré précédemment) et la description

	System <del>-</del>	Interfaces 🗸	Firewall 👻	Services -	VPN -	Status 🕶	Diagnostics 👻	Help 🗸	<b>\$</b> 2 <b>*</b>
System / R	outing	/ Static Rout	es / Edit						幸 Ш 🗏 🕄
Edit Route En	try								
Destination r	network	192.168.10.96 Destination network	k for this static r	oute				/	27 🗸
G	iateway	Vers_LAN0 - 192. Choose which gate	168.10.29 way this route a	pplies to or add a	new one first	~			
D	isabled	Disable this stat Set this option to di	<b>ic route</b> isable this static	route without re	moving it fron	n the list.			
Des	cription	LAN3 A description may b	pe entered here t	for administrative	e reference (no	ot parsed).			
		Save							

Il ne faut pas oublier de confirmer avec Apply Changes.

	System -	Interfaces 👻	Firewall 🗸	Services -	VPN -	Status 👻	Diagnostics 👻	Help 🗕	<b>≜</b> 2 €
Sys	tem / Routing /	Static Rout	es						Lil 🗏 😧
The s The c	The static route configuration has been changed. The changes must be applied for them to take effect.								
Gate	ways Static Routes	Gateway Gro	ups						
Stat	ic Routes								
	Network	G	ateway			Interf	ace De	scription	Actions
$\odot$	192.168.10.32/27	١	/ers_LAN0 - 192	2.168.10.29		LAN	L	AN1	
$\oslash$	192.168.10.64/27	١	/ers_LAN0 - 192	2.168.10.29		LAN	L	AN2	<b>₽</b> □ <b>○</b> <u><u></u><u></u><u></u><u></u></u>
$\odot$	192.168.10.96/27	١	/ers_LAN0 - 192	2.168.10.29		LAN	U	AN3	

### **4-PORTAIL CAPTIF**

Ici l'objectif va être d'installer un portail captif sur le Pare-Feu PFsense.

Un portail captif est un système de contrôle d'accès à un réseau informatique, souvent utilisé dans les environnements publics tels que les cafés, les hôtels, les aéroports ou les entreprises. Son objectif principal est de sécuriser l'accès à Internet en obligeant les utilisateurs à passer par une page d'authentification avant d'accéder au réseau.

Pour le faire allez dans Services/Captive Portal et sélectionner Add



On renseigne ici le nom de la zone (du portail captif) et avec une petite description.

	rstem 👻	Interfaces 🕶	Firewall 🗸	Services 🕶	VPN 🗸	Status 👻	Diagnostics 🗸	Help 🗸	0
Services / Ca	aptive P	ortal / Add	Zone						≑ ਘ 🗏 😧
Add Captive Po	rtal Zone								
Zone n	ame V Zo	VIFI one name. Can only	y contain letters	, digits, and unde	erscores (_) a	nd may not sta	rt with a digit.		
Zone descrip	ntion P	ortail Captif Wife description may b	e entered here fo	or administrative	reference (no	ot parsed).			
	E	🕄 Save & Continu	e						

Puis dans Authentification on clique sur Base de données locale pour Serveur d'authentification et Serveur d'authentification secondaire.



Une fois ajouté on le retrouve dans la liste des portails captif et on peut modifier ses propriétés dans actions.

	System 👻	Interfaces 🗸	Firewall 🗸	Services -	VPN 🗸	Status 👻	Diagnostics 👻	Help 👻		•
Services /	Captive F	Portal								iii 🗐 🕄
Captive Port	tal Zones									
Zone	Interfac	es	Numbe	r of users		D	escription		Actions	
WIFI	WIFI		0			F	Portail Captif Wifi		e 🖉	

#### Il faut désactiver MAC filtering

	This field will be accessible through \$PORTAL_REDIRURL\$ variable in captiveportal's HTML pages.
After authentication Redirection URL	Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.
Blocked MAC address redirect URL	Blocked MAC addresses will be redirected to this URL when attempting access.
Preserve users database	Preserve connected users across reboot If enabled, connected users won't be disconnected during a pfSense reboot.
Concurrent user logins	Multiple  Disabled: Do not allow concurrent logins per username or voucher. Multiple: No restrictions to the number of logins per username or voucher will be applied. Last login: Only the most recent login per username or voucher will be granted. Previous logins will be disconnected. First login: Only the first login per username or voucher will be granted. Further login attempts using the username or voucher will not be possible while an initial user is already active.
MAC filtering	Disable MAC filtering     If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC     address of the client cannot be determined (usually because there are routers between prSense and the clients). If this is enabled, RADIUS MAC     authentication cannot be used.
Pass-through MAC Auto Entry	Enable Pass-through MAC automatic additions     When enabled, a MAC passthrough entry is automatically added after the user has successfully authenticated. Users of that MAC address will never     have to authenticate again. To remove the passthrough MAC entry either log in and remove it manually from the MAC tab or send a POST from another     eystem. If this is enabled, the logout window will not be shown.
Per-user bandwidth restriction	Enable per-user bandwidth restriction
Use custom captive portal page	Enable to use a custom captive portal login page     If set a portal.html page must be created and uploaded. If unchecked the default template will be used
Captive Portal Login	Page
Display custom logo	Enable to use a custom uploaded logo

Nous allons maintenant ajouter des groupes et utilisateurs qui pourront se connecter au portail captif de la zone WIFI.

Aller dans System/User Manager et puis Groups faire Add. On renseigne les informations diverses, dans les Assigned Privileges il faut ajouter le rôle User – Services : Captive Portal Login.

Users Groups S	ettings Authentication Servers		
Group Properties			
Group name	Potall		
Scope	Local Warning: Changing this setting may affect the loca	al groups file, in which case a reboot may be required for the changes to take effect.	
Description	Pour le portail captif Group description, for administrative information of	only	
Group membership	admin	▲ test	*
	Not members	Members	
	>> Move to "Members"	Move to "Not members	
	Hold down CTRL (PC)/COMMAND (Mac) key to se	elect multiple items.	
Assigned Privileges			
	Name	Description	Action
	User - Services: Captive Portal login	Indicates whether the user is able to login on the captive portal.	<b>İ</b>
			+ Add
	Save		

Users Groups	Settings Authentication Servers							
User Properties								
Defined by	USER							
Disabled	This user cannot login							
Username	test							
Password	······							
Full name	test User's full name, for administrative information only							
Expiration date	Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY							
Custom Settings	Use individual customized GUI options and dashboard layout for this user.							
Group membership	Bedmine							
	≫ Move to "Member of" list							
	Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.							
Certificate	No private CAs found. A private CA is required to create a new user certificate. Save the user first to import an external certificate.							
Keys								
Authorized SSH Keys								

#### CONCLUSION

La mise en place de PFsense en virtualisation offre une solution de pare-feu robuste et configurable. Les étapes ci-dessus permettent de déployer PFsense, configurer les règles de filtrage, et assurer une gestion efficace de la sécurité du réseau.

Il restera quelques tests à effectuer avec un PC dans le LAN WIFI en essayant de se connecter sur le portail captif.

