

PFSENSE

Formateur : Franck Thalmensy
Etablissement :

PFSENSE

est un routeur/pare-feu open source basé sur le système d'exploitation FreeBSD.

Fonctionnement :

1 site consulté = 1 connexion = 2 états (connexion entrante/sortant)
50 000 connexions = 100 000 états = ~ 100 Mo de RAM
500 000 connexions = 1 000 000 états = ~ 1 Go de RAM

VPN :

Opter pour un processeur supportant l'AES-NI

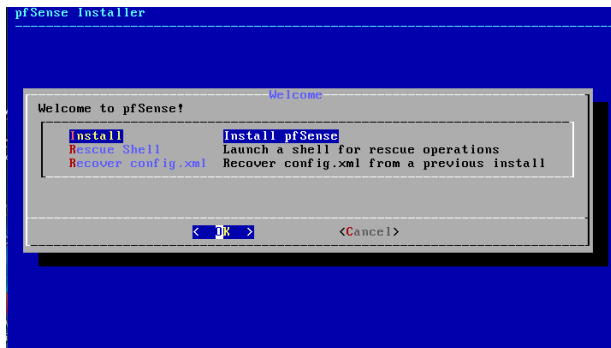
SNORT :

Peut avoir une consommation de mémoire-vive de l'ordre de 1 à 2 Go.

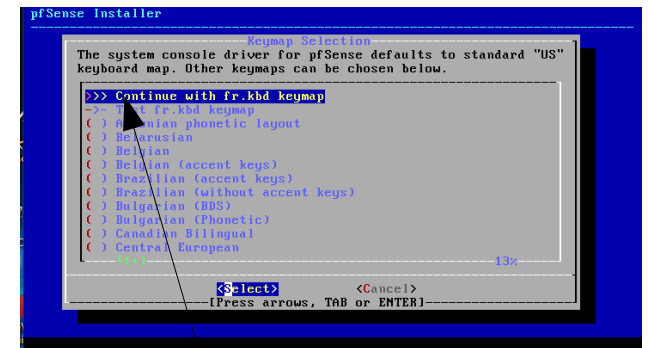
SQUID :

Squid utilise beaucoup le disque-dur (contrairement à pfSense).
il faut compter environ 15 Mo de mémoire-vive pour 1 Go de cache sur le disque-dur.

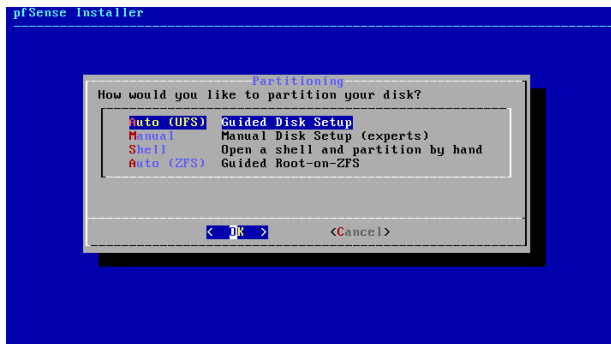
Installation



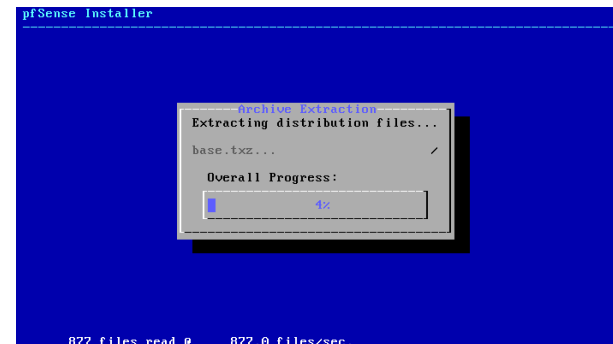
Le clavier



Continue



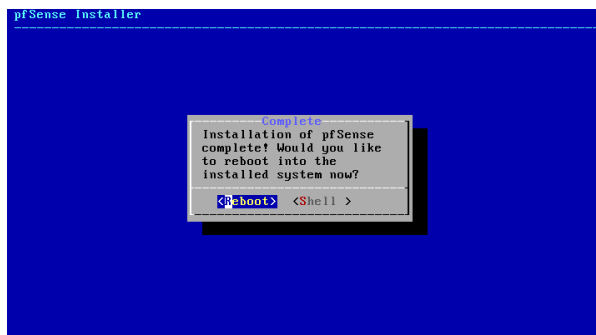
Auto (pour le formatage)



Auto (pour le formatage)



No



Reboot

Retirer le CD (pour ne pas repartir sur une installation)

Après une brève installation manuelle pour assigner les interfaces réseaux, il s'administre ensuite à distance depuis l'interface web et gère nativement les VLAN (802.1q)

(WAN) →
(LAN) →

```
FreeBSD/i386 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.3.2-RELEASE (i386 full-install) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.100.115/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

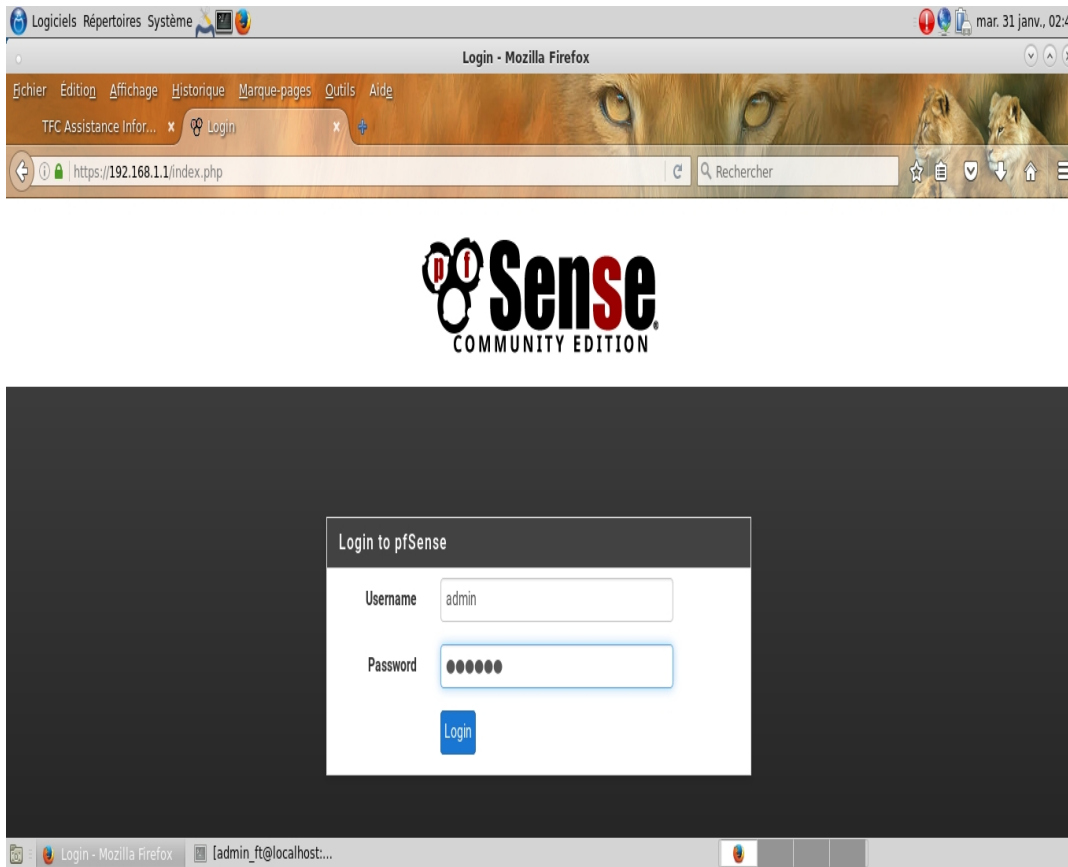
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

WAN correspond a l'interface réseaux connecter à internet
LAN notre réseaux

L'accès web n'est possible que côté LAN

L'interface Web <http://192.168.1.1>

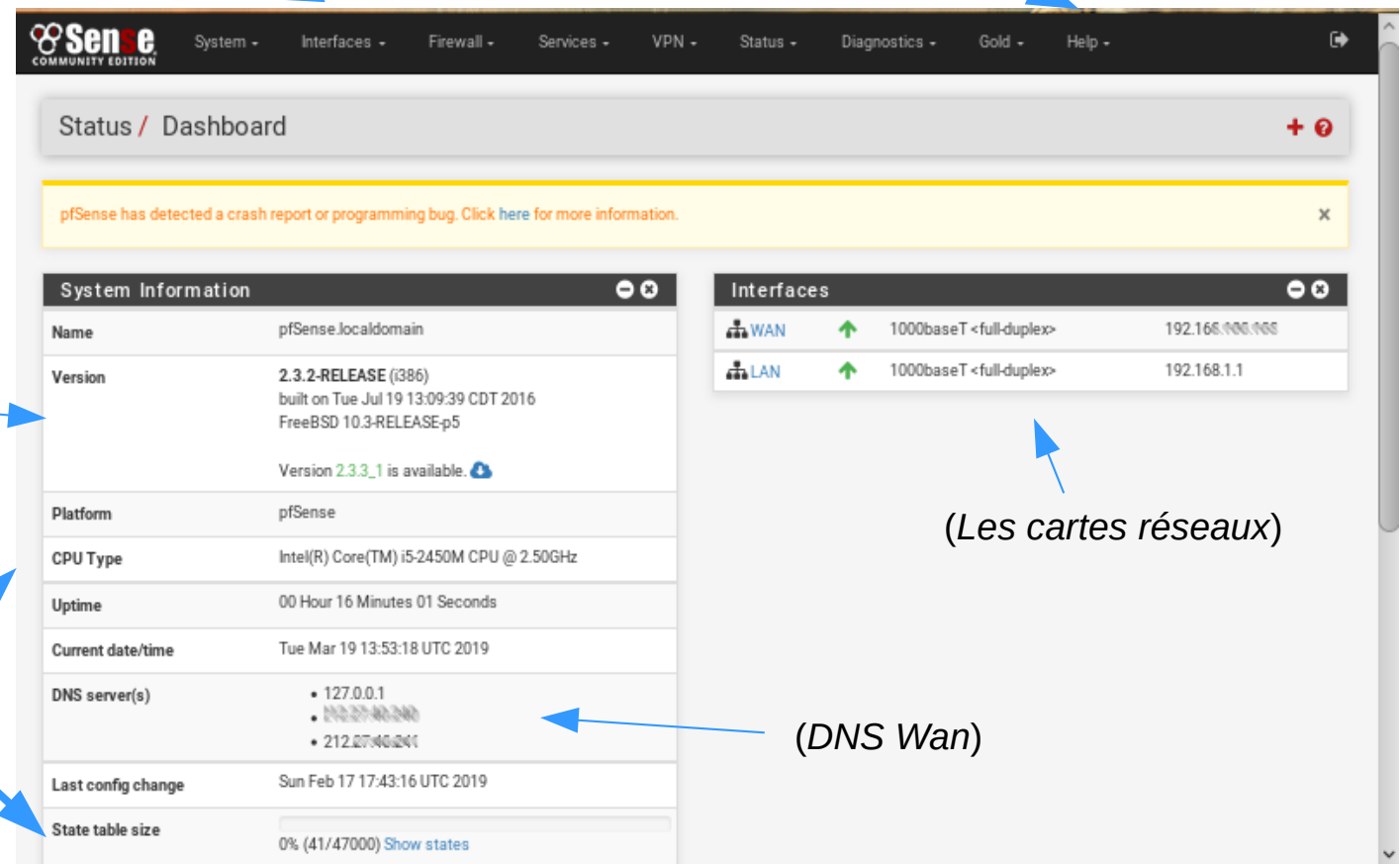


Utilisateur admin
Password pfense

Sommaire

Présentation de Pfsense

(Les différents menus)



The screenshot shows the pfSense Status / Dashboard page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is divided into two columns. The left column, titled 'System Information', contains a table with various system details. The right column, titled 'Interfaces', contains a table with network interface information. Annotations with blue arrows point to specific elements: 'System Information' is labeled '(Version de pfsense)', the 'Version' field is labeled '(Informations sur votre ordinateur)', the 'WAN' interface is labeled '(Les cartes réseaux)', and the 'DNS server(s)' field is labeled '(DNS Wan)'.

System Information	
Name	pfSense.localdomain
Version	2.3.2-RELEASE (i386) built on Tue Jul 19 13:09:39 CDT 2016 FreeBSD 10.3-RELEASE-p5 Version 2.3.3_1 is available.
Platform	pfSense
CPU Type	Intel(R) Core(TM) i5-2450M CPU @ 2.50GHz
Uptime	00 Hour 16 Minutes 01 Seconds
Current date/time	Tue Mar 19 13:53:18 UTC 2019
DNS server(s)	<ul style="list-style-type: none"> 127.0.0.1 192.168.1.1 212.27.40.241
Last config change	Sun Feb 17 17:43:16 UTC 2019
State table size	0% (41/47000) Show states

Interfaces	
WAN	1000baseT <full-duplex> 192.168.1.1
LAN	1000baseT <full-duplex> 192.168.1.1

Menu

System

Interfaces

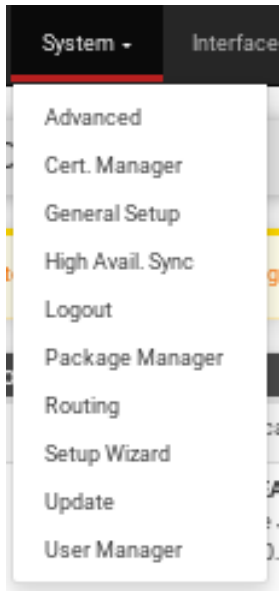
Firewall

Services

Squid

Menu

System



→ **Cert. Manager**

Permet de créer des certificats

→ **Package Manager**

Permet d'installer des paquets

Mettre le Clavier en fr

→ **User Manager**

Utilisateurs Pfsense

→ **User Manager**

Utilisateurs Pfsense

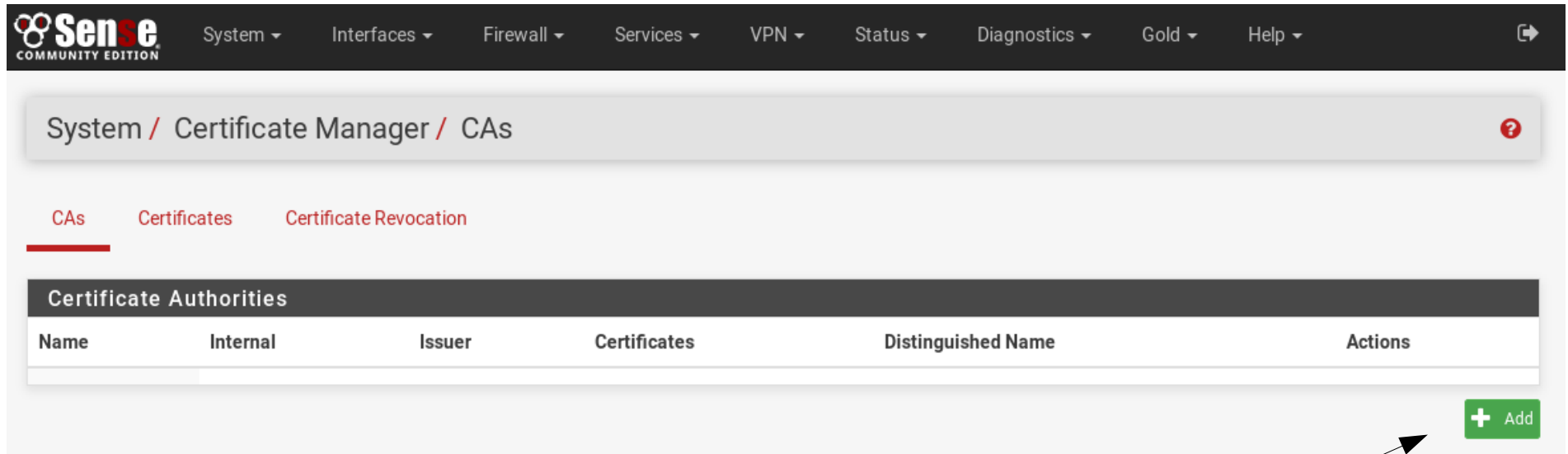
Menu

System/Cert.Manager

Création d'une autorité de certification 1/3

Les certificats SSL (Secure Sockets Layer), parfois appelés certificats numériques, sont utilisés pour créer une connexion cryptée entre le client et le serveur.

→ CAs



The screenshot shows the pfSense Sense interface. The top navigation bar includes the Sense logo and various menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. Below the navigation bar, the breadcrumb trail reads "System / Certificate Manager / CAs". The main content area has three tabs: "CAs" (selected), "Certificates", and "Certificate Revocation". Under the "CAs" tab, there is a table titled "Certificate Authorities". The table has columns for Name, Internal, Issuer, Certificates, Distinguished Name, and Actions. At the bottom right of the table, there is a green button with a plus sign and the text "Add". An arrow points from the word "Add" to this button.

Name	Internal	Issuer	Certificates	Distinguished Name	Actions
------	----------	--------	--------------	--------------------	---------

+ Add

Add

Menu

[System/Cert.Manager](#)

Création d'une autorité de certification 2/3

Descriptive name	<input type="text" value="Vm_Tfc"/>
Method	<input type="text" value="Create an internal Certificate Authority"/>
Internal Certificate Authority	
Key length (bits)	<input type="text" value="2048"/>
Digest Algorithm	<input type="text" value="sha256"/> <small>NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.</small>
Lifetime (days)	<input type="text" value="3650"/>
Country Code	<input type="text" value="FR"/>
State or Province	<input type="text" value="Paris"/>
City	<input type="text" value="France"/>
Organization	<input type="text" value="Tfcvm"/>
Email Address	<input type="text" value="tfc@chezmoi.fr"/>
Common Name	<input type="text" value="ca-tfcinfo"/>

Explication :**Descriptive name** : Le nom (ex:Societe)**Method** : Création d'un nouveaux certificat**Key lenght** : Longueur de la clé de chiffrement**Common Name** : sans espace et unique

Menu





System/Cert.Manager

Création d'une autorité de certification 3/3

Voici notre certificat !

System / Certificate Manager / CAs

CAs Certificates Certificate Revocation

Certificate Authorities					
Name	Internal	Issuer	Certificates	Distinguished Name	Actions
Vm_Tfc	✓	self-signed	0	emailAddress=tfc@chezmoi.fr, ST=Paris, O=Tfcvm, L=France, CN=ca-tfcinfo, C=FR Valid From: Tue, 31 Jan 2017 16:04:26 +0100 Valid Until: Fri, 29 Jan 2027 16:04:26 +0100	   

+ Add

Notre autorité de Certificat réussi

Après avoir fait le Cas, nous allons faire le Certificat Serveur

Menu

System/Cert.Manager



Certificat Serveur 1/4

→ Certificates

System / Certificate Manager / Certificates 

CA's Certificates Certificate Revocation

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (588fce01b1117) Server Certificate CA: No, Server: Yes	self-signed	emailAddress=admin@pfSense.localdomain, ST=State, O=pfSense webConfigurator Self-Signed Certificate, L=Locality, CN=pfSense-588fce01b1117, C=US Valid From: Tue, 31 Jan 2017 00:36:33 +0100 Valid Until: Sun, 24 Jul 2022 01:36:33 +0200	webConfigurator	 

+ Add

Add

Menu

System/Cert.Manager

Certificat Serveur 2/4

CAS
Certificates
Certificate Revocation

Add a New Certificate

Method

Create an internal Certificate

Descriptive name

Certificat_pour_Srv

Menu

System/Cert.Manager

Certificat Serveur 3/4

Internal Certificate	
Certificate authority	Vm_Tfc
Key length	2048
Digest Algorithm	sha256
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.	
Certificate Type	Server Certificate
Type of certificate to generate. Used for placing restrictions on the usage of the generated certificate.	
Lifetime (days)	3650
Country Code	FR
State or Province	Paris
City	France
Organization	Tfcvm
Email Address	tfc@chezmoi.fr
Common Name	certif-server-tfc
Alternative Names	FQDN or Hostname
Type	Value
Add	+ Add

Explication :

Certificate authority : Notre Cas Certificate

Certificate Type : Server Certificate

Lifetime (days) : 3650 Jours, durée de vie du certificat








Common Name : sans espace et unique

Menu

System/Cert.Manager

Certificat Serveur 4/4

Votre Certificat serveur est prêt

CAs <u>Certificates</u> Certificate Revocation				
Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (588fce01b1117) Server Certificate CA: No, Server: Yes	self-signed	emailAddress=admin@pfSense.localdomain, ST=State, O=pfSense webConfigurator Self-Signed Certificate, L=Locality, CN=pfSense-588fce01b1117, C=US Valid From: Tue, 31 Jan 2017 00:36:33 +0100 Valid Until: Sun, 24 Jul 2022 01:36:33 +0200	webConfigurator	  
Certificat_pour_Srv Server Certificate CA: No, Server: Yes	Vm_Tfc	emailAddress=tfc@chezmoi.fr, ST=Paris, O=Tfcvm, L=France, CN=certif-serv-tfc, C=FR Valid From: Sun, 12 Feb 2017 14:37:01 +0100 Valid Until: Wed, 10 Feb 2027 14:37:01 +0100		   
				 Add

Après avoir fait le **Cas** et le **certificat** Serveur il reste le certificat client

Menu

System/Cert.Manager








Certificat Client 1/3

→ Certificates

System / Certificate Manager / Certificates

CAs Certificates Certificate Revocation

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (588fce01b1117) Server Certificate CA: No, Server: Yes	self-signed	emailAddress=admin@pfSense.localdomain, ST=State, O=pfSense webConfigurator Self-Signed Certificate, L=Locality, CN=pfSense-588fce01b1117, C=US Valid From: Tue, 31 Jan 2017 00:36:33 +0100 Valid Until: Sun, 24 Jul 2022 01:36:33 +0200	webConfigurator	  
Cert (serveur) Server Certificate CA: No, Server: Yes	Vm_Tfc	emailAddress=tfc@chezmoi.fr, ST=Paris, O=Tfvcvm, L=France, CN=certif-server-tfc, C=FR Valid From: Tue, 31 Jan 2017 21:42:31 +0100 Valid Until: Fri, 29 Jan 2027 21:42:31 +0100		   

+ Add

le certificat serveur est déjà crée

Add

Menu

[System/Cert.Manager](#)

Certificat Client 2/3

Internal Certificate	
Certificate authority	<input type="text" value="Vm_Tfc"/>
Key length	<input type="text" value="2048"/>
Digest Algorithm	<input type="text" value="sha256"/> <small>NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.</small>
Certificate Type	<input type="text" value="User Certificate"/> <small>Type of certificate to generate. Used for placing restrictions on the usage of the generated certificate.</small>
Lifetime (days)	<input type="text" value="3650"/>
Country Code	<input type="text" value="FR"/>
State or Province	<input type="text" value="Paris"/>
City	<input type="text" value="France"/>
Organization	<input type="text" value="Tfcvm"/>
Email Address	<input type="text" value="tfc@chezmoi.fr"/>
Common Name	<input type="text" value="certif-client-tfc"/>
Alternative Names	<div><div><input type="text" value="FQDN or Hostname"/></div><div><input type="text"/></div></div> <div>TypeValue</div>
<div>Add</div> <div><div>+</div>Add</div>	

Explication :**Certificate Type :** User Certificate**Common Name :** sans espace et unique













Add

Menu

System/Cert.Manager

Certificat Client 3/3

Votre Certificat Client est prêt

CAs Certificates Certificate Revocation				
Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (588fce01b1117) Server Certificate CA: No, Server: Yes	self-signed	emailAddress=admin@pfSense.localdomain, ST=State, O=pfSense webConfigurator Self-Signed Certificate, L=Locality, CN=pfSense-588fce01b1117, C=US Valid From: Tue, 31 Jan 2017 00:36:33 +0100 Valid Until: Sun, 24 Jul 2022 01:36:33 +0200	webConfigurator	  
Certificat_pour_Srv Server Certificate CA: No, Server: Yes	Vm_Tfc	emailAddress=tfc@chezmoi.fr, ST=Paris, O=Tfcvm, L=France, CN=certif-serv-tfc, C=FR Valid From: Sun, 12 Feb 2017 14:37:01 +0100 Valid Until: Wed, 10 Feb 2027 14:37:01 +0100		   
Cert (client) User Certificate CA: No, Server: No	Vm_Tfc	emailAddress=tfc@chezmoi.fr, ST=Paris, O=Tfcvm, L=France, CN=certif-client-tfc, C=FR Valid From: Sun, 12 Feb 2017 14:49:00 +0100 Valid Until: Wed, 10 Feb 2027 14:49:00 +0100		   
				 Add

Tous les Certificats ont été créés

Il ne reste plus qu'à configurer :

- Le serveur VPN
- Créer un utilisateur pour le VPN_

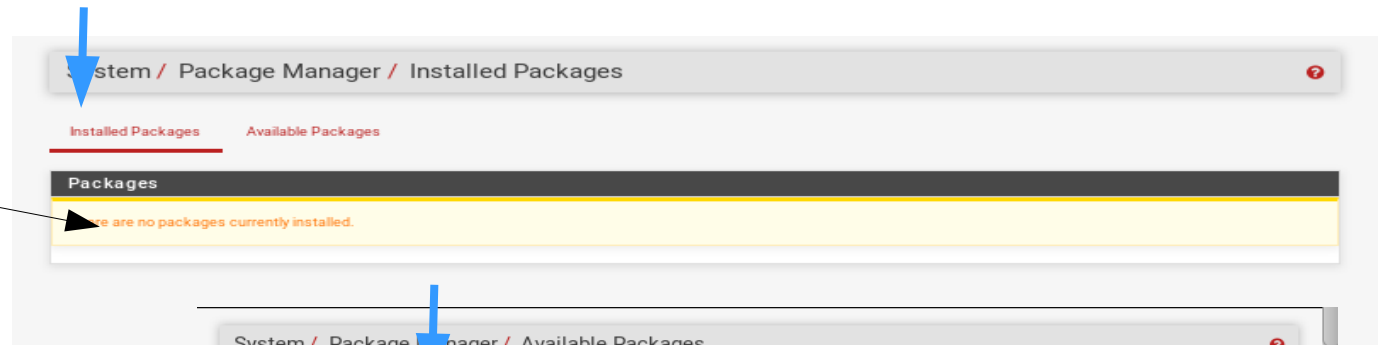
Menu

System/Package Manager

Pfsense basé sur FreeBSD donc il utilise les commande pkg pour gérer manuellement des packages FreeBSD

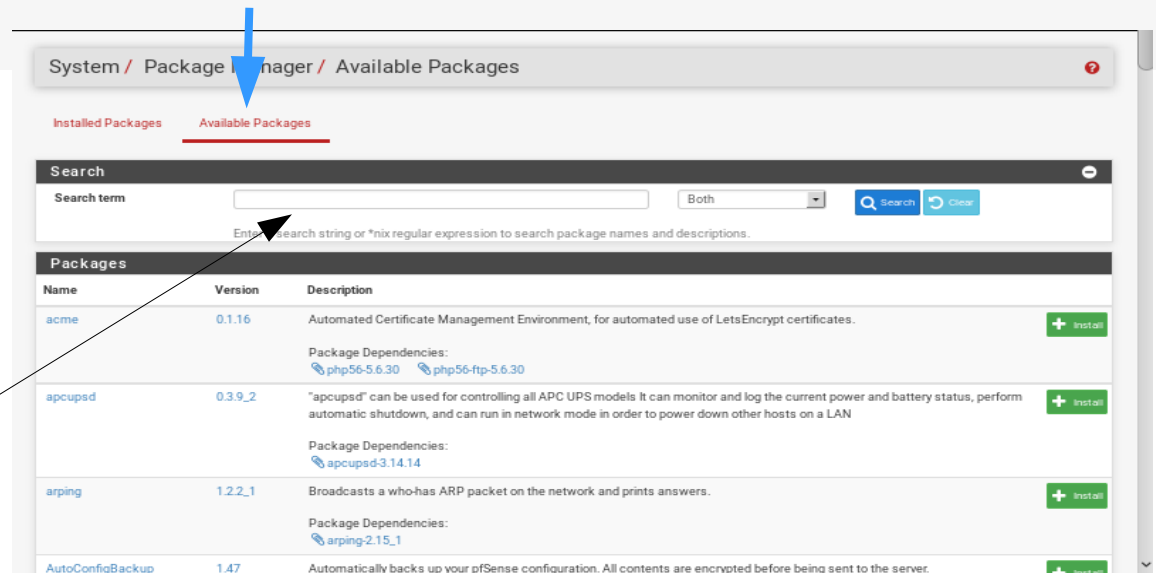
→ Installed Packages

(Package installer sur votre ordinateur)



→ Available Packages

(Package disponible)



Vous pouvez rechercher ou parcourir la liste

Menu

System/Package Manager

Programme

Récupéré le package **squid et squidGuard**

Par default le Proxy (ou serveur mandataire) n'est pas installer, sur Pfsense c'est Squid

Le Proxy s'occupe :

- Du cache (désigne un espace disque dédié aux pages les plus souvent visitées)
- Du filtrage Web (se fera par les packet squid squidguard)
- Authentification
- Reverse-Proxy (Permet au utilisateur Internet d'accéder au serveur interne)

Configuration

Récupéré le package **Open-VM-Tools**

Installer Open-VM-Tools :

- Sur une machine virtuel VmWare

Configuration

Menu

System/User Manager

Pfsense permet de gérer des utilisateurs pour vos accès Web/Vpn

(Vos utilisateurs)

System / User Manager / Users

Users

Groups

Settings

Authentication Servers

Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	

+ Add

Delete

(Vos Groupes)

System / User Manager / Groups

Users Groups Settings Authentication Servers

Groups			
Group name	Description	Member Count	Actions
admins	System Administrators	1	Edit
all	All Users	1	Edit

[+ Add](#)

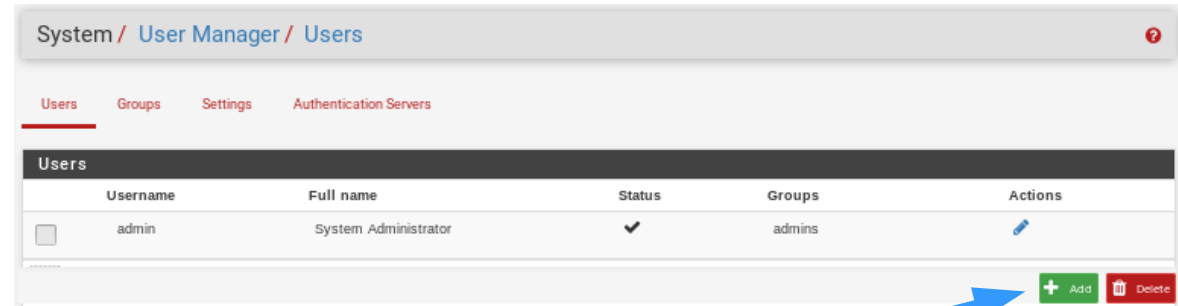
Utilisateurs Web

Menu

System/User Manager

Utilisateur Captive Portal 1/5

Création d'un utilisateur pour accéder à Internet (Captive Portal activé)



1) Add



User Properties

Defined by: USER

Disabled: ☐ This user cannot login

Username: fred

Password: [masked]

Full name: [empty]

Expiration date: [empty]

Custom Settings: ☐ Use individual customized GUI options and dashboard layout for this user.

Group membership: admins

Not member of: [empty]

Member of: [empty]

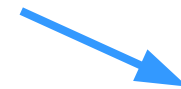
Certificate: ☐ Click to create a user certificate

(Le nom)

(Password)

(Groupe d'appartenance)

2) Save



Menu

System/User Manager

Utilisateur Captive Portal 2/5

Création du groupe (Captive Portal)

(Le nom du groupe)

Group Properties

Group name

Scope

Local

Description

Group description, for administrative information only

Group membership

Not members

Members

» Move to "Members"

« Move to "Not members"

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Save

4) Save

System / User Manager / Groups

Users Groups Settings Authentication Servers

Group name	Description	Member Count	Actions
admins	System Administrators	1	
all	All Users	1	

+ Add

3) Add

Menu

System/User Manager

Utilisateur Captive Portal 3/5

Dès que vous avez créé le groupe nous allons ajouter

- les utilisateurs et lui attribuer la fonctionnalité Captive Portal

System / User Manager / Groups

Users Groups Settings Authentication Servers

Group name	Description	Member Count	Actions
admins	System Administrators	1	
all	All Users	2	
TFC_Web_User	Ok pour le WEB	1	

+ Add

5) Edit group

Group Properties

Group name: TFC_Web_User

Scope: Local

Description: Ok pour le WEB
Group description, for administrative information only

Group membership

Not members: admin

Members: fred

Move to "Members" Move to "Not members"

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

(Utilisateur hors du groupe)

(Utilisateur dans le groupe)

6) Ajouts des utilisateurs

7) Add

Assigned Privileges

Name	Description	Action

+ Add

Menu

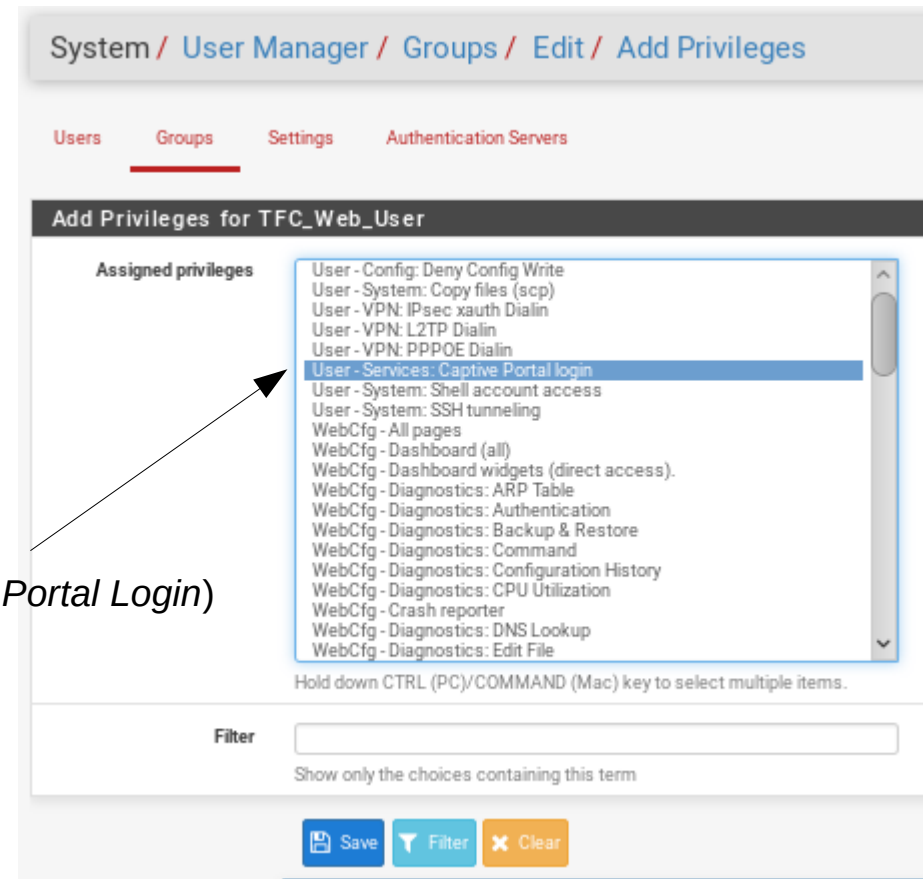
System/User Manager

Utilisateur Captive Portal 4/5

On choisie le privilège qui permet d'accéder au Portal

(User – Services:Captive Portal Login)

Save







Menu

System/User Manager

Utilisateur Captive Portal 5/5

System / User Manager / Groups ?

Users Groups Settings Authentication Servers

Groups			
Group name	Description	Member Count	Actions
admins	System Administrators	1	
all	All Users	2	
TFC_Web_User	Ok pour le WEB	1	 

+ Add

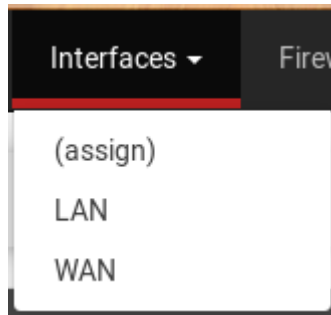
(Votre Groupes Web)

(nbr d'utilisateurs)

Menu

Interfaces

Permet de configurer vos différentes interface



Votre :

Wan
Lan

Menu

Interfaces

Les paramètres sont identique pour votre WAN/LAN

(Vous pouvez modifier le nom)


(Dhcp/Static)

General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="WAN"/> Enter a description (name) for the interface here.
IPv4 Configuration Type	<input type="text" value="DHCP"/>
IPv6 Configuration Type	<input type="text" value="DHCP6"/>
MAC Address	<input type="text" value="xx:xx:xx:xx:xx:xx"/> This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU	<input type="text"/> If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	<input type="text"/> If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and Duplex	<input type="text" value="Default (no preference, typically autoselect)"/> Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Menu

Interfaces

Les paramètres sont identique pour votre WAN/LAN

Send IPv6 prefix hint	<input type="checkbox"/> Send an IPv6 prefix hint to indicate the desired prefix size for delegation
Debug	<input type="checkbox"/> Start DHCP6 client in debug mode
Do not wait for a RA	<input type="checkbox"/> Required by some ISPs, especially those not using PPPoE
Do not allow PD/Address release	<input type="checkbox"/> dhcp6c will send a release to the ISP on exit, some ISPs then release the allocated address or prefix. This option prevents that signal ever being sent
Reserved Networks	
Block private networks and loopback addresses	<input type="checkbox"/> Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	<input checked="" type="checkbox"/> Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.
	

décocher la case *Block private networks and loopback addresses*.
(pour accéder à l'interface de gestion)



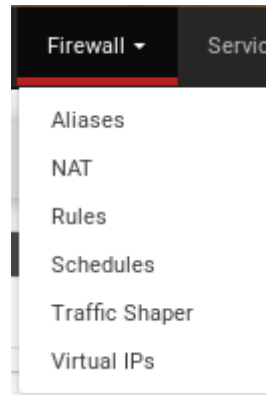
Autorise le Port 443

Menu

Firewall

Firewall → Rules → Lan

Permet de configurer les règles



→ **NAT**

Redirection

→ **Rules**

Règles de firewall Wan/Lan

→ **Virtual IPs**

l'équilibrage de charge (failover)

Menu

Firewall/Rules

Exemples de Règles pour le LAN

(Règles sur Lan)

(Règles DNS)

(Règles HTTP)

(Règles HTTPS)

Exemples de Règles pour le LAN

FloatingWANLAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/5.23 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
0/97 KiB	IPv4 UDP	LAN net	*		53 (DNS)	*	none			
0/4.18 MiB	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none			
0/4.23 MiB	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none			
0/58 KiB	IPv4 ICMP	*	*	WAN net	*	*	none			
0/10 KiB	IPv4 ICMP	*	*	LAN net	*	*	none			

Add

Add

Delete

Save

Separator

Exemples de Règles pour le WAN

(Règles sur Wan)

(Règles ICMP)



Exemples de Règles pour le WAN

Floating

WAN

LAN

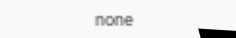
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<div><div></div><div></div></div>	✓ 0/0 B	IPv4 TCP	*	*	WAN address	80 (HTTP)	*	none			<div><div></div><div></div><div></div><div></div><div></div></div>
<div><div></div><div></div></div>	✓ 0/6 KiB	IPv4 ICMP	*	*	*	*	*	none			<div><div></div><div></div><div></div><div></div><div></div></div>
<div><div></div><div></div></div>	✓ 0/57 KiB	IPv4 TCP	*	*	192.168.1.100	80 (HTTP)	*	none		NAT	<div><div></div><div></div><div></div><div></div><div></div></div>

Add Add Delete Save Separation

(Règles Nat)

(Règles Nat)



Menu

Firewall/Rules/LAN

Règles par défaut pour le LAN

Firewall / Rules / LAN

Floating WAN LAN

(Règles HTTP/HTTPS)

(Règles IPv4)

(Règles IPv6)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 3/26.65 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Logout Rule	⚙️
✓ 0/6.76 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	📌 ⚙️ 🗑️
✓ 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	📌 ⚙️ 🗑️

↑ Add ↓ Add 🗑️ Delete 💾 Save ➕ Separator

Les autorisation les plus haut (valide) si plus bas l'autorisation contredit la 1er elle ne seras pas prit en compte

Règles HTTP/HTTPS : pour accéder à l'interface de gestion

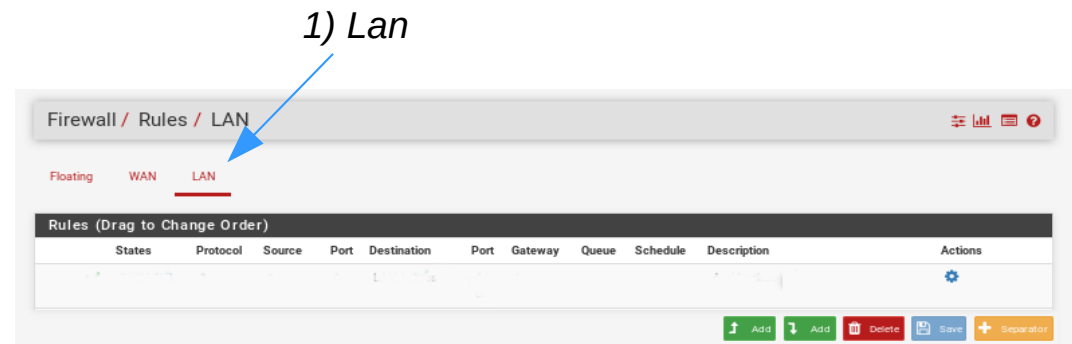
IPv4 : tout autoriser

IPv6 : tout autoriser

Menu

Firewall/Rules/LAN

Autorisée le Port 80 sur le Lan



Edit Firewall Rule

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Select this option to disable this rule without removing it from the list.

Interface LAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP/UDP
Choose which IP protocol this rule should match.

Source

Source ☐ invert match. LAN net Source Address /

Display Advanced Display Advanced

Destination

Destination ☐ invert match. any Destination Address /

Destination port range HTTP (80) From Custom To HTTP (80) Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

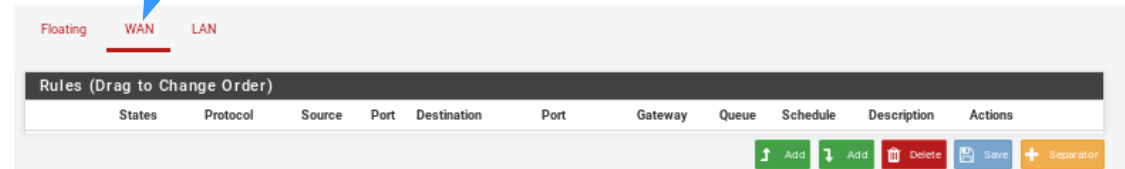
(Action)

Port 80

Menu

Firewall/Rules/WAN

1) Wan



(Action)

2) Add

Autorisée l' ICMP sur le Wan

Edit Firewall Rule

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface WAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol ICMP
Choose which IP protocol this rule should match.

ICMP type any
If ICMP is selected for the protocol above, an ICMP type may be specified here.

(icmp)

Menu

Firewall/Rules/WAN

Exemples de Règles pour le WAN

Firewall / Rules / WAN

Floating WAN LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 890 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	✓ 0 / 9 KiB	IPv4 ICMP any	*	*	*	*	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			
<input type="checkbox"/>	✓ 0 / 211 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			

Add Add Delete Save Separator

(icmp)

Autorisée l'accès à l'interface de gestion (Wan)

Menu

Firewall/NAT/Portforward

Redirection du Port 80

Edit Firewall Rule

Action:

Disabled: ☐ Enable this rule

Associated filter rule: This is associated with a NAT rule. Editing the interface, protocol, source, or destination of associated filter rules is not permitted. [View the NAT rule](#)

Interface:

Address Family:

Protocol:

Source

Source: ☐ Invert match. Source Address:

Display Advanced: ☒ Display Advanced

Destination

Destination: ☐ Invert match.

Destination port range:

Specify the destination port or port range for this rule. The field may be left empty if only filtering a single port.

Port 80

Ip (local)

1) Port Forward

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NAT

Rules

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
									<input type="button" value="Add"/> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Save"/> <input type="button" value="Separator"/>

2) Add

Redirection

du Wan Port 80 vers un Port 80 sur un Serveur Local

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NAT

Rules

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.1.100 80 (HTTP)	<input type="button" value="Add"/> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Save"/> <input type="button" value="Separator"/>

Menu

Services

Service permet de configurer les différents service ainsi que les pluggins (que vous pouvez installer)

Services ▾	VPN ▾
Captive Portal	→ Captive Portal Gère les accès internet
DHCP Relay	
DHCP Server	→ DHCP Server Configuration du service DHCP
DHCPv6 Relay	
DHCPv6 Server & RA	
DNS Forwarder	
DNS Resolver	

Menu

Services/DHCP Server/Lan

Pfsense peut être utilisé comme serveur DHCP ou relai DHCP

Configuration :

en tant que serveur DHCP

(deny) Autorisation par adresse Mac

(réseau)

(range)

Services / DHCP Server / LAN

LAN

General Options

Enable ☒ Enable DHCP server on LAN interface

Deny unknown clients ☐ Only the clients defined below will get DHCP leases from this server.

Ignore denied clients ☐ Denied clients will be ignored rather than rejected.
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Subnet 192.168.1.0

Subnet mask 255.255.255.0

Available range 192.168.1.1 - 192.168.1.254

Range
From To

Menu

Services/DHCP Server/Lan

Option WINS/DNS

(DNS servers)
vide pour utilisé ceux de Pfsense
Si vous avez AD indiquer l'adresse

(Gateway)
vide pour utilisé ceux de Pfsense

(Domain name)
Nom FQDN

Servers	
WINS servers	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>
DNS servers	<input type="text" value="DNS Server 1"/>
	<input type="text" value="DNS Server 2"/>
	<input type="text" value="DNS Server 3"/>
	<input type="text" value="DNS Server 4"/>
Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.	

Other Options	
Gateway	<input type="text"/>
The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.	
Domain name	<input type="text"/>
The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.	
Domain search list	<input type="text"/>
The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.	

Menu

Services/DHCP Server/Lan

Option WINS/DNS

(Failover peer IP)

Si vous avez 2 Pfsense

(Dynamic DNS)

Serveur DNS dynamique

(Mac Adresse Control)

Filtre les accès au DHCP par adresses MAC

(NTP)

Serveurs de temps

(TFTP)

Serveurs TFTP pour l'approvisionnement de téléphone IP DHCP 66

(LDAP)

Serveurs LDAP

(Enable network booting)

Activer le boot network ainsi que le nom du fichier

(Additional Boot/DHCP options)

Ajout n'importe quelle option DHCP

Menu

Services/Captive Portal

Le portail captif, permet de demander une authentification pour pouvoir accéder à internet

Service → Captive portal

Services / Captive Portal

Captive Portal Zones				
Zone	Interfaces	Number of users	Description	Actions
<div>+ Add</div>				

Add

1) Création du Portail nom du groupe avec ca description

Services / Captive Portal / Add Zone

Add Captive Portal Zone

Zone name

Zone name. Can only contain letters, digits, and underscores (_) and may not start with a digit.

Zone description

A description may be entered here for administrative reference (not parsed).

Save

Menu

Services/Captive Portal

2) Activé Portail

Captive Portal Configuration	
Enable	<input checked="" type="checkbox"/> Enable Captive Portal
Interfaces	<div><div>WAN</div><div>LAN</div></div> <p>Select the interface(s) to enable for captive portal.</p>
Maximum concurrent connections	<div><div>3</div><div></div></div> <p>Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.</p>
Idle timeout (Minutes)	<div><div></div><div></div></div> <p>Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.</p>
Hard timeout (Minutes)	<div><div></div><div></div></div> <p>Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).</p>
Pass-through credits per MAC address.	<div><div></div><div></div></div> <p>Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.</p>

l'interface , le nbr de client

Menu

Services/Captive Portal

Authentication : local User Manager

Authentication	
Authentication method	<input type="radio"/> No Authentication <input checked="" type="radio"/> Local User Manager / Vouchers <input type="radio"/> RADIUS Authentication
<input checked="" type="checkbox"/> Allow only users/groups with "Captive portal login" privilege set	

Seul : les (users) ou (groups) avec les droits (Captive Portal login) pourront accéder à Internet

pfSense captive portal

Welcome to the pfSense Captive Portal!

Username:

Password:

Continue

Le Captive Portal à été crée

Il ne reste plus qu'a configurer :
- Crée les utilisateurs Web

Services

Mettre le Clavier en fr


System → Package Manager

Récupéré le package **Shellcmd**

Maintenant il faut le configuré :

Service → Shellcmd

Shellcmd Configuration	
Command	<input type="text" value="kbdcontrol -l /usr/share/vt/keymaps/fr.kbd"/> Enter the command to run.
Shellcmd Type	<div><div>shellcmd</div><div>Choose the shellcmd type.</div><div><p>shellcmd will run the command specified towards the end of the boot process.</p><p>earlyshellcmd will run the command specified at the beginning of the boot process.</p><p>afterfilterchangeshellcmd will run after each filter_configure() call. See /etc/inc/filter.inc source code for "documentation". N.B.: Only one entry of this type can be configured!</p><p>disabled will save the command in package configuration but it will NOT run on boot.</p><p>See Executing commands at boot time for detailed explanation.</p></div></div>
Description	<input type="text" value="keyb fr"/> Enter a description for this command.

 Save

dans command : kbdcontrol -l /usr/share/vt/keymaps/fr.kbd


SquidGuard

Services → SquidGuard

Blacklist url

Blacklist options

Blacklist	<input type="checkbox"/> Check this option to enable blacklist Do NOT enable this on NanoBSD installs!
Blacklist proxy	<input type="text"/> 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	<input type="text"/> 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).

 Save

Utilisons cette blacklist dans (blacklist URL):

www.shallalist.de/Downloads/shallalist.tar.gz

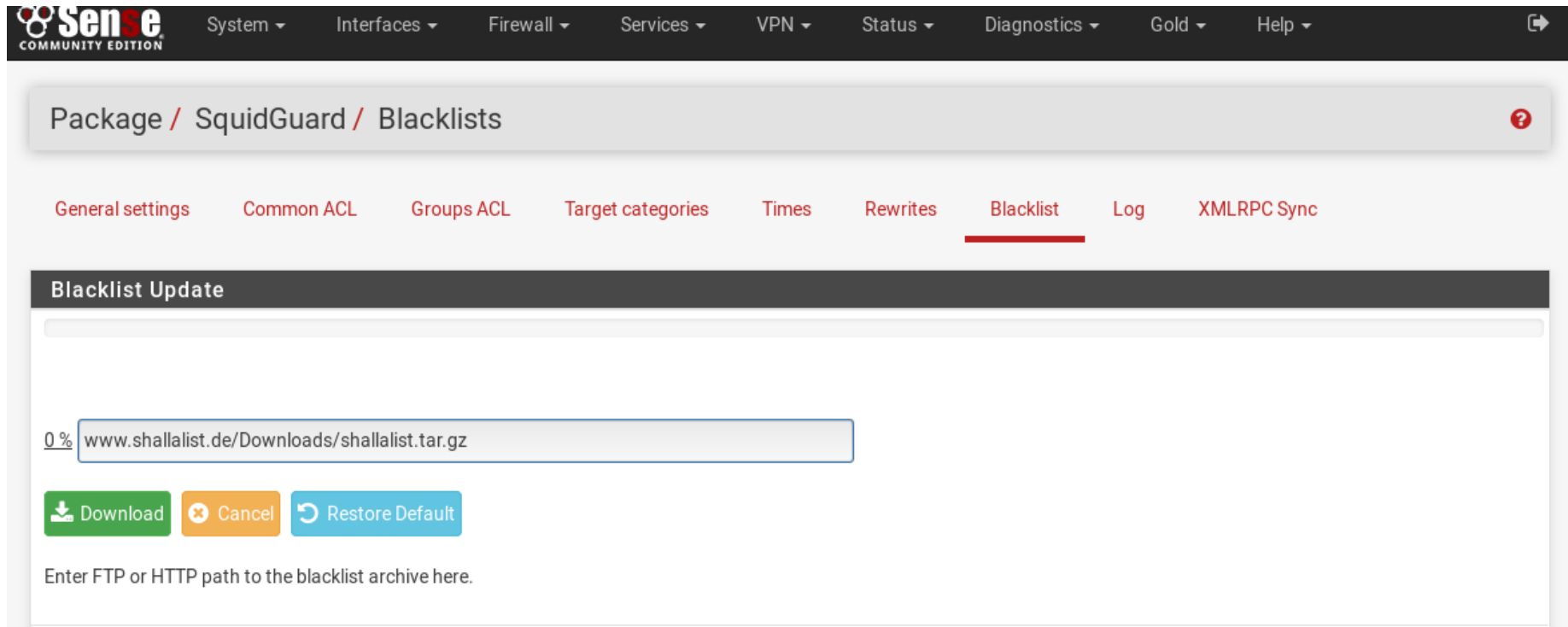
<http://urlblacklist.com/cgi-bin/commercialdownload.pl?type=download&file=bigblacklist>

ftp://ftp.univ-tlse1.fr/blacklist/blacklists_for_pfsense.tar.gz

SquidGuard

Services → SquidGuard

Mettre à jour la Blacklist



The screenshot shows the SquidGuard configuration page in the Sense Community Edition web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The breadcrumb trail indicates the path: Package / SquidGuard / Blacklists. The 'Blacklist' tab is selected and underlined. Below the tabs, the 'Blacklist Update' section features a progress bar at 0%, a text input field containing the URL 'www.shallalist.de/Downloads/shallalist.tar.gz', and three buttons: 'Download' (green), 'Cancel' (orange), and 'Restore Default' (blue). A note at the bottom states: 'Enter FTP or HTTP path to the blacklist archive here.'

Proxy Server

Services → Squid Proxy Server

Squid General Settings	
Enable Squid Proxy	<input checked="" type="checkbox"/> Check to enable the Squid proxy. Important: If unchecked, ALL Squid services will be disabled and stopped.
Keep Settings/Data	<input checked="" type="checkbox"/> If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls. Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
Proxy Interface(s)	<div> <div>LAN</div> <div>WAN</div> <div>loopback</div> </div> <p>The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.</p>
Proxy Port	<input type="text" value="3128"/> This is the port the proxy server will listen on. Default: 3128
ICP Port	<input type="text"/> This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.
Allow Users on Interface	<input checked="" type="checkbox"/> If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets.
Patch Captive Portal	This feature was removed - see Bug #5594 for details!
Resolve DNS IPv4 First	<input type="checkbox"/> Enable this to force DNS IPv4 lookup first. This option is very useful if you have problems accessing HTTPS sites.
Disable ICMP	<input type="checkbox"/> Check this to disable Squid ICMP pinger helper.
Use Alternate DNS Servers for the Proxy Server	<input type="text"/> To use DNS servers other than those configured in System > General Setup , enter the IP(s) here. Separate entries by semi-colons (;)

Activer le proxy

Proxy Server

si besoins Vider le cache dans


Services → Squid Proxy Server Local Cache

Squid Hard Disk Cache Settings	
Hard Disk Cache Size	<input type="text" value="100"/> Amount of disk space (in megabytes) to use for cached objects.
Hard Disk Cache System	<input type="text" value="ufs"/> This specifies the kind of storage system to use. i
Clear Disk Cache NOW	Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron. i If you wish to clear cache immediately , click this button once : Clear Disk Cache NOW
Level 1 Directories	<input type="text" value="16"/> Specifies the number of Level 1 directories for the hard disk cache. i
Hard Disk Cache Location	<input type="text" value="/var/squid/cache"/> This is the directory where the cache will be stored. Default: /var/squid/cache i
Minimum Object Size	<input type="text" value="0"/> Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)
Maximum Object Size	<input type="text" value="4"/> Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB) i

Proxy Server

Services → Squid Proxy Server

Activer les logs

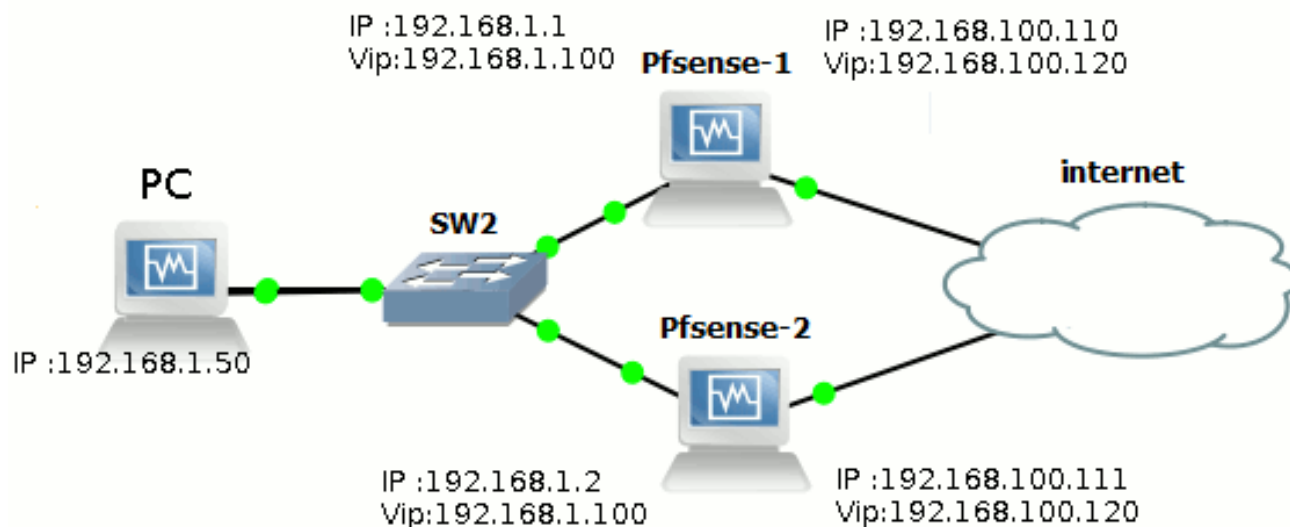
Logging Settings	
Enable Access Logging	<input checked="" type="checkbox"/> This will enable the access log. Warning: Do NOT enable if available disk space is low.
Log Store Directory	<input type="text" value="/var/squid/logs"/> The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs Important: Do NOT include the trailing / when setting a custom location.
Rotate Logs	<input type="text"/> Defines how many days of logfiles will be kept. Rotation is disabled if left empty.
Log Pages Denied by SquidGuard	<input type="checkbox"/> Makes it possible for SquidGuard denied log to be included on Squid logs. Click Info for detailed instructions. 

Page d'erreur Web
`/usr/local/www/sgerror.php`

Menu

Firewall/Virtual IPs

2 Pfsense redondants, permet d'avoir 2 Routeurs pour l'équilibrage de charge ou en cas d'une défaillance de l'un



CARP (Common Address Redundancy Protocol) est un protocole permettant à plusieurs hôtes de partager une adresse IP

Pfsync est protocole permettant de synchroniser entre deux serveurs l'état des connexions en cours. Il est recommandée d'utilisée une IP dédié ou LAN

XML-RPC est un protocole permettant la réplication de données d'un serveur vers un autres

Firewall/Virtual IPs

1) Création de notre IP Virtuel

Firewall / Virtual IPs

Virtual IP Address

Virtual IP address	Interface	Type	Description	Actions
+ Add				

2) Add

Edit Virtual IP

Type: ☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface:

Address type:

Address(es): /

Virtual IP Password:

VHID Group:

Advertising frequency:



Description:

Save

Virtual IP Password : seras demander par le serveur secondaire
VHID Group : 1 (Group d'appartenance)
Advertising frequency : 1 (seconde) temps inactivité avant de basculé
Skewv : 0 (master) 1..254(slave)

Firewall/Virtual IPs

Le LAN est crée

Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
192.168.1.120/24 (vhid: 1)	LAN	CARP	Master Lan	 

 Add

Add

Pour le WAN

Edit Virtual IP

Type

☐ IP Alias
 ☒ CARP
 ☐ Proxy ARP
 ☐ Other

Interface

WAN

Address type

Single address

Address(es)

192.168.100.120

/ 24

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password

••••••••

Enter the VHID group password.

••••••••

Confirm

VHID Group

2

Enter the VHID group that the machines will share.

Advertising frequency

1

Base

0

Skew

The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.


Description

Master Wan

A description may be entered here for administrative reference (not parsed).

Save

Save



Menu






Lan

Wan

PortForward

Firewall/Virtual IPs

Le WAN et le LAN sont crée

Virtual IP Address					
Virtual IP address	Interface	Type	Description	Actions	
192.168.1.120/24 (vhid: 1)	LAN	CARP	Master Lan		
192.168.100.120/32 (vhid: 2)	WAN	CARP	Master Wan		
					 Add

Des que vous avec configuré les Serveurs

Nous allons vérifier l'état de nos IP Virtuelles

Status → CARP (failover)

Status / CARP

Temporarily Disable CARP

Enter Persistent CARP Maintenance Mode

CARP Interfaces

CARP Interface	Virtual IP	Status
LAN@1	192.168.1.150/24	MASTER

pfSync Nodes

pfSync nodes:

0b947150

3ebcf465

bd204680

Sur le Serveur n°1
(master)

Status / CARP

Temporarily Disable CARP

Enter Persistent CARP Maintenance Mode

CARP Interfaces

CARP Interface	Virtual IP	Status
LAN@1	192.168.1.150/32	BACKUP

pfSync Nodes

pfSync nodes:

3758085e

397fa848

be95b127

d080bc25

Sur le Serveur n°2
(slave)

Création de l'IP Virtuel réussi

Il faut que les clients maintenant point sur l'IP 192.168.1.150

Firewall → Nat


Nous modifions la règles de firewall

Firewall / NAT / Outbound





Port Forward 1:1 **Outbound** NAT

General Logging Options

Mode ☒ Automatic outbound NAT rule generation. (IPsec passthrough included) ☐ Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below) ☐ Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT) ☐ Disable Outbound NAT rule generation. (No Outbound NAT rules)

 Save

Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<div> Add  Add  Delete  Save</div>									

Automatic Rules:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓ WAN	127.0.0.0/8 192.168.1.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓ WAN	127.0.0.0/8 192.168.1.0/24	*	*	*	WAN address	*	✕	Auto created rule

Pour passer à :
Hybrid Outbound NAT rule generation.(Automatic Outbound NAT + rules below)

Port Forward
1:1
Outbound
NAT

General Logging Options

Mode
☐

Automatic outbound NAT rule generation.
(IPsec passthrough included)

☒

Hybrid Outbound NAT rule generation.
(Automatic Outbound NAT + rules below)

☐

Manual Outbound NAT rule generation.
(AON - Advanced Outbound NAT)

☐

Disable Outbound NAT rule generation.
(No Outbound NAT rules)

Save

Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<div> Add Add Delete Save </div>									

Automatic Rules:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓ WAN	127.0.0.0/8 192.168.1.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓ WAN	127.0.0.0/8 192.168.1.0/24	*	*	*	WAN address	*	✗	Auto created rule

Save
Add

Pour l'interface WAN

Edit Advanced Outbound NAT Entry

Disabled ☐ Disable this rule

Do not NAT ☐ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules. In most cases this option is not required.

Interface Choose which interface this rule applies to. In most cases "WAN" is specified.

Protocol Choose which protocol this rule should match. In most cases "any" is specified.

Source / Type Source network for the outbound NAT mapping. Port

Destination / Type Destination network for the outbound NAT mapping. Port

☐ Not Invert the sense of the destination match.

Source Notre réseaux LAN

Translation

Address

Port ☐ Static port Enter the source port or range for the outbound NAT mapping.

Adress Notre IP WAN

Misc

No XMLRPC Sync ☐ Prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

Description A description may be entered here for administrative reference (not parsed).

Save

Création du NAT réussi

Modifier le DHCP pour prendre en compte en Gateway notre VIP 192.168.1.120

Services → DHCP Server

Other Options	
Gateway	<input type="text" value="192.168.1.120"/> <small>The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.</small>
Domain name	<input type="text"/> <small>The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.</small>
Domain search list	<input type="text"/> <small>The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.</small>
Default lease time	<input type="text" value="7200"/> <small>This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.</small>
Maximum lease time	<input type="text" value="86400"/> <small>This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.</small>
Failover peer IP	<input type="text"/> <small>Leave blank to disable. Enter the interface IP address of the other machine. Machines must be using CARP. Interface's advskew determines whether the DHCPd process is Primary or Secondary. Ensure one machine's advskew < 20 (and the other is > 20).</small>
Static ARP	<input type="checkbox"/> Enable Static ARP entries <small>This option persists even if DHCP server is disabled. Only the machines listed below will be able to communicate with the firewall on this interface.</small>

Failover peer IP (Optionnelle) permet de partager le lease DHCP, si le champs est renseigner vous devez modifier sur Pfsense secondaire la valeur (skew) qui doit être supérieur à 20

Création du DHCP réussi

Modifier OpenVpn pour prendre en compte en Gateway notre VIP 192.168.1.120

System → High Avail. Sync

State Synchronization Settings (pfsync)	
Synchronize states	<input checked="" type="checkbox"/> pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)
Synchronize Interface	<div>LAN</div> <p>If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.</p>
pfsync Synchronize Peer IP	<div>192.168.1.2</div> <p>Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.</p>

Synchronize states : Cocher la case pour activer la synchronisation
pfsync Synchronize Peer IP : Ip du serveur de secours (LAN)

Config de : XMLRPC Sync

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP
 Enter the IP address of the firewall to which the selected configuration sections should be synchronized.
 XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
 Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username
 Enter the webConfigurator username of the system entered above for synchronizing the configuration.
 Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password
 Enter the webConfigurator password of the system entered above for synchronizing the configuration.
 Do not use the Synchronize Config to IP and password option on backup cluster members!

Select options to sync

- ☒ user manager users and groups
- ☒ authentication servers (e.g. LDAP, RADIUS)
- ☒ certificate Authorities, Certificates, and Certificate Revocation Lists
- ☒ firewall rules
- ☒ firewall schedules
- ☒ firewall aliases
- ☒ NAT configuration
- ☒ sec configuration
- ☒ openVPN configuration
- ☒ HCP Server settings
- ☒ L2L Server settings
- ☒ static Route configuration
- ☒ Load Balancer configuration
- ☒ virtual IPs
- ☒ traffic Shaper configuration
- ☒ traffic Shaper Limiters configuration
- ☒ DNS Forwarder and DNS Resolver configurations
- ☒ captive Portal
- ☒ **Flush All**

Synchronize Config to IP : Ip du serveur de secours (LAN)

Remote System Username : saisir un compte avec password

Select options to sync : Sélectionnée les services a synchroniser sur le serveur de secours

Sur le Serveur Secondaire

State Synchronization Settings (pfsync)	
Synchronize states	<input checked="" type="checkbox"/> pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)
Synchronize Interface	<div>LAN</div> <p>If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.</p>
pfsync Synchronize Peer IP	<div>192.168.1.1</div> <p>Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.</p>

Synchronize Config to IP : (Optionnelle) Ip du serveur Maitre (LAN)

Config de : XMLRPC Sync

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP

Enter the IP address of the firewall to which the selected configuration sections should be synchronized.

XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!

Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username

Enter the webConfigurator username of the system entered above for synchronizing the configuration.

Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password

Enter the webConfigurator password of the system entered above for synchronizing the configuration.

Do not use the Synchronize Config to IP and password option on backup cluster members!

Confirm

Select options to sync

- ☐ User manager users and groups
- ☐ Authentication servers (e.g. LDAP, RADIUS)
- ☐ Certificate Authorities, Certificates, and Certificate Revocation Lists
- ☐ Firewall rules
- ☐ Firewall schedules
- ☐ Firewall aliases
- ☐ AT configuration
- ☐ Sec configuration
- ☐ OpenVPN configuration
- ☐ DHCP Server settings
- ☐ iOL Server settings
- ☐ Static Route configuration
- ☐ Load Balancer configuration
- ☐ Virtual IPs
- ☐ Traffic Shaper configuration
- ☐ Traffic Shaper Limiters configuration
- ☐ DNS Forwarder and DNS Resolver configurations
- ☐ Captive Portal

[Toggle All](#)

Rien a indiquer à partir de maintenant la synchronisation devrait fonctionner

Autoriser le flux sur le firewall

Si le port https n'est pas ouvert, vous pouvez lui attribuer une règle

Edit Firewall Rule

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match. LAN net Source Address /

Display Advanced Display Advanced

Destination

Destination ☐ Invert match. This firewall (self) Destination Address /

Destination port range HTTPS (443) HTTPS (443)
From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Save

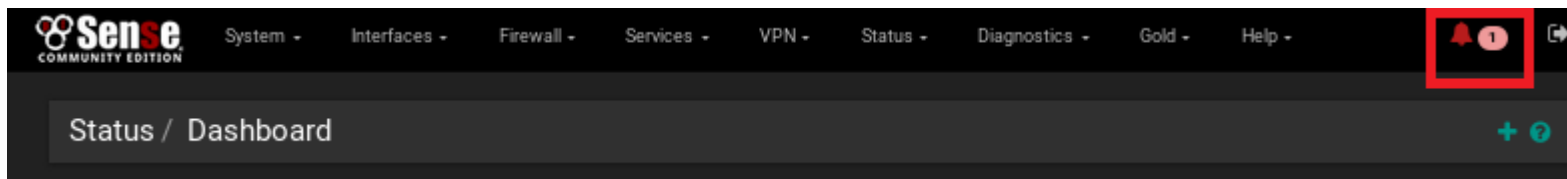
La nouvelle règles est :

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/3.52 MiB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/26 KiB	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none			
<input type="checkbox"/>	7/364 KiB	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/>	0/13 KiB	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP	LAN net	*	This Firewall	443 (HTTPS)	*	none		Dédié au firewall	
<div> Add Add Delete Save Separator </div>											

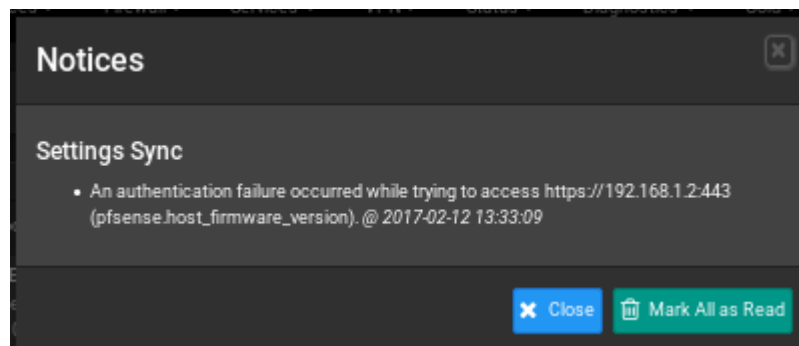
Autorisation du flux réussi

Voir les erreurs

Si une erreur est trouvée par Pfsense



cliquer sur la cloche



Ici le message indique qu'il y a sans-doute une erreur avec le mot de passe ou le compte utilisateur

Faites des tests

- Redémarré le serveur, débrancher le câble réseaux pour vérifier que le primaire devient bien master