

pfSense

- [Installation de pfSense 2.5](#)
- [Installation, attribution de cartes et adresses IP](#)
- [Ajouter un proxy Zabbix](#)
- [Paramétrage via l'interface web](#)
- [Ajouter l'agent Zabbix](#)
- [Mise à jour](#)
- [Paramètres généraux](#)
- [Règles de pare-feu](#)
- [Plugins](#)
- [Reverse-proxy](#)

Installation de pfSense 2.5

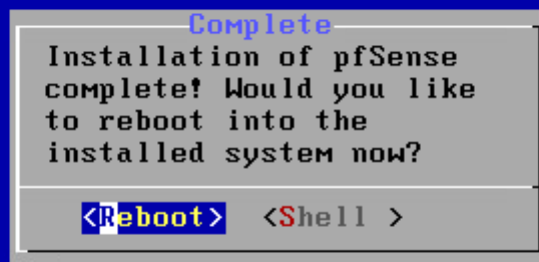
On commence par définir la langue du clavier (French), puis on installe en mode Auto.

On clique sur "No" ici.



On reboot.

pfSense Installer



Je n'ai pas de VLAN. On peut en ajouter plus tard via l'interface Web.

```
Starting device manager (devd)...done.
Loading configuration.....done.
Updating configuration....done.
Warning: Configuration references interfaces that do not exist: em0 em1

Network interface mismatch -- Running interface assignment option.
vnx0: link state changed to UP
vnx1: link state changed to UP
vnx2: link state changed to UP
vnx3: link state changed to UP
vnx4: link state changed to UP

Valid interfaces are:

vnx0      00:0c:29:95:38:aa (down) VMware VMXNET3 Ethernet Adapter
vnx1      00:0c:29:95:38:8c (down) VMware VMXNET3 Ethernet Adapter
vnx2      00:0c:29:95:38:b4 (down) VMware VMXNET3 Ethernet Adapter
vnx3      00:0c:29:95:38:96 (down) VMware VMXNET3 Ethernet Adapter
vnx4      00:0c:29:95:38:a0 (down) VMware VMXNET3 Ethernet Adapter

Do VLANs 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]?
```

Pour chaque interface, on définit laquelle désigne laquelle (on peut comparé les adresses MAC sur l'ESXI).

```
VMX1: link state changed to UP
VMX2: link state changed to UP
VMX3: link state changed to UP
VMX4: link state changed to UP
```

Valid interfaces are:

```
VMX0      00:0c:29:95:38:aa (down) VMware VMXNET3 Ethernet Adapter
VMX1      00:0c:29:95:38:8c (down) VMware VMXNET3 Ethernet Adapter
VMX2      00:0c:29:95:38:b4 (down) VMware VMXNET3 Ethernet Adapter
VMX3      00:0c:29:95:38:96 (down) VMware VMXNET3 Ethernet Adapter
VMX4      00:0c:29:95:38:a0 (down) VMware VMXNET3 Ethernet Adapter
```

Do VLANs 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
(VMX0 VMX1 VMX2 VMX3 VMX4 or a):

Enter the WAN interface name or 'a' for auto-detection
(VMX0 VMX1 VMX2 VMX3 VMX4 or a): VMX1

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(VMX0 VMX2 VMX3 VMX4 a or nothing if finished): VMX3

Enter the Optional 1 interface name or 'a' for auto-detection
(VMX0 VMX2 VMX4 a or nothing if finished): VMX4

Enter the Optional 2 interface name or 'a' for auto-detection
(VMX0 VMX2 a or nothing if finished): VMX0

Enter the Optional 3 interface name or 'a' for auto-detection
(VMX2 a or nothing if finished): VMX2

The interfaces will be assigned as follows:

```
WAN    -> VMX1
LAN    -> VMX3
OPT1   -> VMX4
OPT2   -> VMX0
OPT3   -> VMX2
```

Do you want to proceed [y;n]?

On attribue ensuite les adresses IP en prenant l'option 2.

Available interfaces:

- 1 - WAN (vnx1 - dhcp, dhcp6)
- 2 - LAN (vnx3 - static)
- 3 - OPT1 (vnx4)
- 4 - OPT2 (vnx0)
- 5 - OPT3 (vnx2)

Enter the number of the interface you wish to configure: █

- 1 - WAN (vnx1 - dhcp, dhcp6)
- 2 - LAN (vnx3 - static)
- 3 - OPT1 (vnx4)
- 4 - OPT2 (vnx0)
- 5 - OPT3 (vnx2)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.199.10

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 WAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.199.254 █

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

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...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 192.168.0.254/24
You can now access the webConfigurator by opening the following URL in your web browser:

<https://192.168.0.254/>

Press <ENTER> to continue. █

Installation, attribution de cartes et adresses IP

```
[CONTEXTE] pfSense
Hypervisor: Origin = "UMwareUMware"
Done.
..... done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.
Updating configuration.....done.
Warning: Configuration references interfaces that do not exist: em0 em1

Network interface mismatch -- Running interface assignment option.
vmx0: link state changed to UP
vmx1: link state changed to UP
vmx2: link state changed to UP

Valid interfaces are:

vmx0      00:0c:29:13:da:6e (down) VMware VMXNET3 Ethernet Adapter
vmx1      00:0c:29:13:da:78 (down) VMware VMXNET3 Ethernet Adapter
vmx2      00:0c:29:13:da:82 (down) VMware VMXNET3 Ethernet Adapter

Do VLANs 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]? █
```

On met non et on attribue les cartes.

```
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VMware Virtual Machine - Netgate Device ID: cb8523ed66fa3073e618

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

WAN (wan)      -> vmx0      -> v4/DHCP4: 192.168.199.109/24
                v6/DHCP6: 2a01:cb08:8b8a:6100:20c:29ff:fe13:da
5e/64
LAN (lan)      -> vmx1      -> v4: 192.168.1.1/24
OPT1 (opt1)   -> vmx2      ->

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: █
```

On attribue ensuite des adresses IP en choisissant l'option 2.

```
Available interfaces:

1 - WAN (vmx0 - dhcp, dhcp6)
2 - LAN (vmx1 - static)
3 - OPT1 (vmx2)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.199.5

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 WAN IPv4 subnet bit count (1 to 31):
> 24

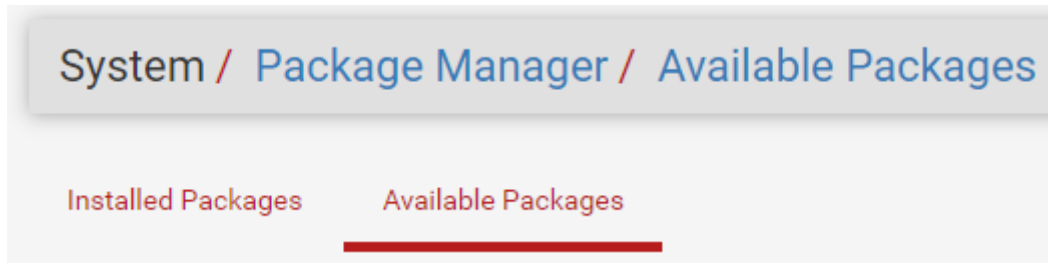
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> █
```

On rentre une passerelle pour l'accès Internet.

On fait de même pour les autres cartes.

Ajouter un proxy Zabbix

Sous "System > Package Manager > Available Packages", on recherche Zabbix Proxy. On prend la dernière version.



Ensuite, sous "Services > Zabbix Proxy", on le configure.

On rentre les informations suivantes :

Server

Server Port

Hostname (nom du proxy, doit correspondre dans Zabbix)

ListenIP (sur quelles interfaces le proxy écoute)

Proxy Mode (Active est par défaut, et préférable)

Config Frequency (fréquence d'actualisation de la configuration, c'est à dire la fréquence de la récupération de configuration de la part du serveur)

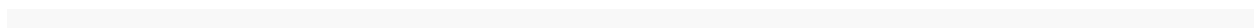
TLSConnect : psk

TLS accept : psk

TLS Psk Identity : identité du proxy psk. Par exemple : homelab. Devra correspondre pour le chiffrement dans Zabbix

TLS PSK : la clé. On peut la générer sur une machine linux via la commande `openssl rand -hex 32`

On clique ensuite sur "Show Advanced Options" et on rajoute :


























```
StartDiscoverers=10
StartVMwareCollectors=2
VMwareFrequency=60
VMwarePerfFrequency=60
VMwareCacheSize=50M
VMwareTimeout=10
```

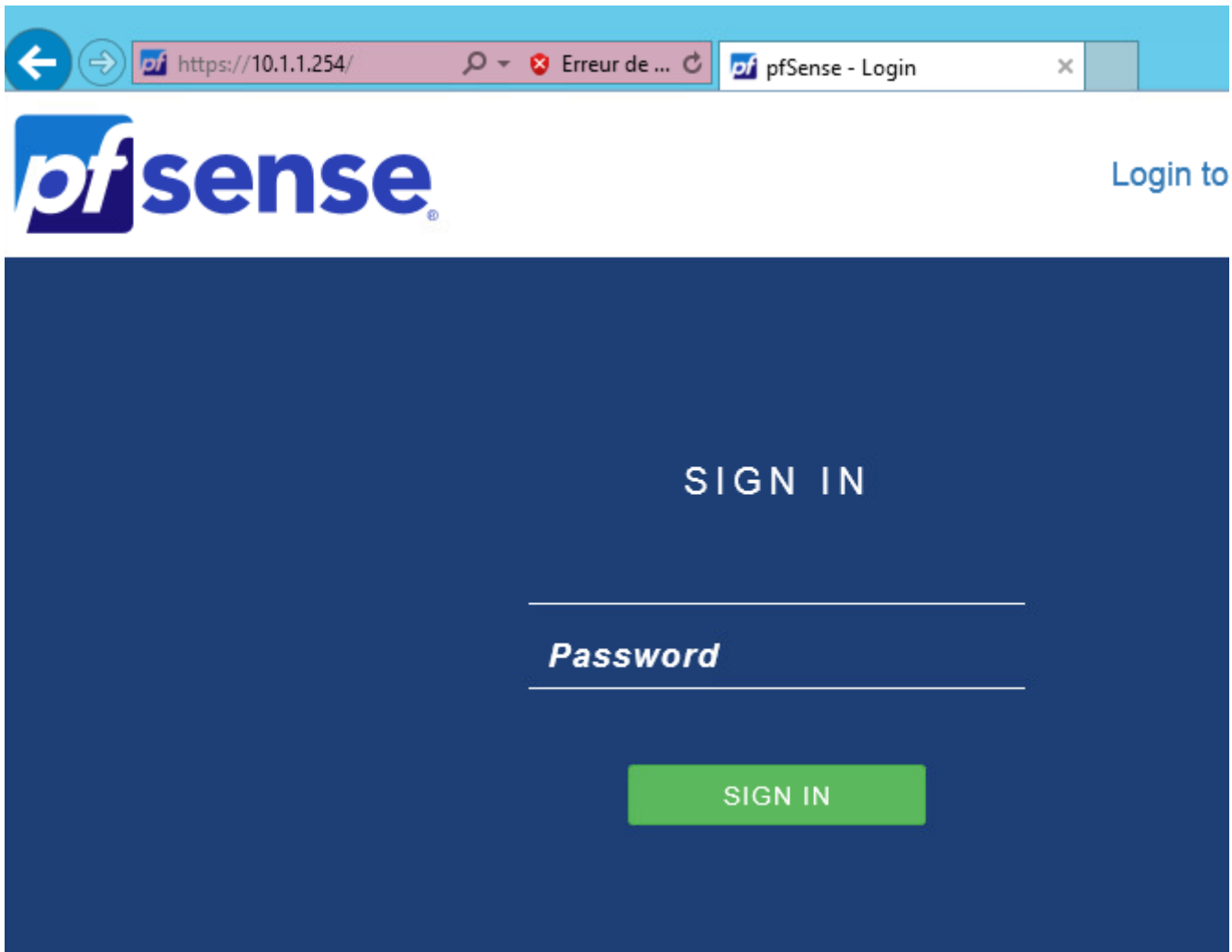
Ces valeurs sont utiles si on supervise un hôte VMware.

On peut vérifier si le service est démarré sous "Status > Services".

Status / [Services](#) ?

Services			
Service	Description	Status	Actions
dpinger	Gateway Monitoring Daemon	✓	    
pcscd	PC/SC Smart Card Daemon	✓	 
syslogd	System Logger Daemon	✓	   
unbound	DNS Resolver	✓	   
vmware-guestd	VMware Guest Daemon	✓	 
vmware-kmod	VMware Kernel Modules	✓	 
zabbix_agentd	Zabbix Agent Host Monitor Daemon	✓	 
zabbix_proxy	Zabbix Proxy Collection Daemon	✓	 

Paramétrage via l'interface web



admin:pfsense

pfSense Setup

Welcome to pfSense® software!

This wizard will provide guidance through the initial configuration of pfSense.

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

pfSense® software is developed and maintained by Netgate®

[Learn more](#)

» Next

General Information

On this screen the general pfSense parameters will be set.

Hostname

EXAMPLE: myserver

Domain

EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers f servers directly. To use the manually configured DNS servers below for client queries, vi enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS

Allow DNS servers to be overridden by DHCP/PPP on WAN

» Next

Time Server Information

Please enter the time, date and time zone.

**Time server
hostname**



Enter the hostname (FQDN) of the time server.

Timezone

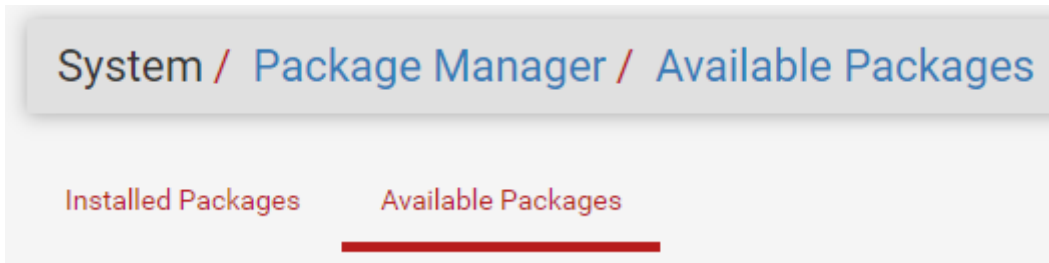


[» Next](#)

On vérifie ensuite les informations puis on clique sur "Reload".

Ajouter l'agent Zabbix





Sous "System > Package Manager > Available Packages", on recherche Zabbix Agent. On prend la dernière version.



Ensuite, sous "Services > Zabbix Agent", on le configure.

On définit les valeurs : Server, Server Active (pour le mode actif), Hostname. Pour le chiffrement, on peut définir les options comme pour le proxy si l'on souhaite chiffrer en local.

Mise à jour

System Information   	
Name	pfSense.littoral1.fr
User	admin@10.1.1.1 (Local Database)
System	VMware Virtual Machine Netgate Device ID: cb8523ed66fa3073e618
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu May 28 2020
Version	2.4.5-RELEASE-p1 (amd64) built on Tue Jun 02 17:51:17 EDT 2020 FreeBSD 11.3-STABLE Version 2.5.0 is available.   Version information updated at Sat Mar 13 14:12:17 CET 2021
CPU Type	Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
MIPS Migration	Enabled

On clique sur le nuage puis on met à jour.

Confirmation Required to update pfSense system.

Branch	<input type="text" value="Latest stable version (2.5.x)"/>
Please select the branch from which to update the system firmware. Use of the development version is at your own risk!	
Current Base System	2.4.5_1
Latest Base System	2.5.0
Confirm Update	<input checked="" type="checkbox"/> Confirm

Paramètres généraux

Changement du port par défaut

Dans System > Advanced :

System / [Advanced](#) / [Admin Access](#) ?

[Admin Access](#) [Firewall & NAT](#) [Networking](#) [Miscellaneous](#) [System Tunables](#) [Notifications](#)

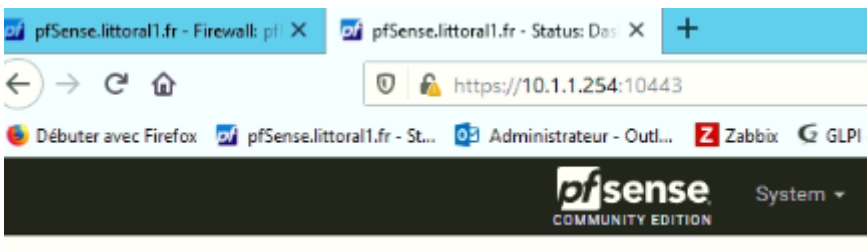
webConfigurator

Protocol HTTP HTTPS (SSL/TLS)

SSL/TLS Certificate ▼
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 immediately after save.

Max Processes ↕
Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.



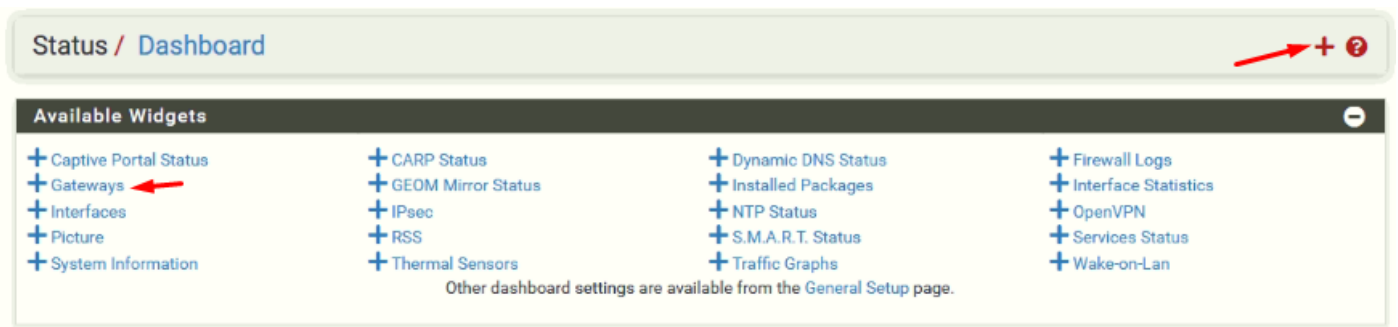
La règle s'est donc modifiée :

Rules (Drag to Change Order)												
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input checked="" type="checkbox"/>	2 / 21.76 MiB	*	*	*	LAN Address	10443 80	*	*		Anti-Lockout Rule		

On coche également cette case. Par défaut, pfsense redirige le port 80 vers le port https.

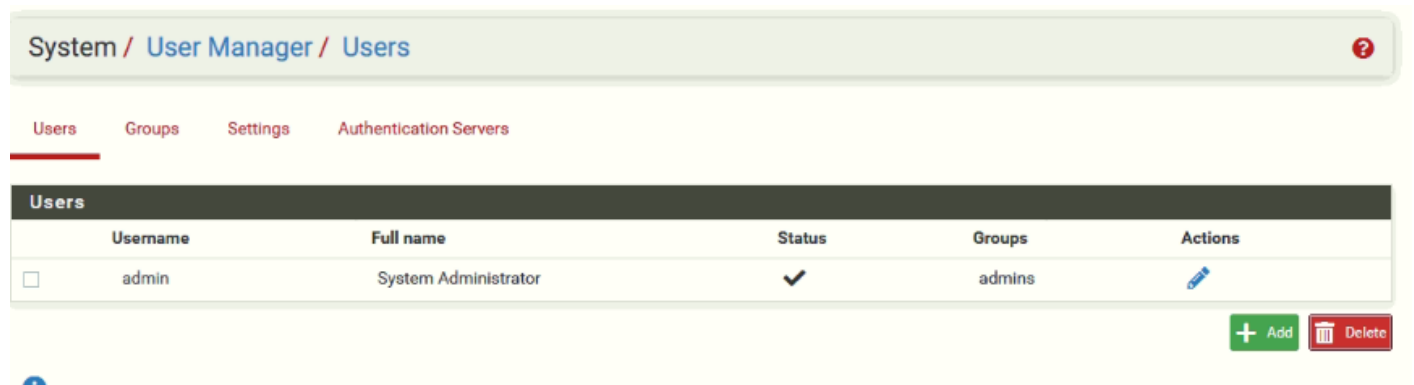
WebGUI redirect Disable webConfigurator redirect rule
When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.

Ajout de widget au menu principal



Création d'un nouveau compte admin

Il est recommandé de créer un autre compte que "admin".



On désactive ensuite le compte admin.

Changement du nom d'interface

Dans Interfaces > Assignments :

Interfaces / OPT1 (em2)

General Configuration

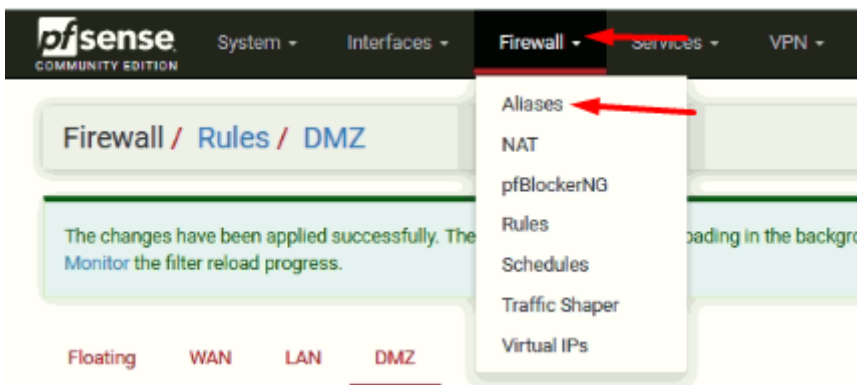
Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="DMZ"/> Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4 ▾
IPv6 Configuration Type	None ▾

On change la description pour "DMZ".

Règles de pare-feu

Le LAN par défaut autorise tout, le WAN rejete tout et la DMZ aussi.

Création d'alias



Properties

Name
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

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

Type

Network(s)

Hint Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.

Network or FQDN /

Règles DMZ

Pour la DMZ, on refuse l'accès au pare-feu (administration).

Edit Firewall Rule

Action

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

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

Protocol
Choose which IP protocol this rule should match.

Source

Source Invert match /

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination Invert match /

Destination Port Range (other) (other)
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.

Extra Options

Log Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description BLOCK Web Interface

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

On bloque l'accès au LAN.

Floating WAN LAN **DMZ**

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	*	*	This Firewall	10443	*	none		BLOCK Web Interface	
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	*	*	*	*	*	none			

Add Add Delete Save Separator

Edit Firewall Rule

Action Block

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 DMZ

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

Address Family IPv4+IPv6

Select the internet Protocol version this rule applies to.

Protocol Any

Choose which IP protocol this rule should match.

Source

Source Invert match any Source Address /

Destination

Destination Invert match Single host or alias My_Private_Network

Extra Options










Log Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description BLOCK Access to LAN

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗	0/0 B	IPv4+6 *	*	*	My_Private_Network	*	*	none	BLOCK Access to LAN	    
<input type="checkbox"/>	✗	0/0 B	IPv4 TCP	*	*	This Firewall	10443	*	none	BLOCK Web Interface	    
<input type="checkbox"/>	✓	0/0 B	IPv4 *	*	*	*	*	*	none		    

Plugins

Pfsense dispose de nombreux plugins installables, comme open-vm-tools (si virtualisé), pfblockerng pour bloquer des sites/IP, agent Zabbix...

Par exemple, arpwatch.

arpwatch

Ce plugin détecte les nouvelles adresses MAC du réseau.

The screenshot shows the pfSense Package Manager interface. At the top, there is a breadcrumb navigation: **System / Package Manager / Available Packages**. Below this, a package entry for **arpwatch** is displayed. The version is **0.2.0_4**. The description reads: "This package contains tools that monitors ethernet activity and maintains a database of ethernet/ip address pairings. It also reports certain changes via email." To the right of the description is a green **+ Install** button. Below the description, the **Package Dependencies:** section lists **arpwatch-3.1** with a small icon. At the bottom left, a dark navigation bar contains **Services** and **VPN** menus. Below this bar, the **Arpwatch** package is highlighted in a light yellow box.

General Options

Enable Arpwatch

Interfaces LAN
DMZ
WAN

The interfaces that will listen for ARP packets.

Notifications recipient

The email address that will receive notifications (warning: may send a lot of notifications in busy networks).

Disable Cron emails Disables Cron email notifications from other packages.

Zero padded ethernet addresses Use zero padded ethernet addresses in *.dat files

Disable CARP/VRPP Disables reporting CARP/VRPP ethernet prefixes.

Disable bogons Disables reporting any bogons.

Disable 0.0.0.0 Disables reporting 0.0.0.0 changes, helpful in busy DHCP networks.

Update vendors Updates the ethernet vendor database, downloaded from <http://standards-oui.ieee.org/oui/oui.csv>.

Clear database Reset the database of collected mac/ip addresses when uninstalling or upgrading Arpwatch.

Suppress MAC

Enter the MAC addresses you want to suppress from the notifications. Type of notification to suppress.

Add

Dans l'onglet Database, on aura une liste.

Package / Arpwatch / Database

Settings Database

Interface	IP address	MAC address	Vendor	Hostname	Timestamp
LAN	10.1.1.101	00:50:56:bf:28:85	unknown		Tue Mar 16 19:39:38 2021
LAN	10.1.1.254	00:50:56:bf:cc:3a	unknown	pfSense	Tue Mar 16 19:39:56 2021
LAN	10.1.1.200	00:50:56:bf:2a:7e	unknown		Tue Mar 16 19:39:56 2021
LAN	10.1.1.1	00:50:56:bf:03:7c	unknown		Tue Mar 16 19:39:52 2021
LAN	10.1.1.100	00:50:56:bf:75:f6	unknown		Tue Mar 16 19:39:52 2021
LAN	10.1.1.3	00:50:56:bf:8c:87	unknown		Tue Mar 16 19:39:19 2021
LAN	10.1.1.105	00:50:56:bf:b3:8f	unknown		Tue Mar 16 19:39:27 2021
LAN	10.1.1.5	00:50:56:bf:ca:92	unknown		Tue Mar 16 19:39:31 2021

pfblockerng

Voir : A VENIR.

Reverse-proxy

On ajoute un certificat SSL (Wildcard) dans System > Cert. Manager, et dans l'onglet "Certificates".

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (5fbd278403e5d) Server Certificate CA: No Server: Yes	self- signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-5fbd278403e5d ⓘ Valid From: Tue, 24 Nov 2020 14:32:20 -0100 Valid Until: Mon, 27 Dec 2021 14:32:20 -0100	webConfigurator	

Add/Sign a New Certificate

Method

Descriptive name

Import Certificate

Certificate Type X.509 (PEM) PKCS #12 (PFX)

Certificate data
Paste a certificate in X.509 PEM format here.

Private key data
Paste a private key in X.509 PEM format here. This field may remain empty in certain cases, such as when the private key is stored on a PKCS#11 token.

Backends

Advanced	Name	Servers	Check	Frontend	Actions
<input type="checkbox"/>	www.littoral1.fr	1	HTTP	shared-frontend	
<input type="checkbox"/>	mail.littoral1.fr	1	none	shared-frontend	

Add Delete Save

Frontends

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		shared-frontend	shared-frontend	192.168.199.5:443	https	www.littoral1.fr if(WEB) mail.littoral1.fr if(MAIL)	

Add Delete Save

Name

Description

Status

External address Define what ip:port combinations to listen on for incoming connections.

Table						
	Listen address	Custom address	Port	SSL Offloading	Advanced	Actions
<input type="checkbox"/>	WAN address (IPv4)	<input type="text"/>	443	<input checked="" type="checkbox"/>	<input type="text"/>	

NOTE: You must add a firewall rules permitting access to the listen ports above.
 If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define Virtual IP addresses on the first). Also note that if you are trying to redirect connections on the LAN select the "any" option. In the port to listen to, if you want to specify multiple ports, separate them with a comma (,). EXAMPLE: 80,8000 Or to listen on both 80 and 443 create 2 rows in the table where for the 443 you would likely want to check the SSL-offloading checkbox.

Max connections

Sets the maximum amount of connections this frontend will accept, may be left empty.

Type

This defines the processing type of HAProxy, and will determine the available options for ssl checks and also several other options

Default backend, access control lists and actions

Access Control lists

Use these to define criteria that will be used with actions defined below to perform them only when certain conditions are met.

Table						
	Name	Expression	CS	Not	Value	Actions
<input type="checkbox"/>	WEB	Host matches:	no	no	www.littoral1.fr	
<input type="checkbox"/>	MAIL	Host matches:	no	no	mail.littoral1.fr	

- 'CS' makes the string matches 'Case Sensitive' so www.domain.tld wil not be the same as WWW.domain.TLD

- 'Not' makes the match if the value given is not matched

Example:

Name	Expression	CS	Not	Value
Backend1acl	Host matches			www.yourdomain.tld
addHeaderAcl	SSL Client certificate valid			

acl's with the same name will be 'combined' using OR criteria.

For more information about ACLs please see [HAProxy Documentation](#) Section 7 - Using ACLs

NOTE Important change in behaviour, since package version 0.32

-acl's are no longer combined with logical AND operators, list multiple acl's below where needed.

-acl's alone no longer implicitly generate use_backend configuration. Add 'actions' below to accomplish this behaviour.

Actions

Use these to select the backend to use or perform other actions like calling a lua script, blocking certain requests or others available.

Table			
	Action	Parameters	Condition acl names
<input type="checkbox"/>	Use Backend	See below	WEB
		backend: www.littoral1.fr	
<input type="checkbox"/>	Use Backend	See below	MAIL
		backend: mail.littoral1.fr	

Example:

Action	Parameters	Condition
Use Backend	Website1Backend	Backend1acl
http-request header set	Headername: X-HEADER-ClientCertValid New logformat value: YES	addHeaderAcl

Default Backend

None

the time (in milliseconds) we accept to wait for data from the client, or for the client to accept data (default 30000).

Use "forwardfor" option

Use "forwardfor" option.

The "forwardfor" option creates an HTTP "X-Forwarded-For" header which contains the client's IP address. This is useful to let the final web server know what the client address was. (eg for statistics on domains)

Use "httpclose" option

http-keep-alive (default)

By default HAProxy operates in keep-alive mode with regards to persistent connections: for each connection it processes each request and response, and leaves the connection idle on both sides between the end of a response and the start of a new request.

Bind pass thru

NOTE: paste text into this box that you would like to pass behind each bind option.

Advanced pass thru

NOTE: paste text into this box that you would like to pass thru in the frontend.

SSL Offloading

Note SSL Offloading will reduce web servers load by maintaining and encrypting connection with users on internet while sending and retrieving data without encryption to internal servers. Also more ACL rules and http logging may be configured when this option is used. Certificates can be imported into the pfSense "Certificate Authority Manager" Please be aware this possibly will not work with all web applications. Some applications will require setting the SSL checkbox on the backend server configurations so the connection to the webserver will also be a encrypted connection, in that case there will be a slight overall performance loss."

SNI Filter

Specify a SNI filter to apply below SSL settings to specific domain(s), see the "crt-list" option from haproxy for details.
EXAMPLE: *.securedomain.tld !public.securedomain.tld

Certificate

Choose the cert to use on this frontend.

- Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)
- Add ACL for certificate Subject Alternative Names.

OCSP

Load certificate ocsp responses for easy certificate validation by the client.
A cron job wil update the ocsp response every hour.

Additional certificates

Which of these certificate will be send will be determined by haproxys SNI recognition. If the browser does not send SNI this will not work properly. (IE on XP is one example, possibly also older browsers or mobile devices).

Table

Certificates	Actions
--------------	---------