

Configuration Parefeu Pfsense

Table des matières

1- Téléchargement.....	2
2- Installation.....	2
3- Configuration.....	2
4- Configuration depuis le Web.....	3
4-1 Première configuration :.....	4
4-2 Configuration des adresses des Interfaces.....	6
4-2-1 WAN.....	6
4-2-2 LAN1.....	7
4-2-3 LAN2.....	9
4-2-3 DMZ.....	10
4-3 Configuration des règles.....	11
4-3-1 LAN1.....	11
4-3-2 LAN2.....	11
4-3-3 DMZ.....	12
4-3-3 WAN.....	12
5- Site sur la DMZ.....	13

1- Téléchargement

Il est conseillé de télécharger Pfsense via le site officiel : <https://www.pfsense.org/>

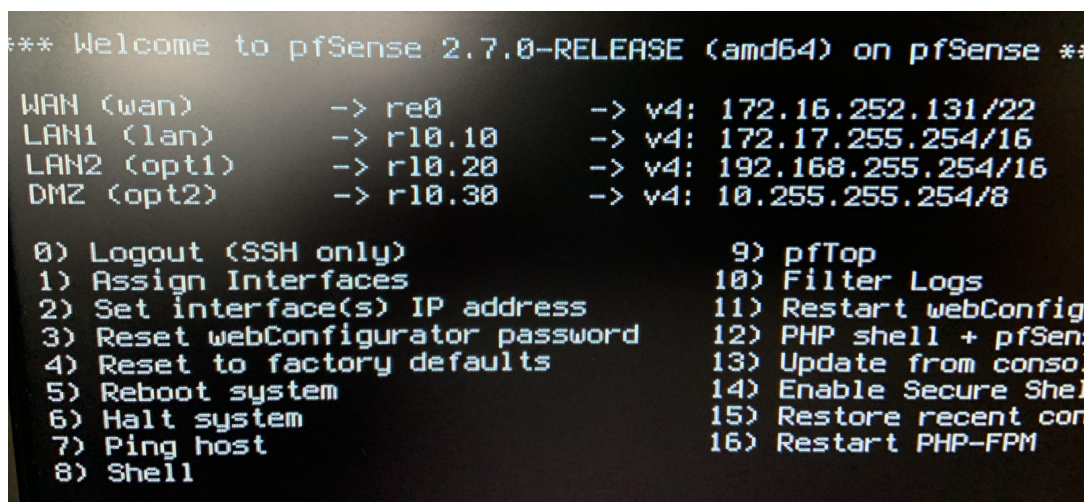
Une fois fait, il faut ensuite graver ce fichier sur une clé USB afin de pouvoir Booter via cette dernière.

2- Installation

On insère ensuite la clé USB dans le poste puis on boot sur cette dernière en suivant les différentes instructions.

3- Configuration

Le PC que nous utilisons et qui fera office de parefeu contient 2 cartes réseau, il va donc falloir en configurer une pour le WAN et la seconde pour les interfaces LAN.



```
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> re0      -> v4: 172.16.252.131/22
LAN1 (lan)     -> rl0.10   -> v4: 172.17.255.254/16
LAN2 (opt1)    -> rl0.20   -> v4: 192.168.255.254/16
DMZ (opt2)     -> rl0.30   -> v4: 10.255.255.254/8

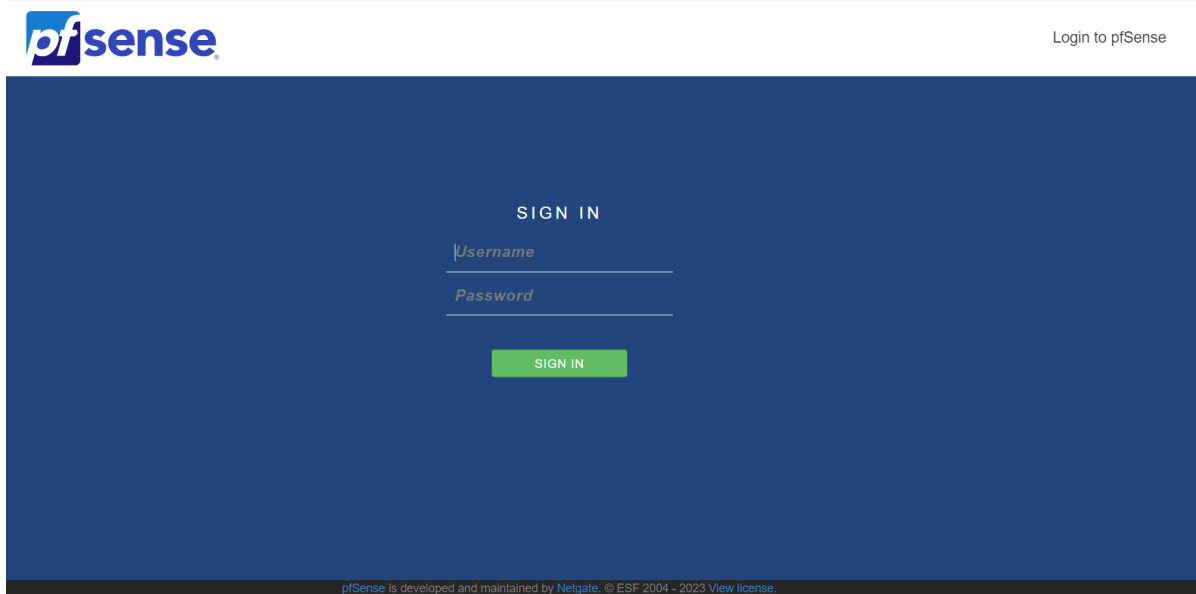
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfig
3) Reset webConfigurator password 12) PHP shell + pfSense
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell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

4- Configuration depuis le Web

On peut accéder à la configuration web via un navigateur grâce à l'adresse du WAN comme montré sur la capture d'écran précédente. (ici 172.16.252.131)

Il faut bien sûr penser à changer l'adresse IPv4 de l'ordinateur avant.

On arrive sur la page suivante :



The image shows the pfSense login page. At the top left is the pfSense logo. At the top right is a link that says "Login to pfSense". The main area has a dark blue background with the text "SIGN IN" in white. Below this are two input fields: "Username" and "Password", both with placeholder text. Below the fields is a green button with the text "SIGN IN". At the bottom of the page, there is a small line of text: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license."

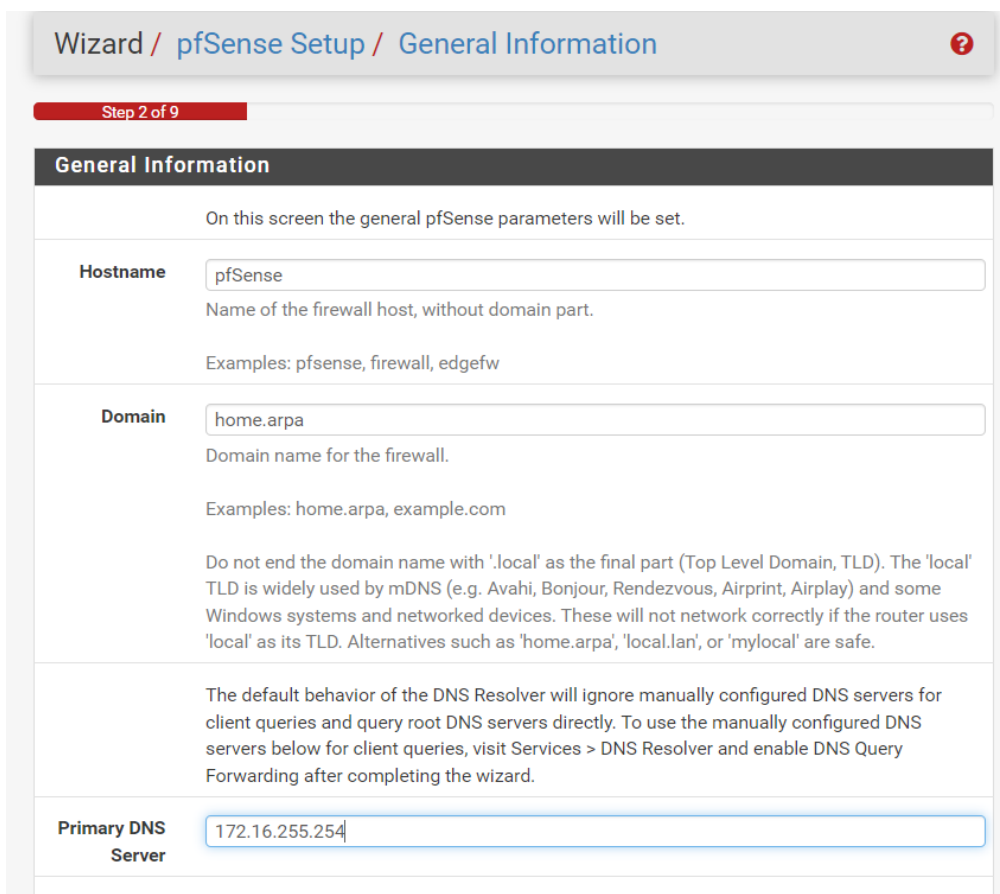
Connexion (par défaut) :

Login : admin

Mdp : pfsense

4-1 Première configuration :




On configure en fonction de nos besoins :



The image shows the pfSense Setup Wizard, specifically the "General Information" screen. The breadcrumb navigation at the top reads "Wizard / pfSense Setup / General Information". Below this is a progress bar indicating "Step 2 of 9". The main heading is "General Information". Below the heading is a paragraph: "On this screen the general pfSense parameters will be set." There are two main sections: "Hostname" and "Domain". The "Hostname" section has a text input field with "pfSense" entered, followed by the text "Name of the firewall host, without domain part." and "Examples: pfsense, firewall, edgefw". The "Domain" section has a text input field with "home.arpa" entered, followed by the text "Domain name for the firewall." and "Examples: home.arpa, example.com". Below the "Domain" section is a paragraph: "Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe." At the bottom of the screen is a section for "Primary DNS Server" with a text input field containing "172.16.255.254".

4-2 Configuration des adresses des Interfaces

4-2-1 WAN

Interfaces / WAN (re0)   

General Configuration

Enable ☒ Enable interface

Description

WAN

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

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

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

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex

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.

Static IPv4 Configuration

IPv4 Address

172.16.252.131

/ 22

IPv4 Upstream gateway

WANGW - 172.16.255.254

+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by [clicking here](#).

Reserved Networks

Block private networks and loopback addresses

☐

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

☒

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.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Save

4-2-2 LAN1

General Configuration

Enable ☒ Enable interface

Description

LAN1

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

XXXXXXXXXXXX

The MAC address of a VLAN interface must be set on its parent interface

MTU

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

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex

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.

Static IPv4 Configuration

IPv4 Address

172.17.255.254

/

16

IPv4 Upstream gateway

None

+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).
Gateways can be managed by [clicking here](#).

Reserved Networks

Block private networks and loopback addresses

☐

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

☐

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.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Save

4-2-3 LAN2

General Configuration

Enable ☒ Enable interface

Description 1
Enter a description (name) for the interface here.

IPv4 Configuration Type ▼

IPv6 Configuration Type 2 ▼

MAC Address
The MAC address of a VLAN interface must be set on its parent interface

MTU
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
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex ▼
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.

Static IPv4 Configuration

IPv4 Address / 16 ▼

IPv4 Upstream gateway + Add a new gateway 3
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).
Gateways can be managed by [clicking here](#).

Reserved Networks

Block private networks and loopback addresses ☐
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 ☐
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.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

📁 Save

4-2-3 DMZ

Interfaces / DMZ (rl0.30)



General Configuration

Enable ☒ Enable interface

1

Description

DMZ

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

2

MAC Address

xxxxxxxxxxxx

The MAC address of a VLAN interface must be set on its parent interface

MTU

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

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex

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.

Static IPv4 Configuration

IPv4 Address

10.255.255.254

/

8

IPv4 Upstream gateway

None

+ Add a new gateway

3

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.

On local area network interfaces the upstream gateway should be "none".

Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).

Gateways can be managed by [clicking here](#).

Reserved Networks

Block private networks
and loopback addresses

☐

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

☐

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.

This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.

Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Save

4-3 Configuration des règles

(Pour la suite vous retrouverez le résultat de mes tests dans le documents intitulé « recettes »)

On va créer des règles afin de donner l'accès aux différentes zones vers Internet. Par défaut le parefeu pfsense a une politique qui bloque tout trafic pour toutes les interfaces.

On peut retrouver les résultats pour les testes sur les recettes 1, 2, 3, et 4

4-3-1 LAN1

On souhaite bloquer le trafic depuis LAN1 vers Lan2. On met donc en place la règle suivante :

Recette 5

Floating WAN LAN1 LAN2 DMZ

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/335 KiB	*	*	*	LAN1 Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/93 KiB	IPv4 TCP/UDP	*	*	WAN net	53 (DNS)	*	none			
<input type="checkbox"/>	0/1 KiB	IPv4 *	LAN1 net	*	LAN2 net	*	*	none			
<input type="checkbox"/>	0/2 KiB	IPv4 *	*	*	*	*	*	none			

Add

Add

Delete

Toggle

Copy

Save

Separator

4-3-2 LAN2

On cherche maintenant a bloquer le trafic depuis LAN2 vers LAN1, on met donc en place une règle sur le même principe que pour le LAN1 :

Recette 6

Floating WAN LAN1 LAN2 DMZ

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	2/59 KiB	IPv4 TCP/UDP	*	*	WAN net	53 (DNS)	*	none			
<input type="checkbox"/>	0/780 B	IPv4 *	LAN2 net	*	LAN1 net	*	*	none			
<input checked="" type="checkbox"/>	4.457K/486.80 MiB	IPv4 *	LAN2 net	*	*	*	*	none			

4-3-3 DMZ

A présent on cherche a bloquer le trafic entre la DMZ et LAN1 et LAN2

Floating WAN LAN1 LAN2 **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	*	WAN net	53 (DNS)	*	none			
<input type="checkbox"/>	✗	0/0 B	IPv4 *	*	DMZ net	*	*	none			
<input type="checkbox"/>	✗	0/0 B	IPv4 *	*	DMZ net	*	*	none			
<input type="checkbox"/>	✓	0/0 B	IPv4 *	*	*	*	*	none			

↑ Add

↓ Add

🗑 Delete

🔄 Toggle

📄 Copy

💾 Save

+ Separator

Recette 7

4-3-3 WAN

On cherche maintenant a bloquer le trafic entre WAN et LAN1 et LAN2

Recette 8

Floating **WAN** LAN1 LAN2 DMZ

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗	0/3 KiB	*	*	Reserved Not assigned by IANA	*	*	*		Block bogon networks	
<input type="checkbox"/>	✓	0/0 B	IPv4	*	WAN net	*	*	none			

↑ Add

↓ Add

🗑 Delete

🔄 Toggle

📄 Copy

💾 Save

+ Separator

5- Site sur la DMZ

Après avoir installé apache2 sur mon linux présent sur ma DMZ je tente une connexion au site via le LAN1 et le LAN 2 :

Web Configurator x 192.168.255.254 x Cours : Enseignement x livrables-phase1.pdf x cahier-des-charges-p x Web Configurator x Apache2 Debian Def x

← → ↻ Non sécurisé | 10.1.1.10

YouTube YouTube Music Moodle BTS SIO LM... Gmail github Mooc Mooc Technicien In... Certification CISCO Connexion Lycée C... LYCEE MERLEAU-P... Titre : La cybers



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the