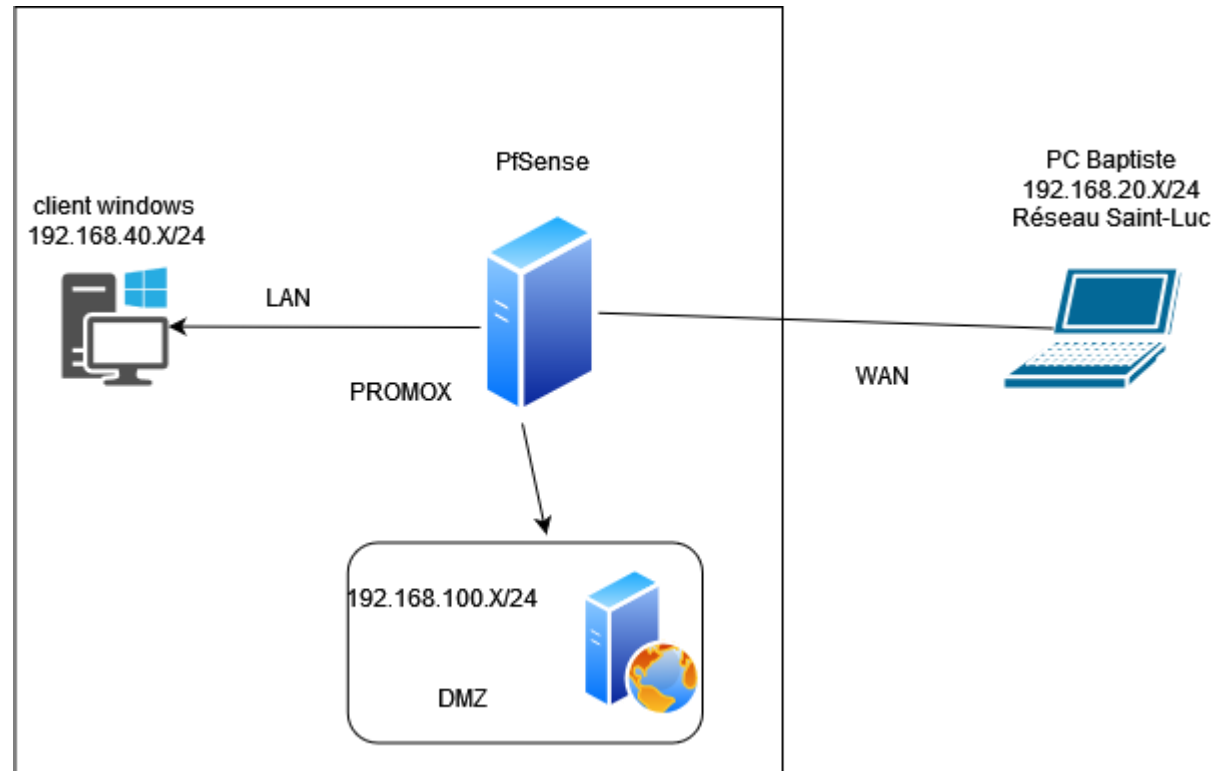




TP – B2

Topologie



Mise en place de PfSense

Création de nos 2 cartes réseaux virtuelles dans Proxmox

- Notre DMZ sera en 192.168.100.1/24
- Notre LAN sera en 192.168.40.1/24

Puis sur notre client Windows qui sera dans notre LAN, nous ajoutons la carte réseau de notre LAN.

vmbr7	Linux Bridge	Yes	Yes	No	192.168.100.1/24	DMZ Baptiste
vmbr8	Linux Bridge	Yes	Yes	No	192.168.40.1/24	Baptiste

Mise en place de PfSense

Dans PfSense, nous allons donc attribuer les cartes réseaux au WAN, LAN et DMZ

Puis nous allons changer l'IP de notre LAN car il est automatiquement en 192.168.1.1/24 alors que nous le voulons en 192.169.40.1/24

Puis notre DMZ sera en 192.168.100.1/24

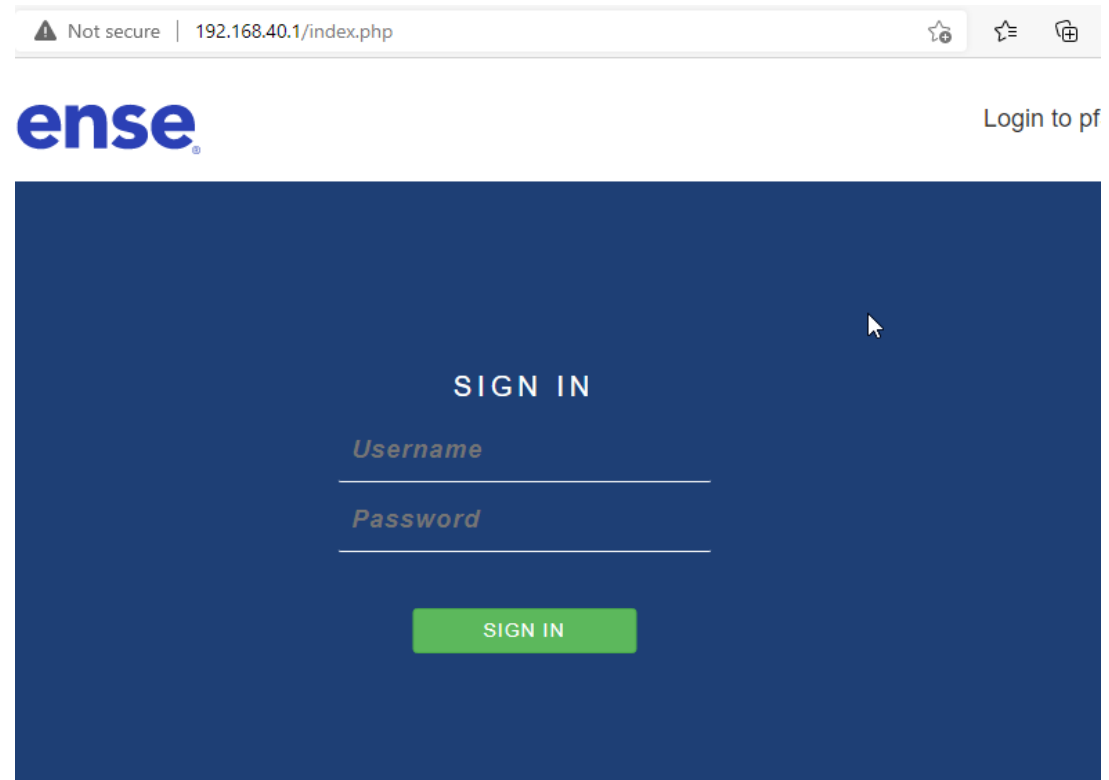
```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***  
  
WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.20.115/24  
LAN (lan)      -> vtnet1      -> v4: 192.168.40.1/24  
DMZ (opt1)     -> vtnet2      -> v4: 192.168.100.1/24
```

Configuration de PfSense

Ensuite sur notre client Windows dans notre LAN.

Nous allons fixer une IP en 192.168.40.X/24 afin qu'il soit sur le même réseau que notre PfSense et pouvoir le configurer via l'interface web.

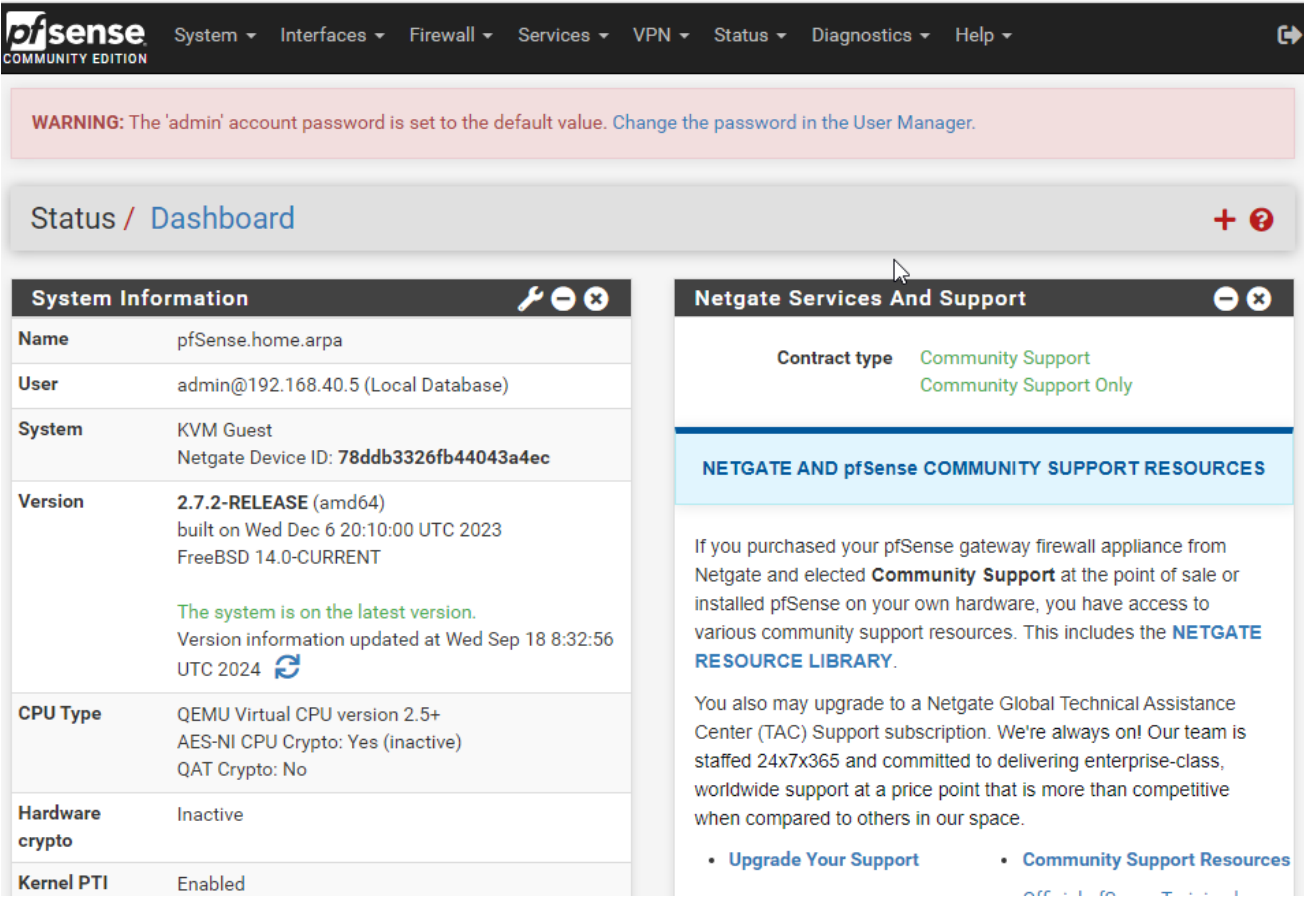
Les Login/mdp sont :
admin / pfsense

A screenshot of a web browser displaying the PfSense login page. The browser's address bar shows '192.168.40.1/index.php' with a 'Not secure' warning. The page features the 'ense' logo in the top left and a 'Login to pf' link in the top right. The main content area has a dark blue background with the text 'SIGN IN' in white. Below this, there are two input fields labeled 'Username' and 'Password' in a light blue font. At the bottom of the form is a green button with the text 'SIGN IN' in white.

Notre interface PfSense est la suivante :

Nous allons modifier les information système du PfSense.

Configuration de PfSense



On se rend dans le General setup afin de modifier les informations suivantes pour notre PfSense

Avec l'ajout du DNS 8.8.8.8 afin d'avoir du réseau et de pouvoir sortir sur le WAN

Configuration du PfSense

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname

pfSense

Name of the firewall host, without domain part.

Examples: pfsense, firewall, edgefw

Domain

pfsense.baptiste

Primary DNS Server

8.8.8.8

Secondary DNS Server

1.1.1.1

Override DNS

☒

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

>> Next

Ajout de la DMZ

Dans notre interfaces web, dans l'onglet interface, nous allons configurer notre DMZ.

Puis on lui ajoute une IP fixe en /24.

Pour finir, nous sauvegardons les changements et cliquons sur **Apply changes**.

Nous voyons donc nos 3 interfaces configurées.

Interfaces / OPT1 (vtnet2)

General Configuration

Enable ☐ Enable interface

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

IPv4 Configuration Type

IPv6 Configuration Type

Interfaces

 WAN	↑	10Gbase-T <full-duplex>	192.168.20.115
 LAN	↑	10Gbase-T <full-duplex>	192.168.40.1
 DMZ	↑	10Gbase-T <full-duplex>	192.168.100.1

Configuration LAN

Ensuite nous allons, bloquer les flux du LAN vers la DMZ.

En revanche nous allons autoriser à voir notre page web depuis le LAN

Source

Source

☐ Invert match

LAN subnets

▼

Source Address

⚙ Display Advanced

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

Destination

Destination

☐ Invert match

Address or Alias

▼

192.168.100.2

Firewall / Rules / Edit

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 (TC returned to the sender, whereas with block the packet is dropped silently. In €

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

Any

▼

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

LAN subnets

▼

Destination

Destination

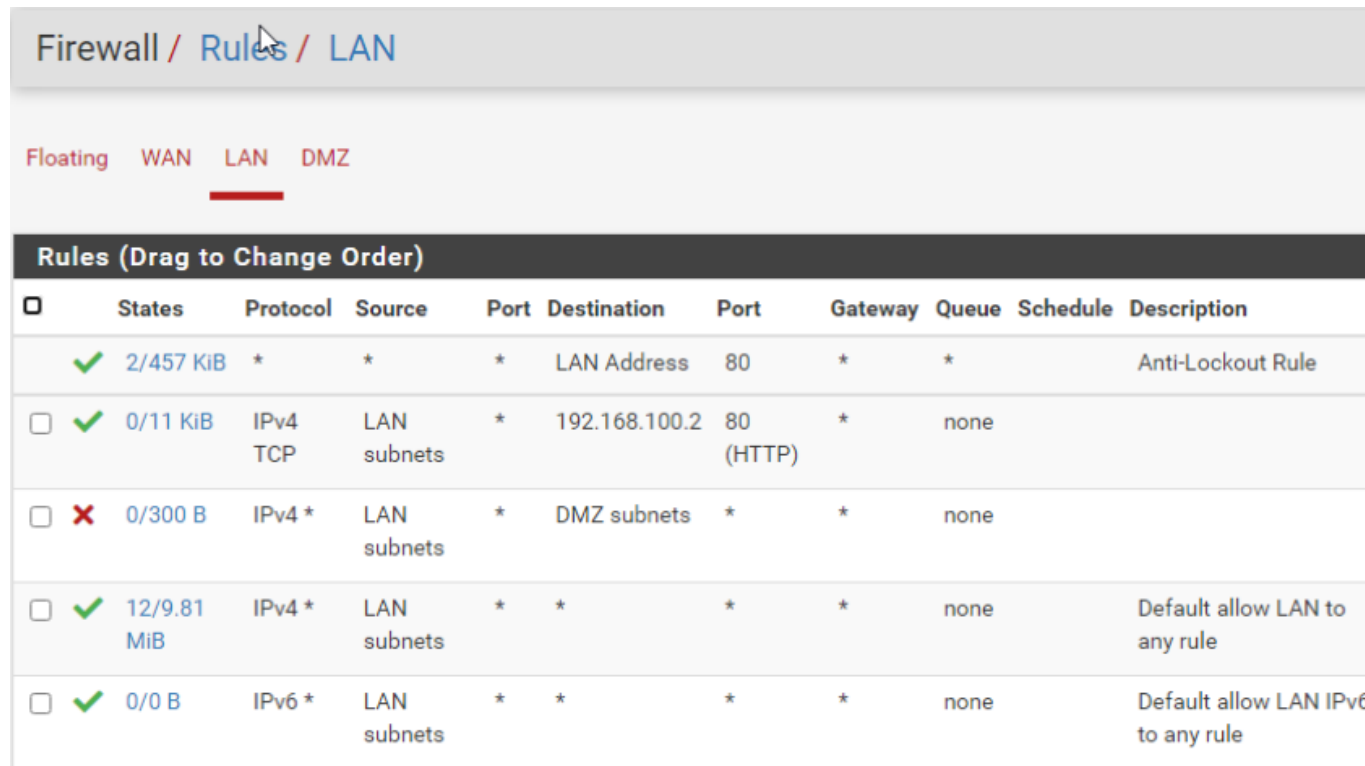
☐ Invert match

DMZ subnets

▼

Configuration LAN

Une fois la configuration finie, nous devons avoir les règles suivantes pour notre LAN.



The screenshot shows the Mikrotik WinBox interface for configuring Firewall Rules. The breadcrumb navigation at the top reads 'Firewall / Rules / LAN'. Below this, there are tabs for 'Floating', 'WAN', 'LAN', and 'DMZ', with 'LAN' being the active tab. The main section is titled 'Rules (Drag to Change Order)' and contains a table of five firewall rules. Each rule row includes a checkbox for enabling the rule, a status icon (green checkmark or red X), the current data usage, the protocol, source and destination addresses, ports, gateway, queue, schedule, and a description.

Rules (Drag to Change Order)										
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☒	✓ 2/457 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule
☐	✓ 0/11 KiB	IPv4 TCP	LAN subnets	*	192.168.100.2	80 (HTTP)	*	none		
☐	✗ 0/300 B	IPv4 *	LAN subnets	*	DMZ subnets	*	*	none		
☐	✓ 12/9.81 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule
☐	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule

Configuration DMZ

Dans notre interface Web de PfSense, nous allons configurer différentes règles.

Nous allons bloquer les flux de la DMZ vers le LAN

Source

Source

☐ Invert match

DMZ subnets

Destination

Destination

☐ Invert match

LAN subnets

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 every remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Bloque les flux vers le LAN

A description may be entered here for administrative reference. A maximum displayed in the firewall log.

Advanced Options

Display Advanced

Save

Configuration DMZ

Ensuite nous allons autoriser notre DMZ à sortir sur le WAN seulement en HTTP et HTTPS

On refait la même règle en changeant HTTP par HTTPS.

The screenshot shows a firewall rule configuration interface. At the top, the 'Source' field is set to 'DMZ subnets'. Below this, there is a 'Display Advanced' button and a note: 'The Source Port Range for a connection is typically random and almost always this setting must remain at its default value, any.' The 'Destination' section is highlighted with a dark header. The 'Destination' field is set to 'Any'. Below this, the 'Destination Port Range' is configured with 'From' set to 'HTTP (80)' and 'To' set to 'HTTP (80)'. A note below the port range fields states: 'Specify the destination port or port range for this rule. The "To" field must be greater than or equal to the "From" field.' The 'Extra Options' section is highlighted with a dark header. It contains a 'Log' checkbox which is unchecked, with a hint: 'Hint: the firewall has limited local log space. Don't turn on logging for remote syslog server (see the Status: System Logs: Settings page).' Below this is the 'Description' field, which contains the text 'Autoriser la sortie vers Internet depuis la DMZ'. At the bottom, there is an 'Advanced Options' section with a 'Display Advanced' button and a 'Save' button.

Source ☐ Invert match DMZ subnets

[Display Advanced](#)

The Source Port Range for a connection is typically random and almost always this setting must remain at its default value, any.

Destination

Destination ☐ Invert match Any

Destination Port Range From HTTP (80) Custom To HTTP (80)

Specify the destination port or port range for this rule. The "To" field must be greater than or equal to the "From" field.

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 remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

A description may be entered here for administrative reference. A maximum of 255 characters is displayed in the firewall log.

Advanced Options [Display Advanced](#)

[Save](#)

Configuration DMZ

Une fois fini nous devons avoir les règles suivantes :

Firewall / Rules / DMZ

Floating WAN LAN DMZ

Rules (Drag to Change Order)										
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☐	✓ 0/30 KIB	IPv4 TCP/UDP	DMZ subnets	*	*	53 (DNS)	*	none		
☐	✓ 0/0 B	IPv4 TCP	DMZ subnets	*	*	443 (HTTPS)	*	none		Autoriser la sortie vers Internet depuis la DMZ
☐	✓ 0/0 B	IPv4 TCP	DMZ subnets	*	*	80 (HTTP)	*	none		Autoriser la sortie vers Internet depuis la DMZ
☐	✗ 0/0 B	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none		Bloque les flux vers le LAN

Redirection de port

Redirection des ports afin que notre page web soit visible sur le réseau

Nous décochons la case suivante afin de voir notre page web.

Reserved Networks

Block private networks and loopback addresses

☐

Blocks traffic from IP addresses that are reserved for unique local addresses per RFC 4193 (fc00::/7) as well as turned on, unless this network interface resides in the

Interface

WAN

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

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

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

Source

Display Advanced

Destination

☐ Invert match.

WAN address

Type

Address/mask

Destination port range

HTTP

From port

Custom

HTTP

To port

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

Address or Alias

192.168.100.2

Type

Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port

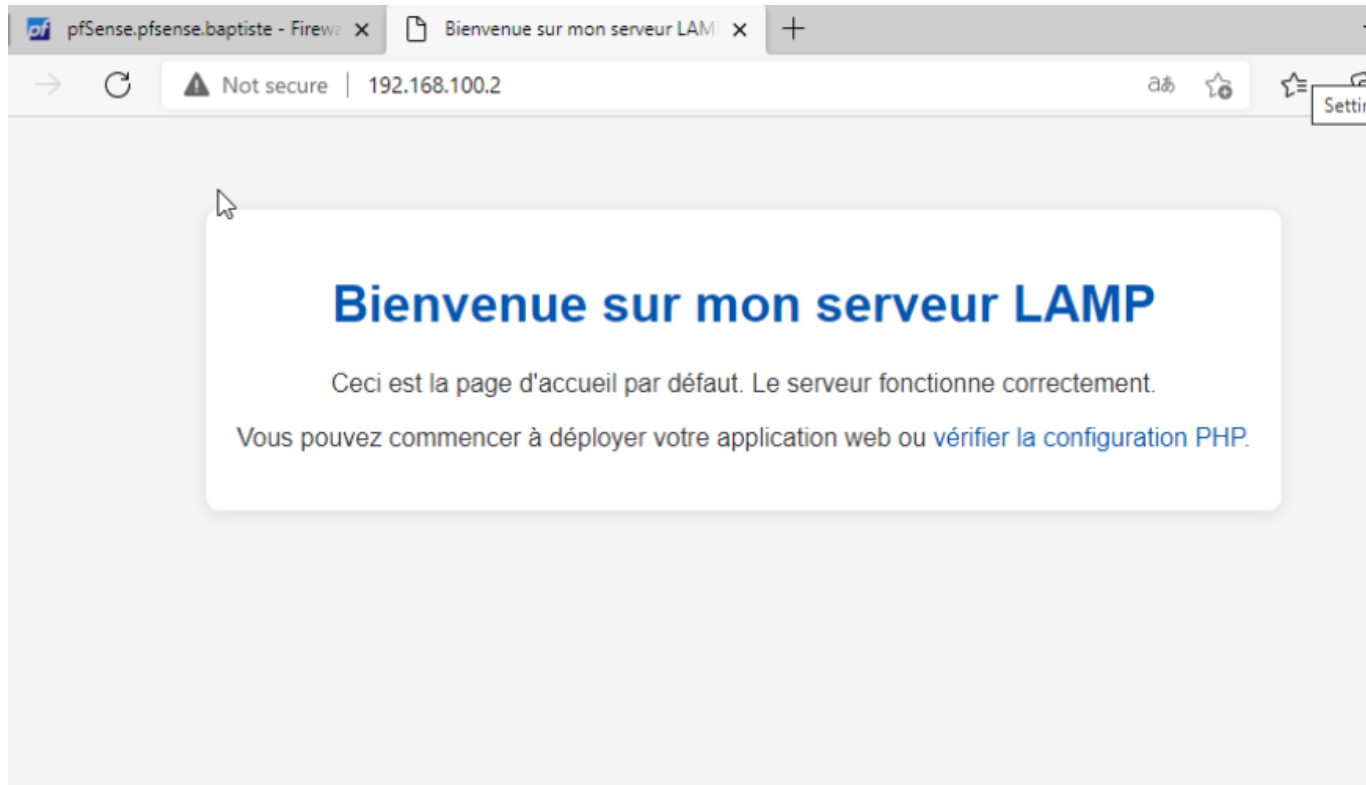
HTTP

Port

Custom

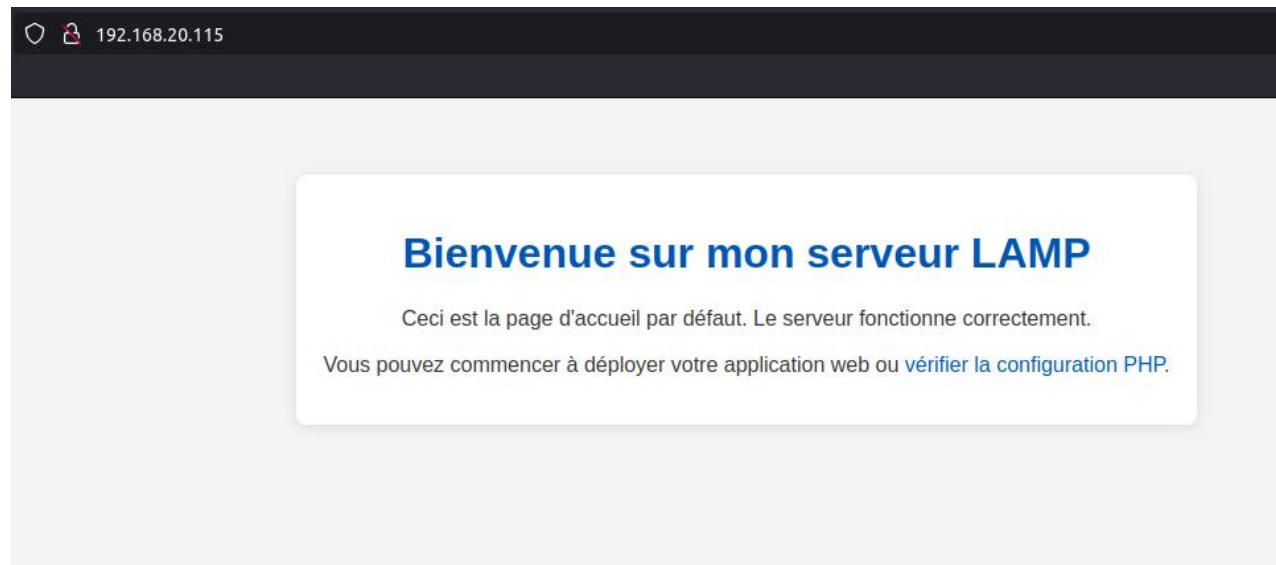
Vérification sur le LAN

On tape l'IP de notre page web afin de savoir si notre configuration est correcte :



Vérification sur le WAN

Sur ma machine reliée au réseau je tape dans la barre de recherche l'IP de mon PfSense en 20.115



Sources

<https://www.it-connect.fr/tuto-vmware-workstation-lab-virtuel-pfsense/>

<https://youtu.be/Vmd9Amz524U?si=0kHpjya86zzop1-3>