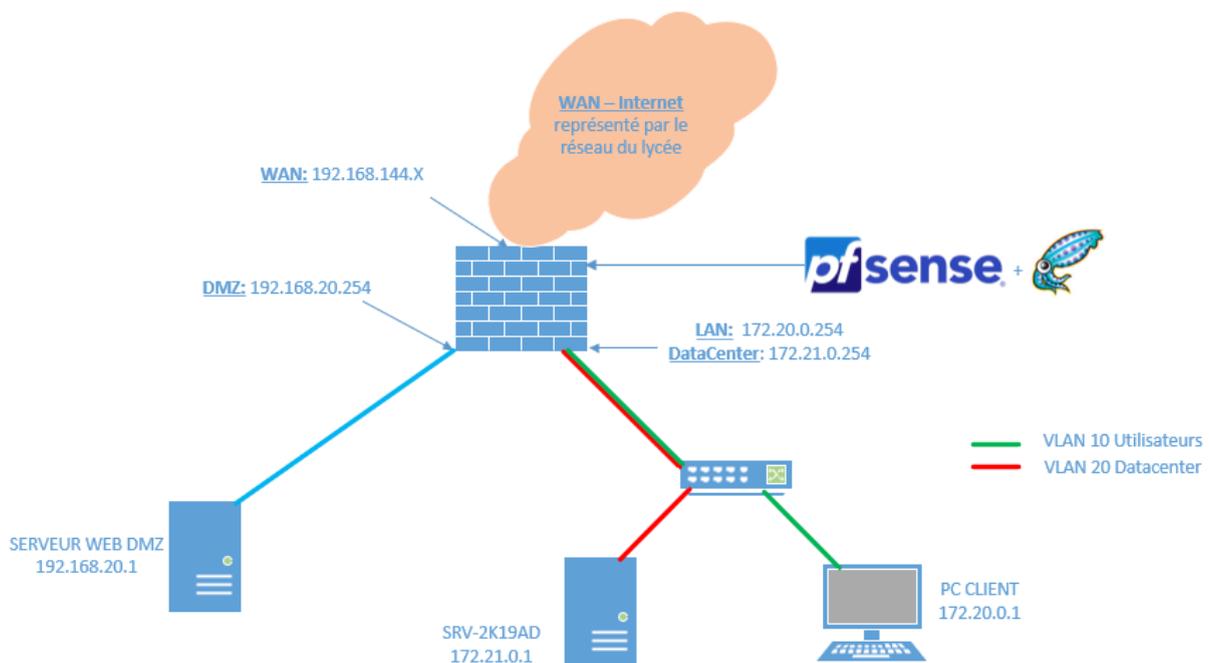


TP PfSense



## I- Contexte

- Segmentation de votre réseau : Actuellement les serveurs du datacenter sont sur le même plan IP et ils sont également tous sur le VLAN par défaut (VLAN1). Il convient donc de segmenter ce réseau en 2 plans IP et 2 vlans différents (VLAN 10 – Utilisateurs et VLAN 20 – Datacenter)
- Mise en place d'un pare-feu Pfsense avec proxy transparent Squid : Pour filtrer votre connexion internet, vous devez mettre en place un pare-feu Pfsense en lieu et place de votre box internet. Ce pare-feu servira à réaliser le routage inter-vlan et à mettre en place une DMZ pour la publication du site internet de la mairie.
- Publication du site internet de la mairie : Dans votre DMZ, mettez en place un serveur Web (Debian avec Apache), pour simuler le site web de la mairie de Bidart utilisez les pages web de votre portfolio. Publiez ensuite le site Web sur Internet » en réalisant une règle de NAT sur le Pfsense. Pour valider le bon fonctionnement, accéder au site en utilisant l'IP Wan du pfsense depuis un PC du réseau de la salle (réseau de la salle = internet dans le cadre de la maquette).



## II- Installation PfSense sur Virtual Box

## Configuration de la VM PfSense sur virtual box :

- Ajouter un disque
- 2go de RAM est suffisant
- Ajout des 3 interfaces réseaux :

Pour le WAN (accès par pont et tout autoriser dans Mode Promiscuité)

The screenshot shows the configuration for Interface 1. The 'Activer l'interface réseau' checkbox is checked. The 'Mode d'accès réseau' is set to 'Accès par pont'. The 'Nom' is 'Realtek PCIe GbE Family Controller'. Under the 'Avancé' section, the 'Type d'interface' is 'Intel PRO/1000 MT Desktop (82540EM)', the 'Mode Promiscuité' is 'Tout autoriser', and the 'Adresse MAC' is '080027B0148F'. The 'Câble branché' checkbox is checked, and there is a 'Redirection de ports' button.

Pour le LAN (réseau interne et tout autoriser dans Mode Promiscuité)

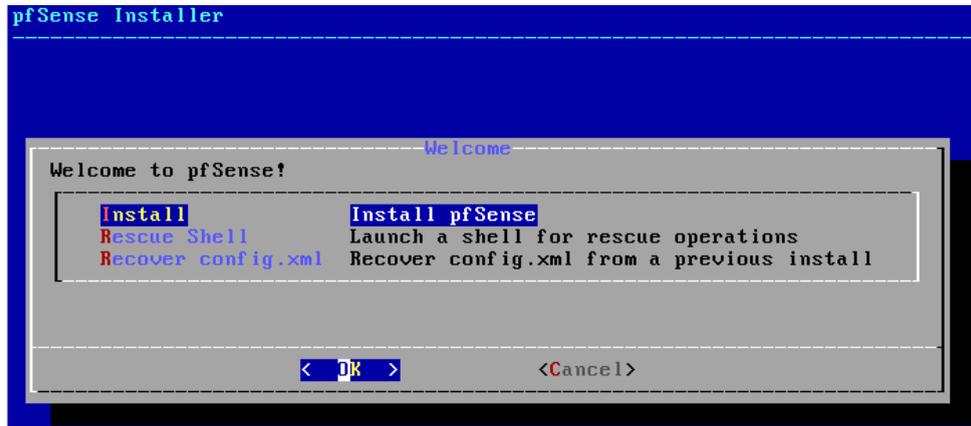
The screenshot shows the configuration for Interface 2. The 'Activer l'interface réseau' checkbox is checked. The 'Mode d'accès réseau' is set to 'Réseau interne'. The 'Nom' is 'intnet'. Under the 'Avancé' section, the 'Type d'interface' is 'Intel PRO/1000 MT Desktop (82540EM)', the 'Mode Promiscuité' is 'Tout autoriser', and the 'Adresse MAC' is '080027ECD1DB'. The 'Câble branché' checkbox is checked, and there is a 'Redirection de ports' button.

Pour la DMZ (réseau interne et tout autoriser dans Mode Promiscuité)

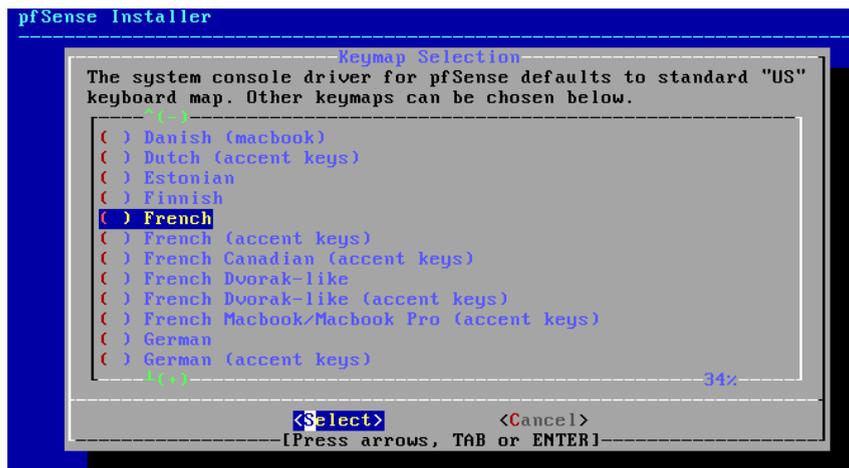
The screenshot shows the configuration for Interface 3. The 'Activer l'interface réseau' checkbox is checked. The 'Mode d'accès réseau' is set to 'Réseau interne'. The 'Nom' is 'intnet'. Under the 'Avancé' section, the 'Type d'interface' is 'Intel PRO/1000 MT Desktop (82540EM)', the 'Mode Promiscuité' is 'Tout autoriser', and the 'Adresse MAC' is '080027ECD1DB'. The 'Câble branché' checkbox is checked, and there is a 'Redirection de ports' button.

## Démarrage sur l'ISO de PfSense :

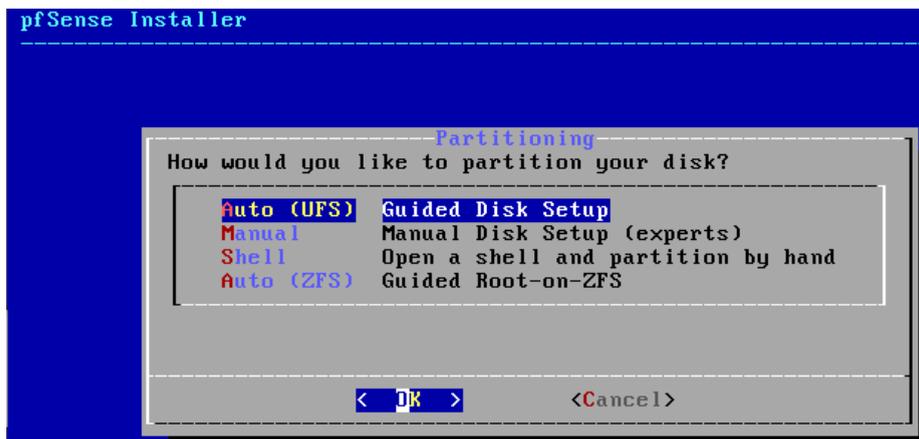
Appuyez sur Entrée :



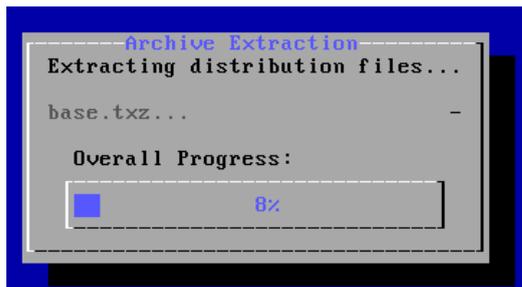
Choix de la langue :



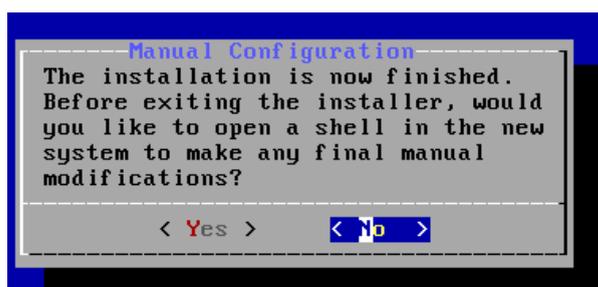
Auto (UFS) :



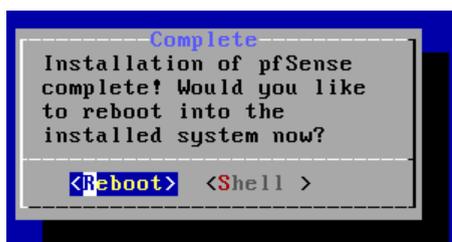
Installation :



No :



Redémarrage du système :



Après redémarrage :

```

pfSense 2.7.2-RELEASE amd64 20231206-2018
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
KVM Guest - Netgate Device ID: 8acff7a0506c5d4ecbca
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)    -> em0      -> v4/DHCP4: 192.168.1.213/24
              v6/DHCP6: 2a02:8420:3918:f701:a00:27ff:fed4:d5
13/64
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:

```

il faut assigner toute les interfaces :

```

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: 1

Valid interfaces are:

em0      08:00:27:d4:d5:13 (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      08:00:27:fa:0f:53 (up) Intel(R) Legacy PRO/1000 MT 82540EM
em2      08:00:27:1d:cd:91 (down) Intel(R) Legacy PRO/1000 MT 82540EM

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

```

OPT1 correspond à la dmz de la passerelle nous allons le renommer plus tard :

```
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 a or nothing if finished): em1

Optional interface 1 description found: OPT1
Enter the Optional 1 interface name or 'a' for auto-detection
(em2 a or nothing if finished): em2
```

après avoir assigner toute les interfaces la 3ème interfaces réseaux qu'on a activer sur virtual box apparaît sur la config du pfsense :

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.213/24
LAN (lan)     -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)   -> em2      ->
```

maintenant il faut mettre les passerelles correspondant pour le lan ainsi que la dmz pour que cela correspondent au schéma réseaux qui nous à été confié :

```
OPT1 -> em2

Do you want to proceed [y|n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
KVM Guest - Netgate Device ID: 8acff7a8586c5d4ecbca

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.213/24
LAN (lan)     -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)   -> em2      ->

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: 2
```

suite à sa ils nous proposes ce que on veut configurer dans notre cas ça seras le lan et la DMZ :

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)

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

quand je choisie de configurer le lan on me propose de mettre en place un dhcp donc on mets n :

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n █
```

```
Enter the number of the interface you wish to configure: 2

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.22.0.254

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 LAN IPv4 subnet bit count (1 to 32):
> 24 █
```

```
The IPv4 LAN address has been set to 172.22.0.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
```

```
https://172.22.0.254/
```

```
Press <ENTER> to continue. █
```

une fois que c'est fait il faut appuyer sur entrer est constaté le changement pour le lan il faut le faire pour la dmz :

```
OPT1 (opt1)      -> em2      ->

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: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 3

Configure IPv4 address OPT1 interface via DHCP? (y/n) n
```

On met l'adresse de la passerelle correspondant :

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 3

Configure IPv4 address OPT1 interface via DHCP? (y/n) n

Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 192.168.20.254

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 OPT1 IPv4 subnet bit count (1 to 32):
> 24
```

```
LAN (lan)      -> em1      -> v4: 172.22.0.254/24
DMZ (opt1)     -> em2      -> v4: 192.168.20.254/24
WAN (em0)      -> em0      -> v4: 172.22.0.254/24
```

### III Mise en place d'un serveur Web

- Installation serveur web :

Mise à jour du système : apt update && apt upgrade

```
root@SRV-DEBIAN-01:~# apt-get update_
```

```
root@SRV-DEBIAN-01:~# apt upgrade
```

Installation Apache 2 : apt install apache2

```
root@SRV-DEBIAN-01:~# apt install apache2
```

Mettre l'ip sur le serveur web dmz :

```
root@SRV-DEBIAN-01:~# cd /etc/network
root@SRV-DEBIAN-01:/etc/network# _
```

pour aller sur l'interface de configuration de l'adresse ip :

```
root@SRV-DEBIAN-01:/etc/network# nano interfaces_
```

```
GNU nano 5.4                               interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.20.1
netmask 255.255.255.0
gateway 192.168.20.254

^G Aide          ^O Écrire      ^W Chercher    ^K Couper      ^T Exécuter    ^C Emplacement  M-U Annuler
^X Quitter      ^R Lire fich. ^_ Remplacer   ^U Coller     ^J Justifier   ^_ Aller ligne M-E Refaire
```

**Il faut enregistrer puis redémarrer le service :**

```
root@SRV-DEBIAN-01:/etc/network# systemctl restart networking.service
```

puis quand cela est fait activer l'interface réseau :

```
root@SRV-DEBIAN-01:/etc/network# ifup enp0s3
root@SRV-DEBIAN-01:/etc/network# _
```

Pour voir si le changement d'adresse ip à été effectué :

```
root@SRV-DEBIAN-01:/var/www/html# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:e2:d0:77 brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.1/24 brd 192.168.20.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 2a02:8428:3918:f701:a00:27ff:fee2:d077/64 scope global dynamic mngtmpaddr
        valid_lft 178sec preferred_lft 178sec
    inet6 fe80::a00:27ff:fee2:d077/64 scope link
        valid_lft forever preferred_lft forever
root@SRV-DEBIAN-01:/var/www/html# _
```

- aller dans la config de la page web :

```
root@SRV-DEBIAN-01:/var/www/html# cd /var/www/html_
```

```
root@SRV-DEBIAN-01:/var/www/html# nano index.html
```

on mets dans <title> </title> "test de la page web" puis control x et sauvegarder :

```
GNU nano 5.4 index.html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <title>test de la page web</title>
  <style type="text/css" media="screen">
* {
  margin: 0px 0px 0px 0px;
  padding: 0px 0px 0px 0px;
}

body, html {
  padding: 3px 3px 3px 3px;

  background-color: #D8DBE2;

  font-family: Verdana, sans-serif;
  font-size: 11pt;
  text-align: center;
}

div.main_page {
  position: relative;
  display: table;

  width: 800px;

  margin-bottom: 3px;
  margin-left: auto;
  margin-right: auto;
  padding: 0px 0px 0px 0px;
}
[ Lecture de 368 lignes ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C EmplacementM-U Annuler
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^_ Aller ligneM-E Refaire
```

### III- Configuration des vlans sur le switch

avant de commencer il faut mettre le switch sous la même plage d'adresses ip que le pc windows 10 client qui est en pour le rappeler 172.20.0.1 donc on vas mettre pour le switch 172.20.0.253

The screenshot displays the Netgear GS108T web management interface. The browser address bar shows the URL 192.168.1.250/base/web\_main.html. The interface includes a navigation menu with tabs for System, Switching, QoS, Security, Monitoring, Maintenance, and Help. The left sidebar lists various configuration options, with IP Configuration selected. The main content area shows the IP Configuration section, where the Static IP Address option is selected. The IP Address field is set to 172.20.0.253, the Subnet Mask is 255.255.255.0, and the Default Gateway is 0.0.0.0. Below this, the Management VLAN section shows the Management VLAN ID set to 1. The interface also includes a LOGOUT button and CANCEL/APPLY buttons at the bottom.

NETGEAR  
Connect with Innovation™

GS108T  
8 Port Gigabit Smart Switch

System Switching QoS Security Monitoring Maintenance Help

Management Device View SNMP LLDP Services

System Information  
IP Configuration  
IPv6 Network Configuration  
IPv6 Network Neighbor  
Time  
Denial of Service  
DNS  
Green Ethernet

### IP Configuration

Dynamic IP Address (DHCP)  
Dynamic IP Address (BOOTP)  
Static IP Address

IP Address: 172.20.0.253  
Subnet Mask: 255.255.255.0  
Default Gateway: 0.0.0.0

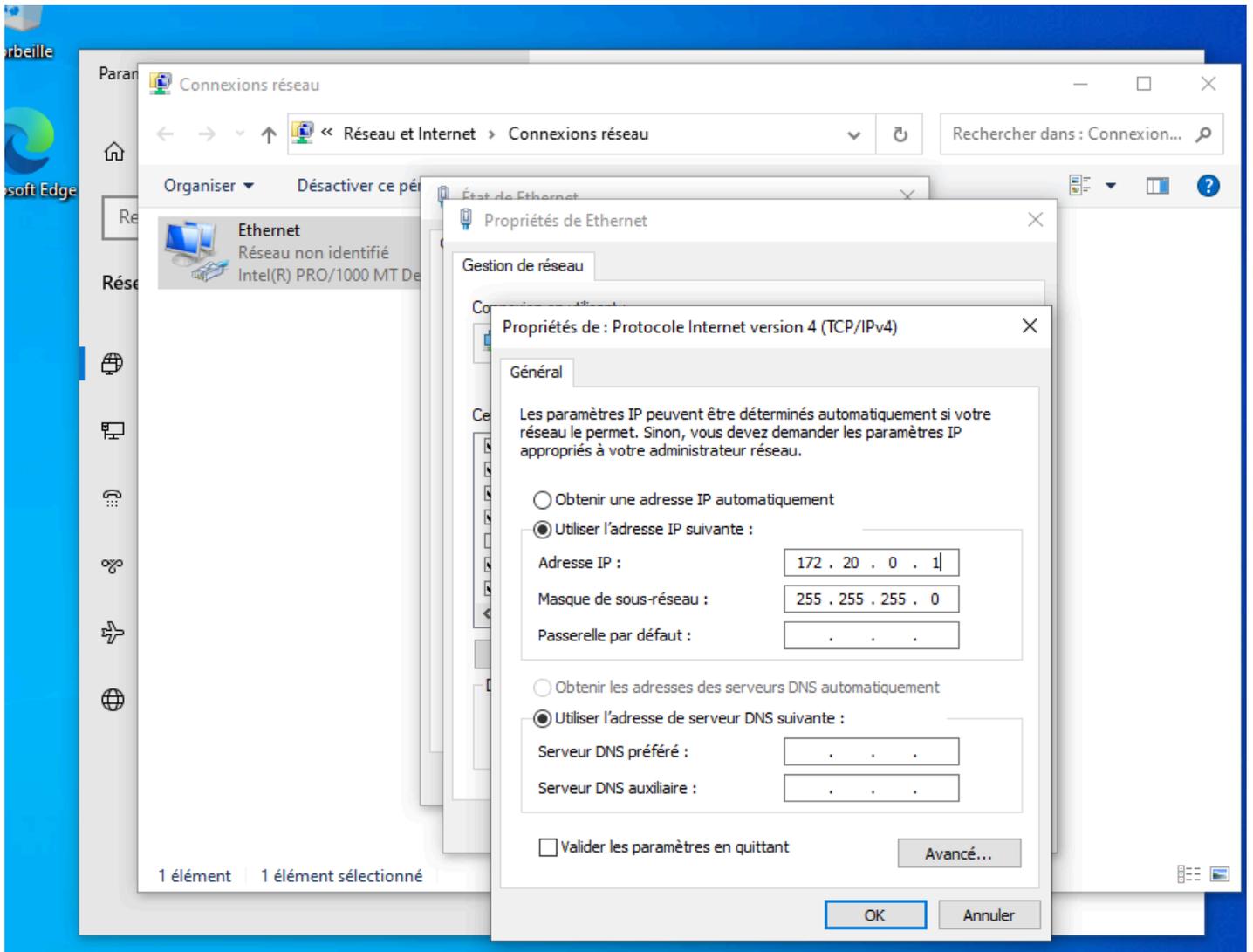
### Management VLAN

Management VLAN ID: 1 (1-4093)

CANCEL APPLY

Copyright © 1996-2018 NETGEAR

il faut changer d'habitude l'adresse ip du windows client car comme on a changé d'adresse ip sur le switch on va perdre la connexion donc on met l'adresse ip du win10 client correspondant au schéma réseau :



pour créer des vlans il faut se rendre dans "Switching", "vlan" et la on constate qu'il y a des vlans prédéfinis mais nous on veut mettre 2 autre vlan qui sont pour le vlan 10 qui est le vlan des utilisateurs et le vlan 20 qui sera celui du datacenter :

donc il faudra entrer l'id du vlan qui correspond au numéro d'identification ainsi que le vlan name qui correspond au nom du vlan pour le retrouver plus facilement dès qu'on aura tout mis il faudra cliquer sur add pour que ça le prenne en compte :

The screenshot shows the Netgear web interface for VLAN Configuration. The browser address bar shows "172.20.0.253/base/web\_main.html". The navigation menu includes System, Switching (selected), QoS, Security, Monitoring, Maintenance, and Help. The sub-menu includes Ports, LAG, VLAN (selected), Voice VLAN, Auto-VoIP, STP, Multicast, and Address Table. The left sidebar shows a tree view with Basic > VLAN Configuration and Advanced. The main content area is titled "VLAN Configuration" and contains a table with the following data:

	VLAN ID	VLAN Name	VLAN Type
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Static ▼
<input type="checkbox"/>	1	Default	Default
<input type="checkbox"/>	2	Voice VLAN	Default
<input type="checkbox"/>	3	Auto-Video	Default

Below the table is a "Reset" section with a "Reset Configuration" button.

The screenshot shows the Netgear web interface for VLAN Configuration. The browser address bar shows "8 Port Gigabit S". The navigation menu is the same as in the previous screenshot. The left sidebar shows a tree view with Basic > Advanced > VLAN Configuration > VLAN Membership > Port PVID Configuration. The main content area is titled "VLAN Configuration" and contains a table with the following data:

	VLAN ID	VLAN Name	VLAN Type
<input type="checkbox"/>	10	Utilisateurs	Static ▼
<input type="checkbox"/>	1	Default	Default
<input type="checkbox"/>	2	Voice VLAN	Default
<input type="checkbox"/>	3	Auto-Video	Default

Below the table is a "Reset" section with a "Reset Configuration" button.

**NETGEAR**  
Connect with Innovation™

GS  
8 Port Gigabit Sm

System | **Switching** | QoS | Security | Monitoring | Maintenance | Help

Ports | LAG | **VLAN** | Voice VLAN | Auto-VoIP | STP | Multicast | Address Table

Basic  
» VLAN  
Configuration  
» Advanced

### VLAN Configuration

:: VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type
<input checked="" type="checkbox"/>	20	Datcenter	Static
<input type="checkbox"/>	1	Default	Default
<input type="checkbox"/>	2	Voice VLAN	Default
<input type="checkbox"/>	3	Auto-Video	Default
<input type="checkbox"/>	10	Utilisateurs	Static

:: Reset

Reset Configuration

ADD DELETED CANCEL

Une fois que les vlans sont configurer il faut maintenant configurer les ports tagged ou non tagged qui sert à :

Trame Tagged et trame Untagged

Lorsque celui communiquera avec le Switch, il ajoutera un identifiant dans la trame et le Switch pourra alors reconnaître l'appartenance à son VLAN et rediriger correctement le trafic. Si l'identifiant n'est pas reconnu, le trafic est supprimé.

Pour commencer la configurer des ports il faut aller dans VLAN Membership et les vlans seront configurer de la manière suivantes :

The screenshot shows the Netgear GS108T web interface. The top navigation bar includes 'System', 'Switching', 'QoS', 'Security', 'Monitoring', 'Maintenance', and 'Help'. The 'Switching' menu is expanded to show 'Ports', 'LAG', 'VLAN', 'Voice VLAN', 'Auto-VoIP', 'STP', 'Multicast', and 'Address Table'. The 'VLAN' menu is further expanded to show 'Basic', 'Advanced', 'VLAN', 'VLAN Membership', and 'Port PVID'. The 'VLAN Membership' configuration page is displayed, showing the following settings:

- VLAN ID: 1
- Group Operation: Untag All
- VLAN Name: Default
- VLAN Type: Default

Below the settings, there are two sections: 'PORT' and 'LAG'. The 'PORT' section shows a table of ports 1 through 8 with their membership status:

Port	1	2	3	4	5	6	7	8
Membership	U	U	U	U	T	U	U	U

The 'LAG' section is currently empty. At the bottom of the page, there are 'CANCEL' and 'APPLY' buttons.

The screenshot shows the Netgear GS108T web interface. The top navigation bar includes 'System', 'Switching', 'QoS', 'Security', 'Monitoring', 'Maintenance', and 'Help'. The 'Switching' menu is expanded to show 'Ports', 'LAG', 'VLAN', 'Voice VLAN', 'Auto-VoIP', 'STP', 'Multicast', and 'Address Table'. The 'VLAN' menu is further expanded to show 'Basic', 'Advanced', 'VLAN', 'VLAN Membership', and 'Port PVID'. The 'VLAN Membership' configuration page is displayed, showing the following settings:

- VLAN ID: 10
- Group Operation: Untag All
- VLAN Name: Utilisateurs
- VLAN Type: Static

Below the settings, there are two sections: 'PORT' and 'LAG'. The 'PORT' section shows a table of ports 1 through 8 with their membership status:

Port	1	2	3	4	5	6	7	8
Membership		U			T			

The 'LAG' section is currently empty. At the bottom of the page, there are 'CANCEL' and 'APPLY' buttons.

Non sécurisé | 172.20.0.253/base/web\_main.html

**NETGEAR** Connect with Innovation™ **GS108T** 8 Port Gigabit Smart Switch

System **Switching** QoS Security Monitoring Maintenance Help LOGOUT

Ports LAG **VLAN** Voice VLAN Auto-VoIP STP Multicast Address Table

> Basic  
 > Advanced  
   > VLAN  
     Configuration  
   > VLAN Membership  
     > Port PVID  
       Configuration

### VLAN Membership

:: VLAN Membership

VLAN ID: 20 Group Operation: Untag All

VLAN Name: Datacenter UNTAGGED PORT MEMBERS

VLAN Type: Static TAGGED PORT MEMBERS

PORT

Port	1	2	3	4	5	6	7	8
			U		T			

LAG

CANCEL APPLY

puis il faut confirmer les attributions au vlans pour sa il faut aller dans Port PVID Configuration sélectionner le port qu'on veut et renseigner le numéro du port du vlan puis apply :

Menu des actions de l'onglet Non sécurisé | 172.20.0.253/base/web\_main.html

**NETGEAR** Connect with Innovation™ **GS108T** 8 Port Gigabit Smart Switch

System **Switching** QoS Security Monitoring Maintenance Help LOGOUT

Ports LAG **VLAN** Voice VLAN Auto-VoIP STP Multicast Address Table

> Basic  
 > Advanced  
   > VLAN  
     Configuration  
   > VLAN Membership  
     > Port PVID  
       Configuration

### Port PVID Configuration

:: PVID Configuration

PORTS LAGS All GO TO INTERFACE  GO

	Interface	PVID Configured (1 to 4093)	Current PVID	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
<input type="checkbox"/>	g2	10	10	Admit All	Disable	0
<input type="checkbox"/>	g1	1	1	Admit All	Disable	0
<input checked="" type="checkbox"/>	g2	10	10	Admit All	Disable	0
<input type="checkbox"/>	g3	20	20	Admit All	Disable	0
<input type="checkbox"/>	g4	1	1	Admit All	Disable	0
<input type="checkbox"/>	g5	1	1	Admit All	Disable	0
<input type="checkbox"/>	g6	1	1	Admit All	Disable	0
<input type="checkbox"/>	g7	1	1	Admit All	Disable	0

LOGOUT

System | **Switching** | QoS | Security | Monitoring | Maintenance | Help

Ports | LAG | **VLAN** | Voice VLAN | Auto-VoIP | STP | Multicast | Address Table

- Basic
- Advanced
  - VLAN
    - Configuration
    - VLAN Membership
    - Port PVID Configuration**

### Port PVID Configuration

**Port PVID Configuration**

PORTS LAGS All GO TO INTERFACE  GO

	Interface	PVID Configured (1 to 4093)	Current PVID	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
<input type="checkbox"/>	g3	20	20	Admit All	Disable	0
<input type="checkbox"/>	g1	1	1	Admit All	Disable	0
<input type="checkbox"/>	g2	10	10	Admit All	Disable	0
<input checked="" type="checkbox"/>	g3	20	20	Admit All	Disable	0
<input type="checkbox"/>	g4	1	1	Admit All	Disable	0
<input type="checkbox"/>	g5	1	1	Admit All	Disable	0
<input type="checkbox"/>	g6	1	1	Admit All	Disable	0
<input type="checkbox"/>	g7	1	1	Admit All	Disable	0
<input type="checkbox"/>	g8	1	1	Admit All	Disable	0

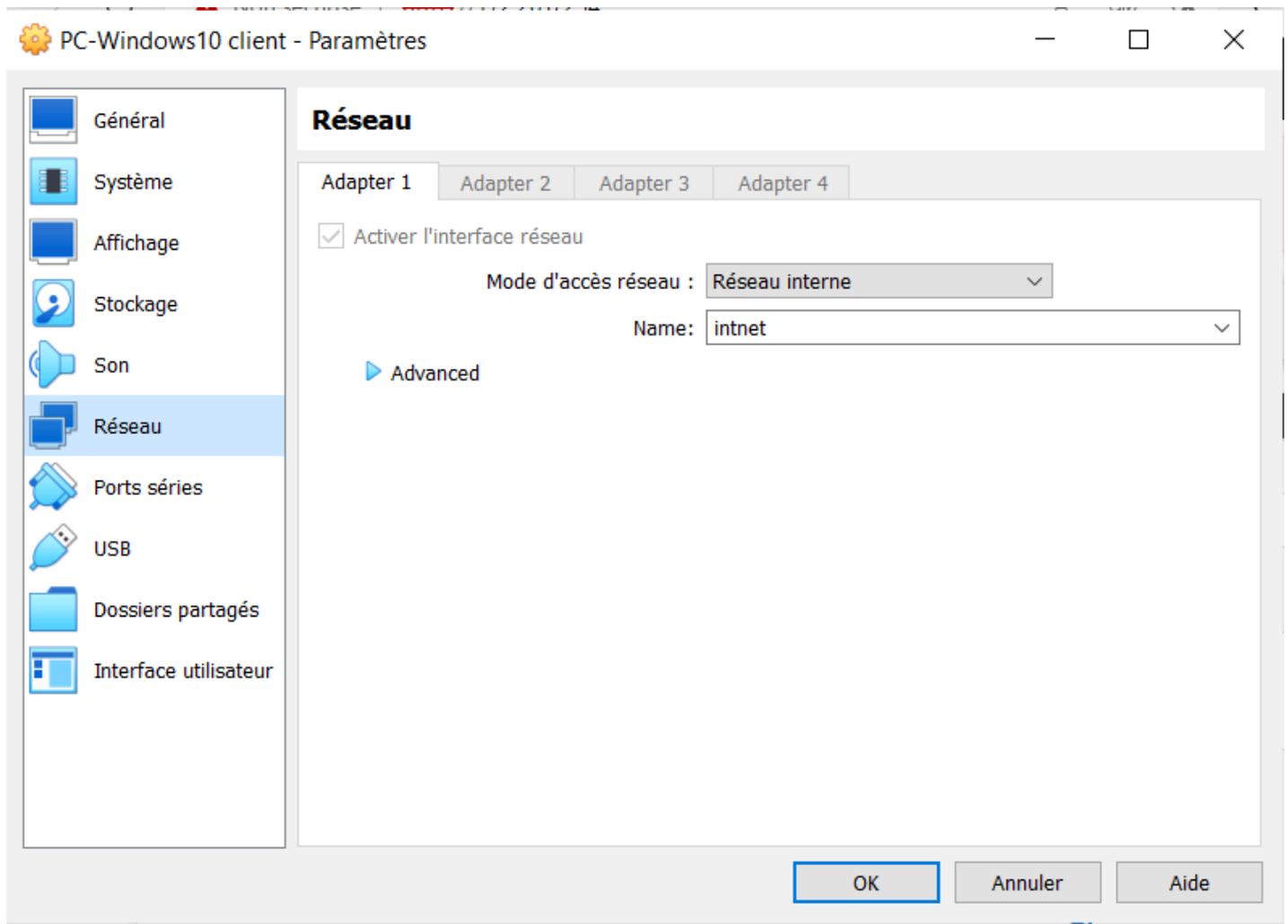
PORTS LAGS All GO TO INTERFACE  GO

CANCEL APPLY

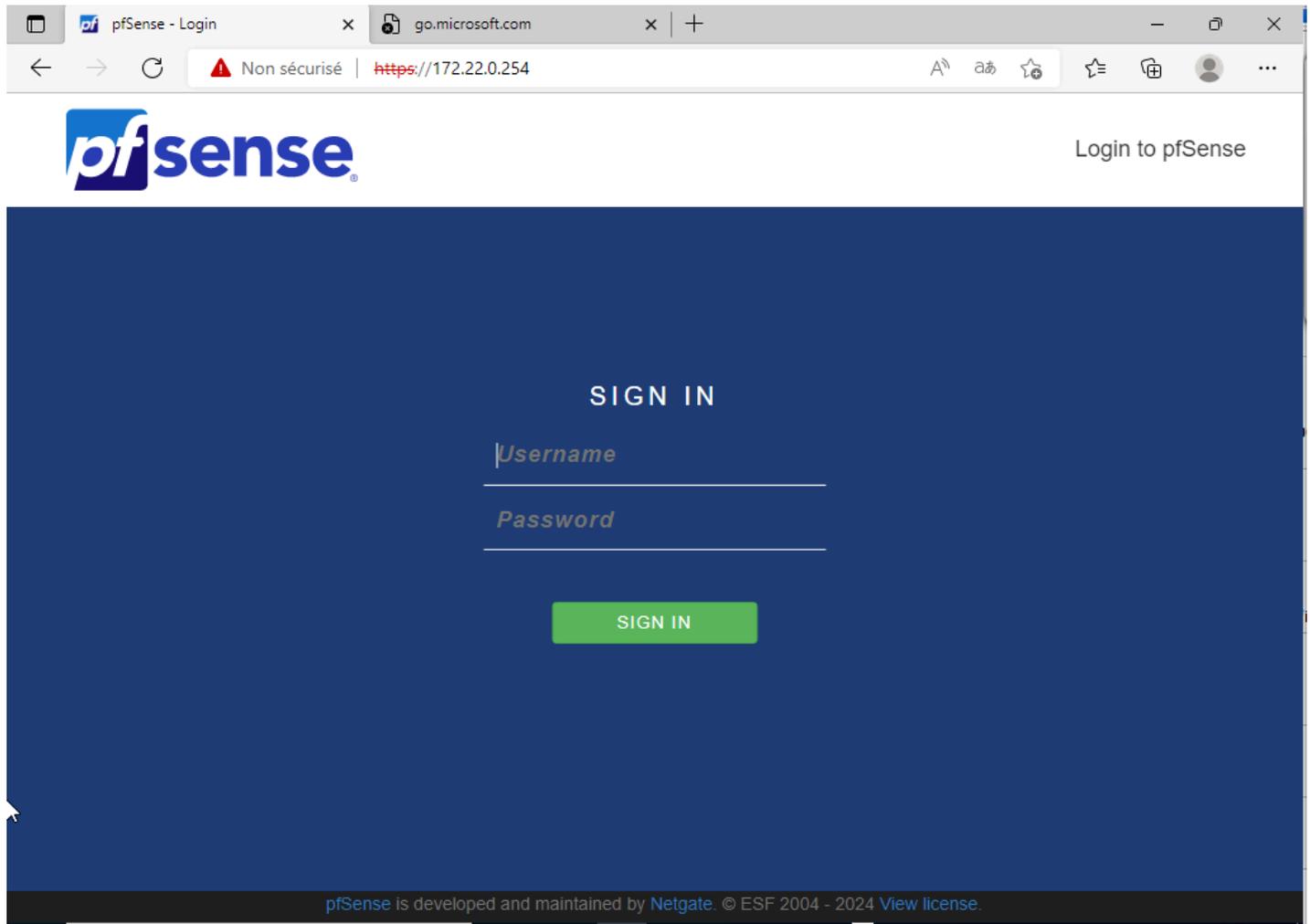
## IV- Configuration du Pfsense sur l'interface web

Pour se connecter à l'interface web du pfsense à partir de la win 10 client il faut paramétrer la carte réseaux de virtualbox et la mettre en dans le lan.

Pour le LAN (réseau interne et tout autoriser dans Mode Promiscuité) :

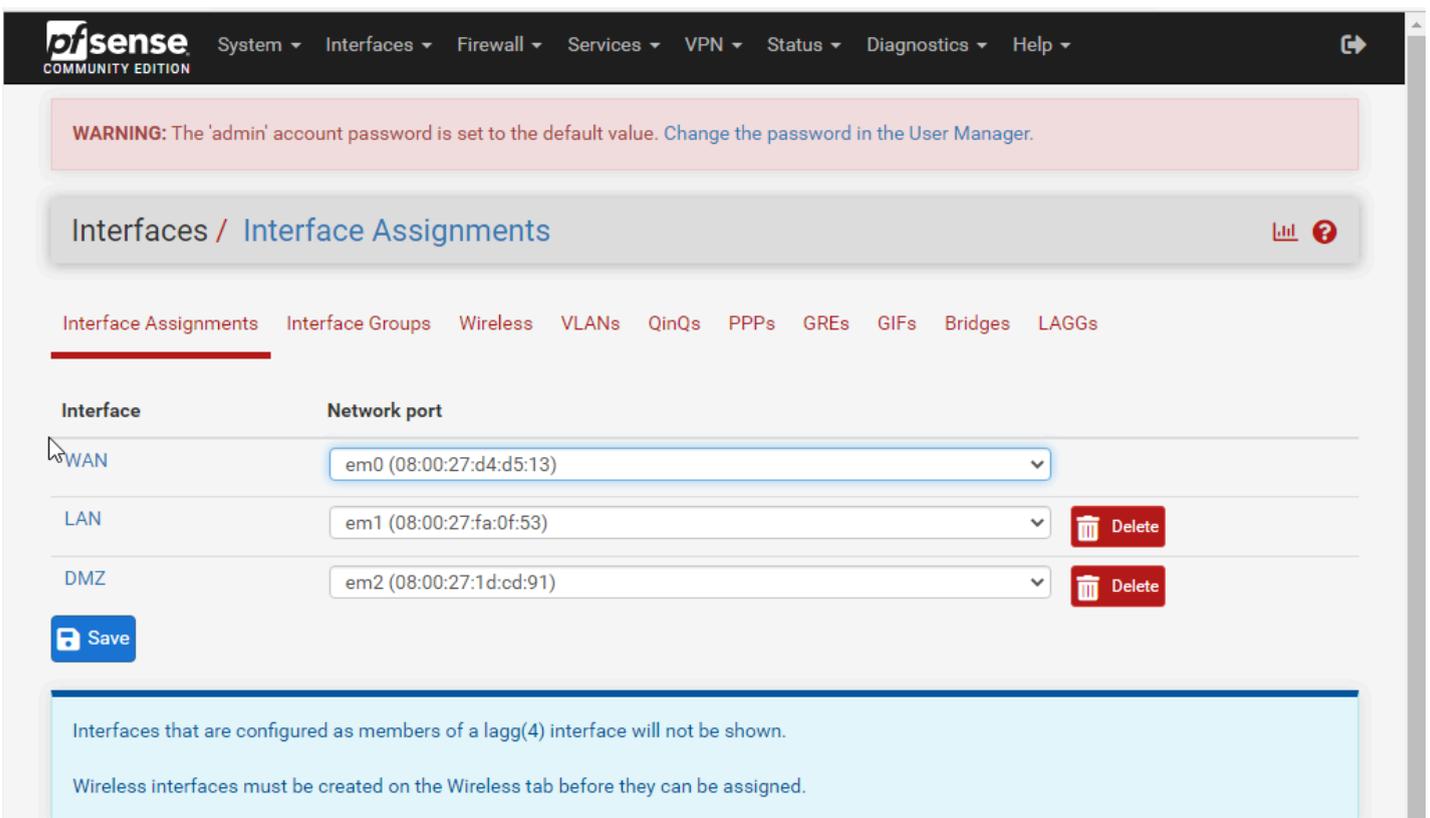
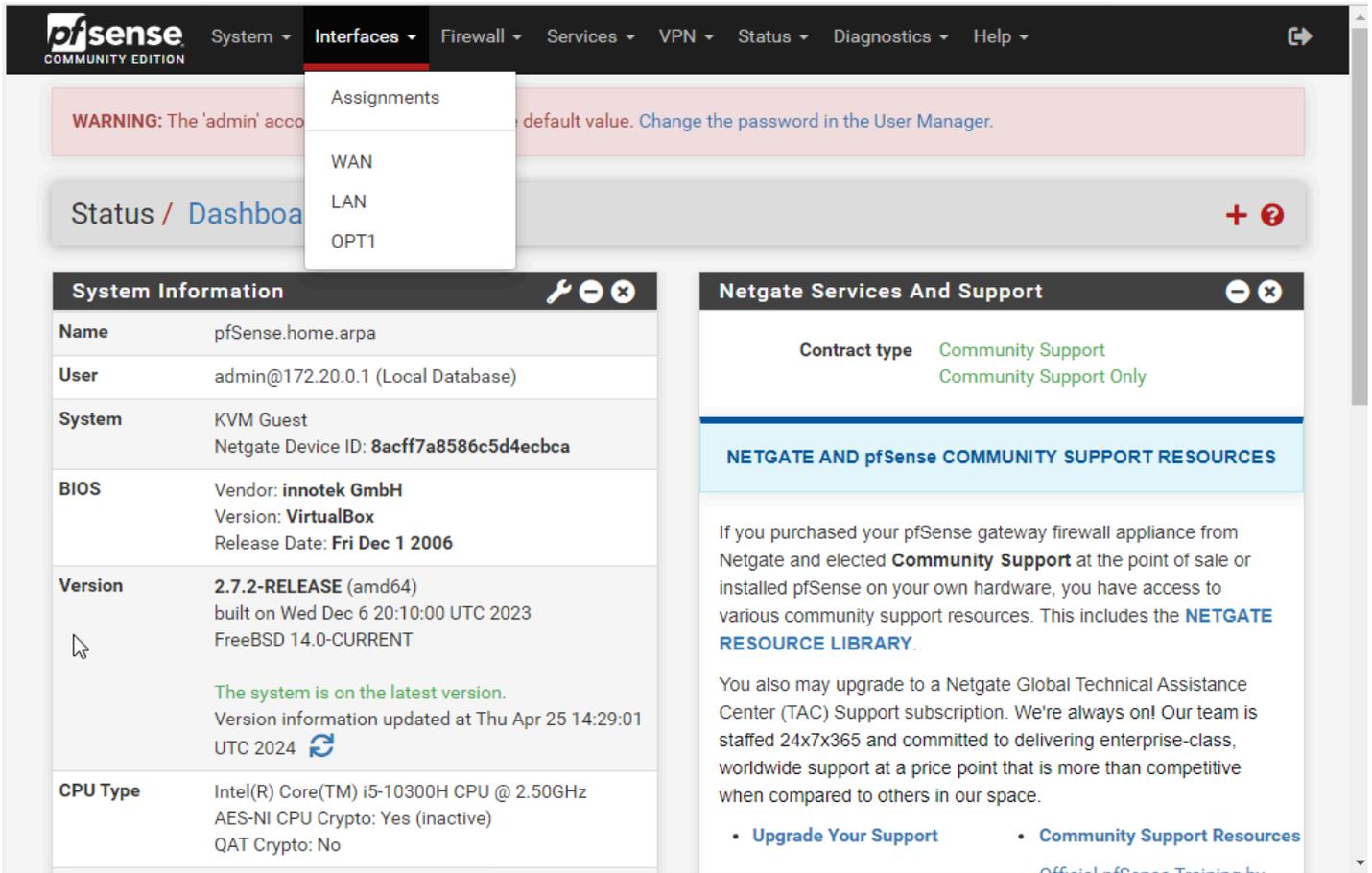


Une fois que cela est fait, on démarre la machine client windows 10 et on va sur le navigateur web pour mettre la passerelle du lan de pfsense pour pouvoir se connecter qui est en 172.22.0.254 . Une fois arriver sur l'interface de connection de pfsense l'username est par défaut admin et le mot de passe pfsense :



Une fois connecté sur la page d'administration de pfSense il faut maintenant créer les vlans sur le pfSense pour cela il faut aller dans config interface et Assignment.

On en profitera pour renommer l'interface OPT1 par DMZ pour le reconnaître plus facilement :



maintenant aller dans vlans pour rajouter les vlans correspondant et il faut le mettre dans l'interface du lan :

The screenshot shows the pfSense web interface. At the top, there is a navigation menu with items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the menu is a warning banner: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The main content area is titled "Interfaces / VLANs" and includes a sub-menu with options: Interface Assignments, Interface Groups, Wireless, VLANs (highlighted), QinQs, PPPs, GREs, GIFs, Bridges, and LAGGs. Below this is a table titled "VLAN Interfaces" with columns: Interface, VLAN tag, Priority, Description, and Actions. A green "+ Add" button is located to the right of the table. A tooltip with an information icon and the text "More information" is visible on the left side. At the bottom of the page, a footer states: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license." The Windows taskbar is visible at the very bottom, showing the search bar and various system icons.

cette configuration c'est pour le vlan 10 des Utilisateurs quand c'est finis on clique sur save et on feras la même chose pour le vlan 20 qui correspond au Datacenter :

The screenshot shows the pfSense web interface for editing a VLAN configuration. The navigation menu is the same as in the previous screenshot. The warning banner is also present. The main content area is titled "Interfaces / VLANs / Edit". Below this is a form titled "VLAN Configuration" with the following fields:

- Parent Interface:** A dropdown menu showing "em1 (08:00:27:fa:0f:53) - lan". Below it, the text reads: "Only VLAN capable interfaces will be shown."
- VLAN Tag:** A text input field containing "10". Below it, the text reads: "802.1Q VLAN tag (between 1 and 4094)."
- VLAN Priority:** A text input field containing "0". Below it, the text reads: "802.1Q VLAN Priority (between 0 and 7)."
- Description:** A text input field containing "Utilisateurs". Below it, the text reads: "A group description may be entered here for administrative reference".

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Interfaces / VLANs / Edit ☰ 📄 ?

### VLAN Configuration

**Parent Interface**  ▾  
Only VLAN capable interfaces will be shown.

**VLAN Tag**   
802.1Q VLAN tag (between 1 and 4094).

**VLAN Priority**   
802.1Q VLAN Priority (between 0 and 7).

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

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 [View license.](#)

Windows taskbar: Tapez ici pour effectuer une recherche, 20°C, 17:07, 25/04/2024

Voici le résultat que vous devez obtenir :

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Interfaces / VLANs ☰ 📄 ?

Interface Assignments   Interface Groups   Wireless   VLANs   QinQs   PPPs   GREs   GIFs   Bridges   LAGGs

### VLAN Interfaces

Interface	VLAN tag	Priority	Description	Actions
em1 (lan)	10		Utilisateurs	
em1 (lan)	20		Datacenter	

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 [View license.](#)

maintenant il faut aller dans l'onglet interface Assignment qui vas permettre de les rajouter sur les ports :

The screenshot shows the pfSense web interface for 'Interface Assignments'. At the top, there is a navigation bar with 'pfSense COMMUNITY EDITION' and menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help. A warning message states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below this is a breadcrumb 'Interfaces / Interface Assignments' with a search icon and a help icon. A horizontal menu contains: Interface Assignments (selected), Interface Groups, Wireless, VLANs, QinQs, PPPs, GREs, GIFs, Bridges, LAGGs. The main content area has a table with two columns: 'Interface' and 'Network port'. The table lists: WAN (em0 (08:00:27:d4:d5:13)), LAN (em1 (08:00:27:fa:0f:53) with a red 'Delete' button), and DMZ (em2 (08:00:27:1d:cd:91) with a red 'Delete' button). Below the table, 'Available network ports:' shows 'VLAN 10 on em1 - lan (Utilisateurs)' with a green '+ Add' button. A blue 'Save' button is at the bottom left. A light blue box contains instructions: 'Interfaces that are configured as members of a lagg(4) interface will not be shown.' and 'Wireless interfaces must be created on the Wireless tab before they can be assigned.'

Interface	Network port
WAN	em0 (08:00:27:d4:d5:13)
LAN	em1 (08:00:27:fa:0f:53) <span>Delete</span>
DMZ	em2 (08:00:27:1d:cd:91) <span>Delete</span>
Available network ports:	VLAN 10 on em1 - lan (Utilisateurs) <span>+ Add</span>

This screenshot is similar to the previous one but shows the result of adding a new interface. The 'Available network ports:' dropdown now shows 'VLAN 20 on em1 - lan (Datacenter)' with a green '+ Add' button. The table now includes a new entry: 'OPT2' assigned to 'VLAN 10 on em1 - lan (Utilisateurs)' with a red 'Delete' button. The 'Save' button remains at the bottom left. A green notification box at the top says 'Interface has been added.' The rest of the interface, including the warning and navigation, is identical to the previous screenshot.

Interface	Network port
WAN	em0 (08:00:27:d4:d5:13)
LAN	em1 (08:00:27:fa:0f:53) <span>Delete</span>
DMZ	em2 (08:00:27:1d:cd:91) <span>Delete</span>
OPT2	VLAN 10 on em1 - lan (Utilisateurs) <span>Delete</span>
Available network ports:	VLAN 20 on em1 - lan (Datacenter) <span>+ Add</span>

Maintenant il faut renommer les interfaces des vlans et rajouter les adresses ip manquants :

pour le vlan 10 et 20 :

**Warning:** The 'admin' account password is set to the default value. Change the password in the User Manager.

### Interfaces / Vlan10 (em1.10)

**General Configuration**

**Enable**  Enable interface

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

**IPv4 Configuration Type**

**IPv6 Configuration Type**

**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

**Enable**  Enable interface

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

**IPv4 Configuration Type**

**IPv6 Configuration Type**

**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**  /

Une fois que les changements seront faites les modifications vont apparaître sur le pfSense :

```
PING 172.21.0.1 (172.21.0.1): 56 data bytes
64 bytes from 172.21.0.1: icmp_seq=0 ttl=128 time=1.463 ms
64 bytes from 172.21.0.1: icmp_seq=1 ttl=128 time=1.448 ms
^CKVM Guest - Netgate Device ID: 59bbd1740b4ab2434542

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.147.59/24
LAN (lan)      -> em1      -> v4: 172.22.0.254/24
DMZ (opt1)     -> em2      -> v4: 192.168.20.254/24
VLAN10 (opt2) -> em1.10   -> v4: 172.20.0.254/24
VLAN20 (opt3) -> em1.20   -> v4: 172.21.0.254/24

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: █
```

Maintenant il faut mettre en place du routage entre les vlans, il faudra mettre des règles de filtrages ainsi que des règles de NAT pour que la dmz puisse être accessible depuis l'ip du wan avec un port qui sera 8080.

il faut avant tout se rendre dans Interfaces /Wan est désactiver cette case pour qu'on puisse le configurer depuis notre wan le pfSense et non en config interne entre le pc client et le pfSense :

**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](#)

Nous allons maintenant faire les règles de filtrages pour chaque interfaces :

Wan :

Firewall / Rules / WAN

Floating **WAN** LAN DMZ OPT2 OPT3

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 1.45 MiB	IPv4 TCP	*	*	WAN address	80 (HTTP)	*	none		
<input type="checkbox"/>	✓	3 / 74 KiB	IPv4 *	*	*	*	*	none			
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	*	*	DMZ address	80 (HTTP)	*	none	NAT	

Add Add Delete Save Separator

lan :

Firewall / Rules / LAN

Floating **LAN** WAN DMZ OPT2 OPT3

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	*	*	*	LAN Address	80	*	*	Anti-Lockout Rule	
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	LAN net	*	DMZ net	*	*	none		
<input type="checkbox"/>	✓	0 / 0 B	IPv6 *	*	*	*	*	none			
<input type="checkbox"/>	✓	0 / 0 B	IPv4 *	LAN net	*	*	*	none		Default allow LAN to any rule	

Add Add Delete Save Separator

dmz :

Firewall / Rules / DMZ

Floating **DMZ** WAN LAN OPT2 OPT3

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	DMZ net	*	*	80 (HTTP)	*	none		
<input type="checkbox"/>	✓	4 / 85 KiB	IPv4 *	*	*	*	*	none			

Add Add Delete Save Separator

Vlan 10 :

Firewall / Rules / OPT2

Floating WAN LAN DMZ OPT2 OPT3

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	*	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/>	✓ 8 / 2.81 MiB	IPv4 *	*	*	*	*	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	WAN address	80 (HTTP)	*	none			

Add Add Delete Save Separator

vlan 20 :

Firewall / Rules / OPT2

Floating WAN LAN DMZ OPT2 OPT3

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	*	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/>	✓ 8 / 2.81 MiB	IPv4 *	*	*	*	*	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	WAN address	80 (HTTP)	*	none			

Add Add Delete Save Separator

une fois que cela est fait on vas mettre la règle de nat qui vas permettre de se connecter à la dmz depuis le wan avec le port personnalisier 8080 :

Rules	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	8080	192.168.20.1	80 (HTTP)		

Legend  
 Pass  
 Linked rule

**Page par défaut d'Apache2 Debian**

**Ça marche!**

Il s'agit de la page d'accueil par défaut utilisée pour tester le bon fonctionnement du serveur Apache2 après installation sur les systèmes Debian. Si vous pouvez lire cette page, cela signifie que le serveur HTTP Apache installé sur ce site fonctionne correctement. Vous devez **remplacer ce fichier** (situé dans `/var/www/html/index.html`) avant de continuer à exploiter votre serveur HTTP.

Si vous êtes un utilisateur normal de ce site Web et que vous ne savez pas de quoi parle cette page, cela signifie probablement que le site est actuellement indisponible en raison de maintenance. Si le problème persiste, veuillez contacter l'administrateur du site.

**Présentation de la configuration**

La configuration par défaut d'Apache2 de Debian est différente de la configuration par défaut en amont et est divisée en plusieurs fichiers optimisés pour l'interaction avec les outils Debian. Le système de configuration est **entièrement documenté dans `/usr/share/doc/apache2/README.Debian.gz`**. Reportez-vous à ceci pour la documentation complète. La documentation du serveur Web lui-même peut être trouvée en accédant au **manuel** si le package `apache2-doc` a été installé sur ce serveur.

La configuration de la configuration pour une installation de serveur Web Apache2 sur les systèmes Debian est la suivante :

```

/etc/apache2/
|-- apache2.conf
|  |-- ports.conf
|  |-- mods activés
|  |-- *.charger
|  |-- *.conf
|-- conf-activé
|  |-- *.conf
|-- compatible avec les sites
|  |-- *.conf

```

Pour finir il faut établir les règles de routage car sans ça il pourront pas communiquer :

System / Routing / Gateways

The changes have been applied successfully.

Gateways Static Routes Gateway Groups

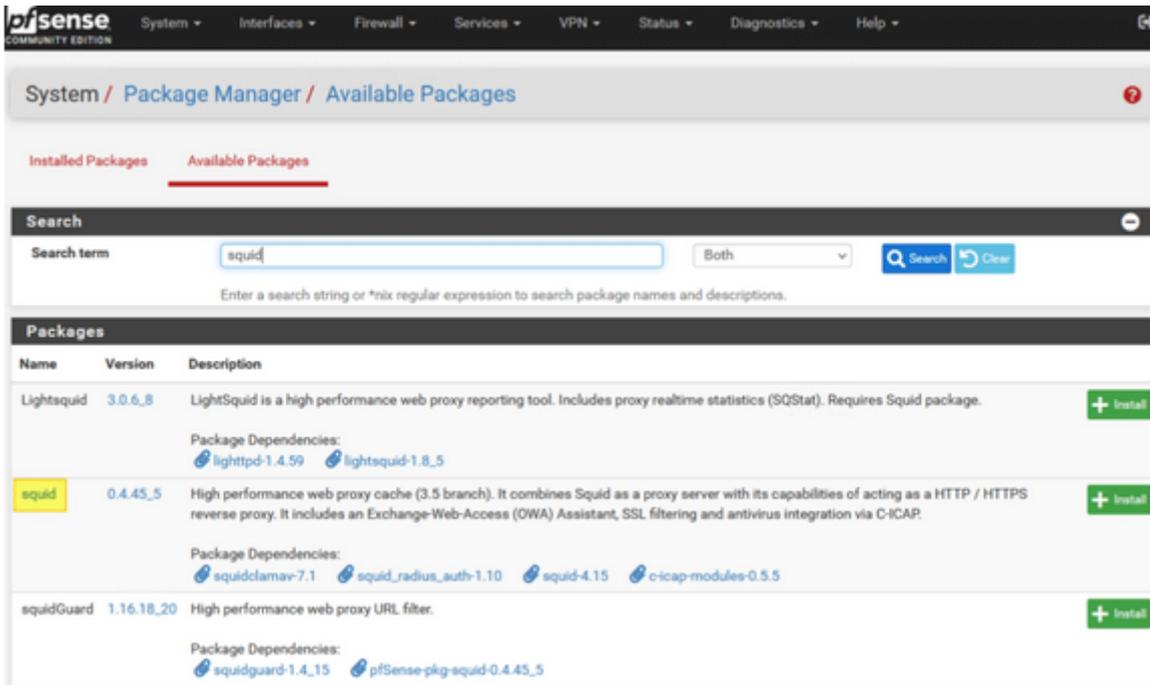
Gateways	Name	Default	Interface	Gateway	Monitor IP	Description	Actions
<input type="checkbox"/>	WAN_DHCP	Default (IPv4)	WAN	192.168.1.1	192.168.1.96	Interface WAN_DHCP Gateway	
<input type="checkbox"/>	WAN_DHCP6		WAN	fe80::1%em0	fe80::1%em0	Interface WAN_DHCP6 Gateway	
<input type="checkbox"/>	Datacenter		VLAN20	172.21.0.254	172.21.0.254		
<input type="checkbox"/>	Utilisateurs		VLAN10	172.20.0.254	172.20.0.254		
<input type="checkbox"/>	DMZ		DMZ	192.168.20.254	192.168.20.254		

Save + Add

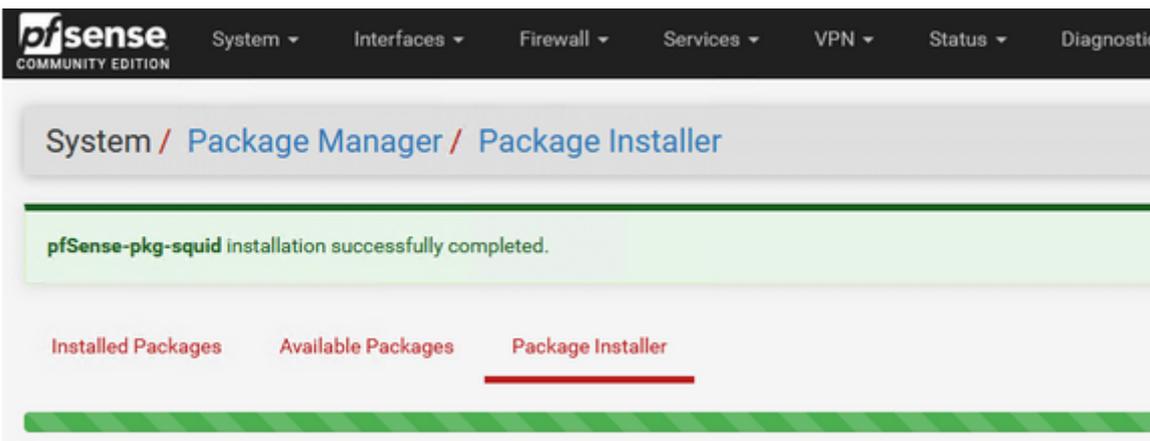
## VI- Installation du proxy squid + squidGuard sur pfsense

Connectez-vous sur l'interface d'administration de PfSense afin d'installer le paquet "squid". Pour cela, sous "System", cliquez sur "Package Manager" et ensuite sur l'onglet "Available Packages".

Recherchez "squid" et cliquez sur le bouton "Install" à droite, au niveau de la ligne correspondante.



À la fin de l'installation, le message "pfSense-pkg-squid installation successfully completed" doit s'afficher.



il faut faire la même chose pour squidGuard :

System / Package Manager / Available Packages

Installed Packages Available Packages

**Search**

Search term:  Both

Enter a search string or \*nix regular expression to search package names and descriptions.

**Packages**

Name	Version	Description	
Lightsquid	3.0.7_3	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	<input type="button" value="+ Install"/>
Package Dependencies: <a href="#">lighttpd-1.4.72</a> <a href="#">lightsquid-1.8_5</a>			
squidGuard	1.16.19	High performance web proxy URL filter.	<input type="button" value="+ Install"/>
Package Dependencies: <a href="#">squidguard-1.4_15</a> <a href="#">pfSense-pkg-squid-0.4.46</a>			

System / Package Manager / Installed Packages

Installed Packages Available Packages

**Installed Packages**

Name	Category	Version	Description	Actions
✓ squid	www	0.4.46	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.	<input type="button" value="Update"/> <input checked="" type="button" value="Current"/> <input type="button" value="Remove"/> <input type="button" value="Information"/> <input type="button" value="Reinstall"/>
Package Dependencies: <a href="#">squidclamav-7.2</a> <a href="#">squid_radius_auth-1.10</a> <a href="#">squid-6.3</a> <a href="#">c-icap-modules-0.5.5_1</a>				
✓ squidGuard	www	1.16.19	High performance web proxy URL filter.	<input type="button" value="Update"/> <input checked="" type="button" value="Current"/> <input type="button" value="Remove"/> <input type="button" value="Information"/> <input type="button" value="Reinstall"/>
Package Dependencies: <a href="#">squidguard-1.4_15</a> <a href="#">pfSense-pkg-squid-0.4.46</a>				

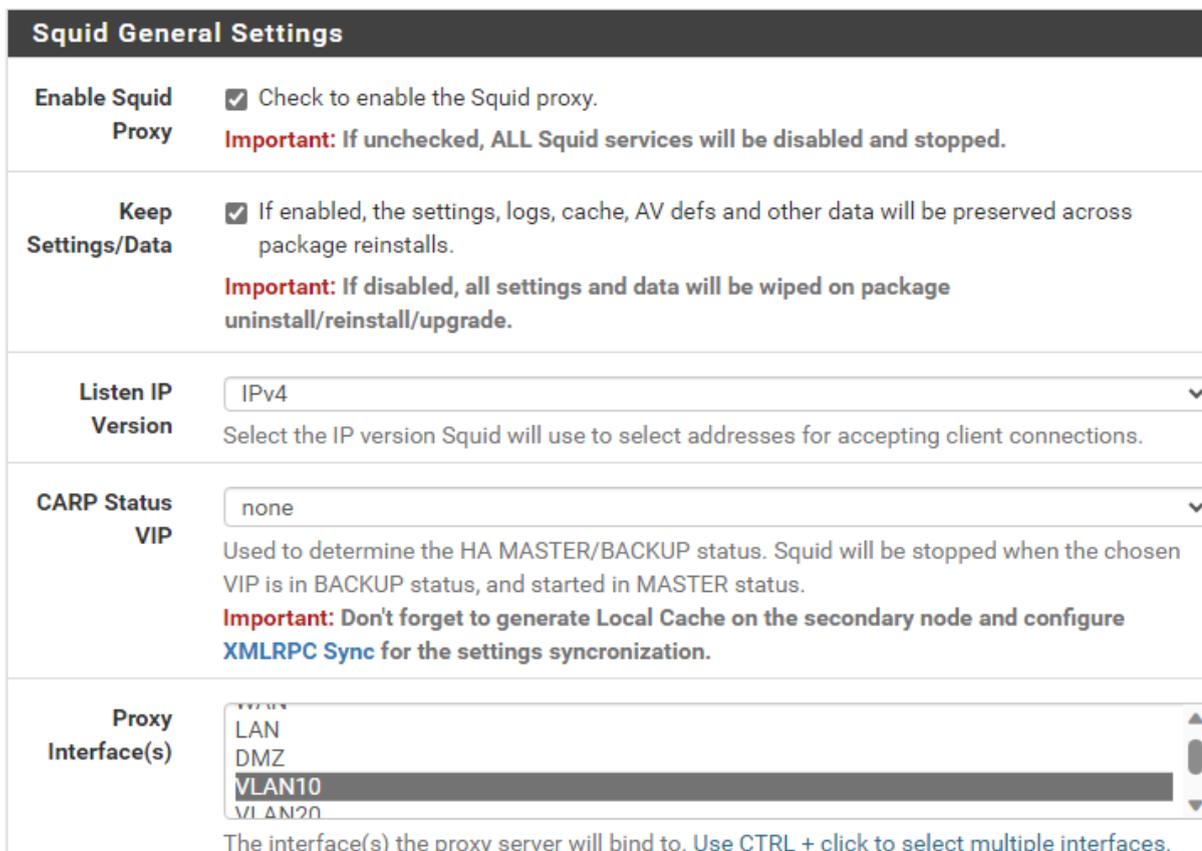
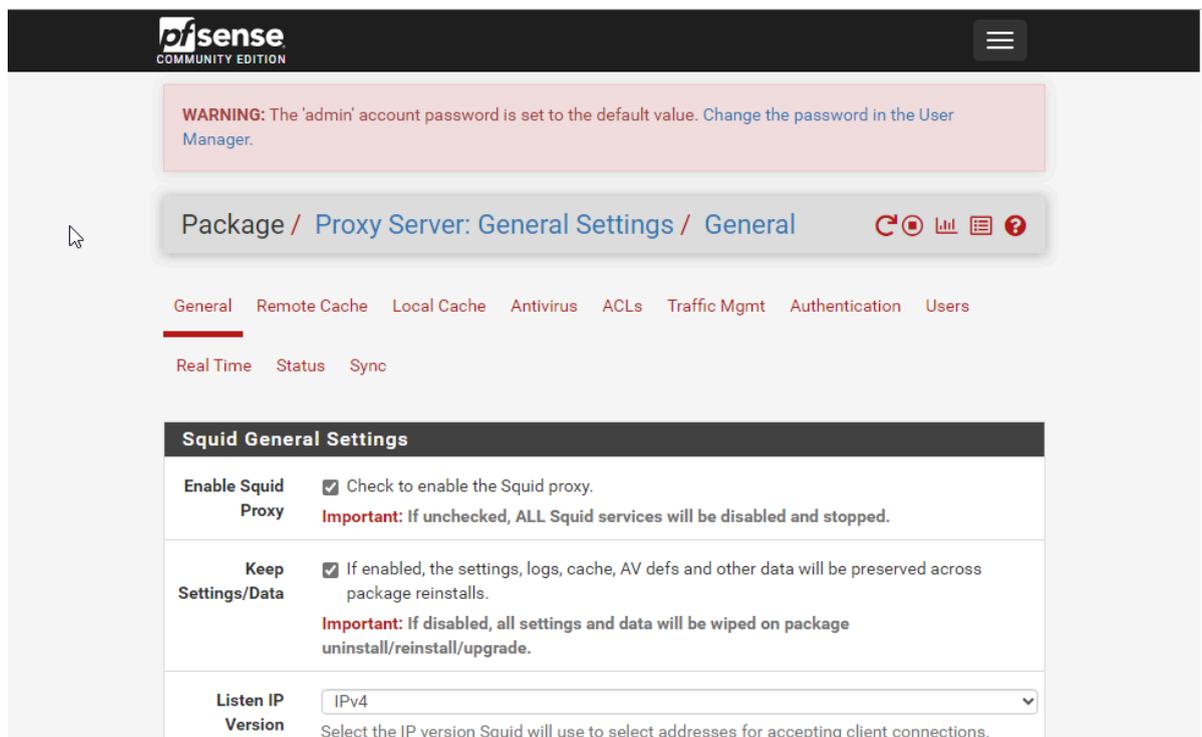
= Update  = Current  
 = Remove  = Information  = Reinstall

Newer version available

Package is configured but not (fully) installed or deprecated

Une fois installés, allez dans "Services" > "Proxy Server" pour configurer Squid.

Il faut activer le service Squid : on doit activer le service Squid en cochant la case "Enable Squid Proxy" dans l'interface web de pfSense. Cela permet de démarrer le service Squid et de le rendre opérationnel sur le pfSense. Il faut aussi ne pas oublier de mettre dans "proxy interfaces" le vlan 10 qui est celui des utilisateurs cela va permettre de filtrer la navigation des utilisateurs .



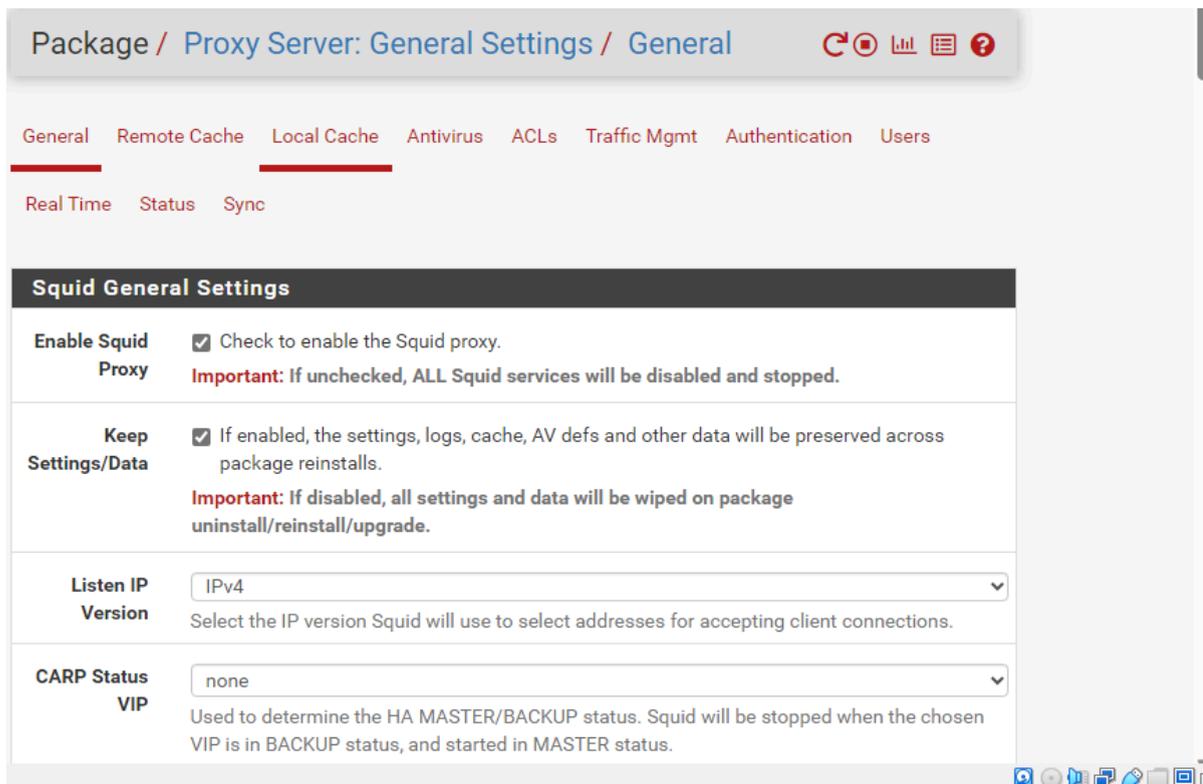
Activation du proxy transparent pour HTTP : Cocher l'option "Transparent HTTP Proxy" dans les paramètres de configuration de Squid sur pfSense permet à Squid d'opérer en tant que proxy transparent pour les connexions HTTP. Cela signifie que Squid interceptera le trafic HTTP sans nécessiter de configuration explicite sur les clients, simplifiant ainsi la gestion du proxy.

The screenshot shows the 'Transparent Proxy Settings' page in pfSense. It features several sections: 'Transparent HTTP Proxy' with a checked checkbox and an information icon; 'Transparent Proxy Interface(s)' with a dropdown menu showing 'LAN', 'DMZ', 'VLAN10', and 'VLAN20'; 'Bypass Proxy for Private Address Destination' with an unchecked checkbox; and 'Bypass Proxy for These Source IPs' with an empty text input field. The page includes detailed instructions and warnings about SSL interception and interface selection.

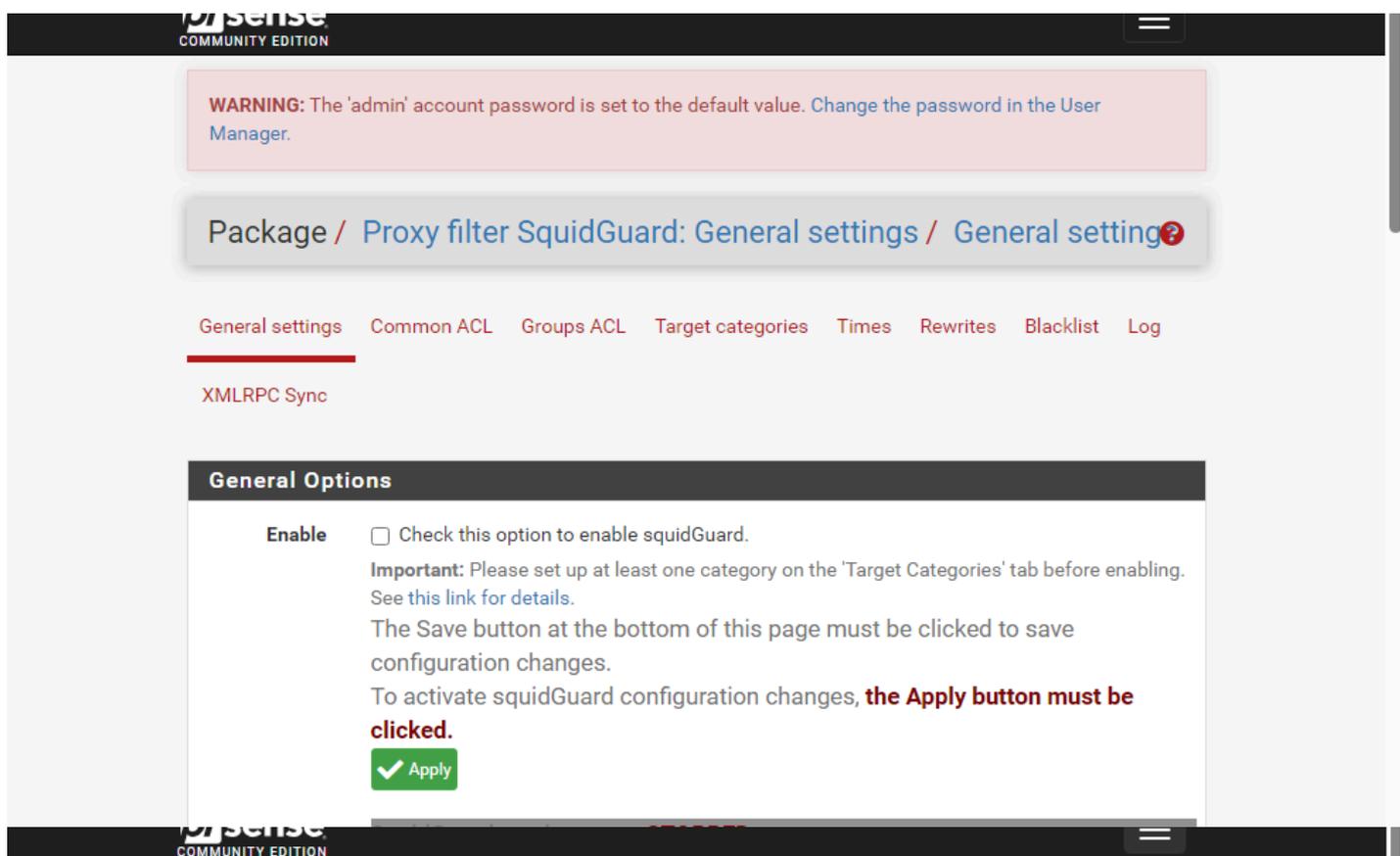
il faut Configurer le hostname : on doit spécifier un nom d'hôte (hostname) pour le serveur Squid. Le hostname est utilisé pour identifier le serveur Squid sur le réseau. Pour le choix du port il faut le laisser par défaut. Ce port est utilisé pour écouter les demandes HTTP et HTTPS entrantes et les traiter en tant que proxy Squid.

The screenshot shows the 'Proxy Server: Remote Proxy Settings' page in pfSense. It includes a warning about the 'admin' account password, a breadcrumb trail, and a navigation menu. The 'General Settings' section is expanded, showing fields for 'Enable' (checked), 'Hostname' (squirrel-proxy), 'Name' (squirrel-proxy), and 'TCP Port' (3128). The page also features a top navigation bar with the pfSense logo and a bottom system tray.

Activation du cache local : on doit activer le cache local dans la configuration de Squid sur pfSense. Le cache local permet de stocker localement les objets web fréquemment demandés, ce qui améliore les performances en réduisant la latence et la bande passante utilisée pour récupérer ces objets à partir d'Internet.



Maintenant il faut configurer squidGuard c'est un logiciel de redirection d'URL, qui peut être utilisé pour contrôler le contenu des sites Web auxquels les utilisateurs peuvent accéder. Pour cela il faut se rendre dans "Services" > "Proxy Filter" > "SquidGuard Proxy Filter". Quand c'est bon il faut aller dans l'option "General settings" pour activer le service car le service est désactiver :



**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

après cela il faut configurer des ACL pour bloquer les réseaux sociaux pour cela on doit aller dans "Services" > "Proxy Filter" > "Target catégories".

Proxy filter SquidGuard: Target categories / Edit / Target categories 

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log

XMLRPC Sync

### General Options

**Name**   
Enter a unique name of this rule here.  
The name must consist between 2 and 15 symbols [a-Z\_0-9]. The first one must be a letter.

**Order**    
Select the new position for this target category. Target categories are listed in this order on ACLs and are matched from the top down in sequence.

**Domain List**

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Package / Proxy filter SquidGuard: Target categories   
/ Target categories

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log

XMLRPC Sync

Name	Redirect	Description
socialnetwork		 
 Add		

Puis il faut aller dans Common ACL pour mettre l'accès de socialnetwork en deny :

Package / Proxy filter SquidGuard: Common Access Control List (ACL) / Common ACL

General settings **Common ACL** Groups ACL Target categories Times Rewrites Blacklist Log

XMLRPC Sync

### General Options

**Target Rules** [socialnetwork !all]

**Target Rules List** + -

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

**Target Categories**

[socialnetwork]	access	deny
Default access [all]	access	deny

Et pour valider le tout on sauvegarde la conf :

**Enable log rotation**  Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.

### Miscellaneous

**Clean Advertising**  Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.

### Blacklist options

**Blacklist**  Check this option to enable blacklist

**Blacklist proxy** [ ]

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** [ ]

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**