

Installation & Configuration d'un DNS, DHCP, Firewall et protocole CARP sous pfSense avec redondance.



Table des matières

1) Introduction	3
1.1. Prérequis.....	4
2.Installation du pfSense (Master & Slave)	5
2)Services Requis	30
1.Configuration du DHCP (suite).....	30
2.Configuration du DNS.....	31
3.Activer le DNS forwarder	32
Configuration Générale	33
1.Les Alias	33
1.Création d'une règle de FireWall.....	35
1.Configuration de CARP.....	36
1.Synchronisation des configurations & Test de Basculement	43
1.CARP	5
Bonus	45
1.Bloquer Youtube.....	45
2.HTTPS	49
3.DNSSEC.....	51
Conclusion Générale	54
1.Avantages de pfSense.....	54
1.Avis globale sur cette installation.....	55
1.Annexe.....	56
.....	
FIN	

1) Introduction

PfSense est un système d'exploitation à part entière, open source, utilisé pour mettre en œuvre un pare-feu, un routeur ou une solution permettant la fourniture d'autres services réseaux. PfSense est une distribution FreeBSD 1 personnalisée, et basée initialement sur le projet m0n0wall, distribution de pare-feu puissant mais léger. PfSense s'appuie sur le principe de base de m0n0wall et reprend la plupart de ses fonctions, en prenant soin de mieux les faire cohabiter, de les sécuriser, de les stabiliser, tout en favorisant la compatibilité du système afin d'y ajouter une variété d'autres services liés essentiellement aux réseaux.

Ce compte-rendu, explique la configuration de base et nécessaires à la quasi-totalité des déploiement, nous verrons la configuration des différents services, tout en respectant les bonnes pratiques.

A son niveau de base, un pfSense peut être utilisé pour remplacer le routeur d'un réseau domestique et pour fournir des fonctionnalités supplémentaires.

Une fois celui-ci installé et configuré, il existe 2 façons d'y accéder à l'*OS :

- *Par Interface web : <http://@IP>
- Par SSH : @IP : *22

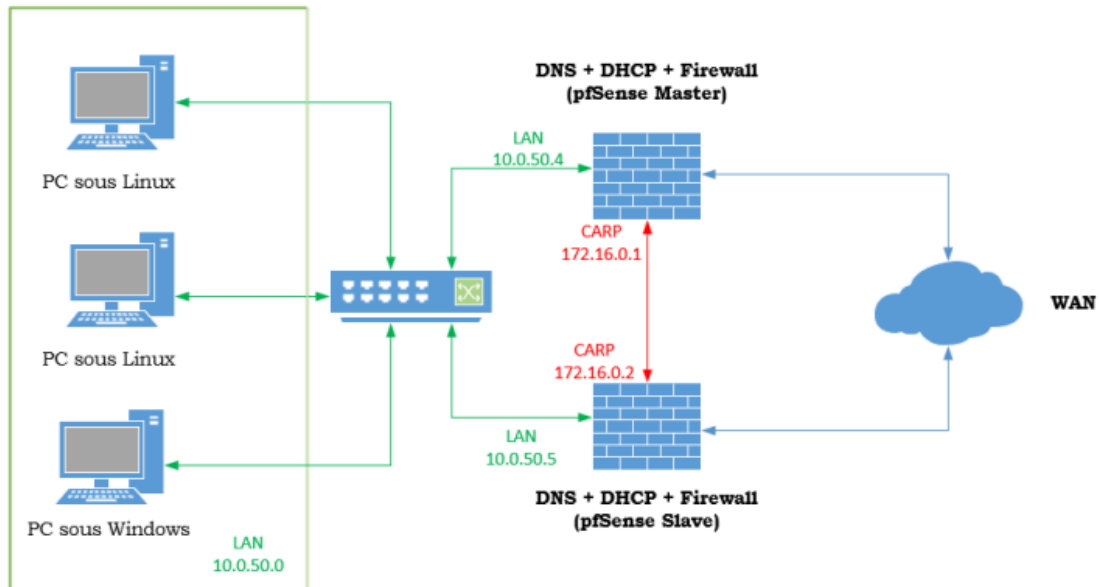
*OS : Operating System ou Système d'exploitation en Français.

*22 : Port par défaut de SSH.

*Interface Web : On verra que par défaut, on accède à l'interface par le protocole http (:80) qui n'est pas sécurisé. Pour des questions de bonnes pratiques, nous verrons que ce port sera changer enfin d'y accéder via https (:443).

1.1) Prérequis

Pour réaliser cette installation nous avons besoin d'une infrastructure virtuelle sous l'applcatif VMware ou VirtualBox ou encore EXSi.



SCHEMA DE NOTRE INFRASTRUCTURE

1.2) Installation de pfSense

Pour l'installation de pfSense, il faudra configurer notre VM de cette façon (Réalisé sous VMWare Workstation 17) :

Device	Summary	
Memory	256 MB	
Processors	1	Destinée au WAN
Hard Disk (SCSI)	20 GB	
CD/DVD (IDE)	Using file PfSense (Master)-fil...	Destinée au LAN (10.0.50.0)
Network Adapter	NAT	
Network Adapter 2	Custom (VMnet2)	
Network Adapter 3	Custom (VMnet3)	Destinée au Protocole CARP (172.16.0.0)
USB Controller	Present	
Display	Auto detect	

INFO : Pas Besoin d'une grosse configuration matérielle, on peut donc mettre le minimum requis (256MB).

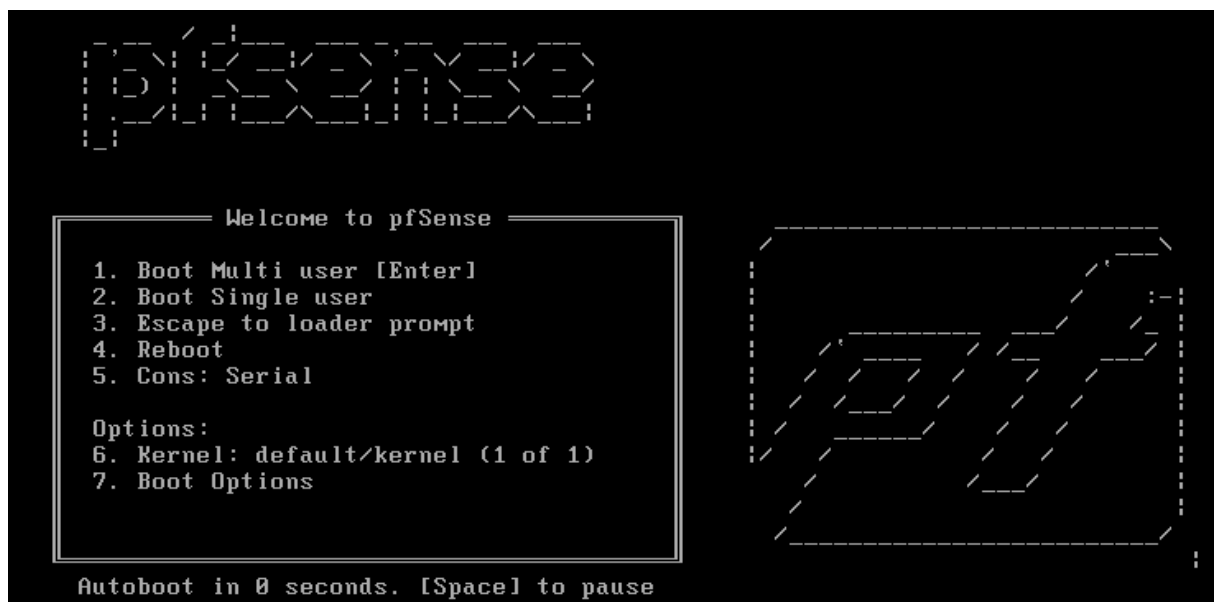
.FREESD (=

Pour l'ISO de pfSense, il suffit de se rendre sur :

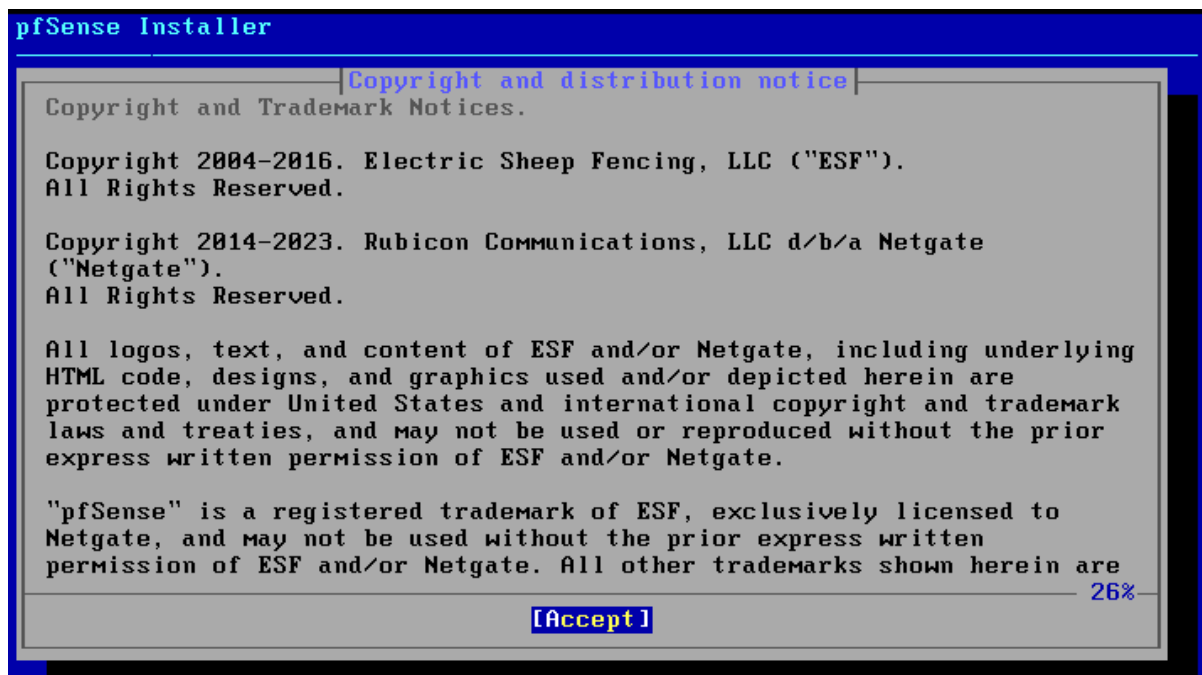
<https://www.pfsense.org/download/>

(Version actuelle de mon installation : 2.7.2)

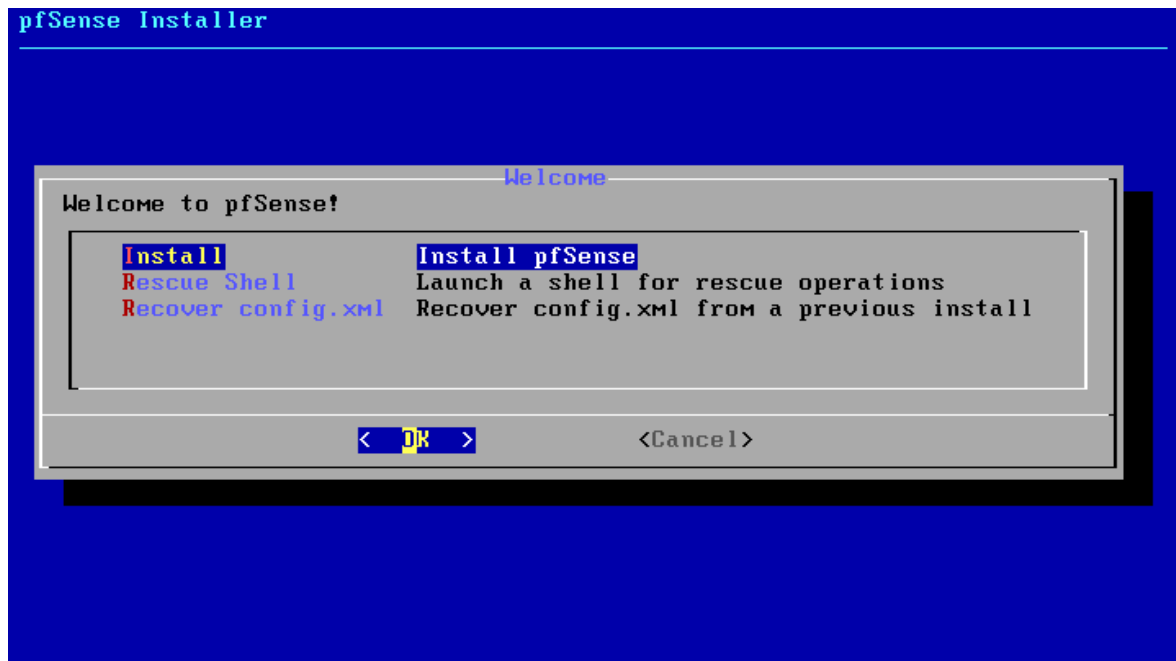
Après avoir insérer l'ISO, nous pouvons démarrer la machine, le setup va démarrer automatiquement après quelques secondes.



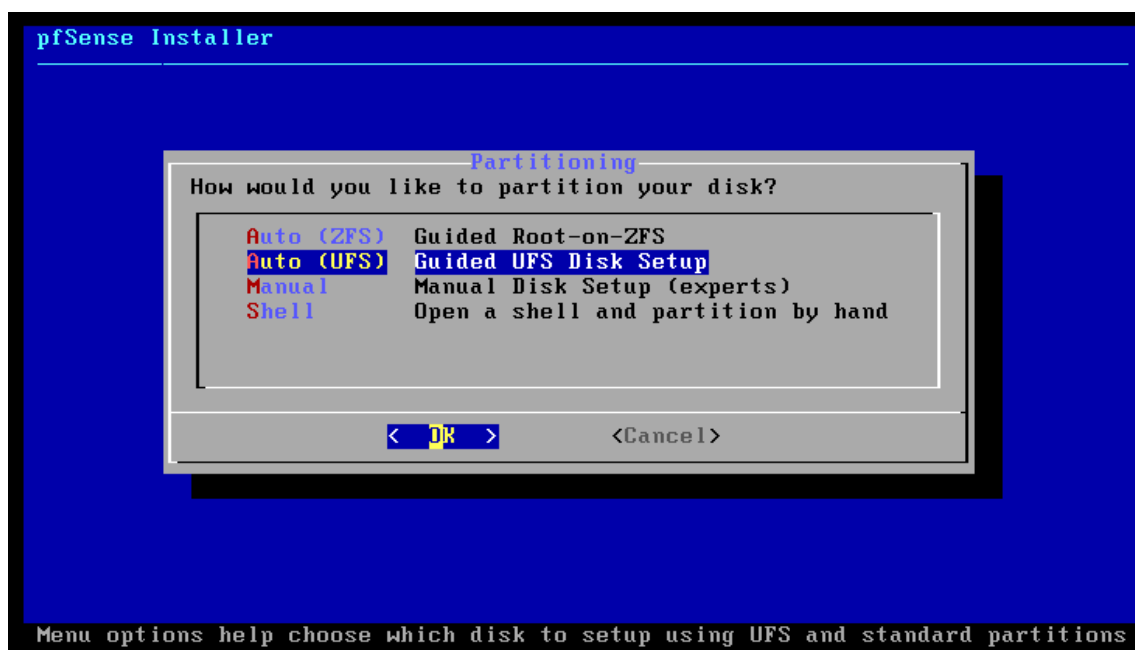
⚠ Important : L'installation va s'effectuer au clavier. Appuyez sur la touche Entrée pour Accepter.



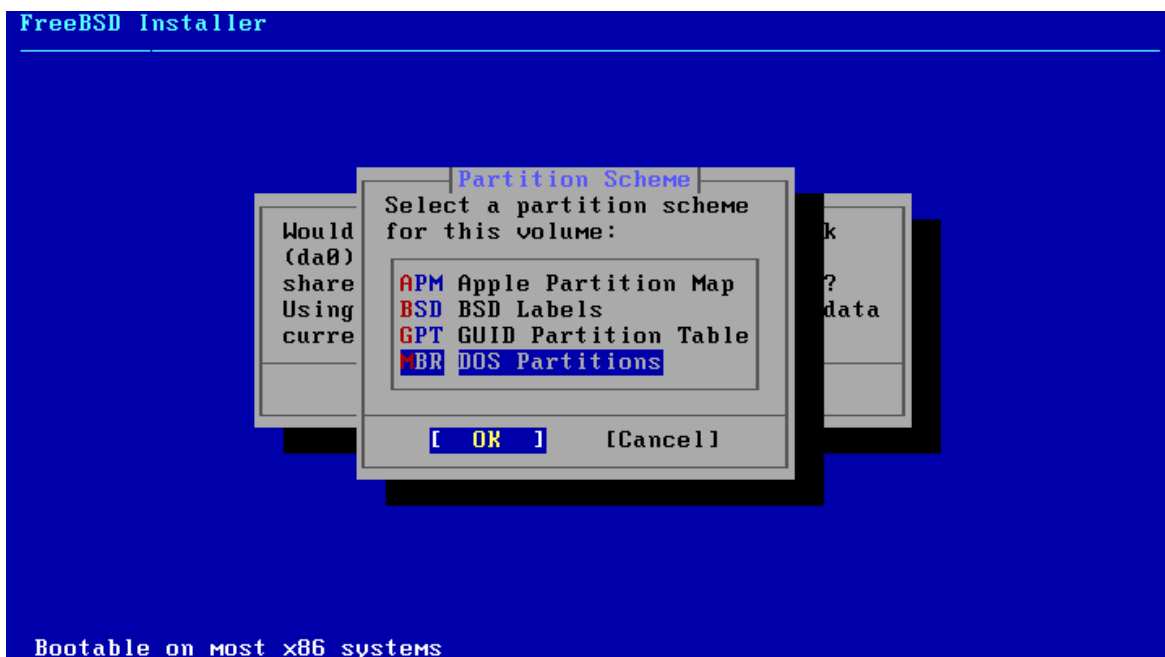
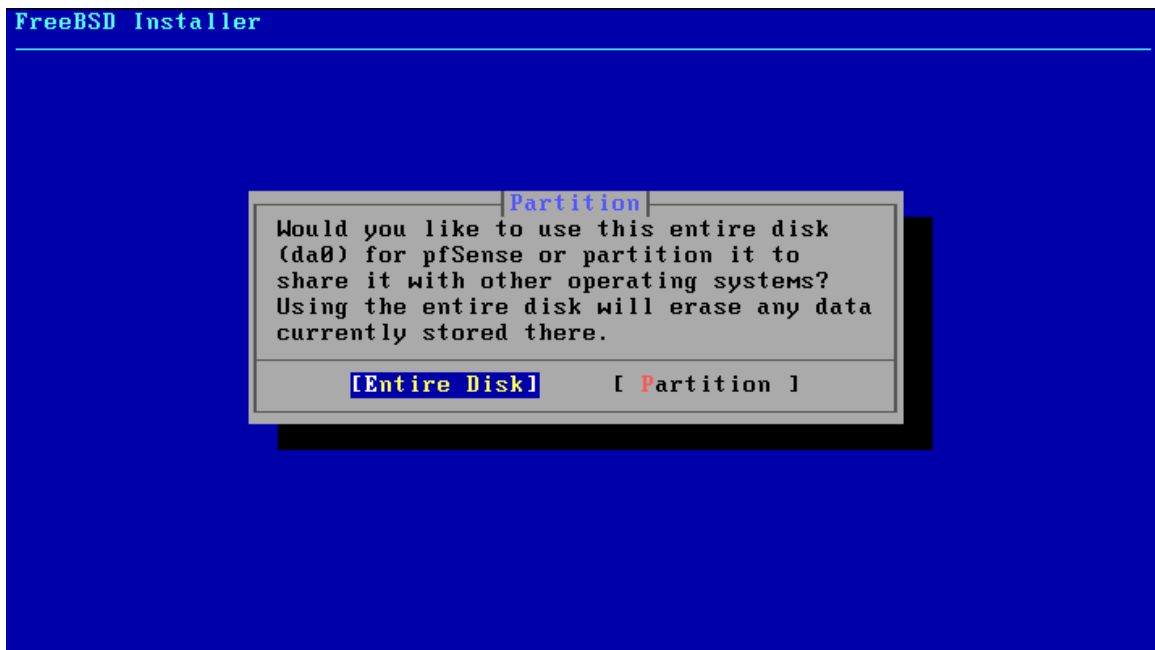
Vérifier que vous êtes bien sur l'onglet **Install**, sinon déplacez vous avec les flèches de votre clavier « ↑↓ » et appuyez sur **Entrée** pour faire **OK**.



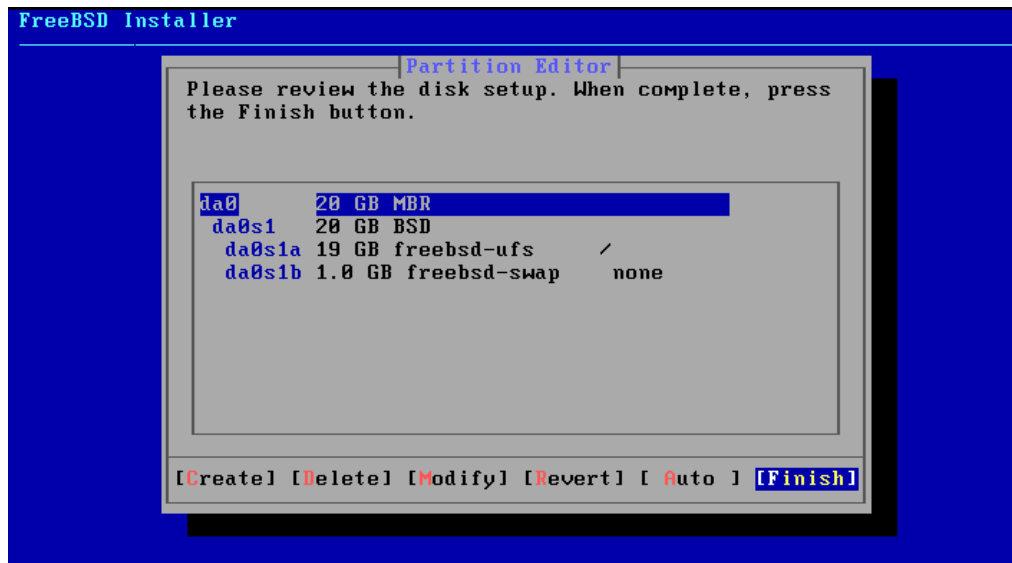
Le setup va vous demander de **partitionner le disque** de stockage de la machine. Avec les touches fléchées de votre clavier, allez sur « **Auto (UFS)** » et appuyez sur **Entrée**.



Sélectionner [Entire Disk] ou [Partitions] (nécessite des connaissances)



Installateur nous propose un découpage sur le disque 0 (nommé ici da0), nul besoin de modifier celle-ci, sélectionner Finish puis Entrée.



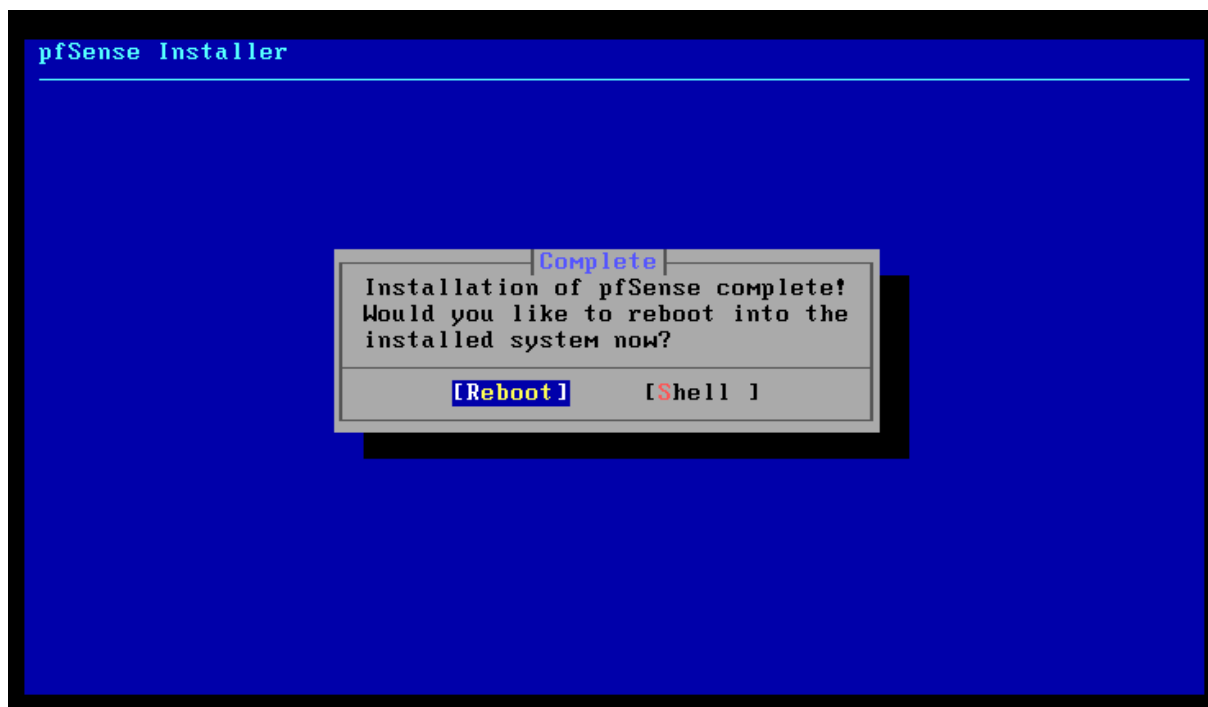
Un dernier avertissement pour demander si on est sûr que le disque sera effacé pour l'installation de pfSense.



L'Installation est en cours.....



Sélectionner Reboot ou Shell (si vous souhaitez apporter des modifications)



A son lancement, pfSense va charger ce qu'il a besoin pour son fonctionnement. (Services)

```
Done.
done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration...2024-03-10T11:15:09.132267+00:00 - php-fpm 603 - - /rc.
linkup: Ignoring link event during boot sequence.
2024-03-10T11:15:09.133552+00:00 - php-fpm 602 - - /rc.linkup: DHCP Client not r
unning on wan (em0), reconfiguring dhclient.
done.
Updating configuration...2024-03-10T11:15:09.204999+00:00 - php-fpm 611 - - /rc.
linkup: Ignoring link event during boot sequence.
done.
Checking config backups consistency.....done.
Setting up extended sysctls...done.
Setting timezone...done.
Configuring loopback interface...done.
Starting syslog...done.
Setting up interfaces microcode...done.
Configuring loopback interface...done.
Configuring WAN interface...done.
Configuring LAN interface...done.
Configuring OPT1 interface...done.
Configuring CARP settings...done.
Syncing OpenVPN settings...done.
Configuring firewall.....█
```

Une fois le démarrage fini, on obtiendra ceci (Configuration qu'on doit obtenir à la fin des configurations de nos interfaces) :

```
FreeBSD/amd64 (pfSense_master.home.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: af7ce57b641007832313

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

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.231.128/24
LAN (lan)      -> em1      -> v4: 10.0.50.4/24
OPT1 (opt1)    -> em2      -> v4: 172.16.0.1/30

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: █
```

⚠ Important : Le clavier est par défaut en qwerty !

Pour la configuration de nos interfaces on sélectionne option 2 « **Set interface(s) IP address** »

```
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator passwd
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
```

On me demande quelle interface je souhaite configurer (2 – LAN).

```
Available interfaces:

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

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

Em0 -> Network Adapter

Em1 -> Network Adapter 2 (10.0.50.0)

Em2 -> Network Adapter 3 (172.16.0.1-2)

qu'on va l'attribuer manuellement, on sélectionne « n » pour répondre Non et on appuie sur Entrée.

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

Ensuite on saisit l'adresse IP qu'on souhaite attribuer à cette interface qui sera la passerelle de sortie de notre réseau local (LAN). Une fois l'adresse IP saisie on appuie sur Entrée pour passer à la suite.

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.0.50.4 █
```

On définit le masque du sous-réseau en notation CIDR, 24 pour notre infrastructure.

⚠ Important : Tout dépend du nombre d'IP qu'on souhaite, en sélectionnant /24, j'ai 256 IP dont $256 - 2 = 254$ hôtes (Réseau – Broadcast). $2^8 - 2 = 254$

Défini par le « Calcul de sous-réseaux »

```
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
```

On nous demande ensuite si le réseau dispose d'une passerelle vers laquelle renvoyer les flux. Ce n'est notre cas, l'interface WAN fait déjà son travail et je n'ai pas d'autre routeur dans mon réseau donc j'appuie sur Entrée pour laisser vide « none ».

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

Je ne souhaite pas configurer d'adresse en IPv6, je réponds donc « n »

```
Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>
```

On souhaite activer le DHCP pour le réseau local donc on saisit « y » pour répondre Oui puis Entrée.

INFORMATION : Le service DHCP peut être activé et configuré plus simplement via l'interface WEB.

```
Do you want to enable the DHCP server on LAN? (y/n) y
```

On nous demande à partir de quand commence l'adressage IP : 10.0.50.10

Puis Quand elle se termine : 10.0.50.30

```
Enter the start address of the IPv4 client address range: 10.0.50.10
Enter the end address of the IPv4 client address range: 10.0.50.30
```

On se rend sur nos machine client (Windows ou Linux) :

Windows :

On tape simultanément sur les touches Windows+R puis on saisit « cmd » et sélectionne Entrée

Taper la commande « ipconfig »

```
C:\Users\CLIENTMK>ipconfig

Configuration IP de Windows

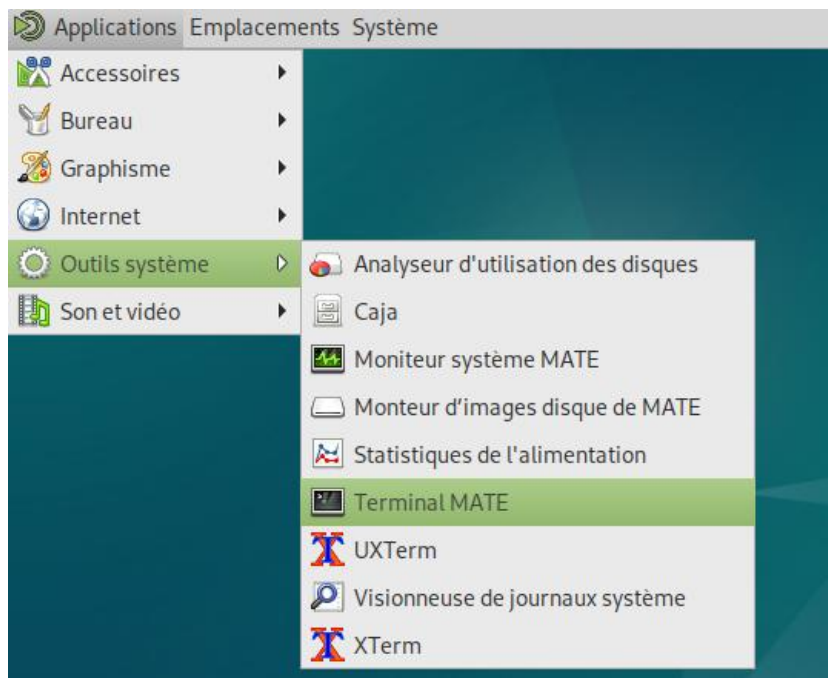
Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . : home.arpa
    Adresse IPv6 de liaison locale. . . . : fe80::fc36:71df:da75:9f04%14
    Adresse IPv4. . . . . : 10.0.50.18
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 10.0.50.4

C:\Users\CLIENTMK>
```

On obtient bien une adresse IP !

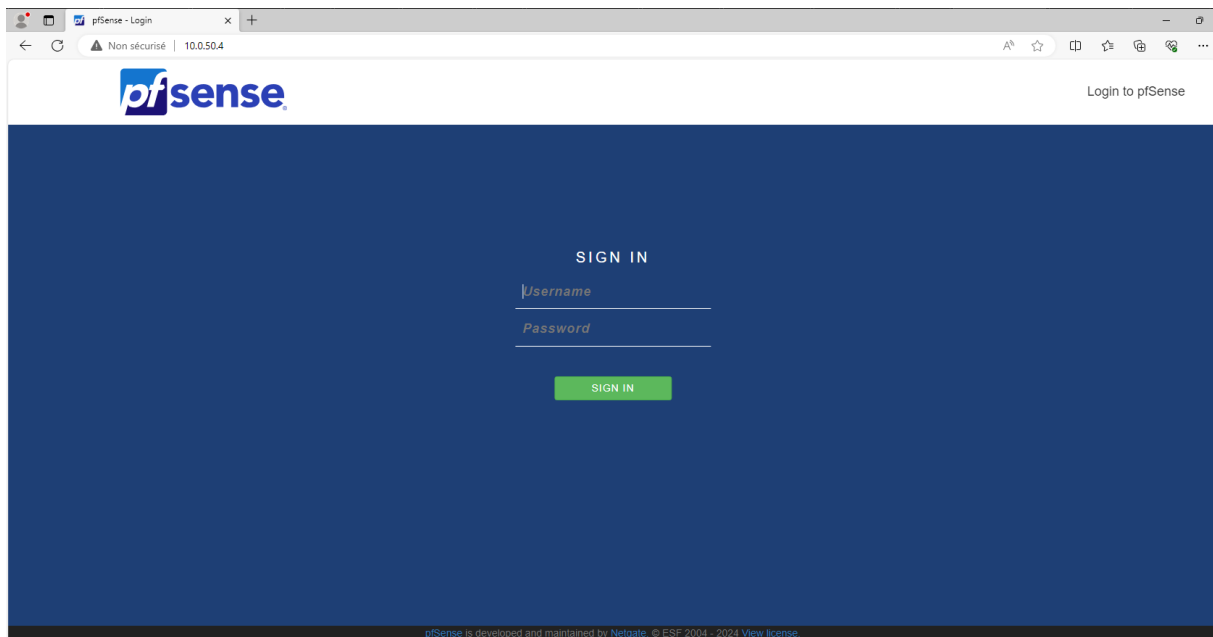
Linux :



Puis arriver sur le terminal on saisit « ip a »

```
root@debian:~# 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 noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:d7:2e:41 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 10.0.50.16/24 brd 10.0.50.255 scope global dynamic noprefixroute ens33
        valid_lft 7144sec preferred_lft 7144sec
    inet6 fe80::20c:29ff:fed7:2e41/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@debian:~#
```

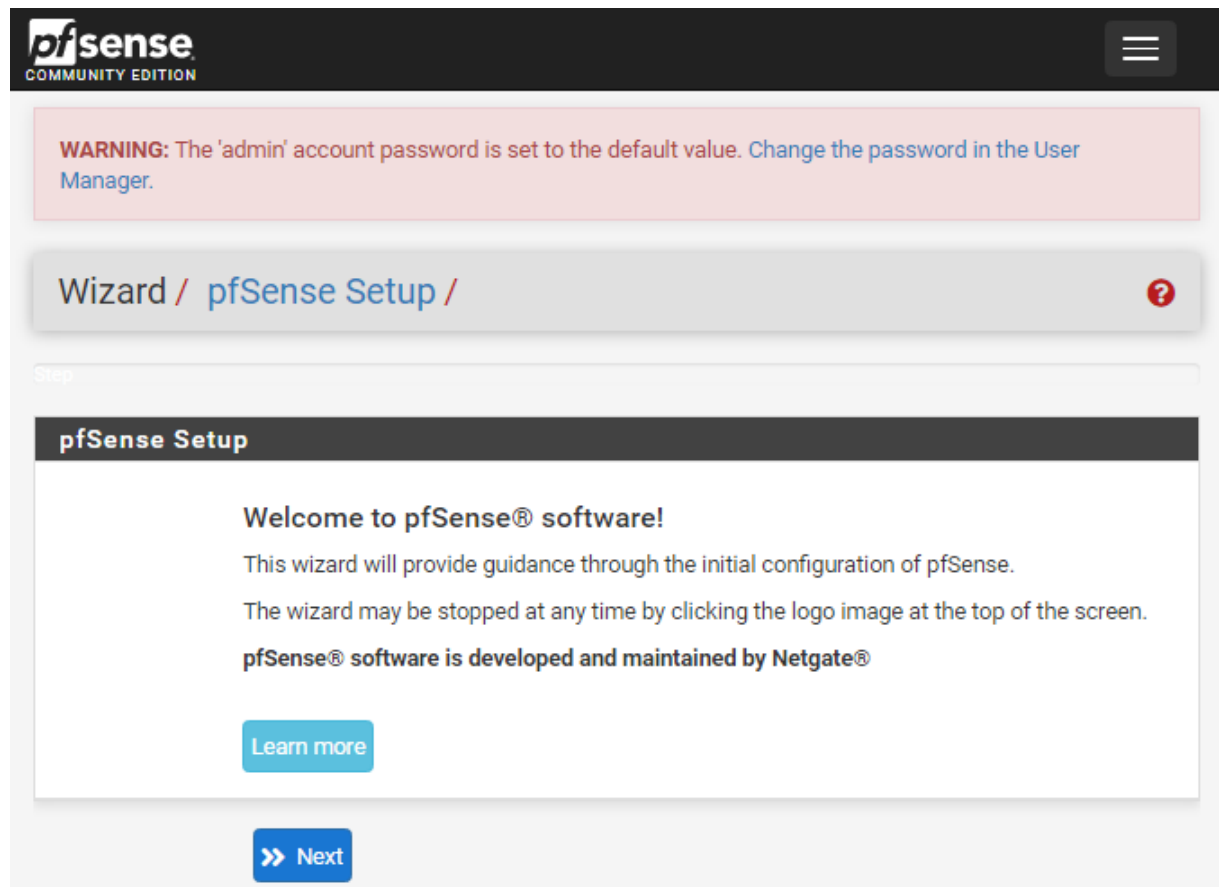
On ouvre le navigateur internet et saisi l'IP donner précédemment pour accéder à notre pfsense.



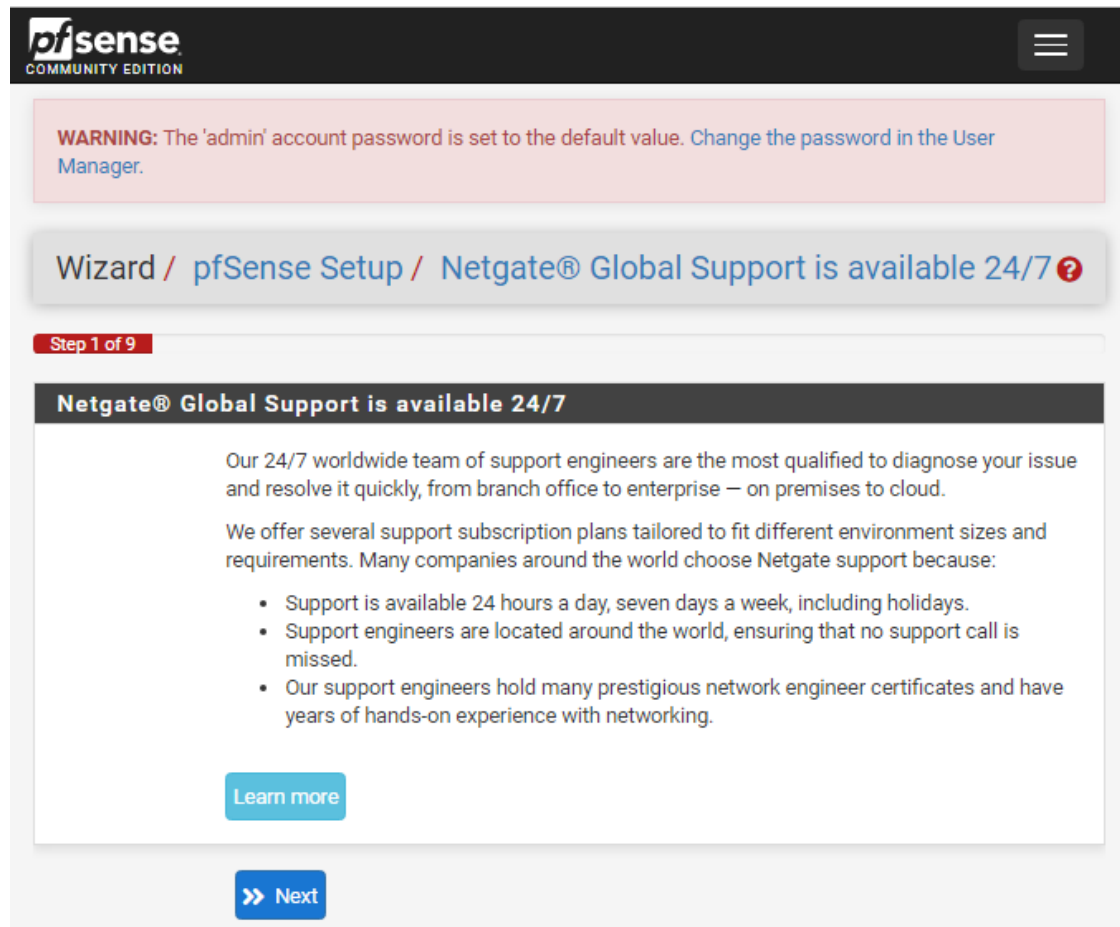
Les identifiants par défaut de pfsense sont les suivants :

- Login : admin
- Mot de passe : pfsense

On arrive sur l'assistant de configuration de pfSense qui va nous permettre de finaliser l'installation de notre firewall.



L'Assistant nous informe qu'il est possible d'avoir un support technique sous condition de souscrire à un contrat (💰) Sélectionner « Next »



The screenshot shows the pfSense Setup Wizard interface. At the top, the pfSense logo and 'COMMUNITY EDITION' are visible. A warning message states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below this, the breadcrumb trail reads: 'Wizard / pfSense Setup / Netgate® Global Support is available 24/7'. The current step is 'Step 1 of 9'. The main heading is 'Netgate® Global Support is available 24/7'. The text describes the 24/7 worldwide support team and lists three reasons why many companies choose Netgate support: 24/7 availability, global support engineers, and experienced network engineers. A 'Learn more' button is present. At the bottom, there is a 'Next' button with a double arrow icon.

pfSense
COMMUNITY EDITION

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

Wizard / pfSense Setup / Netgate® Global Support is available 24/7 ?

Step 1 of 9

Netgate® Global Support is available 24/7

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise — on premises to cloud.

We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.

[Learn more](#)

» Next

On peut choisir le nom du firewall et déclarer notre nom de Domain si on en possède un dans notre réseau. On peut également déclarer un serveur DNS local.

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname
 Name of the firewall host, without domain part.
 Examples: pfsense, firewall, edgefw

Domain
 Domain name for the firewall.
 Examples: home.arpa, example.com

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.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and 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](#)

1.1.1.1 - DNS de CloudFlare

8.8.8.8 - DNS de Google

Choisissez « **Europe/Paris** » dans la **Timezone** et on poursuit.

The screenshot shows the pfSense Setup Wizard interface. At the top, the pfSense logo and 'COMMUNITY EDITION' are visible. The breadcrumb trail reads 'Wizard / pfSense Setup / Time Server Information'. A progress bar indicates 'Step 3 of 9'. The main section is titled 'Time Server Information' and contains the instruction 'Please enter the time, date and time zone.' Below this, there are two input fields: 'Time server hostname' with the value '2.pfsense.pool.ntp.org' and a sub-instruction 'Enter the hostname (FQDN) of the time server.', and 'Timezone' with a dropdown menu showing 'Europe/Paris'. A blue 'Next' button is at the bottom.

pfSense
COMMUNITY EDITION

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname: 2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.

Timezone: Europe/Paris

Next

Ensuite nous arrivons à la configuration de l'interface WAN. Elle est configurée automatiquement par DHCP, je n'y touche pas.

Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType: DHCP

General configuration

MAC Address

 This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xxxxxxxx:xxxx:xxxx or leave blank.

MTU

 Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS

 If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Si on a besoin d'attribuer une IP fixe à cette interface WAN, c'est dans cette partie que ça se définit, sinon, on continue.

Static IP Configuration

IP Address

Subnet Mask
32

Upstream Gateway

DHCP client configuration

DHCP Hostname

 The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

La partie « **PPPoE configuration** » sert en général à mettre les **identifiants fournis par votre FAI**. Ce sont ces identifiants qui sont définis dans votre box internet actuellement. Si vous souhaitez placer un firewall à la place de la box, il sera nécessaire de remplir cette partie.

PPPoE configuration	
PPPoE Username	
PPPoE Password	
Show PPPoE password	☐ Reveal password characters
PPPoE Service name	 Hint: this field can usually be left empty
PPPoE Dial on demand	☐ Enable Dial-On-Demand mode This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.
PPPoE Idle timeout	 If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

La partie suivante « **PPTP configuration** » servira plutôt au **montage d'un VPN point à point** (*Protocole de tunnel point-à-point, à éviter car peu sécurisé, plutôt privilégier son petit frère IPSEC*).

PPTP configuration	
PPTP Username	
PPTP Password	
Show PPTP password	☐ Reveal password characters
PPTP Local IP Address	
pptplocalsubnet	32 ▼
PPTP Remote IP Address	
PPTP Dial on demand	☐ Enable Dial-On-Demand mode This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.
PPTP Idle timeout	 If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

Les deux dernières options de cette page définissent que tout trafic entrant sur l'interface WAN et venant d'une classe d'adresse réseau privé est automatiquement bloqué. **Comme notre infra est ici virtuelle, on veut obligatoirement faire communiquer des réseaux privés, on n'utilise pas réellement une adresse publique.** Il est **donc nécessaire dans le cadre d'un labo de décocher ces 2 cases** sinon on peut avoir des petits soucis (;).

RFC1918 Networks

Block RFC1918 Private Networks

☐ Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks

☐ Block non-Internet routed networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

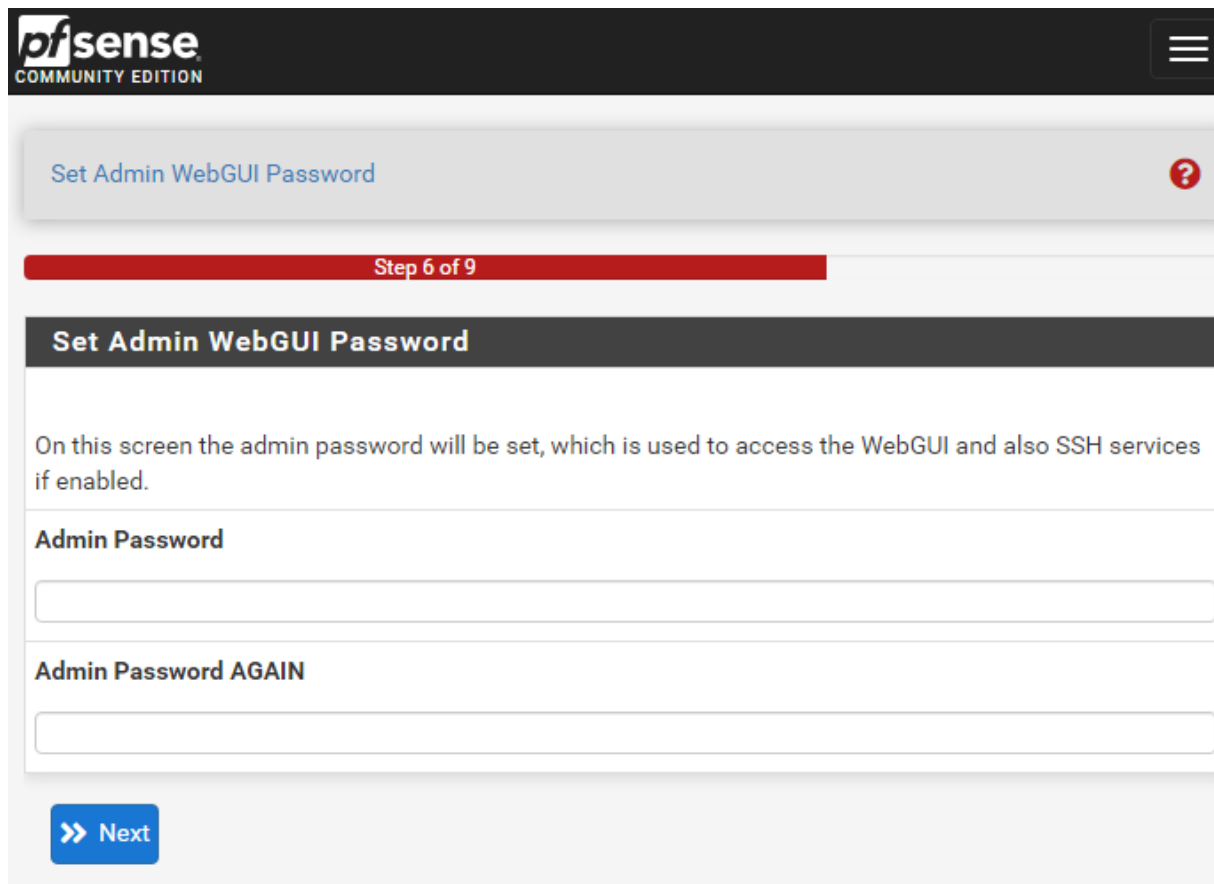
>> Next

Nous n'avons donc rien modifier de spécial sur notre interface WAN ici, vous pouvez poursuivre.

L'assistant de pfsense passe donc cette fois-ci à l'**interface côté LAN**. Vous pouvez changer ici l'adresse IP de l'interface LAN de pfSense (*nous l'avons déjà fait en amont*).

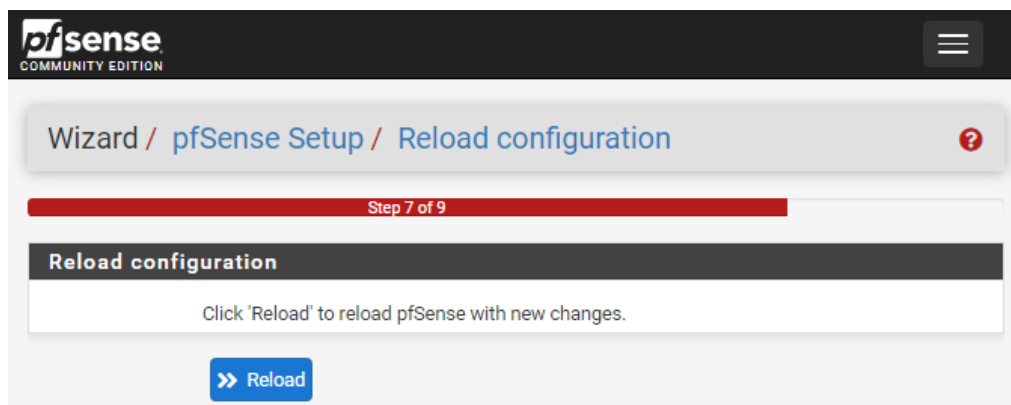
The screenshot shows the pfSense Community Edition web interface. At the top, there's a header with the pfSense logo and a menu icon. Below the header, a grey bar contains the text 'Configure LAN Interface' and a red question mark icon. A red progress bar indicates 'Step 5 of 9'. The main content area is titled 'Configure LAN Interface' and contains the following text: 'On this screen the Local Area Network information will be configured.' Below this, there are two sections: 'LAN IP Address' with a text input field containing '10.0.50.4' and a note 'Type dhcp if this interface uses DHCP to obtain its IP address.', and 'Subnet Mask' with a dropdown menu showing '24'. At the bottom left, there is a blue button with a double arrow and the text 'Next'.

Durant la phase de configuration, il est également nécessaire de changer les identifiants par défaut du compte admin de pfsense.



The screenshot shows the pfSense Community Edition WebGUI Setup Wizard at Step 6 of 9. The title bar at the top reads "Set Admin WebGUI Password" with a red question mark icon. Below the title bar is a red progress bar indicating "Step 6 of 9". The main heading is "Set Admin WebGUI Password". The text below the heading states: "On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled." There are two input fields: "Admin Password" and "Admin Password AGAIN". At the bottom left, there is a blue button with a double arrow and the text "Next".

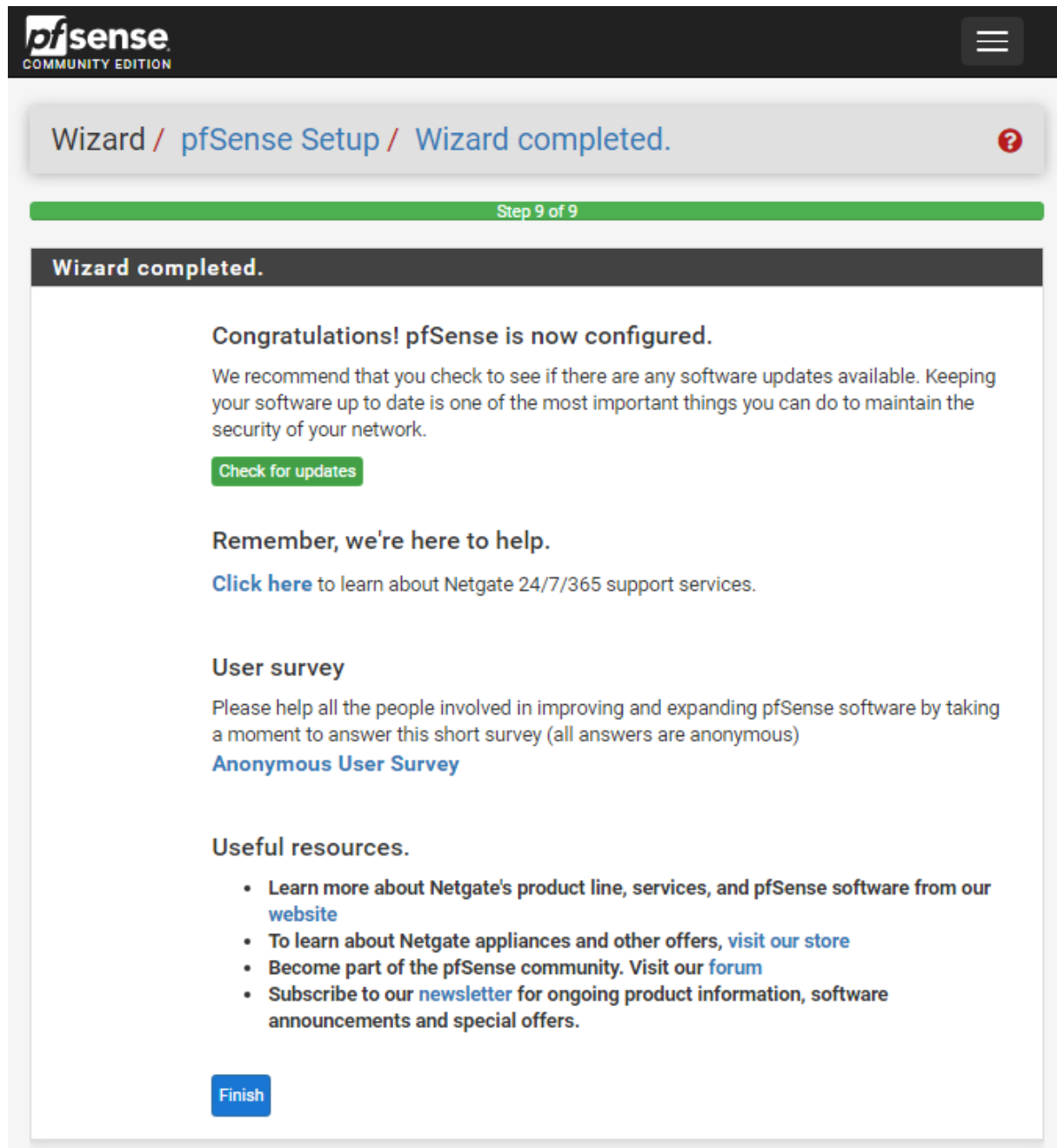
La phase finale de l'installation de pfsense est terminée. Cliquez sur **Reload** pour recharger pfsense.



The screenshot shows the pfSense Community Edition WebGUI Setup Wizard at Step 7 of 9. The title bar at the top reads "Wizard / pfSense Setup / Reload configuration" with a red question mark icon. Below the title bar is a red progress bar indicating "Step 7 of 9". The main heading is "Reload configuration". The text below the heading states: "Click 'Reload' to reload pfSense with new changes." At the bottom left, there is a blue button with a double arrow and the text "Reload".

Patientez quelques secondes, la page va se recharger d'elle-même.

A la fenêtre suivante, cliquez sur le bouton **Finish**.



The screenshot shows the pfSense Setup Wizard completion screen. At the top, the pfSense logo and 'COMMUNITY EDITION' are visible. The breadcrumb trail reads 'Wizard / pfSense Setup / Wizard completed.' with a help icon. A green progress bar indicates 'Step 9 of 9'. The main heading is 'Wizard completed.' followed by a congratulatory message: 'Congratulations! pfSense is now configured.' Below this, a recommendation to check for updates is shown with a 'Check for updates' button. A reminder to seek help is followed by a link to Netgate support services. A 'User survey' section encourages participation in an 'Anonymous User Survey'. A 'Useful resources' section lists links to the website, store, forum, and newsletter. A 'Finish' button is located at the bottom left.

pfSense
COMMUNITY EDITION

Wizard / pfSense Setup / Wizard completed. ?

Step 9 of 9

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

[Anonymous User Survey](#)

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

[Finish](#)

Cliquez sur le bouton « **Accept** » pour valider les points législatifs divers.

Copyright and Trademark Notices.

Copyright© 2004-2016. Electric Sheep Fencing, LLC ("ESF"). All Rights Reserved.

Copyright© 2014-2023. Rubicon Communications, LLC d/b/a Netgate ("Netgate"). All Rights Reserved.

All logos, text, and content of ESF and/or Netgate, including underlying HTML code, designs, and graphics used and/or depicted herein are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of ESF and/or Netgate.

"pfSense" is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All other trademarks shown herein are owned by the respective companies or persons indicated.

pfSense® software is open source and distributed under the Apache 2.0 license. However, no commercial distribution of ESF and/or Netgate software is allowed without the prior written consent of ESF and/or Netgate.

ESF and/or Netgate make no warranty of any kind, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. ESF and/or Netgate shall not be liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of any software, information, or material.

Restricted Rights Legend.

No part of ESF and/or Netgate's information or materials may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of ESF and/or Netgate. The information contained herein is subject to change without notice.

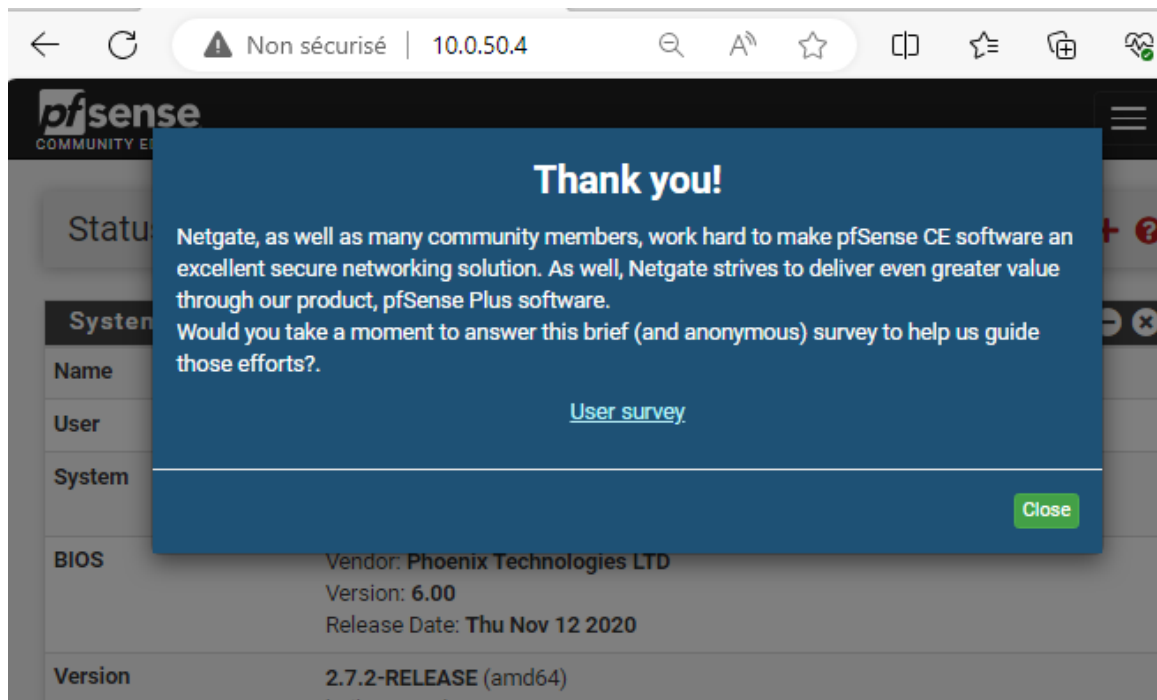
Use, duplication or disclosure by the U.S. Government may be subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance.

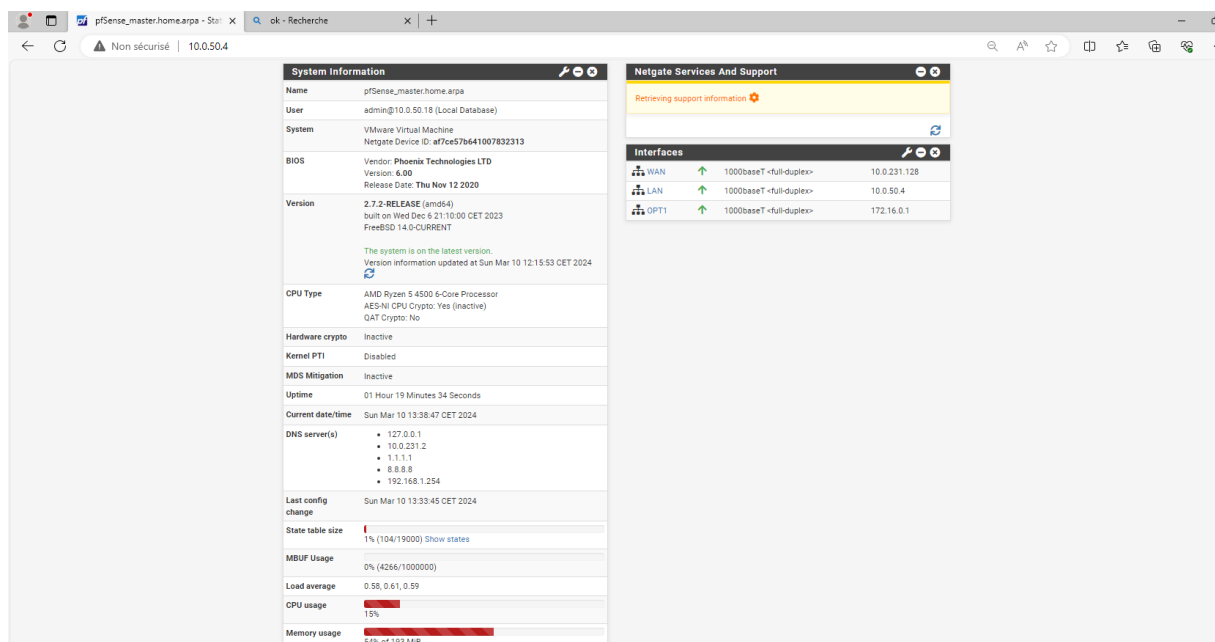
The export and re-export of software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, Licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government's Enemies List; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that Licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Accept

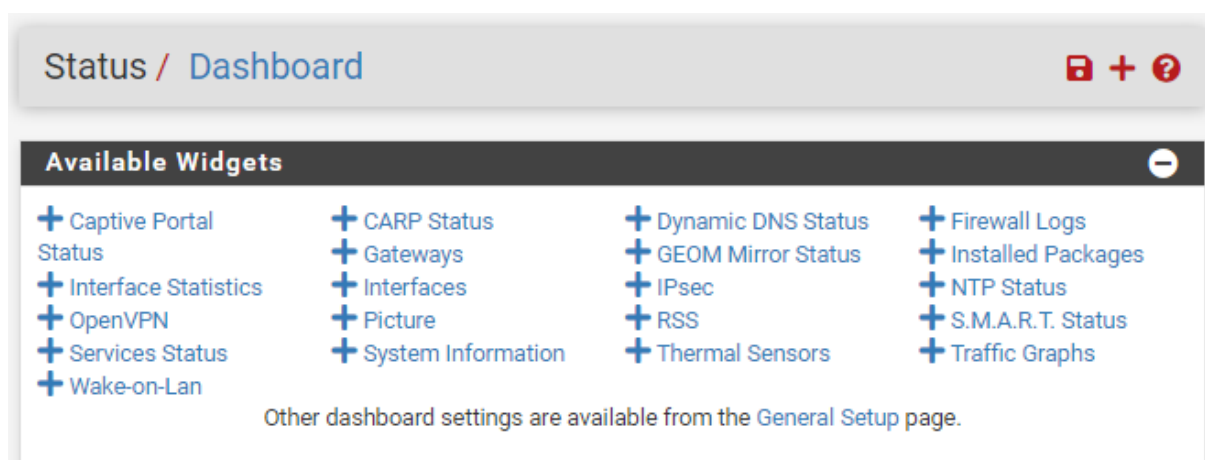
On nous demande si on souhaite répondre à un sondage, on clique sur close.



On arrive sur le tableau de bord de notre pfSense. Où on retrouvera les infos sur l'utilisation des ressources de la machine elle-même, ses différentes adresses IP, version & mises à jour.



Cette **vue est personnalisable** est cliquant sur le **petit + en haut à droite** dans la barre de titre.



2) Service Requis

1.1 Configuration du DHCP serveur :

Pour configurer le DHCP via l'interface WEB, on se rend dans l'**onglet Services -> DHCP Server**

General DHCP Options	
DHCP Backend	ISC DHCP
Enable	☒ Enable DHCP server on LAN interface
BOOTP	☐ Ignore BOOTP queries
Deny Unknown Clients	Allow all clients When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied Clients	☐ Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers	☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Primary Address Pool	
Subnet	10.0.50.0/24
Subnet Range	10.0.50.1 - 10.0.50.254
Address Pool Range	10.0.50.13 10.0.50.245 From To The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools	+ Add Address Pool If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

On active le DHCP

On saisi à partir de quand commence notre @IP et jusqu'à où elle s'arrête.

⚠ Important : N'oublier pas de Cliquer sur « Save » !

1.2 Configuration du DNS serveur :

Pour configurer le DNS, on se rend dans l'onglet **Services -> DNS Resolver -> General Settings**

General DNS Resolver Options

Enable ☒ Enable DNS resolver

Listen Port 53
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

Enable SSL/TLS Service ☐ Respond to incoming SSL/TLS queries from local clients
Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.

SSL/TLS Certificate GUI default (65df33284a307)
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

SSL/TLS Listen Port 853
The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.

Network Interfaces
All
WAN
LAN
OPT1
Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.

Outgoing Network Interfaces
All
WAN
LAN
OPT1
Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.

Strict Outgoing Network Interface Binding ☐ Do not send recursive queries if none of the selected Outgoing Network Interfaces are available.
By default the DNS Resolver sends recursive DNS requests over any available interfaces if none of the selected Outgoing Network Interfaces are available. This option makes the DNS Resolver refuse recursive queries.

System Domain Local Zone Type Transparent
The local-zone type used for the pfSense system domain (System | General Setup | Domain). Transparent is the default.

On active le *DNS Resolver

Par défaut, Le DNS Resolver s'applique à toutes les interfaces.

On n'y touche pas dans notre cas.

« SAVE »

Définition DNS RESOLVER : Les résolveurs DNS sont un composant essentiel du Domain Name System (DNS). Ils agissent en tant que contrepartie interrogative aux serveurs de noms DNS qui leur répondent. Du point de vue de l'utilisateur, un DNS resolver sert d'interface de transmission entre l'utilisateur ou l'application et les serveurs de noms.

3) Activer le DNS Forwarder

Le DNS forwarder de pfSense permet de résoudre les requêtes DNS des clients DHCP (mappés ou non) ainsi que des entrées DNS saisies manuellement. Le DNS forwarder permet également de renvoyer les requêtes DNS des clients pour un domaine particulier.

On se rend sur **Services -> DNS Forwarder**

General DNS Forwarder Options

Enable ☒ **Enable DNS forwarder** ← On active le DNS Forwarder

DHCP Registration ☒ **Register DHCP leases in DNS forwarder**
If this option is set machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. The domain in **System: General Setup** should also be set to the proper value.

Static DHCP ☒ **Register DHCP static mappings in DNS forwarder**
If this option is set, IPv4 DHCP static mappings will be registered in the DNS forwarder so that their name can be resolved. The domain in **System: General Setup** should also be set to the proper value.

Prefer DHCP ☐ **Resolve DHCP mappings first**
If this option is set DHCP mappings will be resolved before the manual list of names below. This only affects reverse lookups (PTR).

DNS Query Forwarding

☐ **Query DNS servers sequentially**
If this option is set pfSense DNS Forwarder (dnsmasq) will query the DNS servers sequentially in the order specified (**System - General Setup - DNS Servers**), rather than all at once in parallel.

☐ **Require domain**
If this option is set pfSense DNS Forwarder (dnsmasq) will not forward A or AAAA queries for plain names, without dots or domain parts, to upstream name servers. If the name is not known from /etc/hosts or DHCP then a "not found" answer is returned.

☐ **Do not forward private network lookups**
If this option is set pfSense DNS Forwarder (dnsmasq) will not forward reverse DNS lookups (PTR) for private addresses (RFC 1918) to upstream name servers. Any entries in the Domain Overrides section forwarding private "n.n.n.in-addr.arpa" names to a specific server are still forwarded. If the IP to name is not known from /etc/hosts, DHCP or a specific domain override then a "not found" answer is immediately returned.

Listen Port
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

Interfaces
Interface IPs used by the DNS Forwarder for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected above are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.

On « DHCP Registration » qui active toutes les correspondances adresses MAC - adresses IP présentes dans la configuration du service DHCP seront joignables directement par le service DNS Forwarder.

4) Configuration générale

1.1) Les Alias

Les alias définissent un groupe de ports, d'hôtes ou de réseaux. Les alias peuvent être référencés par des règles de pare-feu, des transferts de port, des règles NAT sortantes et d'autres endroits du pare-feu. L'utilisation d'alias donne lieu à des ensembles de règles nettement plus courts, auto-documentés et plus gérables.

On se rend dans Firewall > Aliases

Name	Type	Values	Description	Actions
CLT_LAN1	Host(s)	10.0.50.0, 10.0.50.1, 10.0.50.2, 10.0.50.3, 10.0.50.4, 10.0.50.5, 10.0.50.6, 10.0.50.7, 10.0.50.8, 10.0.50.9...		[Edit] [Copy] [Delete]
SLAVE_PFsense	Host(s)	172.16.0.2		[Edit] [Copy] [Delete]
YOUTUBE_BLOQUER	Network(s)	172.217.18.206/32, www.youtube.com		[Edit] [Copy] [Delete]

On voit les Aliases que j'ai configuré.

Pour Ajouter un Alias, on procède comme ceci :

- On clique sur **+ADD**

Firewall / Aliases / Edit

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 

Host(s)

Hint Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN

Le type si c'est un hôte ou réseau, port, URL..

Définition FQDN (Full Qualifed Domain Name) : désigne l'adresse complète et unique d'un site Internet.

Exemple : <https://btssio.org>.

1.2) Création d'une règle de FireWall

On se rend dans **FireWall -> Rules** puis on sélectionne l'interfaces (WAN, LAN, OPT1)

Puis **↑ADD** pour ajouter une règle.

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
 ☐ Invert match /
 [Display Advanced](#)
 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
 ☐ Invert match /
 Destination Port Range
 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
 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](#)
 [Save](#)

Action :
Bloquer,Autoriser,Refuser

Interface LAN,WAN,OPT1

IPv4/IPv6 ou IPv4+IPv6

Protocol TCP,UDP,ICMP.. ou
Tous

La source -> ex : LAN

La Destination -> ex : @IP
d'un serveur
d'administration.

1.3) Configuration de CARP

Le protocole CARP (Common Address Redundancy Protocol) permet à plusieurs équipements réseaux de partager une même adresse IP. C'est une alternative libre au protocole propriétaire HSRP de CISCO, par exemple. Les machines partageant cette IP font parties du groupe de redondance. On y trouve un équipement « maitre » et les autres « esclaves ». Ces derniers sont destinés à prendre le relais en cas de défaillance du premier équipement.

Dans notre cas, nous allons utiliser CARP pour créer un routeur / pare-feu redondant, avec serveurs DNS + DHCP. Nos clients prendront l'IP virtuelle comme passerelle par défaut. Ainsi, en cas de panne de notre routeur principal, le second répondra aux requêtes de nos clients en toute transparence et sans coupures.

Nous avons laissé une interface disponible «Network Adapter 3 »

Pour la configurer, il suffit d'aller dans **Interfaces -> Assign**

Interfaces / Interface Assignments

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

Interface	Network port	
WAN	em0 (00:0c:29:bf:ea:73)	
LAN	em1 (00:0c:29:bf:ea:7d)	Delete
OPT1	em2 (00:0c:29:bf:ea:87)	Delete

Save

On clique sur « OPT1 »

Interfaces / OPT1 (em2)

General Configuration

Enable ☒ Enable interface ← Activation de l'interface

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

IPv4 Configuration Type ← Static, DHCP, PPP, PPPoE, PPTP ou L2TP.

IPv6 Configuration Type

MAC Address
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
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 /

IPv4 Upstream gateway + 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.

Le choix du CIDR /30 est une question de bonnes pratiques et de sécurité, On sait qu'on doit lier 2 servers (Master & SLAVE) via CARP donc 2 IP alors il suffit de faire le calcul $2^n > @IP$.

$$(2^{32} - 30) - 2 = 2 \text{ IP}$$

172.16.0.1 = Serveur Maître

172.16.0.2 = Serveur Slave

Ensuite, sur le serveur Maître nous, devons lui indiquer une règle de firewall autorisant le trafics sur l'interface CARP.

FireWall -> Rules -> CARP, puis on insère la règle suivante :

Firewall / Rules / OPT1

Floating WAN LAN **OPT1**

Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	✓	0/0 B	IPv4 *	OPT1 address	*	OPT1 address	*	*	none		

Add Add Delete Toggle Copy Save Separator

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 /

Destination

Destination ☐ Invert match /

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
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](#)

Rule Information

Tracking ID	1709729403
Created	3/6/24 13:50:03 by admin@10.0.50.15 (Local Database)
Updated	3/6/24 13:50:28 by admin@10.0.50.15 (Local Database)

Save

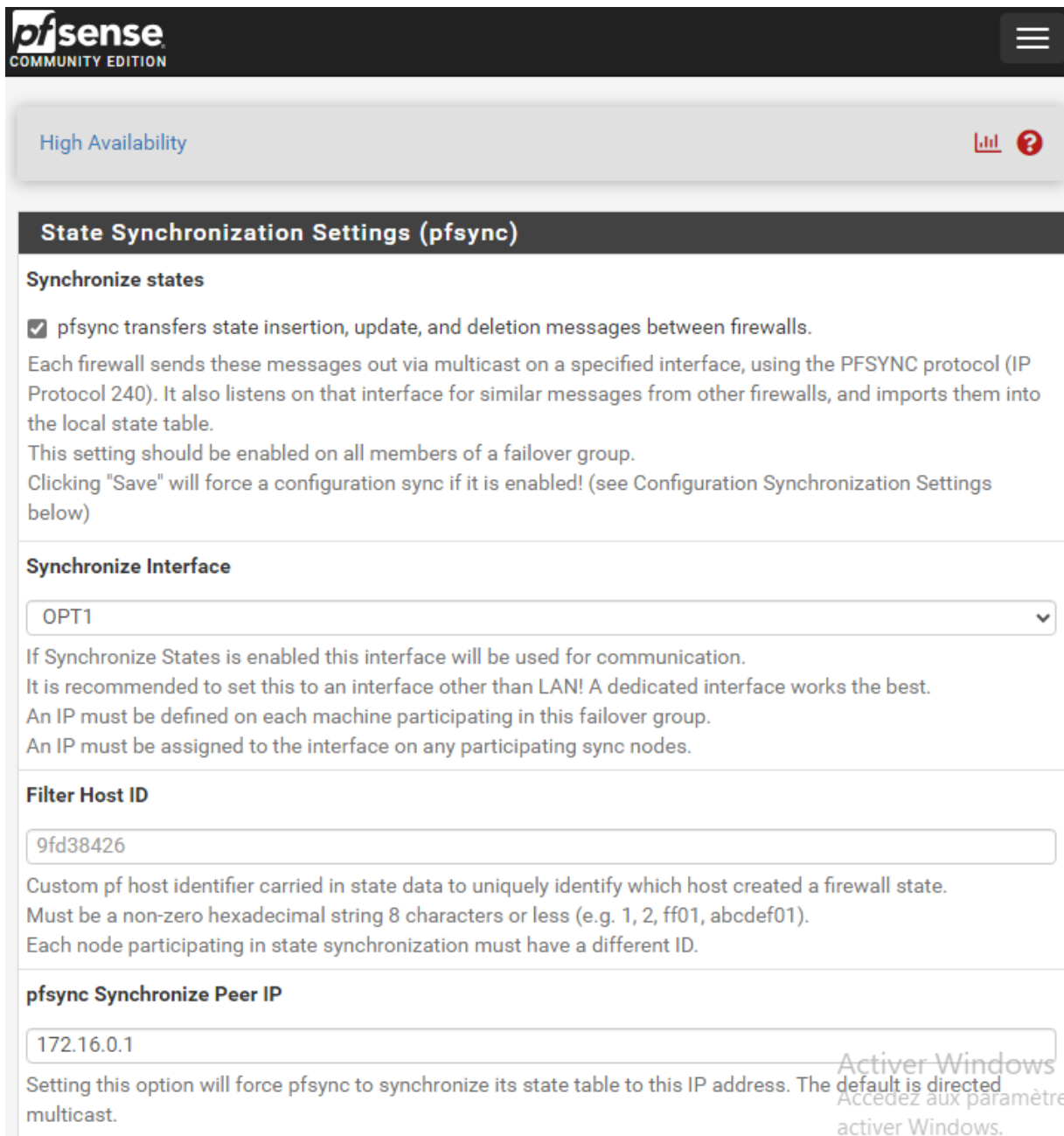
Ensuite nous allons activer la réplication entre les deux routeurs.

On va dans **System -> High Availability Sync**.

Sur le pfSense maître, On configure la partie pfsync en choisissant l'interface CARP, et l'@IP de notre pfSense Slave (172.16.0.2) dans notre cas, Puis dans la partie XMLRPC Sync), on saisit l'IP et Login de notre slave ainsi que la configuration à répliquer. Il est conseillé de cocher toutes les cases pour éviter tout problème.

State Synchronization Settings (pfsync)	
Synchronize states	☒ pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking 'Save' will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)
Synchronize Interface	OPT1 If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN. A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.
Filter Host ID	07832313 Custom of host identifier carried in state data to uniquely identify which host created a firewall state. Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcd01). Each node participating in state synchronization must have a different ID.
pfsync Synchronize Peer IP	172.16.0.2 Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.
Configuration Synchronization Settings (XMLRPC Sync)	
Synchronize Config to IP	172.16.0.2 Enter the IP address of the firewall to which the selected configuration sections should be synchronized. XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly! Do not use the Synchronize Config to IP and password option on backup cluster members!
Remote System Username	admin Enter the webConfigurator username of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and username option on backup cluster members!
Remote System Password	 Enter the webConfigurator password of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and password option on backup cluster members! Confirm
Synchronize admin	☐ synchronize admin accounts and autoupdate sync password. By default, the admin account does not synchronize, and each node may have a different admin password. This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.
Select options to sync	☒ User manager users and groups ☒ Authentication servers (e.g. LDAP, RADIUS) ☒ Certificate Authorities, Certificates, and Certificate Revocation Lists ☒ Firewall rules ☒ Firewall schedules ☒ Firewall aliases ☒ NAT configuration ☒ IPsec configuration ☒ OpenVPN configuration (Implies CA/Cert/URL Sync) ☒ DHCP Server settings ☒ DHCP Relay settings ☒ DHCPv6 Relay settings ☒ WoL Server settings ☒ Static Route configuration ☒ Virtual IPs ☒ Traffic Shaper configuration ☒ Traffic Shaper Limiters configuration ☒ DNS Forwarder and DNS Resolver configurations ☒ Captive Portal ☒ Toggle All
Save	

On va sur l'interface de notre pfSense Slave, cette fois-ci **seulement** la partie pfsync est à configurer :



pfSense
COMMUNITY EDITION

High Availability  

State Synchronization Settings (pfsync)

Synchronize states

☒ pfsync transfers state insertion, update, and deletion messages between firewalls.

Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.

This setting should be enabled on all members of a failover group.

Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface

OPT1 

If Synchronize States is enabled this interface will be used for communication.

It is recommended to set this to an interface other than LAN! A dedicated interface works the best.

An IP must be defined on each machine participating in this failover group.

An IP must be assigned to the interface on any participating sync nodes.

Filter Host ID

9fd38426

Custom pf host identifier carried in state data to uniquely identify which host created a firewall state.

Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01).

Each node participating in state synchronization must have a different ID.

pfsync Synchronize Peer IP

172.16.0.1

Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Dans Firewall / Virtual IPs on déclare cette nouvelle IP sur l'interface LAN.

Il est également possible de déclarer une IP pour le WAN ou une éventuelle DMZ. Il faudra simplement changer le VHID Group qui est à 1 par défaut.

Firewall / Virtual IPs				
Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
10.0.50.1/24 (vhid: 1)	LAN	CARP	IP Virtuelle LAN	 
10.0.231.127/24 (vhid: 2)	WAN	CARP	WAN1	 

 Add

Configuration de l'IP virtuelle LAN :

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type ☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface

Address type

Address(es) /
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password
Enter the VHID group password. Confirm

VHID Group
Enter the VHID group that the machines will share.

Advertising frequency
Base Skew

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

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

 Save

Enfin, il faut modifier notre serveur DHCP du LAN pour déclarer cette IP en tant que passerelle par défaut.



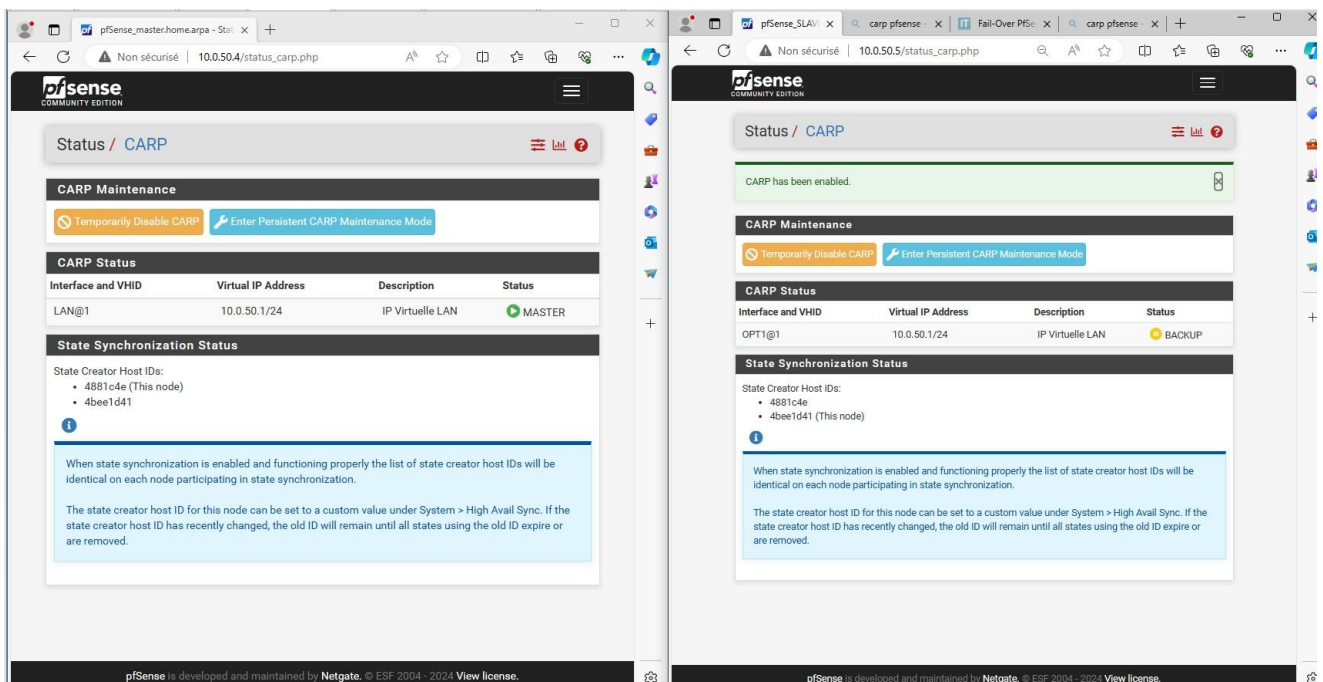
Other Options

Gateway

The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.

5) Synchronisation des Interfaces et Test de basculement

Nous allons commencer par vérifier l'état de la synchronisation entre nos deux servers pfSense Master et pfSense Slave.



En prenant un client du LAN, nous allons pinger la Gateway (ou une IP externe) et éteindre le pfSense Master principal.

On constate le moment de la bascule avec deux paquets dupliqués (les deux routeurs répondent à ce moment-là) ou une perte d'un paquet. Il n'y a pas eu d'interruption de service, et le second routeur est passé avec le statut MASTER.

Les services rebasculeront sur le routeur principal lorsqu'il sera de nouveau opérationnel.

```
C:\Users\CLIENTMK>ping 10.0.50.1 -t

Envoi d'une requête 'Ping' 10.0.50.1 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.0.50.1:
    Paquets : envoyés = 15, reçus = 13, perdus = 2 (perte 13%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

```
Microsoft Windows [version 10.0.19045.2006]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\CLIENTMK>ping 8.8.8.8 -t

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=7 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Réponse de 10.0.50.18 : Impossible de joindre l'hôte de destination.
Réponse de 10.0.50.18 : Impossible de joindre l'hôte de destination.
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 19, reçus = 16, perdus = 3 (perte 15%),
Durée approximative des boucles en millisecondes :
    Minimum = 7ms, Maximum = 9ms, Moyenne = 8ms
```

```
Configuration IP de Windows
```

```
Carte Ethernet Ethernet0 :
```

```
Suffixe DNS propre à la connexion. . . : home.arpa
Adresse IPv6 de liaison locale. . . . : fe80::fc36:71df:da75:9f04%14
Adresse IPv4. . . . . : 10.0.50.18
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 10.0.50.4
```

```
Carte Ethernet Connexion réseau Bluetooth :
```

```
Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . :
```

```
C:\Users\CLIENTMK>ipconfig
```

```
Configuration IP de Windows
```

```
Carte Ethernet Ethernet0 :
```

```
Suffixe DNS propre à la connexion. . . : home_slave.arpa
Adresse IPv6 de liaison locale. . . . : fe80::fc36:71df:da75:9f04%14
Adresse IPv4. . . . . : 10.0.50.18
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 10.0.50.1
```

```
Carte Ethernet Connexion réseau Bluetooth :
```

```
Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . :
```

BONUS

1.1/Bloquer YouTube

Pour bloquer un site, dans notre cas « YouTube », on va aller dans **Firewall -> Aliases -> Add**

Pour trouver son IP, il suffit de faire un ping de www.youtube.fr.

```

Terminal
Fichier Édition Affichage Recherche Terminal Aide
PING youtube.com (172.217.18.206) 56(84) bytes of data.
64 bytes from par10s38-in-f14.1e100.net (172.217.18.206): icmp_seq=1 ttl=110 time=20.7 ms
64 bytes from par10s38-in-f14.1e100.net (172.217.18.206): icmp_seq=2 ttl=110 time=20.5 ms
64 bytes from ham02s14-in-f206.1e100.net (172.217.18.206): icmp_seq=3 ttl=110 time=19.9 ms
64 bytes from ham02s14-in-f206.1e100.net (172.217.18.206): icmp_seq=4 ttl=110 time=20.6 ms
64 bytes from ham02s14-in-f206.1e100.net (172.217.18.206): icmp_seq=5 ttl=110 time=21.3 ms
64 bytes from par10s38-in-f14.1e100.net (172.217.18.206): icmp_seq=6 ttl=110 time=20.5 ms
64 bytes from par10s38-in-f14.1e100.net (172.217.18.206): icmp_seq=7 ttl=110 time=21.3 ms
64 bytes from ham02s14-in-f206.1e100.net (172.217.18.206): icmp_seq=8 ttl=110 time=21.1 ms
64 bytes from ham02s14-in-f206.1e100.net (172.217.18.206): icmp_seq=9 ttl=110 time=20.5 ms
^C

```

On connaît maintenant l'adresse @IP de YouTube.

On ajoute un site en tant qu'Alias, dans notre cas « YouTube », on va aller dans **Firewall -> Aliases -> Add**

On inclut le **FQDN**.

Firewall / Aliases / Edit

Properties

Name
BLOCK_YTB

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)

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 www.youtube.com / 32	Entry added Thu, 07 Mar 2024 21:20:03 +0000 Delete
142.250.200.238 / 32	Entry added Thu, 07 Mar 2024 21:20:03 +0000 Delete

Save
Export to file
Add Network

Firewall Aliases IP				
Name	Type	Values	Description	Actions
CLT_LAN1	Host(s)	10.0.50.0, 10.0.50.1, 10.0.50.2, 10.0.50.3, 10.0.50.4, 10.0.50.5, 10.0.50.6, 10.0.50.7, 10.0.50.8, 10.0.50.9...		  
SLAVE_PFsense	Host(s)	172.16.0.2		  
YOUTUBE_BLOQUER	Network(s)	172.217.18.206/32, www.youtube.com		  
 Add				

Nos Aliases avec
Notre réseau @IP,

Youtube

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 (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

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

Interface

LAN

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

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Address or Alias

CLT_LAN1

Destination

Destination

☐ Invert match

Address or Alias

YOUTUBE_BLOQUER

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

bloquer youtube site

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

Rule Information

Tracking ID

1709128905

Created

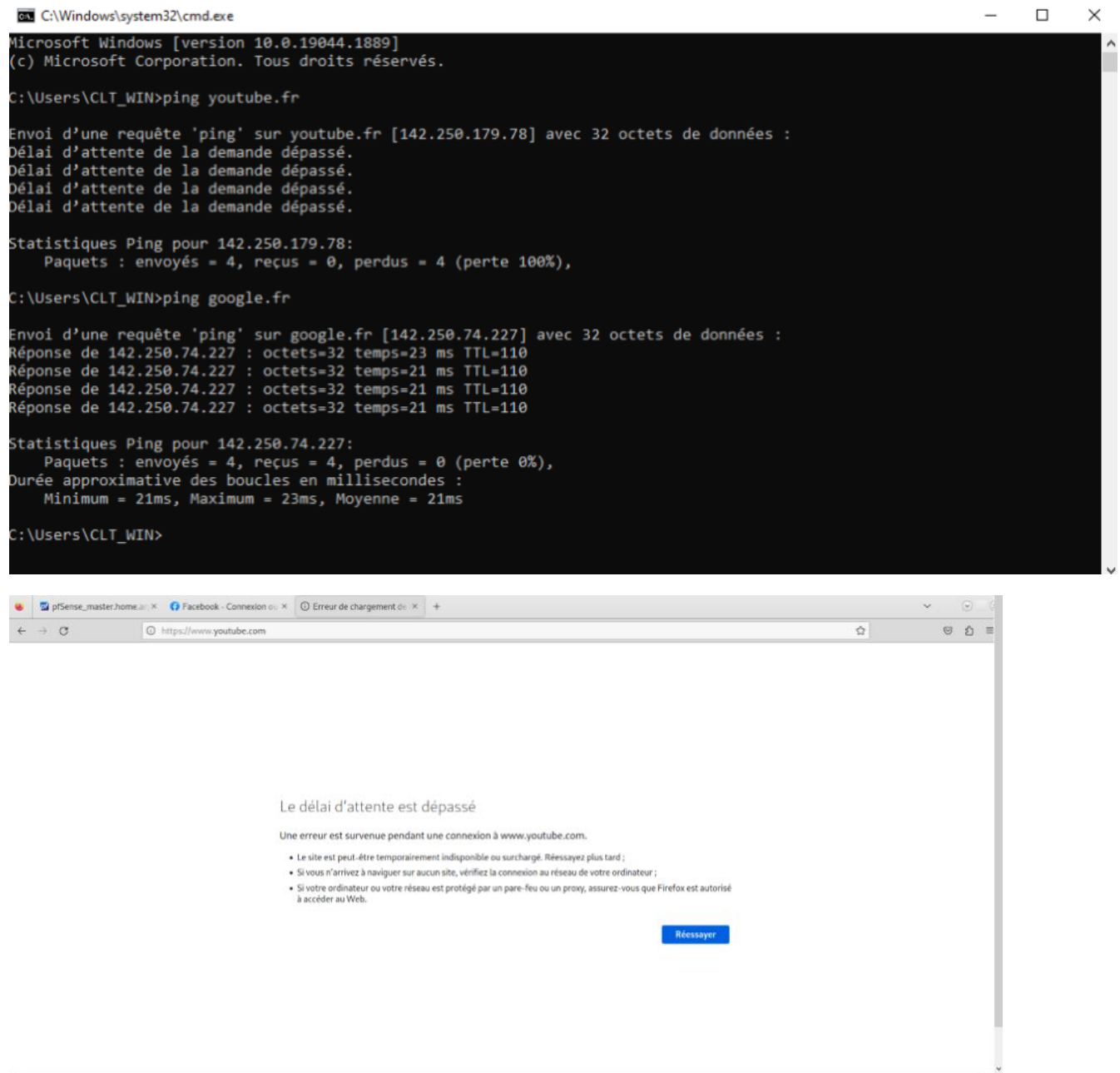
2/28/24 15:01:45 by admin@10.0.50.13 (Local Database)

Updated

3/7/24 21:30:45 by admin@10.0.50.18 (Local Database)

 Save

Test du blocage de YouTube



The image shows two screenshots. The top screenshot is a Windows command prompt window titled 'C:\Windows\system32\cmd.exe'. It displays the results of two ping commands. The first command is 'ping youtube.fr' with IP address [142.250.179.78], showing four timeouts. The second command is 'ping google.fr' with IP address [142.250.74.227], showing four successful responses with 21-23 ms latency. The bottom screenshot is a web browser window showing the YouTube homepage. The address bar displays 'https://www.youtube.com'. The page content shows a message: 'Le délai d'attente est dépassé' (The timeout has expired). Below this, it states 'Une erreur est survenue pendant une connexion à www.youtube.com.' and lists three possible causes: the site being temporarily unavailable, a network connection issue, or a firewall/proxy blocking access. A 'Réessayer' (Retry) button is visible at the bottom right of the error message.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.19044.1889]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\CLT_WIN>ping youtube.fr

Envoi d'une requête 'ping' sur youtube.fr [142.250.179.78] avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 142.250.179.78:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

C:\Users\CLT_WIN>ping google.fr

Envoi d'une requête 'ping' sur google.fr [142.250.74.227] avec 32 octets de données :
Réponse de 142.250.74.227 : octets=32 temps=23 ms TTL=110
Réponse de 142.250.74.227 : octets=32 temps=21 ms TTL=110
Réponse de 142.250.74.227 : octets=32 temps=21 ms TTL=110
Réponse de 142.250.74.227 : octets=32 temps=21 ms TTL=110

Statistiques Ping pour 142.250.74.227:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 21ms, Maximum = 23ms, Moyenne = 21ms

C:\Users\CLT_WIN>
```

Le délai d'attente est dépassé

Une erreur est survenue pendant une connexion à www.youtube.com.

- Le site est peut-être temporairement indisponible ou surchargé. Réessayez plus tard ;
- Si vous n'arrivez à naviguer sur aucun site, vérifiez la connexion au réseau de votre ordinateur ;
- Si votre ordinateur ou votre réseau est protégé par un pare-feu ou un proxy, assurez-vous que Firefox est autorisé à accéder au Web.

Réessayer

HTTPS)

Aller dans **System -> Advanced -> Admin Access**

System / Advanced / Admin Access

Admin Access Firewall & NAT Networking Miscellaneous System Tunables Notifications

webConfigurator

Protocol ☐ HTTP ☒ **HTTPS (SSL/TLS)**

SSL/TLS Certificate GUI default (65df33284a307) 
 Certificates known to be incompatible with use for HTTPS are not included in this list, such as certificates using incompatible ECDSA curves or digest algorithms.

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.

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.

HSTS ☐ Disable HTTP Strict Transport Security
 When this is unchecked, Strict-Transport-Security HTTPS response header is sent by the webConfigurator to the browser. This will force the browser to use only HTTPS for future requests to the firewall FQDN. Check this box to disable HSTS. (NOTE: Browser-specific steps are required for disabling to take effect when the browser already visited the FQDN while HSTS was enabled.)

OCSP Must-Staple ☐ Force OCSP Stapling in nginx
 When this is checked, OCSP Stapling is forced on in nginx. Remember to upload your certificate as a full chain, not just the certificate, or this option will be ignored by nginx.

WebGUI Login Autocomplete ☒ Enable webConfigurator login autocomplete
 When this is checked, login credentials for the webConfigurator may be saved by the browser. While convenient, some security standards require this to be disabled. Check this box to enable autocomplete on the login form so that browsers will prompt to save credentials (NOTE: Some browsers do not respect this option).

GUI login messages ☐ Lower syslog level for successful GUI login events
 When this is checked, successful logins to the GUI will be logged as a lower non-emergency level. Note: The console bell behavior can be controlled independently on the Notifications tab.

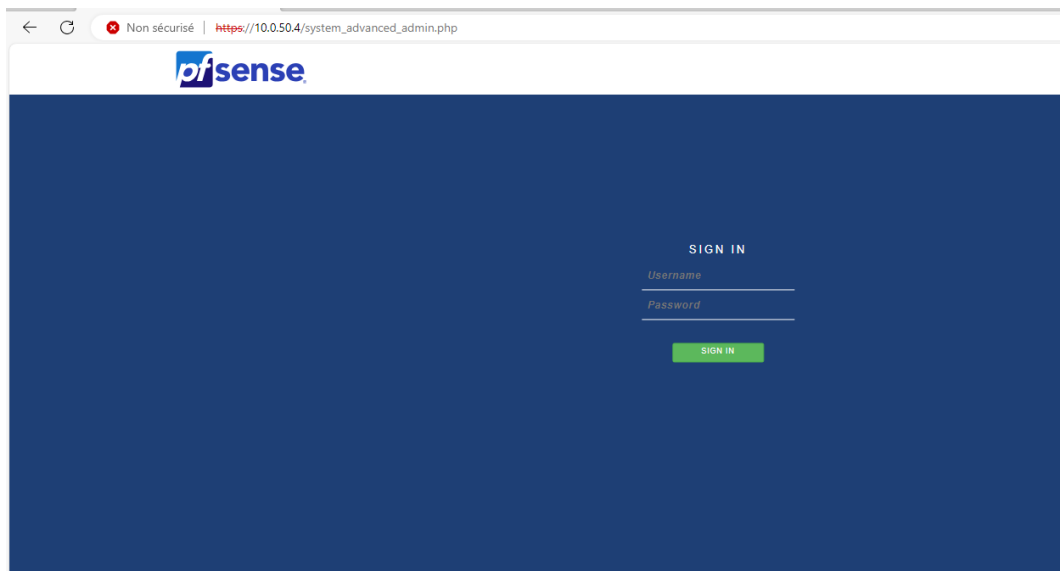
Roaming ☒ Allow GUI administrator client IP address to change during a login session
 When this is checked, the login session to the webConfigurator remains valid if the client source IP address changes.

Anti-lockout ☐ Disable webConfigurator anti-lockout rule
 When this is unchecked, access to the webConfigurator on the LAN interface is always permitted, regardless of the user-defined firewall rule set. Check this box to disable this automatically added rule, so access to the webConfigurator is controlled by the user-defined firewall rules (ensure a firewall rule is in place that allows access, to avoid being locked out!) Hint: the "Set interface(s) IP address" option in the console menu resets this

The changes have been applied successfully.
 One moment...redirecting to https://10.0.50.4/system_advanced_admin.php in 20 seconds.

On sélectionne
HTTPS

On « Save »



Nous voici sur notre interface en HTTPS !

DNSSEC)

Le DNSSEC (Domain Name System Security Extensions, extensions de sécurité du système de noms de domaine) est une signature cryptographique qui est ajoutée aux enregistrements DNS afin de sécuriser les données transmises sur les réseaux IP (protocole Internet).

System -> General Setup

On saisit le HostName DNS de Cloud Flare et Google.

DNS Server Settings

DNS Servers	1.1.1.1	cloudflare-dns.com	@IP DNS + HostName	Delete
	8.8.8.8	dns.google		Delete

Enable SSL/TLS Service

☒ Respond to incoming SSL/TLS queries from local clients

Configures the DNS Resolver to act as a DNS over SSL/TLS service. This option supports DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.

Sécurisation des transfert

SSL/TLS Listen Port

853

The port used for responding to SSL/TLS DNS queries. It should normally be set to TCP/UDP port 853.

*DNS over TLS (Port :853)

DNSSEC

☒ Enable DNSSEC Support

Python Module

☐ Enable Python Module

Enable the Python Module.

DNS Query Forwarding

☒ Enable Forwarding Mode

If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under [System > General Setup](#) or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).

☒ Use SSL/TLS for outgoing DNS Queries to Forwarding Servers

When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.

DHCP Registration

☒ Register DHCP leases in the DNS Resolver

If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. Note that this will cause the Resolver to reload and flush its resolution cache whenever a DHCP lease is issued. The domain in [System > General Setup](#) should also be set to the proper value.

Static DHCP

☒ Register DHCP static mappings in the DNS Resolver

If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in [System > General Setup](#) should also be set to the proper value.

OpenVPN Clients

☐ Register connected OpenVPN clients in the DNS Resolver

If this option is set, then the common name (CN) of connected OpenVPN clients will be registered in the DNS Resolver, so that their name can be resolved. This only works for OpenVPN servers (Remote Access SSL/TLS or User Auth with Username as Common Name option) operating in 'tun' mode. The domain in [System: General Setup](#) should also be set to the proper value.

Display Custom Options

[Display Custom Options](#)

On active DNSSEC

SSL

On l'inclue Dans le DHCP

Définition DNS over TLS : **DNS over TLS (DoT)** est un protocole de sécurité pour le chiffrement et l'encapsulation des requêtes et des réponses DNS via le protocole TLS. Le but de la méthode est d'augmenter la confidentialité et la sécurité des utilisateurs en empêchant les écoutes et la manipulation des données DNS

Test du fonctionnement DNSSEC

On va dans **Diagnostics -> DNS Lookup**

On saisit une adresse, dans mon cas j'ai choisi « **www.btssio.org** »

Puis on obtient ceci :

Results	
Result	Record type
91.220.197.80	A

Timings	
Name server	Query time
127.0.0.1	7 msec
10.0.231.2	42 msec
1.1.1.1	153 msec
8.8.8.8	15 msec
192.168.1.254	12 msec

More Information	
Ping	
Traceroute	

On va dans **Diagnostics -> States -> States**

Puis on saisit à **Filter expression** **853** qui correspond au **port DoT**

Diagnostics / States / States 

States [Reset States](#)

State Filter 

Interface

Filter expression

Rule ID

 Filter

States

Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes	
LAN	tcp	10.0.50.18:64853 -> 10.0.50.4:443	FIN_WAIT_2:FIN_WAIT_2	6 / 6	952 B / 502 B	

Conclusion Générale

Avantage de pfSense :

- Gratuit, même si la machine ou la vm qui hébergera Pfsense ne l'est pas, la solution en elle-même ne coûte rien.
- Les évolutions d'un logiciel libre, comme ses mises à jour, dépendent d'une communauté de développeurs et non pas d'un éditeur unique.
- La communauté développe chaque partie des logiciels libres et Open Source. Le développement communautaire favorise la réactivité lorsqu'il s'agit de corriger un bug ou une faille de sécurité.

Désavantages de pfSense :

- Parce que c'est libre, tout le monde peut étudier son fonctionnement et trouver des failles.
- Un firewall matériel est plus stable qu'un firewall logiciel comme pfsense, le vendeur "contrôle" son hardware et à conçu son firewall autour de cette hardware.
- Vous n'avez aucune garantie si vous avez un problème matériel ou logiciel, vous devez vous débrouiller ou alors payer pour du support.
- L'interface peut en rebuter plus d'un, elle peut paraître peu intuitive et trop fournis.

Avis Globale sur cette installation :

- J'ai trouvé cette installation, intéressante on peut voir qu'avec pfSense on peut à peu près tout faire et tout ça gratuit, il ne demande pas beaucoup de ressources parfaites pour un petit réseau d'entreprises qui tourne avec un serveur pas tout récent. Pas trop de difficulté rencontrée, j'ai aimé le concept de management de pfSense et le re-utiliserai dès que j'en aurai l'occasion. J'ai continué à chercher d'autres solutions qui pourront notamment être utilisées prochainement.

ANNEXE :

Liste des masques de sous-reseaux

CIDR	bits disponibles	Masque de sous-réseau	Nombre d'hôtes par sous-réseau
/1	31	128.0.0.0	$2^{31}-2 = 2\,147\,483\,646$
/2	30	192.0.0.0	$2^{30}-2 = 1\,073\,741\,822$
/3	29	224.0.0.0	$2^{29}-2 = 536\,870\,910$
/4	28	240.0.0.0	$2^{28}-2 = 268\,435\,454$
/5	27	248.0.0.0	$2^{27}-2 = 134\,217\,726$
/6	26	252.0.0.0	$2^{26}-2 = 67\,108\,862$
/7	25	254.0.0.0	$2^{25}-2 = 33\,554\,430$
/8	24	255.0.0.0	$2^{24}-2 = 16\,777\,214$
/9	23	255.128.0.0	$2^{23}-2 = 8\,388\,606$
/10	22	255.192.0.0	$2^{22}-2 = 4\,194\,302$
/11	21	255.224.0.0	$2^{21}-2 = 2\,097\,150$
/12	20	255.240.0.0	$2^{20}-2 = 1\,048\,574$
/13	19	255.248.0.0	$2^{19}-2 = 524\,286$
/14	18	255.252.0.0	$2^{18}-2 = 262\,142$
/15	17	255.254.0.0	$2^{17}-2 = 131\,070$
/16	16	255.255.0.0	$2^{16}-2 = 65\,534$
/17	15	255.255.128.0	$2^{15}-2 = 32\,766$
/18	14	255.255.192.0	$2^{14}-2 = 16\,382$
/19	13	255.255.224.0	$2^{13}-2 = 8\,190$
/20	12	255.255.240.0	$2^{12}-2 = 4\,094$
/21	11	255.255.248.0	$2^{11}-2 = 2\,046$
/22	10	255.255.252.0	$2^{10}-2 = 1\,022$
/23	9	255.255.254.0	$2^9-2 = 510$
/24	8	255.255.255.0	$2^8-2 = 254$
/25	7	255.255.255.128	$2^7-2 = 126$
/26	6	255.255.255.192	$2^6-2 = 62$
/27	5	255.255.255.224	$2^5-2 = 30$
/28	4	255.255.255.240	$2^4-2 = 14$
/29	3	255.255.255.248	$2^3-2 = 6$
/30	2	255.255.255.252	$2^2-2 = 2$
/31	1	255.255.255.254	$2^1-0 = 2$
/32	0	255.255.255.255	$2^0-0 = 1$

Services	Ports
Modbus	502
Telnet	23
FTP	21
SMTP	25
NTP	123
BOOTP	67
DHCP	67
HTTP	80
DNS	53
POP	110
SNMP	161