**Documentation d'installation** 



# Installation PFSENSE (Redondance, Filtrage, NAT, VPN)



18/03/2018

**Yohan Fresneau** 

### Sommaire

1.	Pourquoi mettre en place pfsense	3
2.	Configuration réseau	3
3.	Installation Pfsense	3
1.	Configuration du serveur pfsenseA	6
2.	Configuration du serveur pfsenseB	. 12
3.	Configuration des adresses IP virtuelle	. 14
4.	Mise en place de régles de filtrage	. 17
5.	Mise en plage de Liste de blockage	. 24
6.	Mise en place d'une journalisation du trafic réseau	. 37

### 1. Pourquoi mettre en place PFSENSE

Pfsense est un routeur/pare-feu qui est libre de droit. Il est entièrement configurable par interface web et il a de nombreux service supporter comme :

- Routage
- DNS
- NAT
- Filtrage
- VPN(open vpn, L2TP, IPSec)
- Et plein d'autres services.

Il y'a aussi la possibilité de faire de la redondance et de la haute disponibilité, et de mettre en place des adresses IP virtuelle.

### 2. Configuration réseau

Pour cette installation, nous allons mettre en place 2 serveurs en redondance et avec une haute disponibilité comme sur le schéma suivant :



### 3. Installation Pfsense



Accepter les termes afin d'installer pfsense

elcome to pfSense!	Ше 1 соме		
<mark>install</mark> Rescue Shell Recover config.xml	<mark>Install pfSense</mark> Launch a shell for Recover config.×Ml	rescue operations froм a previous install	
٢	D <mark>R &gt;</mark> <ca< td=""><td>ncel&gt;</td><td></td></ca<>	ncel>	

Sélectionner « Installer pfsense »

Nous allons sélectionner le clavier français en azerty, pour cela effectuer ces actions

( ) Estonian I	SO-8859-15			
() Finnish Co	depage 850			
J Finnish 18	U-8859-1 .diam ISO 00E0 1	(accept low)		
() French Lan	auran rob-6659-1 rak-liko	(accent keys)		
() French Duo	rak-like (accont	kous)		
() French ISO	-8859-1	NOV37		
() French ISU	-8859-1 (accent	kevs)		
( ) French Mac	book/Macbook Pro	ISO-8859-15 (	(accent keys)	
( ) German Cod	epage 850			
( ) German ISO	-8859-15			
( ) German ISO	-8859-15 (accent	keys)		
			36%	

Sélectionner « French ISO-8859-1 »

>>> Continue with fr iso kbd keyman	
->- Test fr.iso.kbd keymap	
( ) Armenian phonetic layout	
( ) Belarusian Codepage 1131	
( ) Belarusian Codepage 1251	
( ) Belarusian ISO-8859-5	
( ) Belgian ISO-8859-1	
( ) Belgian ISO-8859-1 (accent keys)	
( ) Brazilian 275 Codepage 850	
( ) Brazilian 275 ISO-8859-1	
( ) Brazilian 275 ISO-8859-1 (accent	keys)
( ) Bulgarian (BDS)	

On confirme bien notre choix, choisir Continuer

Une fois le clavier choisi, on installe le système sur le disque

pfSense In 	nstaller
	Partitioning           Ном would you like to partition your disk?           Auto (UFS)         Guided Disk Setup           Manual         Manual Uisk Setup           Shell         Open a shell and partition by hand
	Auto (2FS) Guided Root-on-2FS

J'ai utilisé le partitionnement automatique, mais cela n'est pas obligé

pfSense Install	er		
	Destado	Distant Production	
	retching	DISTRIBUTION	
	MANIFEST	[ Done	1
	base.txz	E 66%	1
	Fetching distribut	tion files	
	Uverall Progres	55	
	L		

La progression d'installation nous indique son état

ofSense Installer	
	Manual Configuration The installation is now finished. Before exiting the installer, would you like to open a shell in the new system to make any final manual modifications? < Yes >

Une fois fini, il nous demande si l'on souhaite redémarrer ou bien afficher le « Shell »

Sélectionner « No », pour redémarrer et si vous voulez utiliser le « Shell » sélectionner « Yes »



Confirmation du choix "Reboot", pour redémarrer

### 4. Configuration du serveur PFSENSE A

Une fois redémarrer, nous avons l'interface de pfsense qui est afficher.

Starting syslogdone.	
Starting CRON done.	
pfSense 2.4.1-RELEASE amd64 Sun Oct 22	2 17:26:33 CDT 2017
Bootup complete	
FreeBSD/amd64 (pfSense.localdomain) (1	tyv0)
VMware Virtual Machine – Netgate Devic	e ID: 20bee1522d68a1935aeb
*** Welcome to pisense 2.4.1-RELEHSE (	amab4) on pisense ***
$UON (uan) = \sum ONO = \sum U4/I$	HCD4 · 192 168 1 85/24
	192.100.1.1/24
A) Logout (SSH onlu)	9) nfTon
1) Assign Interfaces	10) Filter Logs
2) Set interface(s) IP address	11) Restart webConfigurator
3) Decot unbConfigurator passuord	12) DHD shall $+$ pfSansa tools
4) Depet to factory defaults	12) Indate from concele
4) Reset to factory defaults	13) Update from console
5) REDOOT SYSTEM	14) Enable Secure Shell (SShd)
6) Halt system	15) Restore recent configuration
7) Ping host	16) Restart PHP-FPM
8) Shell	
Enter an ontion' 2	

Nous devons changer l'adresses de nos interface « Wan » et « Lan », pour cela sélectionner « 2 »

UMware Virtual Machine - Netgate Device ID: 20bee1522d68a1935aeb \*\*\* Welcome to pfSense 2.4.1-RELEASE (aMd64) on pfSense \*\*\* WAN (wan) -> eM0 -> v4/DHCP4: 192.168.1.85/24 LAN (lan) -> eM1 -> v4: 192.168.1.1/24 Ø) 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) Enter the number of the interface you wish to configure: 2

On sélectionne l'interface « Lan », qui est le choix « 2 »

WA	N (wan)	-> ем0	-> v4/]	DHCP4	P4: 192.168.1.85/24	
LA	N (lan)	-> ем1	-> v4:	192.	2.168.1.1/24	
0) 1) 2) 3) 4) 5) 6) 7) 8)	Logout (SSH Assign Inter Set interfac Reset webCor Reset to fac Reboot syste Halt system Ping host Shell	only) faces ce(s) IP addres: figurator pass tory defaults M	s word	9) 10) 11) 12) 13) 14) 15) 16)	) pfTop ) Filter Logs ) Restart webConfigurator ) PHP shell + pfSense tools ) Update from console ) Enable Secure Shell (sshd) ) Restore recent configuration ) Restart PHP-FPM	
Ent	er an ontion:	2				
	ci an option.	2				
Ava	ilable interf	aces:				
1 - 2 -	WAN (ем0 – d LAN (ем1 – s	lhcp, dhcp6) static)				
Ent	er the number	of the interf	ace you	wis}	sh to configure: 2	
Ent > 1	er the new Lf 72.16.0.252	N IPv4 address	. Press	s <em< td=""><td>ENTER&gt; for none:</td><td></td></em<>	ENTER> for none:	

Ont défini l'adresse IP de notre interface



Et l'on indique le masque de sous réseau de notre réseau en « CIDR »

8) Shell
Enter an option: 2
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6) 2 - LAN (em1 - static)
Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <enter> for none: &gt; 172.16.0.252</enter>
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 31): > 24
For a WAN, enter the new LAN IPv4 upstream gateway address. For a LAN, press <enter> for none: &gt;</enter>

On ignore la question demander, en appuyant sur « Entrer »

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)

2 - LAN (em1 - static)

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

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

> 172.16.0.252

Subnet Masks are entered as bit counts (as in CIDR notation) in pfSense.

e.g. 255.255.0.0 = 24

255.255.0.0.0 = 16

255.0.0.0 = 8

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

> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.

For a LAN, press <ENTER> for none:

>

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

On fait de même, car nous avons un réseau en IPv4

```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.0.252
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 31):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on LAN? (y/n)
```

Nous pouvons ou non utiliser un serveur DHCP, pour mon cas j'en ai utiliser un pour faciliter la distribution d'IP

1 - WAN (em0 - dhcp, dhcp6) 2 - LAN (em1 - static) Enter the number of the interface you wish to configure: 2 Enter the new LAN IPv4 address. Press <ENTER> for none: > 172.16.0.252 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 31): > 24 For a WAN, enter the new LAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none: > Enter the new LAN IPv6 address. Press <ENTER> for none: > Do you want to enable the DHCP server on LAN? (y/n) y Enter the start address of the IPv4 client address range: 172.16.0.1

Si l'on utilise un DHCP, nous devons saisir le début de la plage d'adresse

Et pour finir avec le DHCP, on saisit la fin de la plage d'adresse

Enter the number of the interface you wish to configure: 2 Enter the new LAN IPv4 address. Press <ENTER> for none: > 172.16.0.252 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 = 18 Enter the new LAN IPv4 subnet bit count (1 to 31): > 24 For a WAN, enter the new LAN IPv4 upstream gateway address. For a WAN, enter the new LAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none: > Enter the new LAN IPv6 address. Press <ENTER> for none: > Do you want to enable the DHCP server on LAN? (y/n) y Enter the start address of the IPv4 client address range: 172.16.0.1 Enter the end address of the IPv4 client address range: 172.16.0.200 Disabling IPv6 DHCPD... Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Il nous ai demander si l'on veut utiliser l'interface web pour configurer pfsense

For a WAN, enter the new LAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none: > Enter the new LAN IPv6 address. Press <ENTER> for none: > Do you want to enable the DHCP server on LAN? (y/n) y Enter the start address of the IPv4 client address range: 172.16.0.1 Enter the end address of the IPv4 client address range: 172.16.0.200 Disabling IPv6 DHCPD... Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y Please wait while the changes are saved to LAN... Reloading filter... Reloading filter... Restarting webConfigurator... The IPv4 LAN address has been set to 172.16.0.252/24 You can now access the webConfigurator by opening the following URL in your web browser: http://172.16.0.252/ Press <ENTER> to continue.

Il nous affiche l'adresse de configuration

http://172.16.0.252/ Press <ENTER> to continue. Message from syslogd@pfSense at Nov 9 19:15:15 ... pfSense php-fpm[339]: /index.php: Successful login for user 'admin' from: 172.16 0.1 VMware Virtual Machine - Netgate Device ID: 20bee1522d68a1935aeb \*\*\* Welcome to pfSense 2.4.1-RELEASE (amd64) on pfSense \*\*\* WAN (wan) LAN (lan) -> v4/DHCP4: 192.168.1.85/24 -> v4: 172.16.0.252/24 -> емØ -> ем1 9) pfTop 10) Filter Logs 0) Logout (SSH only) Assign Interfaces
 Set interface(s) IP address 11) Restart webConfigurator12) PHP shell + pfSense tools Reset webConfigurator password 13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM 4) Reset to factory defaults Reboot system 6) Halt system 7) Ping host 8) Shell Enter an option: 2

On fait de même avec l'interface « Wan »

VMware Virtual Machine – Netgate Device ID: 20bee1522d68a1935aeb \*\*\* Welcome to pfSense 2.4.1-RELEASE (amd64) on pfSense \*\*\* -> v4/DHCP4: 192.168.1.85/24 WAN (wan) -> ем0 LAN (lan) -> v4: 172.16.0.252/24 -> ем1 9) pfTop 10) Filter Logs 11) Restart webConfigurator 12) PHP shell + pfSense tools 13) Update from console 14) Enable Secure Shell (sshd) 0) Logout (SSH only) 1) Assign Interfaces Set interface(s) IP address
 Reset webConfigurator password
 Reset to factory defaults Reboot system 5) 6) Halt system 7) Ping host 8) Shell 15) Restore recent configuration16) Restart PHP-FPM Enter an option: 2 Available interfaces: - WAN (ем0 - dhcp, dhcp6) LAN (em1 - static) Enter the number of the interface you wish to configure: 1

On sélectionne donc l'interface « 1 »

\*\*\* Welcome to pfSense 2.4.1-RELEASE (amd64) on pfSense \*\*\* -> v4/DHCP4: 192.168.1.85/24 WAN (wan) -> емØ LAN (lan) -> v4: 172.16.0.252/24 -> ем1 9) pfTop 10) Filter Logs 0) Logout (SSH only) 1) Assign Interfaces 11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd) 2) Set interface(s) IP address 3) Reset webConfigurator password 4) Reset to factory defaults 5) Reboot system 15) Restore recent configuration16) Restart PHP-FPM 6) Halt system 7) Ping host 8) Shell Enter an option: 2 Available interfaces: – WAN (ем0 – dhcp, dhcp6) – LAN (ем1 – static) Enter the number of the interface you wish to configure: 1 Configure IPv4 address WAN interface via DHCP? (y∕n) n

#### On saisit une adresse IP fixe, on refuse donc la configuration par DHCP

10 / 42 Installation PFSENSE (Redondance, Filtrage, NAT, VPN)

LAN (lan) $\rightarrow em1 \rightarrow v4:$	172.16.0.252/24			
<ul> <li>Ø) Logout (SSH only)</li> <li>1) Assign Interfaces</li> <li>2) Set interface(s) IP address</li> <li>3) Reset webConfigurator password</li> <li>4) Reset to factory defaults</li> <li>5) Reboot system</li> <li>6) Halt system</li> <li>7) Ping host</li> <li>8) Shell</li> </ul>	<ul> <li>9) pfTop</li> <li>10) Filter Logs</li> <li>11) Restart webConfigurator</li> <li>12) PHP shell + pfSense tools</li> <li>13) Update from console</li> <li>14) Enable Secure Shell (sshd)</li> <li>15) Restore recent configuration</li> <li>16) Restart PHP-FPM</li> </ul>			
Enter an option: 2				
Available interfaces:				
1 – WAN (ем0 – dhcp, dhcp6) 2 – LAN (ем1 – static)				
Enter the number of the interface you wish to configure: 1				
Configure IPv4 address WAN interface via DHCP? (y∕n) n				
Enter the new WAN IPv4 address. Press > 192.168.1.201	s <enter> for none:</enter>			

On indique donc l'adresse IP de l'interface

6) Halt system 7) Ping host 8) Shell	15) Restore recent configuration 16) Restart PHP-FPM
Enter an option: 2	
Available interfaces:	
1 – WAN (ем0 – dhcp, dhcp6) 2 – LAN (ем1 – static)	
Enter the number of the interface you	wish to configure: 1
Configure IPv4 address WAN interface v	via DHCP? (y∕n) n
Enter the new WAN IPv4 address. Press > 192.168.1.201	s <enter> for none:</enter>
Subnet masks are entered as bit counts e.g. 255.255.255.0 = 24 255.255.0.0 = 16 255.0.0.0 = 8	: (as in CIDR notation) in pfSense.
Enter the new WAN IP∨4 subnet bit cour > 24	nt (1 to 31):

Le masque de sous réseau en « CIDR »

Enter an option: 2 Available interfaces: 1 - WAN (em0 - dhcp, dhcp6) 2 - LAN (em1 - static) Enter the number of the interface you wish to configure: 1 Configure IPv4 address WAN interface via DHCP? (y/n) n Enter the new WAN IPv4 address. Press <ENTER> for none: > 192.168.1.201 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 = 8 Enter the new WAN IPv4 subnet bit count (1 to 31): > 24 For a WAN, enter the new WAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none: >

11 / 42 Installation PFSENSE (Redondance, Filtrage, NAT, VPN)

On ignore la question, en appuyant sur « entrer »

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)

2 - LAN (em1 - static)

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

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

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

> 192.168.1.201

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.

e.g. 255.255.00 = 24

255.255.00 = 16

255.0.00 = 8

Enter the new WAN IPv4 subnet bit count (1 to 31):

> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.

For a LAN, press (ENTER> for none:

>

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

Notre réseau « Wan », étant aussi en IPv4, on répond « non »

2 - LAN (em1 - static)
Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv4 address. Press <enter> for none: &gt; 192.168.1.201</enter>
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 = 8
Enter the new WAN IPv4 subnet bit count (1 to 31): $>$ 24
For a WAN, enter the new WAN IPv4 upstreaм gateway address. For a LAN, press <enter> for none: &gt;</enter>
Configure IPv6 address WAN interface via DHCP6? (y∕n) n
Enter the new WAN IPv6 address. Press <enter> for none: ▶ ■</enter>

On fait de même pour cette question, en appuyant sur « entrer »

# 5. Configuration du serveur PFSENSE B

On fait de meme avec le serveur pfsenseB, avec cette configuration :

Lan: 192.168.1.202/24, Activation de la configuration web

Wan: 172.16.0.253/24

La configuration du 2<sup>émè</sup> PFSENSE est identique, seul les IP des cartes réseaux change.

# 6. Interface Web PFSENSE

Pour cela, se connecter sur le panel PFSENSE

pfsense		LogIn to ptSense
	SIGN IN Username	
ptiense is @ 2004-3	3012 by flatsceri Conselastiatives. L.C. delapers) Al Highla Beerkeld (skiel könne)	

Login : admin Password : pfsense

Nous avons le dashboard de PFSENSE, avec les informations principale et les informations système.

System Information       P © 0         Name       pfSense.loaddomain         System       VirtueBox Virtual Machine Netgate Device IC (#200co05533606a6/4         BIOS       Verdiant Virtual Box Version         Version       2.4.2-RELEASE-p1 (mid6/s) built on Tub Data 12 3/4.26 GST 2017 FreeBSD 11.1-RELEASE-p6         The system is on the lasest version. Version       2.4.2-RELEASE-p1 (Structure)         Diff Diff Provided at Thu Mar 114.00-51 UTC 2018       Community Support at the point of ake, you can register your community is aubacrytein for access to JGEnse Gold.         CPU Type       Intel(R) X can(R) (PULY3440 (\$2.2360Hz) AES/NI CPU Crypto: No       - Community Support at the point of ake, you can register your community is aubacrytein for access to JGEnse Gold.         CPU Type       Intel(R) X can(R) (PULY3440 (\$2.2360Hz) AES/NI CPU Crypto: No       - Community Support at Become - Upgrade Your Support Subscription you Mit have your Netgate Device ID (NO) from your fiveral asception you Mit have your Netgate Device ID (NO) from your fiveral asception you Mit have your Netgate Device ID (NO) from your fiveral asception you Mit have your Netgate Device ID (NO) from your fiveral asception you Mit have your Netgate Device ID (NO) from your fiveral in a sefer place. You have your Netgate Device ID (NO) from your fiveral in a sefer place. You have your Netgate Device ID (NO) from your fiveral in a sefer place. You have your Netgate Device ID (NO) from your fiveral in a sefer place. You have your Netgate Device ID (NO) from your fiveral in a sefer place. You have your Netgate Device ID (NO) from your fiveral in a sefer place. You have your Netgate Device ID (NO) from your fiver	Status / Das	shboard	+ 0				
Name     pfSense locabionein       System     Riediate Derive Dit / Huad Machine Netgate Derive Dit / Huad Nachine System     Centract type Community Support Only       BIOS     Vandor: Inscholl     Centract type Variation     Centract type Community Support Only       BIOS     Vandor: Inscholl     Centract type Variation     Centract type Community Support Only       Version     2.4.2-RELEXES-11 (mrd65) Dublic on Tubox 12 3/4/26 Cort 2017, FreeBO11.1-RELEASE-p5     Hyou purchased your pfSense gateway freeval applance fram Netigate and Community Support of network of policy our port al account Version Information opdated at Th Macr 11 4/00-51 UTC 2018     Hyou purchased your pfSense gateway freeval applance fram Netigate and Community Support at the for access to pfSense Code.       CPUT type     Intel(R) Xon(R) CPUX3440 @ 2.630412 ASEN CPU Cryptor No     - Register Your Support at the Septem intel Septem in	System Inform	nation FOO	Netgate	Service	es And Support		00
System     Virtual Box Virtual Machine Netgete Evrice UL: f200ec05533606a6f4       BIOS     Variani VirtualBox Release Date: Fri Des 12066       Version     2.4.2-RELESE-p1 (smd6.6) built on Tubes 12 13/4.20 C037 2017 FreeBDD 11.1 RELEASE-p6       The system is on the laster version. Version information updated at Thu Mar 11.4.09:51 UTC 2018       CPU Type     Intel® (Swort) CPU X3/4.0 @ 2.830Hz AESIN CPU Cryster. No       Uptime     22 Hours 4P Minute DD Seconds       Uptime     22 Hours 4P Minute DD Seconds       DS server(s)     - 127.0.0.1       Biste server(s)     - 127.0.0.1	Name	pfSense.localdomain	0	ontract te	no Community Supp	and a	
BIOS       Variador: Linotek 0mbH Variador: VirtualBox Release Date: Fr Die 1 2006       NETGAT E AND pfSense COMMUNITY SUPPORT RESOURCES         Version       2.4.2-RELEASE-p1 (amd6.6) built on Tue Due 12 13.43/26 CST 2017 FreeBSD 11.1-RELEASE-p6 TereBSD 11.1-RELEASE-p6       Hype purchased your pfSense gateway fiswall appliance from Neighte an Community Support at the point of aiks you can register your community of variaon information updated at Thu Mar 11.409.51 UTC 2018         CPU Type       Intel(R) Xeon(R) CPU X3440 (b) 2.530 Hz AESHA CPU Crystor: No       - Log into your portal accour Upgrade Year Support Reso Variaon information updated at Thu Mar 11.409.51 UTC 2018         CPU Type       Intel(R) Xeon(R) CPU X3440 (b) 2.530 Hz AESHA CPU Crystor: No       - Metgrate Global Support Subscription - Log into your portal accour Upgrade Year Support Subscription - Variaon information updated at Thu Mar 11.409.51 UTC 2018         DNS acreer(s)       - 127.0.0.1         State table size       Dis (Ja30/97000) Show strates         MBUF Usage       2% (1016/61006)         Laad average       0.22.0.38.0.45         CPU usage       Retiveron CPU I data 0	System	VirtualBox Virtual Machine Netgate Device ID: f <b>d20bcc056383606a6f4</b>			Community Suppr	ort Only	
Version       2.4.2-RELEASE-p1 (amd6.6) built on Tue Due 12 13.43.26 CST 2017 Free38D0 11.1-RELEASE-p6         The system is on the latest tweram. Variation information updated at Thu Mar 11.409.51 UTC 2018       If you purchased your (Free38D0 11.1-RELEASE-p6         The system is on the latest tweram. Variation information updated at Thu Mar 11.409.51 UTC 2018       Image: State Sta	BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006		NETGATE	E AND pfSense COMMU	NITY SUPPORT R	ESOURCES
CPU Type       Intel(R) Xean(R) CPU X3440 (⊉ 2.530Hz AE5HX CPU Cryste:N0       • Others in Edente training or Notice in Edente Notice in Ede	Version	2.4.2-RELEASE-p1 (amd64) built on Twe Dear 21 35:452 0 ST 2017 FreeBSD 11.1-RELEASE-p6 The system is on the latest version. Version Information updated at Thu Mar 1 14:09:51 UTC 2018 😂	If you purch Community subscription • Registr • Upgrad	rased you rSupport In for acce ar Your Su Ie Your Su	ur pfSense gatewsy frew at the point of sale, you ess to pfSense Gold. upport Subscription upport	<ul> <li>all appliance from can register your</li> <li>Log into your p</li> <li>Community Sector</li> </ul>	n Netgate and elected community support portal account upport Resources
Uptime         23 Hours 49 Minutes 00 Seconds           Current date/Ume         Thu Mar 1145625 UTC 2018           DNS aerver(s)         • 127.0.0.1           Last cenfig change         Thu Mar 114:10:13 UTC 2018           State table size         D% (439/97000) Show states           MBUF Usage         €% (1016/61006)           Lead average         0.22, 0.38, 0.45           CPU usage         Retrieven CPU data 0	СРИ Туре	Intel(R) Xeon(R) CPU X3440 @ 2.53GHz AES-NI CPU Crypto: No	Netgate     Netgate	e Global S e Professi	support FAQ ional Services	<ul> <li>Official pfSens</li> <li>Visit Netgate.c</li> </ul>	e Training by Netgate com
Current date/time Thu Mar 1 14:56:55 UTC 2018 Priyou decide to purchase a Natigate Global Support subscription, you Mit have your Kelgate Decide 10 (NO) from your freewall in orde to validate support for the unit. Write down your KOI and store it in a safe place. Yo purchase support have. Interfaces Lead average 0:22, 0:38, 0.45 CPU usage Retrieven CPU date 0	Uptime	23 Hours 49 Minutes 00 Seconds					
DNS server(s)     • 127.0.0.1       Last cenfig change     Thu Mar 1 14:10:13 UTC 2018       State table size     D% (439/97000) Show states       BUF Usage     2% (1016/61006)       Lead average     0.22, 0.38, 0.45       CPU usage     Retrieving CPU data 0	Current date/time	Thu Mar 1 14:56:25 UTC 2018	If you de	cide to pu	archase a Netgate Globa	Support subscrip	ation, you MUST
Last config change Thu Mar 1 14:10:13 UTC 2018 purchase support have.  State table size D% (459/97000) Show states  MBUF Usage Exterior 000 Show states  Lead average 0.22, 0.38, 0.45  CPU usage Retrieving CPU date 0	DNS server(s)	• 127.0.0.1	support 1	for this un	nit. Write down your NBI	and store it in a s	afe place. You can
State table size         D% (439/97000) Show strites         Interfaces           MBUF Usage         2% (1016/51006)         1000bsseT < full-duplexo	Last config change	Thu Mar 1 14:10:13 UTC 2018	purchase	e support	here.		
MBUF Usage         Intertaces           2% (1016/61006)         ▲ WAN         1000baseT < full-duplex>         192.168.0           Laad average         0.22, 0.38, 0.45         ▲ LAN         1000baseT < full-duplex>         192.168.0           CPU usage         Retrieving CPU data ©         1000baseT < full-duplex>         172.16.0	State table size	0% (439/97000) Show states					Ø
Load average 0.22, 0.38, 0.45 ALLN A 1000baseT -full-duplex> 172.15.03	MBUF Usage	2% (1016/61006)	Threatace The WAN	15	1000baseT <full-dupl< td=""><td>90&gt;</td><td>192.158.0.2</td></full-dupl<>	90>	192.158.0.2
CPU usage Retrieving CPU data 0	Load average	0.22, 0.38, 0.45	-LAN	*	1000baseT «full-duple	80>	172.16.0.254
state of the state	CPU usage	Retrieving CPU data 🛱					

Nous avons le tableau de board avec pleins d'informations a propos du routeur/Firewall.

# 7. Configuration des adresses IP virtuelle (Haut Dispo)

La configuration des adresses IP, permet un basculement entre deux adresses IP. Cela permet de faire une redirection d'adresse IP. Si l'adresse 172.16.0.252 est down, il n'est pas possible de passer instantanément en adresse 172.16.0.253. Alors que si l'on créer une adresse IP en 172.16.0.254, qui permet de faire une redondance sur des adresses IP. Cela est utiliser pour les routeurs et les serveurs. Cela permet de rediriger le flux vers le serveur et en cas de chute de celui-ci le basculement est invisible pour l'utilisateur. Nous allons mettre en place une IP virtuelle entre deux PFSENSE coté Wan et Lan. La mise en place et identique sauf la carte réseau qui diffère.



Dans « Firewall / Virtual IPs », nous pouvons mettre en place les deux IP virtuelle coté Wan et Lan

#### Nous allons créer l'IP virtuelle se trouvant, coté WAN

Type Interface	IP Alas     WAN	Proxy ARP     Oth	r.
Address type	Single address	•	
Address(es)	192.168.1.200 The mask must be the network's subnet mask. It do	es not specify a CIDR range.	/ 24 *
Virtual IP Password	Enter the VHID group password.	Confirm	
VHID Group	1 Enter the VHID group that the machines will share.	•)	
Advertising frequency	1 Dase The frequency that this machine will advertise. 0 m	O     Skew eans usually master. Otherwise the lowest combinati	• of both values in the cluster determines the
Description	Adresse IP Watt CARP(FailDiver) - 192.166.1.200 A description may be entered here for administrativ	s oferance (not parsed).	
	🖹 Save		

On créer notre IP virtuel WAN, comme ceci

Nous allons créer l'IP virtuelle se trouvant, coté WAN.

Ебн VIRtual IP-	IP Alian CARP Other	
Interface	LAN •	
Address type	Single address v	
Address(es)	172 16 0 254 / 24 • The mask must be the network's subnet mask. It does not specify a CIDII range.	
Virtual IP Password	Enter the VHED group password. Confirm	
VHID Group	2 . Enter the VHED group that the machines will ahare.	
Advertising frequency	1 0 • 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	Advesse IP Lan CARR/Nallover) 172.16.0.254 A description may be entered here for administratore reference (not parsed).	

On fait de même pour l'interface Lan.

Nous allons pouvoir appliquer les paramètres

	COMMUNITY ESTION	nterfaces - Firewal	I - Services	• VPN • Status • Diagnostics • Help •	(+	
	Firewall / Virtual IPs				θ	
	The VIP configuration has been one The changes must be applied for th	inged. em to take effect.			Apply Changes	
	Virtual IP Address					
	Virtual IP address	Interface	Туре	Description	Actions	
	192 168 1 200/24 (vhid: 1)	WAN	CARP	Adresse IP Wan CARP(FailOver) - 192.168.1.200	/0	
	172,16.0.254/24 (vhid: 2)	LAN	CARP	Adresse IP Lan CARP(FallOver) 172.10.0.254	/0	
	0					
						5
		pfSense = 0.2004-20	17 by Rubicon Co	mmunications, LLC (Netgate) All Poglats Reserved. (view license)		

On à un récapitulatif de nos IP virtuelle. Il faut appliquer les parametres pour activer l'IP virtuelle

On peut voir dans le staus CARP, et savoir si l'interface est en "Master" ou bien en "Backup"

COMMUNITY ENTION	Interfaces • Firewall •	Services • VPN •	Status +	Diagnostics +	Help +	0+	
Status / CARP						5 Lat. 0	
Temporarily Disable CARP	Enter Peralatent CARP Mainte	nance Mode					
CARP Interfaces							
CARP Interface		Virtual IP			Status		
WAN(01		192.168.1.200/24			O MASTER		
LAN@2		172.16.0.254/24			O MASTER		
pfSync Nodes							
pfSync nodes							
407bd4a8							
#91878#9							
							₽.
	<b>pfSense</b> is 0-7004 - 2017 b	Rubicon Communications, L	LC (Netgate) All	Rights Roservoid (M	ew license)		

On peut voir le status des IP virtuelle, on voit que le PfsenseA est bien en master

of sense System -	Interfaces + Finawall + Services + VPN + Statu	s - Diagnostics • Holp •	Ge
Status / CARP			<b>≣ I</b> M 0
🖉 Temporally Disable CARD	Enter Persistent CARP Maintenance Mode		
CARP Interface	Virtual IP	Status	
WANUT	192.168.1.200/24	SACKUP	
LAN@2	172.16.0.254/24	C BACKUP	
pfSync Nodes			
pfSyne nodes:			
0365314			
			þ
	pfSense is (5.2004 - 2017 b) Rubicon Communications, LLC (Netge	te) All Rights Reserved [view license]	

Le statut des IP virtuelle sur le second PFSENSE, il sont donc bien en backup

On peut voir le status des IP virtuelle, on voit que le PfsenseB est lui en backup

# 8. Configuration de la redondance

La mise en place de la redondance, nous permet une réplications des régles de filtrage, NAT, VPN, etc.... Ce permet de devoir effectuer la création d'une régle ou autre, uniquement d'un seul coté. La réplication s'effectue automatiquement.

Nous allons mettre en place la redondance de Pfsense, afin d'avoir les memes paramétrages coté PfsenseA et PfsenseB. La configuration doit être actif des deux cotés

# 9. Mise en place de règles de filtrage

Les règles de filtrages permettent de mettre des restrictions sur des protocoles, Port, adresse IP.

Pour mettre en place des règles de filtrage coté WAN, nous devons désactiver une règle, car elle nous empêche d'ajouter des règles.

Floati	ng WAN	LAN									
	-	•									
Rul	es (Drag	to Chang	je Order)								
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
×	0 /384 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	•
×	0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	0

Nous devons enlever ces deux règles

Pour cela, nous devons aller dans les paramètres de l'interface WAN(Interfaces / WAN), ou bien cliquer sur l'engrenage à coté de nos deux règles de refus.

	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 Confi	iguration
IPv4 Address	192.168.1.253 / 24 🗸
IPv4 Upstream gateway	None  Add a new gateway
	If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.
Reserved Networ	rks
Block private	
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. Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.
	P Save

Nous devons décocher les deux règles dans "Reserved Networks", elle empêche de créer des règles ce sont des sécurités actives de base.

On doit se retrouver donc sans nos deux cases cocher



Aucune ne doit être cocher

#### Une fois enlever, nous devons appliquer les modifications



Pour appliquer nous devons juste cliquer sur "Apply Changes"

Comme on peut le voir maintenant, les deux règles ne sont plus présentes et nous pouvons donc en créer de nouvelles.

Firewal	I / Rules	/ WAN								
Floating V	AN LAN									
-	_									
Rules (Di	ag to Chan	ge Order)			017					
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
No rulae ar	ourrantly defu	ned for this i	ntorface							
- Ho ruico un	- carrently den	on this interf	nor will !	a blockod until a		re added Cli	ck the buttor	wer e bbe of r	rulo	

Pour ajouter une règle, nous devons cliquer sur "Add"

Il y'a plusieurs actions qui peuvent être appliquer sur la régles :

- Block : Détruit le paquet sans retour vers la source
- Reject : Un retour est effectué vers la source disant qu'il est refusé \_
- Pass : Accepte le paquet

Nous devons sélectioner notre interface (WAN ou LAN), sur la quelle la regle sera actif

On sélectionne si cela concerne IPv4 ou IPv6, ou bien les deux

Et pour finir on paramettre notre régle, c'est-à-dire le protocole, la source et la destination et la source et on peut aussi mettre une description afin de savoir rapidement son action.

Edit Firewall Rul	e					
Action	Block		~			
	Choose what to do wit Hint: the difference be returned to the sender	th packets that match the tween block and reject is ; whereas with block the p	criteria specified bel that with reject, a pac backet is dropped sile	ow. cket (T( ently. In	CP RST or ICMP port unrea either case, the original pa	achable for UDP) is acket is discarded.
Disabled	Disable this rule					
	Set this option to disa	ble this rule without remo	ving it from the list.			
Interface	WAN		~			
	Choose the interface f	rom which packets must	come to match this r	ule.		
Address Family	IPv4		~			
	Select the Internet Pro	tocol version this rule app	blies to.			
Protocol	Any		~			
	Choose which IP proto	ocol this rule should mate	h.			
Source						
Source	Invert match.	any		~	Source Address	1
Destination						
Destination	Invert match.	any		$\sim$	Destination Address	1
Extra Options						
Log	Log packets that a	re handled by this rule				
	Hint: the firewall has li	imited local log space. Do	n't turn on logging fo	r everyt	thing. If doing a lot of logg	jing, consider using a
	remote syslog server	(see the Status: System L	ogs: Settings page).			
Description	Bloque tout le trafic					
	A description may be displayed in the firewa	entered here for administ all log.	rative reference. A ma	aximun	n of 52 characters will be u	used in the ruleset and

Dans ce cas-là c'est une régle de blockage, mais le principle est le meme pour toutes régles.

Cliquer sur "Save", afin de créer notre règle.

Attention la règles de blocage doit être effectuer en dernière coté LAN, elle risque de bloquer l'accès à l'interface web. Pour le coté LAN et WAN, le principe est le même. Il est possible de désactiver l'utilisations de certains protocoles ou bien bloquer une partie du réseau au certaines machines. Cet outil et pratique et puissant. Une liste de protocole et de port est pré-enregistrer, mais il est possible d'utiliser d'autres ports garce à la ligne "**Other**".

Il faut faire attention aux protocoles à bloquer, le plus simple est de désactiver tous les protocoles/Ports et créer une autorisation pour chaque protocoles/Ports ce qui augmente la sécurité du réseau.

Faire attention à l'interface web coté Wan, ne pas oublier de vérifier la règle de l'interface web. Il y a une règle déjà créer normalement et ne doit pas être supprimer.

LAN

Address

✔ 1/1.58

MiB

80

Anti-Lockout Rule

Une fois notre règle créer, nous devons l'appliquer

	evv		Rules /	WAN								÷ 🔟 🗖 6
The The	firew char	vall rule ( nges mu	configuratio st be applie	n has beer d for them	n chang to take	ed. effect.						✓ Apply Changes
Float	ing	WAN	LAN									
Float	ing es (	WAN (Drag t	LAN o Change	e Order)								
Float Rul	ing es (	WAN (Drag t States	LAN to Change Protocol	e Order) Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

Cliquer sur "Apply Changes", afin d'activer notre règle.

Nous allons voir comment ajouter une règle coté WAN à destination du PFSENSE, comme le fait d'utiliser le serveur VPN(OpenVPN) de PFSENSE.

	es / Edit				₩ 🗖 (
Edit Firewall Rul	e				
Action	Pass		~		
	Choose what to do with Hint: the difference betw returned to the sender, w	packets that match veen block and reject vhereas with block th	he criteria specified below. is that with reject, a packet e packet is dropped silently.	(TCP RST or ICMP port unrea In either case, the original pa	achable for UDP) is acket is discarded.
Disabled	Disable this rule Set this option to disable	e this rule without re	noving it from the list.		
Interface	WAN		~		
	Choose the interface fro	om which packets mu	ist come to match this rule.		
Address Family	IPv4		~		
	Select the Internet Proto	ocol version this rule	applies to.		
Protocol	TCP/UDP		~		
	Choose which IP protoco	ol this rule should m	atch.		
Source					
		any	~	Source Address	1
Source	invert match.			0	
	The Source Port Range this setting must remain	for a connection is ty nat its default value,	pically random and almost any.	never equal to the destination	ı port. In most cases
Destination	_	anu		Destinction Address	1
Destination Destination	Invert match.	any	~	Destination Address	1
Destination           Destination           Destination           Destination Port	DpenVPN (119.	any	OpenVPN (119- 🗸	Destination Address	1
Destination <u>Destination</u> Destination Port Range	Invert match. OpenVPN (119.  From	any	OpenVPN (119) To To	Destination Address Custom	
Destination <u>Destination</u> Destination Port Range	Invert match.  OpenVPN (119.  From Specify the destination p	Custom Custor or port range for	OpenVPN (119, V To this rule. The "To" field may l	Destination Address Custom be left empty if only filtering a	/ single port.
Destination Destination Destination Port Range Extra Options	Invert match.  OpenVPN (119.  From Specify the destination p	any Custom port or port range for	OpenVPN (119: V To this rule. The "To" field may l	Destination Address Custom De left empty if only filtering a	/ single port.
Destination Destination Port Range Extra Options Log	Invert match.  OpenVPN (119.  From Specify the destination p  Log packets that are Hint: the firewall has limit remote syslog server (see	any Custom boort or port range for handled by this rule ited local log space. se the Status: System	To To To Don't turn on logging for eve Logs: Settings page).	Destination Address Custom be left empty if only filtering a	/ single port.
Destination Destination Destination Port Range Extra Options Log Description	Invert match.  OpenVPN (119.  From Specify the destination p Log packets that are Hint: the firewall has limi remote syslog server (se Autorisation protocole V	any Custom bort or port range for handled by this rule ited local log space. the Status: System	To To this rule. The "To" field may l Don't turn on logging for eve Logs: Settings page).	Destination Address Custom be left empty if only filtering a	1 single port.
Destination Destination Port Range Extra Options Log Description	Invert match.  OpenVPN (119  From Specify the destination p  Log packets that are Hint: the firewall has limi remote syslog server (se A description may be ent displayed in the firewall	any Custom bort or port range for handled by this rule tick local log space. ee the Status: System VPN tered here for admini log.	Don't turn on logging for eve Logs: Settings page).	Destination Address Custom be left empty if only filtering a rything. If doing a lot of loggin um of 52 characters will be un	/ single port.

Exemple de règle de filtrage autorisent le protocole OpenVPN, elle reste semblable à toute autres protocoles

Une fois nos règles créer, nous devons les appliquer. Nous avons une rapide vision sur les règles et leurs actions. Attentions leurs ordres et important. Si la règle de blocage est en première aucune des règles après sera fonctionne.

The firewall rule configuration has been changed. The changes must be applied for them to take effect.								pply Changes				
Floa	ating	WAN	LAN									
Ru	ıles	(Drag	to Change	Order)								
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	~	0 /0 B	IPv4 TCP/UDP	*	*	*	1194 (OpenVPN)	*	none		Autorisation protocole VPN	±∕©0
	×	0/0 B	IPv4 *	*	*	*	*	*	none		Bloque tout le trafic	±
									t i	Add 🧎	Add 🛍 Delete 🖺 Sav	e 🕂 Separate
A												

# 10. Mise en place redirection de port(NAT/PAT)

La redirection de port permet de transferer un port exemple :

Routeur 192.168.1.200 Machine 172.16.0.102

Port d'entrer 192.168.1.200 :8080 Port de sortie 172.16.0.102:80

	System - Interfaces -	Firewall - S	ervices - VI
Status /	Dashboard	Aliases NAT (M	_
System In	formation	Rules Schedules	0 ⊖ ۶
Name	pfSense.localdomain	Traffic Shaper	
System	VirtualBox Virtual Machine Netgate Device ID: <b>fd20bcc0</b>	Virtual IPs	
BIOS	Vendor: innotek GmbH		

Pour cela, nous devons aller dans « Firewall / Nat »

### Voila un exemple de régles qui sont translaté

R	ules	k										
			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
Ma	chine	e Hop	per - 172.1	6.0.101								Û
8	~	24	WAN	TCP			WAN address	8081	172.16.0.101	80 (HTTP)	Serveur Web - Hopper	Ø 🗋 🖻
	~	24	WAN	TCP	*	*	WAN address	2121	172.16.0.101	21 (FTP)	Serveur FTP - Hopper	100
0	~	<b>)</b> ¢	WAN	TCP	10 C	- #C	WAN address	2201	172.16.0.101	22 (SSH)	Serveur Web - Hopper	D 🖬
	~	24	WAN	TCP/UDP			WAN address	8001	172.16.0.101	8000	Serveur Ajenti - Hopper	/ 🗋 🖻
	~	24	WAN	TCP	1	*).	WAN address	49152 - 50000	172.16.0.101	49152 - 50000	Serveur FTP Port Passif - Hopper	Ø 🗋 🖻
Ma	chin	e Phy	sique - 172	16.0.102								Û
	~	25	WAN	TCP	×.	. <del>1</del> .	WAN address	8080	172.16.0.102	80 (HTTP)	Serveur Web - Physique	100
0	~	2\$	WAN	TCP/UDP	w.		WAN address	33890	172.16.0.102	3389 (MS RDP)	RDP - Physique	100
	~	24	WAN	TCP/UDP	*	*	WAN address	33891	172.16.0.102	33891	RDP - Hopper	Ø 🗋 🖬
	~	<b>2</b> ¢	WAN	TCP/UDP	*		WAN address	33892	172.16.0.102	33892	RDP - Intratec	<sup>1</sup>
0	~	<b>C</b>	WAN	TCP/UDP	- <b>*</b> S	*	WAN address	33893	172.16.0.102	33893	RDP - Centreon	<00
0	~	2\$	WAN	TCP/UDP	w.	*	WAN address	33894	172.16.0.102	33894	RDP - PFSENSE	♪□□
Ma	chine	e Intra	atec - 172.1	6.0.103								Û
	~	24	WAN	TCP	*	*	WAN address	2203	172.16.0.103	22 (SSH)	Serveur SSH - Intratec	/ 🗋 🖻
8	~	<b>)</b> ¢	WAN	TCP	10	10	WAN address	1138	172.16.0.103	1138	Serveur Web - Intratec	/ 🗋 🛍
0	~	<b>2</b> ¢	WAN	TCP			WAN address	8003	172.16.0.103	8000	Serveur Ajenti - Intratec	Ø 🗋 🖬
Ma	chine	e Cen	treon - 172	16.0.104								Û
	~	24	WAN	TCP	•	•	WAN address	8084	172.16.0.104	80 (HTTP)	Serveur Web - Centreon	/ 🗋 🖬
8	~	24	WAN	TCP	. *		WAN address	2204	172.16.0.104	22 (SSH)	Serveur SSH - Centreon	/00
Ma	chin	e PFS	ENSE - 172	2.16.0.254								Û
0	~	2¢	WAN	TCP	*	*	WAN address	8888	172.16.0.254	80 (HTTP)	Serveur Web - PFSENSE	Ø 🗇 🖬
	~	24	WAN	TCP	*		WAN address	22254	172.16.0.254	22 (SSH)	Serveur SSH - PFSENSE	/ 🗋 🖻
										1 Add	1 Add 前 Delete 🖺 Save 🛃	Separator

Exemple de régles qui peuvent être crées

Pour créer une régle NAT, cliquer sur "ADD"



Pour cela, nous devons cliquer sur « ADD »

dit Redirect Entry						
Disabled	Disable this rule					
No RDR (NOT)	Disable redirection for	or traffic matching this rule				
	This option is rarely neer	ded. Don't use this without thorou	igh knowledge of the implicati	ions.		
Interface	WAN		•			
	Choose which interface	this rule applies to. In most cases	s "WAN" is specified.			
Protocol		Notre protocole				
	Choose which protocol t	this rule should match. In most ca	ases "TCP" is specified.			
Source	Display Advanced					
Destination	Invert match.	WAN address	,	•	1	
		Туре		Address/mask		
Destination port range	Other	<ul> <li>Port Externe</li> </ul>	Other	<ul> <li>Saisir port si ran</li> </ul>	ger	
Redirect target IP	From port Specify the port or port r	Custom range for the destination of the pa machine en interne	To port acket for this mapping. The 'to'	Custom offield may be left empty if only	v mapping a single port.	
Redirect target IP	From port Specify the port or port r IP Enter the internal IP addi e.g.: 192.168.1.12	Custom range for the destination of the parameters machine en interne ress of the server on which to ma	To port acket for this mapping. The 'to p the ports.	Custom	r mapping a single port.	
Redirect target IP Redirect target port	From port Specify the port or port or IP Enter the internal IP addi e.g.: 192.168.1.12 Other	Custom range for the destination of the pa machine en interne ress of the server on which to ma	To port acket for this mapping. The 'to p the ports.	Custom i field may be left empty if only Port interne	mapping a single port.	
Redirect target IP Redirect target port	From port Specify the port or port or IP Enter the internal IP addi e.g.: 192.168.1.12 Other Port	Custom range for the destination of the parameters machine en interne ress of the server on which to ma	To port socket for this mapping. The 'to p the ports.	Custom v field may be left empty if only Port interne	mapping a single port.	
Redirect target IP Redirect target port	From port Specify the port or port or P Enter the internal IP add e.g.: 192.168.1.12 Other Port Specify the port on the n	Custom range for the destination of the pr machine en interne ress of the server on which to ma machine with the IP address enter	To port acket for this mapping. The 'to p the ports. Custom red above. In case of a port rar	Custom c field may be left empty if only Port interne nge; specify the beginning por	mapping a single port.	wil
Redirect target IP	From port Specify the port or port r IP Enter the Internal IP add e.g.: 192.168.1.12 Other Port Specify the port on the n calculated automaticality identical	Custom range for the destination of the po machine en interne ress of the server on which to ma nachine with the IP address enter ).	To port scket for this mapping. The 'to' p the ports. Custom red above. In case of a port rar	Custom field may be left empty if only Port interne nge, specify the beginning port	mapping a single port.	wil
Redirect target IP Redirect target port Description	From port Specify the port or port or IP Enter the internal IP add e.g.: 192.168.1.12 Other Port Specify the port on the n calculated automatically This is usually identical Description	Custom Custom machine en interne ress of the server on which to me machine with the IP address enter ). to the "From port" above: addin de la renérer facilie	To port Lacket for this mapping. The to p the ports. Custom ed above. In case of a port rar	Custom field may be left empty if only Port interne nge, specify the beginning por	r mapping a single port.	liw
Redirect target IP Redirect target port Description	From port Specify the port or port in Entre the internal IP add e.g.: 192.168.1.12 Other Port Specify the port on the in calculated automatically This is usually identical to Description A description may be en	Costom ange for the destination of the pi machine en interne reas of the server on which to ma nachine with the IP address enter 0, to the "From port" above. afin de la repérer facile steed here for administrative refe	To port Locket for this mapping. The to p the ports. Uustom ed above. In case of a port rar ment reroe (not parsed).	Custom field may be left empty if only Port interne nge, specify the beginning por	mapping a single port.	wi
Redirect target IP Redirect target port Description No XMLRPC Sync	From port : Specify the port or port r P Enter the internal IP add e.g. : 192.168.1.12 Other Port Specify the port on the n calculated automatically This is usually identical Description may be en D not automatically	Costom anage for the destination of the parameter of the destination of the parameters of the server on which to ma neachine with the IP address enter ), to the "From port" above. afin de la repérer facille tend here for administrative refe sympt to other codministrative refe	To port acket for this mapping. The to p the ports. Used above. In case of a port rar ment ence (not parsed).	Custom 2 field may be left empty if only Port interne nge, specify the beginning port	mapping a single port. machine	wi
Redirect target IP Redirect target port Description No XMLRPC Sync	From port: Specify the port or port in Enter the internal IP and the internal IP and e.g.:192.168.1.12 Other Port Specify the port on the extensional calculated automatically This is usually identical to <b>Description</b> A description my be em ID on on automatically Do not automatically	Costom analyse for the destination of the pu- machine en interner machine with the IP address enter () to the "From port" above. afin de la repérer facile teterd here for administrative refr synct to other CARP members Matter from automatically sync	To port to port p the ports. te above. In case of a port rar ment terree (not parsed). Ing to other CARP members. 1	Custom field may be left empty if only Port interne nge, specify the beginning pon This does NOT prevent the rule	mapping a single port. machine to fithe range (the end port from being overwritten or	wi
Redirect target IP Redirect target port Description No XMLRPC Sync NAT reflection	From port Specify the port or port or IP Enter the internal IP and e.g.:192.168.1.12 Other Port Specify the port on the calculated automatically This is usually identical to Mesoription A description may be O on of automatically This prevents the rule or Use system default	Costom anage for the destination of the pa- machine en interner machine with the the destination of the machine with the the destination of the anachine with the the destination of the machine with the the destination of the destination of the machine with the the destination of the destination of the machine with the destination of the destination of the destination of the machine with the destination of the destination of the destination of the machine with the destination of the	To port To port port the rorthis mapping. The to port the ports. To the ports. To use of a port ran ment ing to other CARP members. I Ty	Custom field may be left empty if only Port interne nge, spealty the beginning port	mapping a single port. machine t of the range (the end port from being overwritten or	wi
Redirect target IP Redirect target IP Description No XMLRPC Sync NAT reflection Filter rule association	From port: Beelity the port or port i Beelity the port or port i Enter the internal IP a Enter the IP and the enter the internal Enter the port on the enter the internal Description A description may be ent Do not automatically Do not automatical	Costom anage for the destination of the pu- machine en interner machine entitle the term of the server on which to ma- machine with the IP address enter <i>i</i> ), to the "From port" above. affin de la repérer facile tered here for administrative refr sync to other CARP members Master from automatically sync use	To port To port port except for this mapping. The to p the ports. w Custom the datove. In case of a port rar ment ment ing to other CARP members. T w	Custom field may be left empty if only Port interne nge, specify the beginning pon This does NOT prevent the rule	mapping a lingle port. machine of the range (the end port from being overwritten or	will Sł

Créer notre régle, puis la sauvegarder

Une fois créer, nous devons la mettre dans le bon séparateur pour mieux se repérer.

Puis, nous devons aller dans « **Firewall / Rules** ». Toutes régles dans rules sont crées grâce au NAT créer précédament, il faut juste effectuer plusieurs manipulations si elle ne sont pas dans le bon ordre.

R	lles	(Drag to Cha	inge Order)									
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
Ma	chine	Hopper - 172.1	5.0.101									Û
	~	18 /17.41 MiB	IPv4 TCP	*	*	172.16.0. <mark>1</mark> 01	80 (HTTP)	*	none		NAT Serveur Web - Hopper	100
	~	1 /339 KiB	IPv4 TCP	*	*	172.16.0.101	22 (SSH)	*	none		NAT Serveur Web - Hopper	±100
0	~	2 /164 KiB	IPv4 TCP	*	*	172.16.0.101	21 (FTP)	*	none		NAT Serveur FTP - Hopper	100 t
1	~	0 /1.47 MiB	IPv4 TCP	×	*	172.16.0. <mark>1</mark> 01	491 <mark>52 - 5</mark> 0000	×	none		NAT Serveur FTP Port Passif - Hopper	1.100
0	~	12 /19.58 MiB	IPv4 TCP/UDP	*	*	172.16.0.101	8000	*	none		NAT Serveur Ajenti - Hopper	100 t
Ma	chine	Physique - 172.	16.0.102									Û
	~	0 /75.99 MiB	IPv4 TCP	*	*	172.16.0.102	80 (HTTP)	*	none		NAT Serveur Web - Physique	100 t
0	4	0 /25 KiB	IPv4 TCP/UDP	*	*	172.16.0.102	3389 (MS RDP)	*	none		NAT RDP - Physique	±100
	~	0 /19 KiB	IPv4 TCP/UDP	*	¥.	172.16.0.102	33891	×.	none		NAT RDP - Hopper	100 t
1	~	0 /14 KiB	IPv4 TCP/UDP	*	*	172.16.0.102	33892	*	none		NAT RDP - Intratec	±100
	~	0 /14 KiB	IPv4 TCP/UDP	38	*	172.16.0.102	33893	*	none		NAT RDP - Centreon	±100
0	~	0 /2 KiB	IPv4 TCP/UDP	*	*	172.16.0.102	33894	*	none		NAT RDP - PFSENSE	100 t
Ma	chine	e Intratec - 172.1	6.0.103									Û
9	~	0 /816 B	IPv4 TCP	*	*	172.16.0.103	1138	*	none		NAT Serveur Web - Intratec	1000
	~	0 /0 B	IPv4 TCP	*	*	172.16.0.103	22 (SSH)	*	none		NAT Serveur SSH - Intratec	100 to
0	~	0 /816 B	IPv4 TCP	*	*	172.16.0.103	8000	*	none		NAT Serveur Ajenti - Intratec	100 t
Ma	chine	Centreon - 172.	16.0.104									Û
۵	~	0 /0 B	IPv4 TCP	*	*	172.16.0.104	22 (SSH)	w	none		NAT Serveur SSH - Centreon	±100
	~	0 /5.47 MiB	IPv4 TCP		*	172,16.0.104	80 (HTTP)	*	none		NAT Serveur Web - Centreon	100 t
Ma	chine	PFSENSE - 172	.16.0.254									Û
	~	7 /3.67 MiB	IPv4 TCP	*	<b>1</b> 5	172.16.0.254	80 (HTTP)	*	none		NAT Serveur Web - PFSENSE	±100
11	~	0 /0 B	IPv4 TCP	×	*	172.16.0.254	22 (SSH)	*	none		NAT Serveur SSH - PFSENSE	±100
0	×	0 /6.64 MiB	IPv4 *	*	*		*	*	none			100 t

Exemple de liste de régles NAT/PAT

Nous devons elever les 2 régles qui bloque toutes entrées « Interface / WAN »

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

Les deux cases doivent être décochées, car elles empechent de faire du filtrage et bloquent toutes les entrées.

Afin de sécuriser notre réseau, nous allons bloquer tout les autres trafiques qui veulent entrer(Si elle n'existe pas). Nous allons donc créer une rule dans « **Firewall / Rules** », qui doit être en dernier. Pour cela, nous devons cliquer sur "**ADD**"



#### La régle doit être identique

rewall / Rules /	Edit 🗵 🛱 🛄 🖻
it 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	WAN   Choose the interface from which packets must come to match this rule.
Address Family	IPv4     T       Select the Internet Protocol version this rule applies to.
Protocol	Any T Choose which IP protocol this rule should match.
urce	
Source	Invert match.     any     Source Address     /
stination Destination	Invert match.  Invert match.  Destination Address  I
tra 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 (s 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 firewa log.
Advanced Options	Display Advanced
le Information	
Created	2/22/18 14:07:38 by admin@172.16.0.102
Updated	2/22/18 14:18:32 by admin@172.16.0.102
	🖺 Save

Cette régle bloque tout le trafic et donc doit être mis tout à la fin, elle permet que tous les autres protocoles/réquetes soit abandoneronner

# 11. Mise en plage de Liste de blockage

Nous allons voir comment mettre en place un liste de blockage, qui permet de refuser l'accés à certains site web, en fonction des catégories (Téléchargement illégale, Site d'achats, Sites adules, etc...).

Pour cela, nous pouvons la créer ou bien en utiliser une déjà prete créer par d'autres personnes qui on ressencer ces sites.

Pour pouvoir mettre en place des listes de blockage, nous devons installer plusieurs packages qui doivent être installer sans ces paquets il nous sera impossible de mettre en place des restriction grace aux listes.

Dans mon cas, je vais mettre en place la blackliste de Toulouse.

Pour cela, nous devons installer les paquets nous devons aller dans "Système / Packages Manager"

Une fois dans le manageur, nous devons aller dans "**Available Packages**" et installer les paquets Squid, SquidGuard et Lightsquid. Nous pouvons rechercher les paquets avec le terme "squid"

Si il nous manque des paquets, il nous sera impossible de mettre en place notre filtrage par rapport a nos sites web.

nstalled Pac	kages A	vailable Packages	
Search			•
Search term		squid Both Q Search O Clear	
		Enter a search string or *nix regular expression to search package names and descriptions.	
Package	5		
Name	Version	Description	
_ightsquid	3.0.6_4	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. Package Dependencies:	🕂 Install
squid	0.4.42_1	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.         Package Dependencies:          % squid-radius_auth-1.10           % squid-3.5.27           % c-icap-modules-0.4.5	🕂 Install
squidGuard	1.16.4	High performance web proxy URL filter. Package Dependencies: % squidguard-1.4_15	+ Install

Chaque paquets doivent être installer séparement

Pour chaque installation une demande de confirmation d'installation nous ai demander

System / Package Manager / Package Installer	0
Installed Packages Available Packages Package Installer	
Confirmation Required to install package pfSense-pkg-squidGuard.	
✓ Confirm	



172

Pour chaque installation, nous avons l'avancement, il est important de ne pas fermer la page, si non l'installation échou.

e wait while the installation of pfSense-pkg-squidGuard completes.	0
e wait while the installation of <b>pfSense-pkg-squidGuard</b> completes.	
nay take several minutes. Do not leave or refresh the page!	
ed Packages Available Packages Package Installer	
rage Installation	
nstalling nfSense-nkg-smidGuard	
ing pfSense-core repository catalogue	
se-core repository is up to date.	
ing pfSense repository catalogue	
se repository is up to date.	
epositories are up to date.	

Nous avons l'avancement et le détail des actions effectuer lors de l'installation

Une fois les paquets installer, nous allons pouvoir installer notre blacklist, pour cela, nous devons aller dans "Services / SquidGuard Proxy Filter".

Nous devons activer la blacklist et nous devons mettre le lien de notre blackliste, ce qui nous permet de la mettre à jour facilement en cas de mise à jour de celle-ci

De	o NOT enable this on NanoBSD installs!
Blacklist proxy	
BI	lacklist upload proxy - enter here, or leave blank.
Fo	ormat: host:[port login:pass] . Default proxy port 1080.

Lien de la blacklist : <u>http://dsi.ut-capitole.fr/blacklists/download/blacklists\_for\_pfsense.tar.gz</u>

Ce n'est pas la seul blackliste existante, mais elle comprend beaucoup de site.

Maintenant, nous devons nous rendre dans "Système / Géneral / Blacklist", puis la télécharger

	Common ACL	Groups ACL	l'arget categories	limes	Rewrites	Blacklist	Log	XIVILREG Sync	
Blacklist Updat	te								
0 % http://dsi.ut-cap	oitole.fr/blacklists/do	wnload/blacklists_	_for_pfsense.tar.gz						
♣ Download	Canad D Postor	o Dofault							
	J Restor	- Activities and a second s							
Enter FTP or HTTP p	oath to the blacklist a	rchive here.							
									3
😢 Blacklist u	pdate Log								
Blacklist u Begin blacklist u	pdate Log								
Blacklist u Begin blacklist u Start download. Download archive J	pdate Log	ole.fr/blacklist	s/download						
Blacklist u Begin blacklist u Start download. Download archive 1 /blacklists_for_p:	pdate Log pdate http://dsi.ut-capit fsense.tar.gz	ole.fr/blacklist	.s/download						
Blacklist up Begin blacklist up Start download. Download archive 1 /blacklists_for_p: Download complete	pdate Log pdate http://dsi.ut-capit fsense.tar.gz	ole.fr/blacklist	s/download						
Blacklist up Begin blacklist up Start download. Download archive 1/ blacklists_for_p: Download complete Unpack archive Scan blacklist.ca	pdate Log pdate http://dsi.ut-capit fsense.tar.gz	ole.fr/blacklist	s/download						
Blacklist u Start download. Download archive I /blacklist_for_p) Download complete Unpack archive Scan blacklist cat	pdate Log pdate http://dsi.ut-capit fsense.tar.gz tegories.	ole.fr/blacklist	s/download						
Blacklist u Begin blacklist u Start download. Download archive 1 /blacklists_for_p. Download complete Unpack archive Scan blacklist car Found 58 items. Start rebuild DB.	pdate Log pdate http://dsi.ut-capit fsense.tar.gz tegories.	ole.fr/blacklist	/s/download						
Blacklist u Start download. Download archive 1 Ohacklist for p Download complete Unpack archive Scan blacklist car Found 58 items. Start rebuild DB. Copy DB to workdi	pdate Log pdate http://dsi.ut-capit fsense.tar.g2 tegories. r.	ole.fr/blacklist	s/download						
Blacklist u Begin blacklist u Start download. Download archive i /blacklists_for_D: Download complete Unpack archive Scan blacklist ca Start rebuild DB. Copy DB to workdii.	pdate Log pdate http://dsi.ut-capit fsense.tar.gz tegories. r. proxy.	ole.fr/blacklist	s/download						
Blacklist u Begin blacklist u Start download. Download archive I /blacklists_for_p: Download complete Unpack archive Scan blacklist car Found 58 items. Start rebuild DB. Copy DB to workdi Blacklist update of	pdate Log pdate http://dsi.ut-capit fsense.tar.gz tegories. r. proxy. complete.	ole.fr/blacklist	:s/download						

Pour mettre à jour ou installer notre liste de blockage, nous devons la télécharger avec le bouton "Download"

Un avancement du téléchargement est fait et la base de données ajoute les éléments de la liste

Package /	SquidGuar	d / Black	lists						
General settings	Common ACL	Groups ACL	Target categorie	s Times	Rewrites	Blacklist	Log XMLR	PC Sync	
Blacklist Upd	ate								
Blacklist DB rebuild	d progress								
1%									
1 %	Cancel 5	Restore Defaul							
1%	Cancel	Restore Default							
1 %	Cancel D	Restore Default	ere.						
1 % ▲ Download Enter FTP or HTTP ③ Blacklist	path to the blac	Restore Defaul	ere.						
1% Download Enter FTP or HTTP Blacklist Begin blacklist Start download.	Cancel D F path to the blac update Log update	Restore Defaul	ere,				_	_	_
1%         Download         Enter FTP or HTTP         Begin blacklist         Start download.         Download archive	Cancel C	Restore Default klist archive he -capitole.fr/l	blacklists/downld	pad			_	_	_
1%       Download       Enter FTP or HTTP       Blacklist       Begin blacklist       Start download       Download archive       Obwnload complet	path to the blac update Log update http://dsi.ut- pfsense.tar.gz e	Restore Default klist archive he -capitole.fr/)	ere.	nad					
1% Download Enter FTP or HTTP Begin blacklist Start download. Download archive /blacklists_for_ Download complete Unpack archive Scan blacklist of	Cancel Ca	Restore Default klist archive he -capitole.fr/1	blacklists/downlo	vad					
1% ► Download Enter FTP or HTTP ► Blacklist Start download. Download archive /blacklists_for_ Download complet Unpack archive Scan blacklist or Found 58 items. Start rabuild DB	Cancel Ca	Restore Default klist archive he -capitole.fr/1	blacklists/downlo	zad			_		
1% ► Download Enter FTP or HTTP ■ Blacklist Begin blacklist Start download Download archive /blacklists_for_ Download complet Unpack archive Scan blacklist c Found 58 items. Start rebuild DB Completed 1 %	Cancel C path to the blace update Log update http://dsi.ut- pfsense.tar.gz e ategories	Restore Default klist archive he -capitole.fr/l	ere.	bad					

Nous avons un status d'avancement du téléchargement de notre blacklist, cela peut prendre un moment

Une fois notre blackliste télécharger et ajouter, nous devons nous rendre dans "Services / SquidGuard Proxy Filter" et activer le service SquidGuard si il ne l'est pas

General settings Con	nmon ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log	XMLRPC Sync	
General Options									
Enable	Important: Ple The Save bu To activate	ease set up at le utton at the b squidGuard c	ast one category on the ottom of this page r configuration change	e 'Target Cate nust be cli es, <b>the App</b>	gories' tab befo cked to save ( <b>Iy button mu</b>	re enabling. Se configuratior <b>st be clicked</b>	e this link 1 1 change I.	or details. S.	

Pour l'activer, cocher la chase "Enable" et cliquer sur "Apply"

On verifie que notre paquet squidGuard soit bien actif

eneral settings Co	mmon ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync
General Options	
Enable	☑ Check this option to enable squidGuard.
	Important: Please set up at least one category on the 'Target Categories' tab before enabling. See this link for details.
	Important: Please set up at least one category on the 'Target Categories' tab before enabling. See this link for details. The Save button at the bottom of this page must be clicked to save configuration changes.

Si il ne démarre pas, il est possible qu'il ne soit pas bien installer ou bien la configuration incorrecte

# 12. Mise en place d'un VPN (OpenVPN)

Il est possible avec PFSENSE de mettre en place directement le VPN sur le routeur, ce qui nous evite d'avoir un serveur dédié à cette tache.

Pour cela, nous devons nous rendre dans "Système / Certificate Manager / CAs"

0.0						
0-						
ce	es Certifica	cate Revocation				
or	uthorities	s				
or	uthorities	s	Cortificator	Dictin	guished Name	guished Name In Lise

Nous devons créer notre autorité de certification, pour cela nous devons l'ajouter grace au bouton "ADD"

Nous allons créer notre autorité de certification.

reate / Edit CA		
Descriptive name	pfSense FireWall	
Method	Create an internal Certificate Authority	~
nternal Certifica	te Authority	
Key length (bits)	2048	×
Digest Algorithm	sha256 NOTE: It is recommended to use an algorithm stro	onger than SHA1 when possible.
Lifetime (days)	3650	ŧ.
Country Code	FR	~
State or Province	Centre-Val-de-Loire	
City	Tours	
Organization	Paul Louis Courier	
rganizational Unit	BTS SIO	
Email Address	yohan.fresneau@outlook.fr	
One News	frequency of the	

Les informations peuvent être modifier et doivent être adapter

### Nous allons créer le certification de notre serveur OpenVPN

Add/Sign a New	Certificate	
Method	Create an internal Certificate	
Descriptive name	pfSense OpenVPN	
Internal Certifica	ate	
Certificate authority	pfSense FireWall	
Key length	2048	
Digest Algorithm	sha256	
	NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.	
Lifetime (days)	3650	
Country Code	FR	
State or Province	Centre-Val-de-Loire	
City	Tours	
Organization	Paul Louis Courier	
Organizational Unit	BTS SIO	
Email Address	yohan.fresneau@outlook.fr	
Common Name	pfsense.sca3.lan	
Certificate Attrib	butes	
Attribute Notes	The following attributes are added to certificates and requests when they are created or signed. These attributes differently depending on the selected mode.	behave
	For Internal Certificates, these attributes are added directly to the certificate as shown.	
Certificate Type	Server Certificate	
	Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting ab the signed certificate.	ilities to,
Alternative Names	FQDN or Hostname	
	Type Value	
	Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the ce	ertificate

Les informations du certification du serveur VPN doivent être identique ou bien adapter

Nous créer un utilisateur qui pourra par la suite se connecter directement au VPN.

Syste	em / User Ma	anager / Users			0
Users	Groups Settings	Authentication Servers			
Users	Groups Settings	Authentication Servers			
Users	Groups Settings	Authentication Servers			
Users	Groups Settings Username	Authentication Servers Full name	Status	Groups	Actions
Users	Groups Settings Username admin	Authentication Servers Full name System Administrator	Status 🗸	Groups admins	Actions J

Pour ajouter un utilisateur, nous devons cliquer sur " ADD"

La création de notre utilisateur se fait comme ceci

Users Groups Settin	gs Authentication Servers		
User Properties			_
Defined by	USER		
Disabled	This user cannot login		
Username	client-openvpn		
Password	•••••	•••••	
Full name	Client VPN User's full name, for administrative information only		
Expiration date	Leave blank if the account shouldn't expire, otherwise enter	the expiration date as MM/DD/YYYY	
Custom Settings	Use individual customized GUI options and dashboard la	yout for this user.	
Group membership	admins		1
	Not member of	Member of	

Cela est identique pour tous autres utilisateurs si l'on souhaite en ajouter d'autres

Nous allons créer le ceritificat pour les client, afin qu'il puissent se connecter au VPN

2	2		
Add/Sign a New	Certificate		
Method	Create an internal Certificate	×	
Descriptive name	Client VPN		
Internal Certifica	te		
Certificate authority	pfSense FireWall	Y	
Key length	2048	~	
Digest Algorithm	sha256 NOTE: It is recommended to use an algorithm	stronger than SHA1 when possible.	
Lifetime (days)	3650		
Country Code	FR	~	
State or Province	Centre-Val-de-Loire		
City	Tours		
Organization	Paul Louis Courier		
Organizational Unit	BTS SIO		
Email Address	yohan.fresneau@outlook.fr		
Common Name	afrance area teal		

	Ine onowing autobase are added to be inicates and requests when they are created or signed. These autobase behave differently depending on the selected mode.
	For Internal Certificates, these attributes are added directly to the certificate as shown.
Certificate Type	User Certificate 🗸
	Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.
Alternative Names	FQDN or Hostname
	Type Value
	Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate a an Alternative Name. The signing CA may ignore or change these values.
Add	+ Add
	😫 Save

Notre certificat est universelle pour tous les clients voulent se connecter, car il se connecte grace à des mot de passe et des nom utilisateur

Nous devons lié ce certificat à notre utilisateur, pour cela nous devons retourner sur notre utilisateur

I I lies individual sustantized CIII antions and deabhoard levout for this uper

t member of Move to "Member of" list Id down CTRL (PC)/COMMAN	D (Mac) key to select multiple	Member of <a> </a> <ul> <li>Move to "Not member of eitems.</li> </ul>	" list
t member of Move to "Member of" list Id down CTRL (PC)/COMMAN	D (Mac) key to select multiple	Member of Move to "Not member of a items.	° list
Move to "Member of" list	ID (Mac) key to select multiple	Move to "Not member of     terns.	" list
ld down CTRL (PC)/COMMAN	ID (Mac) key to select multiple	e items.	
herited from	Name	Description	Action
			+ Add
ime		CA	
			+ Add
	nerited from	me Name	me Description

Nous devons cliquer sur "ADD", dans "User Certificates"

Nous devons séléctionner le certificat au quelle on le lie

System / Cert	ficate Manager / Certificates / Edit	•
CAs Certificates C	artificate Revocation	
Add/Sign a New (	ertificate	
Method	Choose an existing certificate	
Descriptive name	client-openvpn	
Choose an Existin	g Certificate	
Eviation Continuation		

On séléctionne notre certificat créer précédament pour nos utilisateurs

Nous allons maintenant, mettre en place notre serveur VPN, nous allons intaller le paquet openVPNclient-export qui va nous permettre de créer nos fichiers pour OpenVPN client.

MMUNITY EDITION			
System / F	Package	Manager / Available Packages	0
Installed Package	s <mark>Availa</mark> bl	e Packages	
Search			Θ
Sea <mark>rch t</mark> erm	o	venvpn Both 🛛 Q Search 🕽 Clear	
	Ent	er a search string or *nix regular expression to search package names and descriptions.	
Packages			
Name	Version	Description	
openvpn-client- export	1.4.14	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	+ Install
		Package Dependencies:	

On cliquer sur intaller afin d'ajouter le paquet

Nous allons installer le serveur VPN et le configurer

cess Server Setup				
s wizard will provide guidance to wizard may be stopped at any	through an OpenVPN Rem time by clicking the logo	iote Access Server Set image at the top of the	up . e screen.	
tion Backend Type		NY 12		
ocal User Access	~			
hi: he	his wizard will provide guidance he wizard may be stopped at any ation Backend Type Local User Access	his wizard will provide guidance through an OpenVPN Rem he wizard may be stopped at any time by clicking the logo ation Backend Type Local User Access	his wizard will provide guidance through an OpenVPN Remote Access Server Set he wizard may be stopped at any time by clicking the logo image at the top of the ation Backend Type Local User Access	his wizard will provide guidance through an OpenVPN Remote Access Server Setup . he wizard may be stopped at any time by clicking the logo image at the top of the screen. ation Backend Type Local User Access



Wizard / Oper	NVPN Remote Acces	s Server Setup /	Certificate Authority Selection	0
	Step 5 of 11			
Certificate Autho	ority Selection			
	OpenVPN Remote Access Ser	ver Setup Wizard		
Choose a Certifi	cate Authority (CA)			
Certificate Authority	ofSense FireWall			

On séléctionne notre autorité de certification, puis on clique sur "Next"

Wizard / Oper	VPN Remote Access Server Setup / Server Certificate Selection	0
	Step 7 of 11	
Server Certificat	e Selection	
	OpenVDN Remote Access Server Setup Wizerd	
Choose a Server	Certificate	
Certificate	nfSansa Onan\/PN	

On séléctionne le certificat que l'on à créer pour notre serveur, puis "Next"

Vizard / Oper	VPN Remote Access Server Setup / Server Setup         Image: Optimized setup / Server Set				
_	Step 9 of 11				
erver Setup					
	OpenVPN Remote Access Server Setup Wizard				
eneral OpenVPI	N Server Information				
lata-face					
Interrace	WAN				
Destanal					
Protocol	0DP ×				
	Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.				
Local Port	1194				
	Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port peeds to be used				
Description					
Description	A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to				
	distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.				
ryptographic Se	ettings				
S Authentication	И				
	Enable authentication of TLS packets.				
enerate TLS Key					
	Automatically generate a shared TLS authentication key.				
TLS Shared Key					
	Paste in a shared TLS key if one has already been generated.				
DH Parameters Length	2048 bit 🗸				
	Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH				
	parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.				
Encryption	AES-256-CBC (256 bit kev. 128 bit block)				
Algorithm					
	The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired. Certain algorithms will perform hetter on different hardware denending on the evailability of				
	supported VPN accelerator chips.				
Auth Digest	SHA1 (160-bit)				
Algorithm					
-	The method used to authenticate traffic between endpoints. This action must match as the aliant and account of the traffic between and points.				

<form><form></form></form>	Tunnel Settings	
<form><form></form></form>	Tunnel Network	10.8.0.0/24 This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.
<form><form><form></form></form></form>	Redirect Gateway	G Force all client generated traffic through the tunnel.
<form><form></form></form>	Local Network	172.16.53.0/24 This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
<form><form></form></form>	Concurrent Connections	Specify the maximum number of clients allowed to concurrently connect to this server.
<form><form></form></form>	Compression	Omit Preference (Use OpenVPN Default)
<form><form></form></form>	Type-of-Service	of time If OpenVPN detects that the data in the packets is not being compressed efficiently.  Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
<form><form></form></form>	Inter-Client Communication	Allow communication between clients connected to this server.
<form><form></form></form>	Duplicate Connections	Allow multiple concurrent connections from clients using the same Common Name.     NOTE: This is not generally recommended, but may be needed for some scenarios.
<form></form>	Client Settings	
<form><form></form></form>	Dynamic IP	☑ Allow connected clients to retain their connections if their IP address changes.
<form></form>	Topology	Subnet – One IP address per client in a common subm Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (IOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".
<form><form></form></form>	DNS Default Domain	Provide a default domain name to clients.
<form><form></form></form>	DNS Server 1	172.16.53.1 DNS server IP to provide to connecting clients.
<form><form></form></form>	DNS Server 2	DNS server IP to provide to connecting clients.
NNS Server 1   DNS Server 1   Network: Time Protocol server to provide to connecting clients.   NTP Server 2   Network: Time Protocol server to provide to connecting clients.   NTP Server 1   Network: Time Protocol server to provide to connecting clients.   NetBiOS Option:   Desuble ceptions: b mode (broadcasts), prode (point-to-point name queries to a WINS server), m-mode (broadcast then queries serve), and h-mode (query name server), then broadcast).   NetBIOS Scope ID   A NetBIOS Scope ID   B C Scope ID   A NetBIOS Scope ID   B C Scope ID	DNS Server 3	DNS server IP to provide to connecting clients.
<form></form>	DNS Server 4	DNS server IP to provide to connecting clients.
NPP Server 2   NetBIOS Options   Belle NetBIOS over TOP/IP:   The server 1   Possible options: b-node (broadcasts), pnode (point hop options (netuding WINS) will be disabled.   NetBIOS Scope ID   Possible options: b-node (broadcasts), pnode (point hop option are queries to a WINS server), mnode (broadcast hen grame server), and hnode (queries ware), the mode and	NTP Server	Network Time Protocol server to provide to connecting clients.
IntellioS Options     IntellioS Node Type     IntellioS Node Type     IntellioS Node Type     Possible options: brode (broadcasts), prode (point to point name queries to a WINS server), mende (broadcast then query name server), and hende (query name server).       NINS Server 1    Andonows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.    Num Server 2   Andonom     Advanced	NTP Server 2	Network Time Protocol server to provide to connecting clients.
NetBIOS Node Type     Possible options: b-nade (broadcasts), p-node (point-to-point name queries to a WINS server), m-nade (broadcast the query name server), and h-nade (query name server, then broadcast).   NetBIOS Scope ID   ANEBIOS Scope ID   Possible options: In a single network to only those nodes with the same NetBIOS scope ID.   WINS Server 1   AVINdows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.   Advanced   Enter arey additional options to add to the OperVPIN server configuration here, separated by a semicolon. EXAMPLE: push to 10.0.0 2552:255.0°.	NetBIOS Options	Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
query name server), and h-node (query name server, then broadcast).     NetBIOS Scope ID     A Nondows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.     A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.     Advanced         Enter any additional options to add to the OpenVPN server configuration here, separated by a semicolon. EXAMPLE push 'rota to 10.0.0.255.255.255.0°.         Plote 1	NetBIOS Node Type	none v Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then
Image: Traffic on a single network to only those nodes with the same NetBIOS scope ID.         Image: Traffic on a single network to only those nodes with the same NetBIOS scope ID.         Image: Traffic on a single network to only those nodes with the same NetBIOS scope ID.         Image: Traffic on a single network to only those nodes with the same NetBIOS scope ID.         Image: Traffic on a single network to only those nodes with the same NetBIOS scope ID.         Image: Traffic on a single network to only those nodes with the same NetBIOS scope ID.         Image: Traffic on a single network to only those nodes with the same NetBIOS scope ID.         Image: Traffic on a single network to only those nodes with the same NetBIOS scope ID.         Image: Traffic on a single network to only those nodes with the same NetBIOS scope ID.         Image: Traffic on a single network to only those nodes with the same NetBIOS scope ID.         Image: Traffic on a single network to only those nodes with the same NetBIOS scope ID.         Image: Traffic on a single network to only those node ID.         Image: Traffic on a single network to only those node ID.         Image: Traffic on a single network to only those node ID.         Image: Traffic on a single network to only those node ID.         Image: Traffic on a single network to only those node ID.         Image: Traffic on a single network to only those node ID.         Image: Traffic on a single network to only those node ID.         Image: Traffic on a single network to no	NetBIOS Scope ID	query name server), and h-node (query name server, then broadcast). A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS
WINS Server 2       A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.         Advanced       Image: Comparison of the OpenVPN server configuration here, separated by a semicolon. EXAMPLE: push Forute 10.0.0.0 255.255.255.0°         Image: Prove is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. View license!       Image: Comparison of the OpenVPN server configuration here, separated by a semicolon. EXAMPLE: push Forust 10.0.0.0 255.255.255.0°	WINS Server 1	Tranc on a single network to only those nodes with the same NetBIOS scope ID.  A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern antiworke
Advanced Advanced Enter any additional options to add to the OpenVPN server configuration here, separated by a semicolon. EXAMPLE: push 'route 10.0.0.0 255.255.255.0° Next  PfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]	WINS Server 2	A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern
Image: State of the state	Advanced	Enter any additional options to add to the OpenVPN server configuration here, separated by a semicolon. EXAMPLE: push
pfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]		*route 10.0.0.0 255.255.255.0*
pfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]		2 - NOX
	E p	Sense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]

Vizard / Oper	nVPN Remote Access Server Setup / Firewall Rule Configuration
	Step 10 of 11
irewall Rule Co	nfiguration
	OpenVPN Remote Access Server Setup Wizard
irewall Rule Co	nfiguration
	Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.
raffic from clie	nts to server
Firewall Rule	Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.
raffic from clie	nts through VPN
OpenVPN rule	

On peut laisser par défaut et faire "Next"

	System + Interfaces + Firewall + Services + VPN + Status + Diagnostics + Help +	G
Wizard /	OpenVPN Remote Access Server Setup / Finished!	0
(	Step 11 of 11	
Finished!		
	OpenVPN Remote Access Server Setup Wizard	
Configuratio	on Complete!	
	The configuration is now complete.	
	To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Exp	port package.
	» Finish	

Notre serveur VPN est installer, nous pouvons donc cliquer sur "Finish"

Notre VPN est donc configurer, il nous reste plus qu'a installer un client VPN sur un poste et ce connecter à distance.

Précedament, nous avons installer un paquets OpenVPN, qui nous permet de prégénere des fichiers de configuration pour les clients VPN.

Il est possible de télécharger le client depuis cette interface.

penVPN / C	ient Export Utility 0		
rver Client Clier	nt Specific Overrides Wizards Client Export Shared Key Export		
penVPN Server			
Remote Access Server	Serveur OpenVPN UDP:1194		
lient Connectio	n Behavior		
Host Name Resolution	Other		
Host Name	172.16.29.3 Enter the hostname or IP address the client will use to connect to this server.		
Verify Server CN	Automatic - Use verify-x509-name (OpenVPN 2.3+) wh v Optionally verify the server certificate Common Name (CN) when the client connects. Current clients, including the most recent versions of Windows, Viscosity, Tunnelblick, OpenVPN on iOS and Android and so on should all work at the default automatic setting.		
	Only use tls-remote if an older client must be used. The option has been deprecated by OpenVPN and will be removed in the next major version. With tls-remote the server CN may optionally be enclosed in quotes. This can help if the server CN contains spaces and certain clients cannot parse the server CN. Some clients have problems parsing the CN with quotes. Use only as needed.		
lock Outside DNS	Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.		
Legacy Client	Do not include OpenVPN 2.4 settings in the client configuration. When using an older client (OpenVPN 2.3.x or earlier), check this option to prevent the exporter from placing known-		
Certificate Expo	't Options		
CS#11 Certificate Storage	Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.		
Microsoft Certificate Storage	Use Microsoft Certificate Storage instead of local files.		
Password Protect Certificate	Use a password to protect the pkcs12 file contents or key in Viscosity bundle.		
Proxy Options			
Use A Proxy	Use proxy to communicate with the OpenVPN server.		
Advanced Additional configuration options			
	انات Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon. EXAMPLE: remote-random;		
	B Save as default		
Search	0		

OpenVPN Clients		
lser	Certificate Name	Export
anent open po		Imme comparators.         Imme comparators.      <
If a client is missing fron certificate does not exist OpenVPN 2.4 requires W The "win6" Windows instal The "XP" Windows instal	n the list it is likely due to a CA mismatch betwe on this firewall, or a user certificate is not asso indows Vista or later allers include the tap-windows6 driver which re lers work on Windows XP and later versions.	een the OpenVPN server instance and the client certificate, the client ociated with a user when local database authentication is enabled. quires Windows Vista or later.

Nous avons les fichiers de config et l'on peut aussi télécharger directement l'installation de OpenVPN

# 13. Mise en place d'une journalisation du trafic réseau

Nous allons utiliser ntopng qui nous permet d'avoir des information détailler des connexion actuelle(Tout ceci se configure dans les paramétres de ntopng dans l'interface graphique). On à aussi un historique de qui à éffectuer des demandes et savoir ce qui rentre et sort du réseau.

Pour installer ntopng	g, il faut aller dans	« System\Package	Manager »
-----------------------	-----------------------	------------------	-----------

Installed Package	s Available Packages				
Search					
Search term		E	Both	¥	Q Search 🕤 Clear
	Enter a search string or *nix descriptions.	regular expression to	search j	backag	ge names and
Packages					

Nous recherchons « ntopng », puis nous l'installons

Installed Packages	Available Packages	Package Installer		
Package Install	ation			
line arguments, ad	d something like the t	ollowing to rc.conf:		
	1.12.17.2.			
ntopng_tiags= /par	n/to/file.conf			
Message from redis	-3.2.10:			
Message from redis ===> CONFIGURATIO	-3.2.10: N NOTE:			
Message from redit	-3.2.10: N NOTE:	the section states fills		
Message from redi: ===> CONFIGURATIO To setup "re /usr/local/e	-3.2.10: NN NOTE: dis" you need to edit tc/redis.conf	the configuration file:		
Message from redis ===> CONFIGURATIO To setup "re /usr/local/e	-3.2.10: N NOTE: dis" you need to edit tc/redis.conf	the configuration file:		
Message from redi: ===> CONFIGURATIO To setup "re /usr/local/e To run redi:	-3.2.10: N NOTE: dis" you need to edit tc/redis.conf from startup, add red	the configuration file: is_enable="YES"		
Message from redi: ===> CONFIGURATIC To setup "re /usr/local/c To run redi: in your /etc	-3.2.10: N NOTE: dis" you need to edit tc/redis.conf from startup, add rec /rc.conf.	the configuration file: is_enable="YES"		

Nous devons attendre que Success soit affichier, car si on quitte la page ntopng ne sera pas completement installer

COMMUNITY EDITION	* Interfaces * Firewall * Services * VPN * Status * Diagnostics * Help * 🙏	2 🗘
Package / Diagn	ostics: ntopng Settings / ntopng Settings	0
ntoping Settings Acc	zess ntopng	
General Options		
Enable ntopng	Check this to enable moping.	1
Keep Data/Settings	Keep intoping settings, graphs and traffic data.     Note: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgradel	
ntopng Admin Password	Enter the password for the ntoping GUI. Minimum 5 characters.	
Confirm ntopng Admin Password		
Interface	UMA VOAN -	
DNS Mode	Decode DNS responses and resolve local numeric IPs only (default)  Configures how name resolution is handled.	
Disable Alerts	Disables all alerts generated by ntopng, such as flooding notifications.	
Local Networks		
Mode	Consider all RFC1918 networks local    Configures how Local Networks are defined. Default: Consider all RFC1918 networks local.	
Custom networks list	CIDR	
Add	+ Add	
Utilities		

Nous allons donc configurer ntopng, pour cela aller dans « Diagnostics / ntopng Settings »

Pour la mise en place, nous alons utiliser un serveur Mysql. Le serveur MySQL va nous permettre de sauvegarder les informations qui passe sur le réseau. Pour cela, nous devons créer une table « ntopng » sur le serveur MySQL.

#### IP: 172.16.0.200

Utilisateur: root

#### Mot de passe: Toor01

Un petit bug existe dans l'interface, il est possible de modifier le temps de rétention des infomation mais si on modifier le temps et que l'on redemarre l'informations n'est pas sauvegarder. Pour mon cas, j'ai trouver une solution qui conciste à enelver les droit de « Delete et Update », afin qu'il ne supprime pas les information au dela de 7 Jours par défaut.

Une fois ceci fait, nous pouvons tester si on à bien accés à la base de données depuis Pfsense avec comme commande

mysql -h 172.16.0.200 -uroot -p

Cette commande doit être fait sur Pfsense(En SSH)

Si la connexion s'effectue bien cela veut dire qu'il est donc possible d'atteindre la base de données.

Il faut « Enable ntopng », puis saisir le mot de passe de l'interface web de ntopng et on séléctionne les deux interfaces Lan et Wan. D'autres parametres peut etre modifier.

Si ce n'est pas le cas voici les solutions possibles :

Configurer le serveur MySQL

nano /etc/mysql/my.cnf	
[mysqld]	
user = mysql	
port=3306	
bind-address=0.0.0.0	

Contenue du fichier « /etc/mysql/my.cnf »

- Verifier les permission de l'utilisateurs
- Verifier le nom d'utilisateur et le mot de passe et l'IP du serveur

Nous allons dire à Pfsense, qu'il doit enregistrer les informations dans la base de données. Nous allons modifier un fichier de config.

### nano /usr/local/pkg/ntopng.inc -l

/usr/local/bin/ntopng -d /var/db/ntopng -S all -D none -q -e -F "mysql;172.16.0.200;ntopng;flows;root;Toor01" -G /var/run/ntopng.pid -s -e {\$http\_args}

{\$disable\_alerts} {\$dump\_flows} {\$ifaces} {\$dns\_mode} {\$aggregations} {\$local\_networks} &

Contenue du fichier « /usr/local/pkg/ntopng.inc ». Ligne 168

Une fois fait, nous allons pouvoir redémarrer et nous connecter.

<u>Utilisateur:</u> admin <u>Mot de passe:</u> <définie précédement> URL: <u>http://<ip\_pfsense>:3000/</u>

Puis, nous allons choisir l'interface que l'on veut voir ou espionner

ntop	 🕈 🔹 🏚 🔹 Flows Hosts 🔹 Devices 🗸	Interfaces - M + O - Q Search Host
Interface: em1 🖀 Packets Protocols ICMP ARP		✓ em1 em0

Puis, nous allons choisir le graphique et nous avons une vue du trafic et des informations rapide

top			• @••	A - Flows	Hosts +	Devices +	Interfaces -	٥.	ტ-	Q Search Host
Interface: em 1 🕷 Packets Protocols ICMP ARP 🔛 🖨 🔺 🖺 🔅	* *									
Chart Flows										
mesenes - Timeframe: 1m 5m 10m 1h 3h 6h 12h 1d 1w 2w 1M 6M	1¥									
Traffic NOTE: Click on the graph to zoom.		Time	Value							
00 koitis	Min	03/11/19 18:37:08	0 bit/s							
	Max	03/11/19 18:06:50	415.6 kbit/s							
0.02715	Last	03/11/19 18:44:32	17.73 kbit/s							
	Average	29.3 kbit/s								
D leafin	Total Traffic	12.57 MB								
	Selection Time									
Secula	Minute Interface Top Talkers									
h Beneristen AMA des eine des einen des einen seinen seine der Alle gebense seine AMA seinerten führen sintere										
ng Community Edition v.3.0.171218	44.31 kbil/s [25 pps]	0	0 bps 0 bps		Ø 18:44:	9 +0000   Uptime	1 h, 14 sec 31 Flows			

Et pour voir en détaille les connexions effectuer, nous utilisons dans « Flows », puis « IPv4 »

enave, emi	<b>W</b> P80	NED PROCOS ICMP		~ * "						
art Plows										
Summary	IPv4 IPv	5								
op <mark>IP</mark> v4	1 Flows	s [11/03/2019 17	7:44:55 - 11/03/20	019 18:44:55]						200
Application	L4 Proto	Client	Server	Begin	End	Traffic Sent	Traffic Received	Total Traffic Y	Info	Avg Tr
SSH	TCP	YOHAN-PC:64269	172.16.0.200.350	11/03/2019 18:05:58	11/03/2019 18:07:41	50.1 KB	272.7 KB	322.8 KB	SSH-2.0-OpenSSH_7.4p1 Debian-10+	25.43 kb
MySQL	TCP	p/Sense.iocaldomain:58541	172.16.0.200 mysql	11/03/2019 18:09:03	11/03/2019 18:13:59	193.83 KB	29.39 KB	223.22 KB		6.16 kb
SSM	TCP	YONAN-PC.64966	p/Sense.localdomain.ssh	11/03/2019 18:18:16	11/03/2019 18:22:51	52.34 KB	127.24 KB	179.58 KB	SSH-2.0-OpenSSH_7.2	5.33 kt
MySQL	TCP	pfSense.iocaldomain:45852	172.16.0.200/mysql	11/03/2019 17:49:26	11/03/2019 17:54:21	149.73 KB	23.09 KB	172.82 KB		4.78 kg
MySQL	TCP	p/Sense.iocaldomain:45852	172.16.0.200/mysql	11/03/2019 18:04:12	11/03/2019 18:09:08	135.84 KB	20.66 KB	156.5 KB		4.32 kt
MySQL	TCP	pfSense.iocaldomain:58641	172.16.0.200 mysql	11/03/2019 17:54:21	11/03/2019 17:59:17	130.38 KB	20.49 KB	150.87 KB		4.16 kt
MySQL	TCP	pfSense.iocaldomain:58641	172.16.0.200/mysql	11/03/2019 18:13:59	11/03/2019 18:18:54	130.94 KB	19.9 KB	150.84 KB		4.17 kt
MySQL	TCP	p/Sense.iocaldomain.58641	172.16.0.200 mysql	11/03/2019 18:04:08	11/03/2019 18:09:03	129.58 KB	19.57 KB	149.14 KB		4.13 kb
MySQL	TCP	p/Sense.iocaldomain.45852	172.16.0.200/mysql	11/03/2019 18:25:51	11/03/2019 18:30:48	129.26 KB	19.57 KB	148.83 KB		4.09 kt
MySQL	TCP	p/Sense.iocaldomain:45852	172.16.0.200/mysql	11/03/2019 17:54:21	11/03/2019 17:59:17	128.03 KB	20.16 KB	148.19 KB		4.09 kt
MySQL	TCP	p/Sense.iocaldomain.58641	172.16.0.200 mysql	11/03/2019 17:59:17	11/03/2019 18:04:08	125.06 KB	18.96 KB	144.06 KB		4.04 kt
MySQL	TOP	pfSense.iocaldomain:45852	172.16.0.200/mysqi	11/03/2019 18:20:55	11/03/2019 18:25:51	124.99 KB	18.98 KB	143.97 KB		3.97 kb
MySQL	TCP	p/Sense.iocaldomain:58541	172.16.0.200:mysql	11/03/2019 17:49:25	11/03/2019 17:54:21	121.6 KB	18.64 KB	140.24 KB		3.88 kb
MySQL	TCP	p/Sense.localdomain.45852	172.16.0.200 mysql	11/03/2019 17:59:17	11/03/2019 18:04:12	120.73 KB	18.22 KB	138.96 KB		3.85 kb

On peut sélectionner le temps voulu grâce au graphique précédent. Nous avons les informations disponibles dans la base de données également.

# 14. Autorisation interfaces web (Sous réseau)

Afin de pouvoir controler notre PFSENSE, depuis un autre réseau, nous avons besoin de désactiver une régle http. Nous devons aller dans « **System / Advanced**», puis cocher cette case.



Le routeur est maintenant administrable depuis d'autres réseaux LAN(Sans régles ACL).

# 15. Changement du mot de passe de l'interface web

Pour modifier le mot de passe pour plus de sécurité, pour cela on va dans « **System / User Manager** » et l'on modifie le compte « **admin** »

User	S					
	Username	Full name	Status	Groups	Actions	
	admin	System Administrator	~	admins	an .	

On clique sur le petit crayon, pour modifier notre compte

System / User	Manager / Users / Edit	Ø
Users Groups	Settings Authentication Servers	
User Properties		
Defined b	y SYSTEM	
Disable	d 📋 This user cannot login	
Usernam	admin	
Passwor		
Full nam	e System Administrator User's full name, for administrative information only	
Expiration dat	e Leave blank if the account shouldn't expire, otherwise enter the expiration	date as MM/DD/YYYY
Custom Setting	s 🛛 Use individual customized GUI options and dashboard layout for this u	ser.
Group membersh	<b>^</b>	admins .
	* Not member of	Member of
	» Move to "Member of" list	≪ Move to "Not member of" list
	Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.	

Nous saisissons notre nouveau mot de passe, puis on clique sur « Save » et notre mot de passe est changé.

# 16. Mise à jour PFSENSE(Update Système)

Les mises à jour sont importantes, niveau fonctionnalité et surtout niveau sécurité

Une mise à jour PFSENSE est facile à faire, pour cela nous devons nous connecter sur le Panel, et sur le Dashboard nous avons la version et comme on peut le voir la version 2.4.1 est disponible, nous pouvons donc la mettre à jour grâce au petit nuage download.

bioo	Vendor, Innotek Onion
	Version: VirtualBox
	Release Date: 12/01/2006
Version	2.3.5-RELEASE (amd64)
	built on Mon Oct 30 11:08:06 CDT 2017
	FreeBSD 10.3-RELEASE-p22
	Version 2.4.1 is available.
	Version 2.4.1 is available.
Platform	Version 2.4.1 is available.

Une demande de confirmation nous ai demandé si l'on veut bien mettre à jour notre version, pour cela cliquer sur « **Confirm** »

System Update Updat	∋ Settings	
Confirmation Require	l to update pfSense system.	
Current Base System	2.3.5	
Latest Base System	2.4.1	
	and the second se	

Puis l'installation se fait, mais on ne doit ni quitter ni fermer cette page car la mise à jour va s'arrêter et risque de planter PFSENSE.

lease wait while th his may take seve	he system update completes. eral minutes. Do not leave or refre	sh the page!		
System Update	Update Settings			
Ipdating Syste	em e the undate system initia	1745		
	a the oppose alactic allection			

Nous avons un message qui nous informe que la mise à jour est fini et que PFSENSE doit redémarrer

System / Update / System Update	0
System update successfully completed.	
System Update Update Settings	
Rebooting Page will automatically reload in 88 seconds	
Updating System The following 1 package(s) will be affected (of 0 checked):	
Installed packages to be UPGRADED: pr5emse-kernel_pr5emse: 2.3.5 → 2.4.2_1 [pf5emse-core]	
Number of packages to be upgraded: 1	
The process will require 6 MiB more space. [1/1] Uggrading pfsense-kernel.pfsense from 2.3.5 to 2.4.2_1 [1/1] Extracting pfsense-kernel.pfsense-2.4.2_1: done ==>> Keeping a copy of current kernel in /boot/kernel.old Umorade is complete. Rebooting in 18 second.	
>>> Unlocking package pkg done. Success	

Puis une fois redémarrer, sur le Dashboard nous avons bien l'information qui nous dit que c'est bien la dernière version que nous avons

version	2.4.2-RELEASE-pr (amuo4)
	built on Tue Dec 12 13:45:26 CST 2017
	FreeBSD 11.1-RELEASE-p6
	The system is on the latest version.
	Version information updated at Thu Mar 1 14:09:51 UTC 2018 📿

42 / 42 Installation PFSENSE (Redondance, Filtrage, NAT, VPN)