



Pare-Feu (pfSense)

Nous allons mettre en place le Pare-feu pfSense. Nous le paramétrons pour qu'il puisse faire les liens entre les Vlan pour que les Serveurs et les clients puissent fonctionner ensemble et donc, avoir une adresse avec le DHCP, communiquer avec l'AD pour rejoindre le domaine et aller chercher des données dans les serveurs de fichier SAMBA. Ensuite nous allons mettre en place un Proxy pour gérer les trafics. Et pour finir nous mettrons en place le load balancing des deux serveurs web depuis pfSense

Un pare-feu (de l'anglais firewall) est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données (paquets).

Sources: Wikipedia

pfSense est un routeur/pare-feu open source basé sur le système d'exploitation FreeBSD. À l'origine un fork de m0n0wall, il utilise le pare-feu à états Packet Filter, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. pfSense convient pour la sécurisation d'un réseau domestique ou de petite entreprise.

Après une brève installation manuelle pour assigner les interfaces réseaux, il s'administre ensuite à distance depuis l'interface web et gère nativement les VLAN.

Comme sur les distributions Linux, pfSense intègre aussi un gestionnaire de paquets pour installer des fonctionnalités supplémentaires, comme un proxy, serveur VoIP1...

Sources: Wikipedia

Etapes de la procédure :

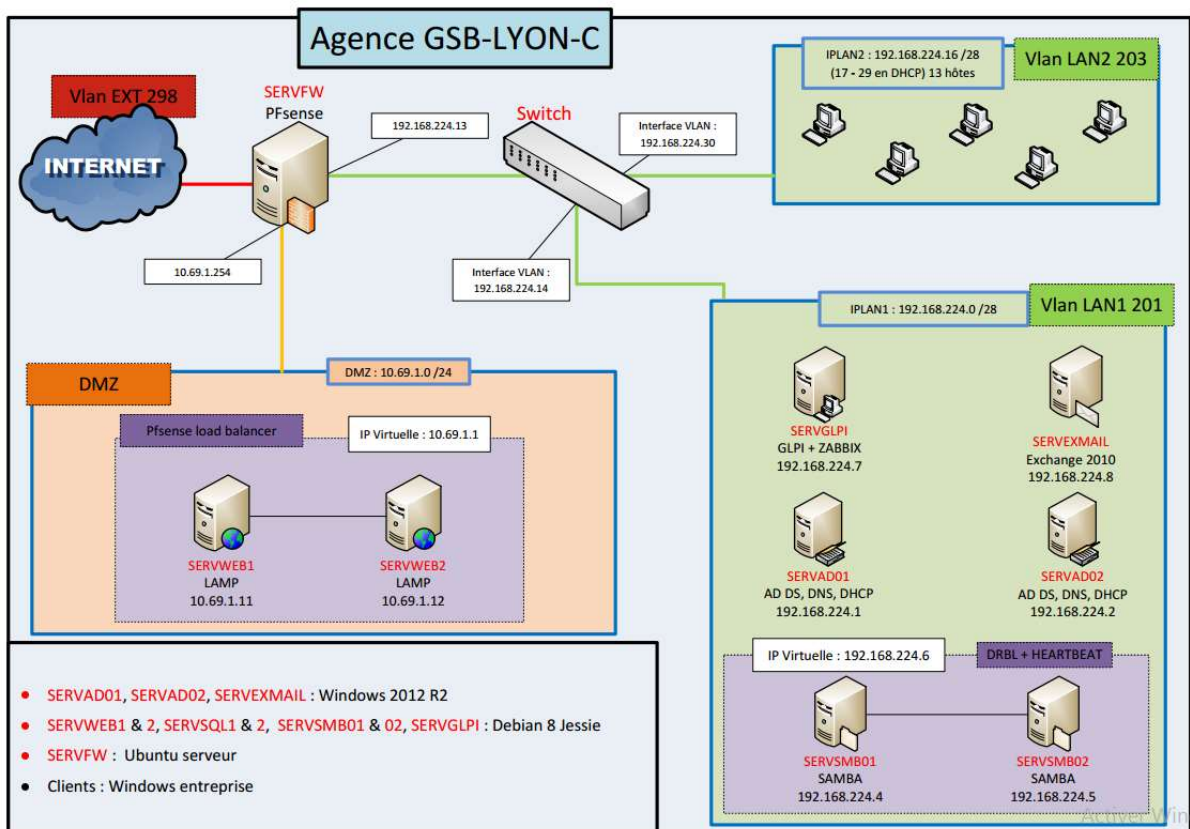
- Installation pfSense
- Administration interface WEB et paramétrage
- Proxy
- "Dhcp relay" et création de la route pour les VLAN
- Haute disponibilité serveur LAMP avec du "load balancing"
- Test du "load balancer"

Prérequis :

Si vous faites ça avec des machines virtuel, créer des machines propres avec l'ISO, et ne pas les cloner pour éviter les problèmes d'ID.

- Une iso " pfSense-CE-2.4.2 "
- Une machine client (dans ce cas-là c'est un Windows 7)
- Deux serveurs web pour le load balancing

Schéma :

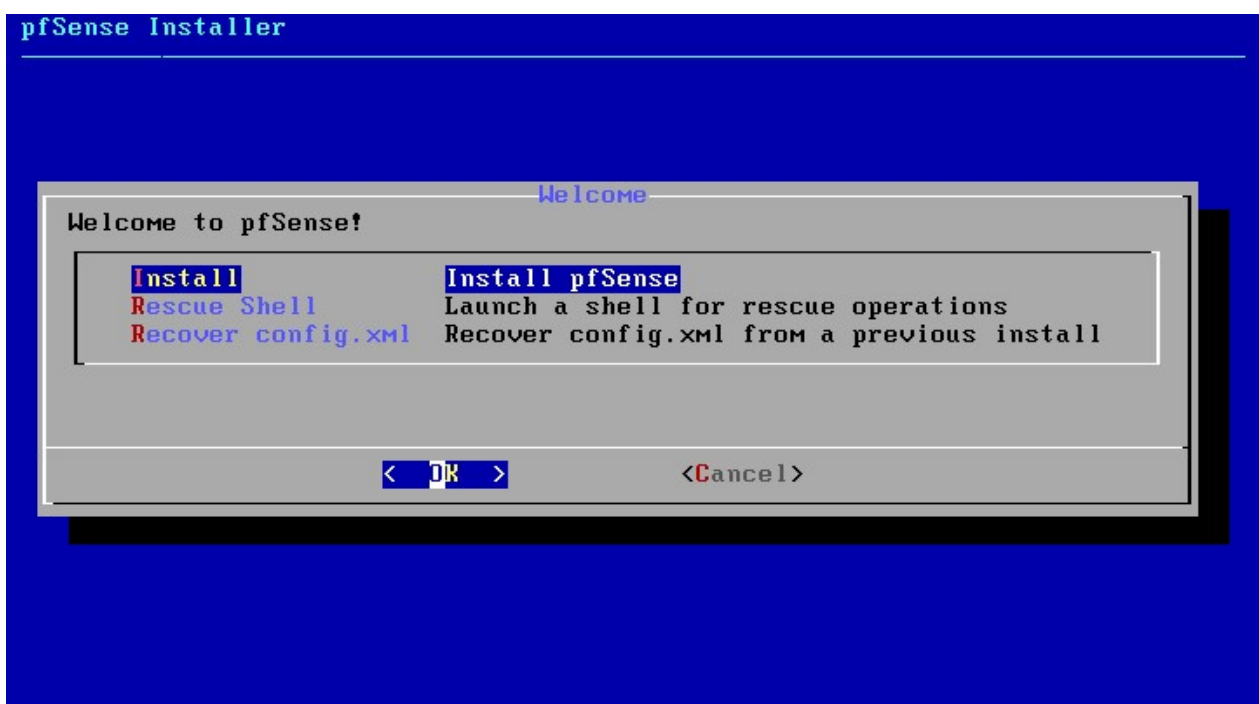


- Paramétrer le nom du serveur " SERVFW "
- Sur SERVFW, il y a cartes 3 réseau :
 - LAN : 192.168.224.13 en VMNET2
 - WAN : DHCP en VMNET0 (bridge)
 - DMZ : 10.69.1.254 en VMNET6

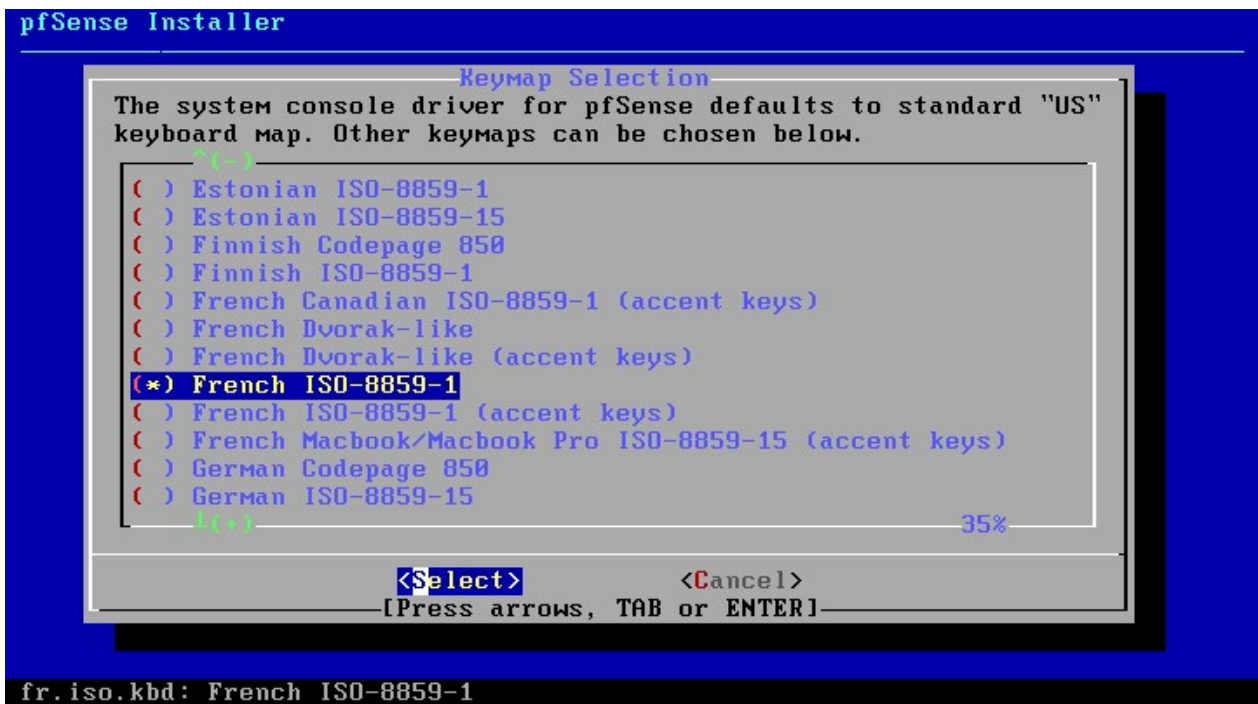
Sur SERVFW

Installation pfSense

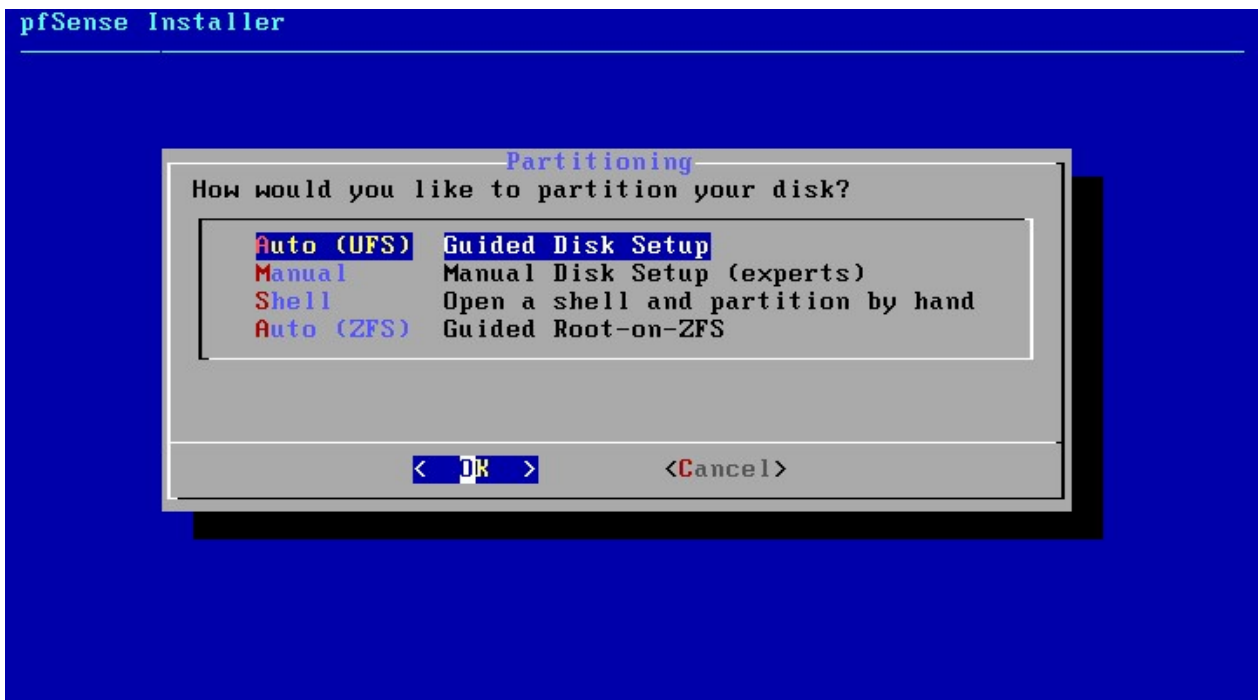
Installer l'ISO " pfSense-CE-2.4.2 "



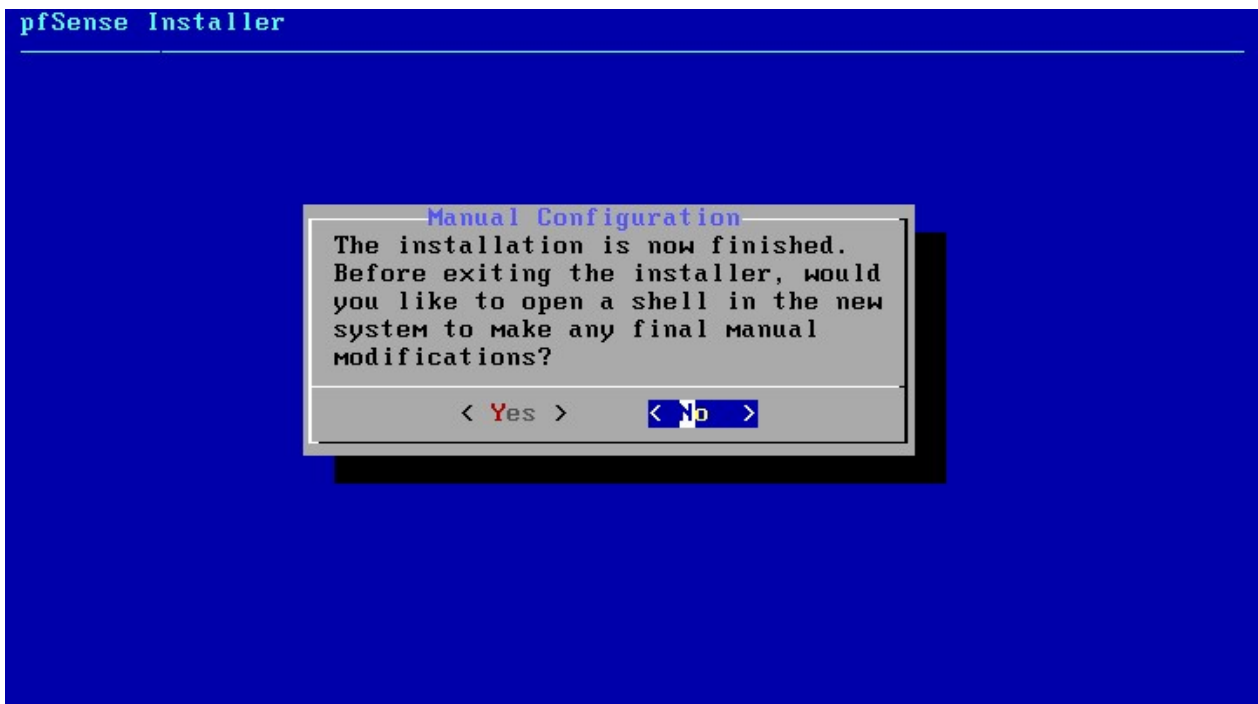
Choisir la langue



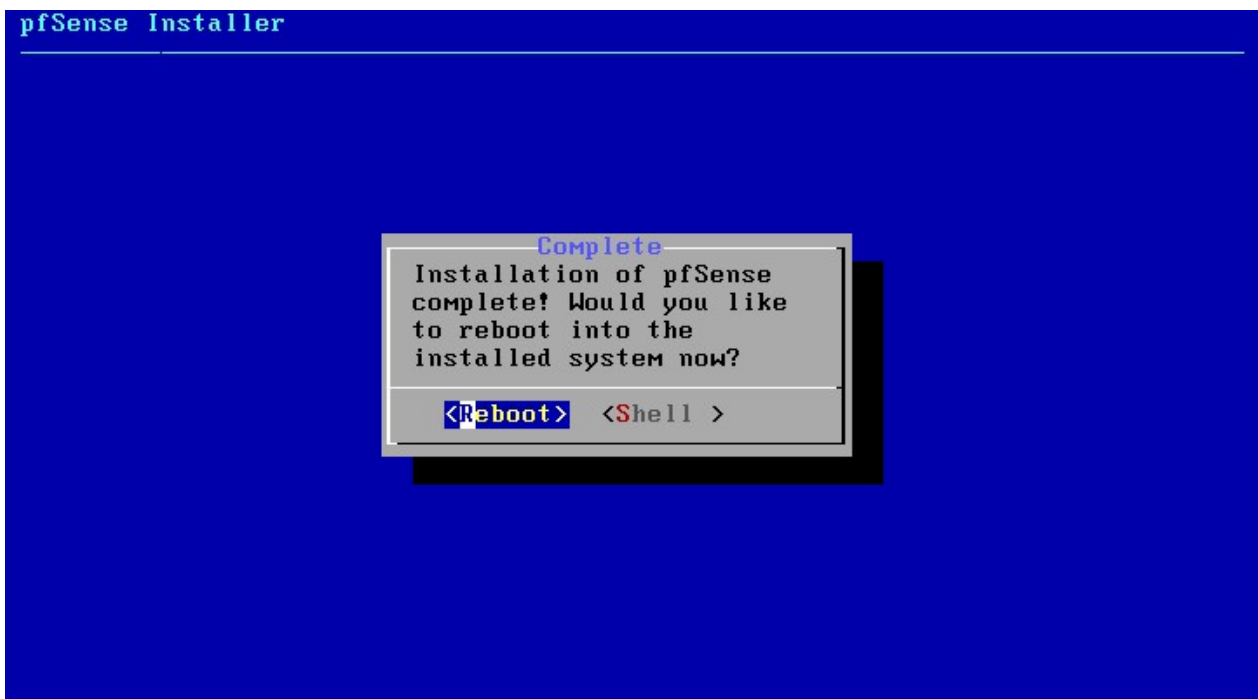
Laisser le partitionnement en Auto



Valider "NO"



Valider "REBOOT"



Au redémarrage, il vous demandera si vous voulez paramétrer les VLAN maintenant. Nous le feront plus tard, allez entrer "n"

```

Launching the init system..... done.
Initializing..... done.
Starting device manager (devd)...kldload: can't load ums: No such file or directory
done.
Loading configuration.....done.
Updating configuration...done.
Warning: Configuration references interfaces that do not exist: em0 em1

Network interface mismatch -- Running interface assignment option.
le0: link state changed to UP
le1: link state changed to UP
le2: link state changed to UP

Valid interfaces are:

le0      00:0c:29:f9:36:5c (down) AMD PCnet-PCI
le1      00:0c:29:f9:36:66 (down) AMD PCnet-PCI
le2      00:0c:29:f9:36:70 (down) AMD PCnet-PCI

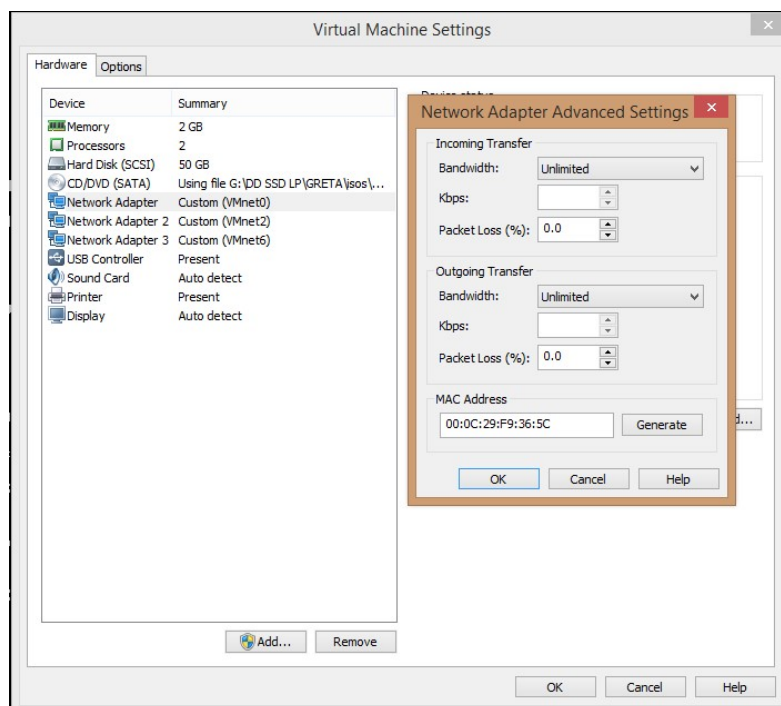
Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

```

Maintenant, nous allons configurer les cartes réseau, et pour cela il faut les adresses MAC de chacune, pour les connaître.

Dans VMware, faites clic droit sur votre VM puis settings. Sélectionner votre première carte réseau puis dans la partie droite sélectionner "Advanced" et là vous verrez votre adresse MAC, notez la et faites la même chose pour les 2 autres cartes réseau.



Maintenant il va vous demander de faire le liens entre vos carte réseau

Et vu que vous avez récupérer les adresses MAC, vous pouvez faire le liens pour que :

- LAN : 192.168.224.13 en VMNET2
- WAN : DHCP en VMNET0 (Bridge)
- DMZ : 10.69.1.254 en VMNET6

```
Warning: Configuration references interfaces that do not exist: em0 em1

Network interface mismatch -- Running interface assignment option.
le0: link state changed to UP
le1: link state changed to UP
le2: link state changed to UP

Valid interfaces are:

le0      00:0c:29:f9:36:5c (down) AMD PCnet-PCI
le1      00:0c:29:f9:36:66 (down) AMD PCnet-PCI
le2      00:0c:29:f9:36:70 (down) AMD PCnet-PCI

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y!n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(le0 le1 le2 or a): le0
```

Faire la meme chose pour chaque carte puis valider.

Vous avez terminé, maintenant vous êtes arrivez sur le menu de pfSense.

```
Starting CRON... done.
pfSense 2.4.2-RELEASE amd64 Mon Nov 20 08:12:56 CST 2017
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 12f83bc74305a84fa754

*** Welcome to pfSense 2.4.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> le0      ->
LAN (lan)      -> le1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> le2      ->

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

Enter an option: 
```


Nous allons configurer l'interface LAN avec l'option "2"

```
Enter an option: 2

Available interfaces:

1 - WAN (le0 - dhcp, dhcp6)
2 - LAN (le1 - static)
3 - OPT1 (le2)

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.224.13

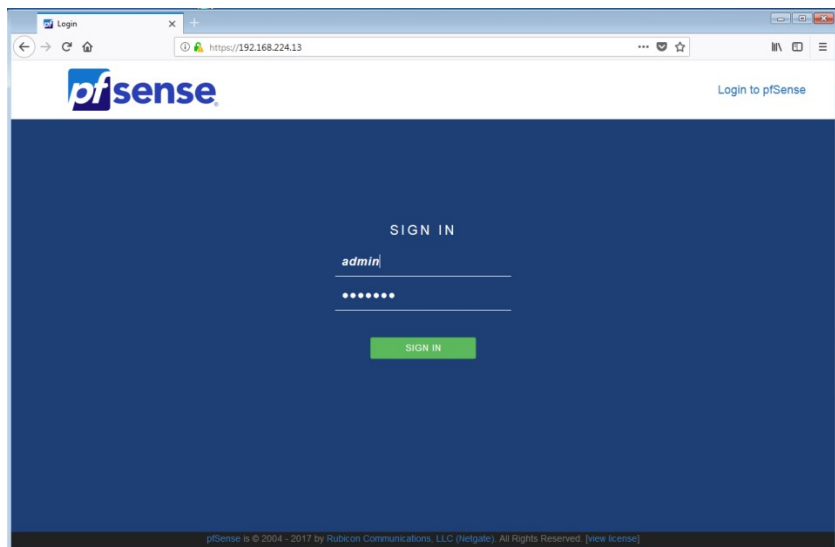
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 28

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

- Choisir l'interface : **Lan**
- Lui donner l'adresse IP : **192.168.224.13**
- Le sous-réseau : **28**
- Gateway : **Entrer (ne rien mettre)**
- adresse IPV6 : **Entrer (ne rien mettre)**
- DHCP : **n**
- Ce mettre en http : **n**
- Pour terminer appuyer sur **enter**

Administration interface WEB et paramétrage



- Prenez la main sur un client dans le réseau LAN configuré en IP fixe Par exemple 192.168.224.5 /28 en vmnet2
 - Grâce a un navigateur, se connecter à l'interface pfSense à l'adresse 192.168.224.13

Connectez-vous à pfSense

Login par défaut : **admin**

Mot de passe par défaut : **pfsense**

Après l'ouverture de session il vous demandera de faire le complément des paramètres. Faire suivant jusqu'à la configuration suivante et entrer les même informations



Décocher "Override DNS" sinon le DHCP du LAN va écraser les configurations

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname: SERVFW
EXAMPLE: myserver

Domain: gsb-lyon-c.cool
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server: 192.168.224.1

Secondary DNS Server: 8.8.8.8

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

[Next](#)

pfSense is © 2004 - 2018 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license](#)

Cliquer sur "Next" pour passer à l'étape suivante

Show PPTP password ☐ Reveal password characters

PPTP Local IP Address: [text box]

pptplocalsubnet: 32

PPTP Remote IP Address: [text box]

PPTP Dial on demand ☐ Enable Dial-On-Demand mode
This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.

PPTP Idle timeout: [text box]
If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

RFC1918 Networks

Block RFC1918 Private Networks ☐ Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

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

[Next](#)

pfSense is © 2004 - 2018 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license](#)

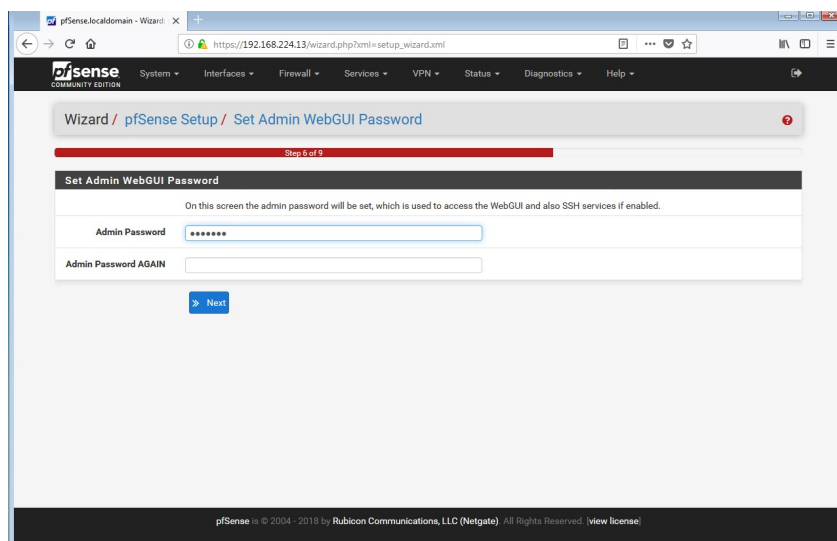
Sur la page suivante il faut juste décocher :

- Block private networks from entering via WAN
- Block non-Internet routed networks from entering via WAN

Car si le serveur n'a pas assez de mémoire vive cela peut engendrer un dysfonctionnement du firewall.

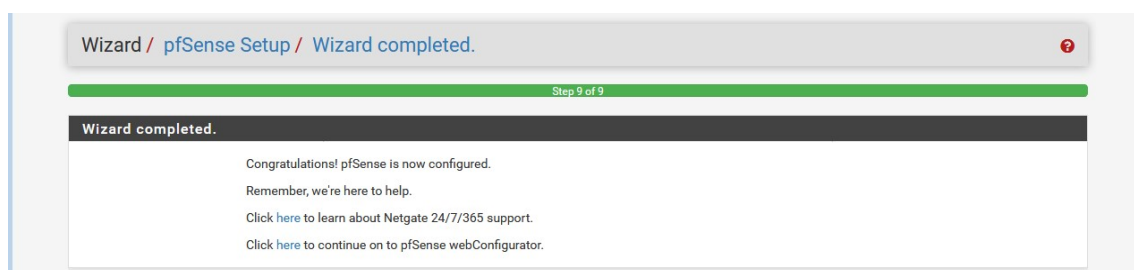
Cliquer sur "Next" pour passer à l'étape suivante

Configurer un nouveau mot de passe : " gsblyon "

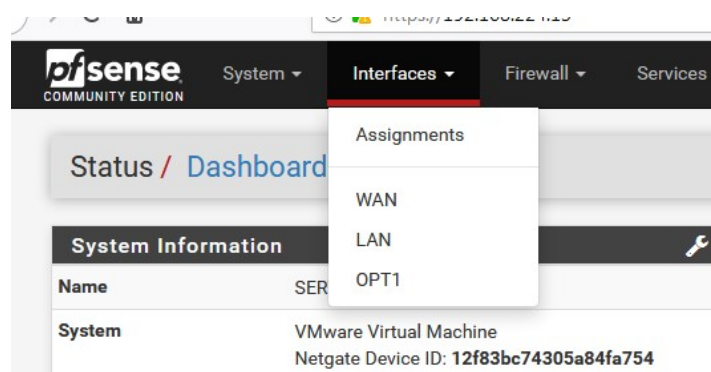


Cliquer sur "Next" pour passer à l'étape suivante
Cliquer sur "reload" (prend à jour les modifications)

Cliquer sur le "here" de :
"Click here to continue on to pfSense webConfigurator."



On va configurer l'adresse IP de notre DMZ.
Aller dans : Interfaces / OPT1



Interfaces / OPT1

General Configuration

Enable ☒ Enable interface

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

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

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

Speed and Duplex
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address /

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

Reserved Networks

Block private networks and loopback addresses ☒
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks ☒
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.

[Save](#)

Remplir avec les mêmes informations

Puis cliquer sur "Save"

Puis cliquer sur "Apply changes" pour appliquer les changements

pfsense COMMUNITY EDITION System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help

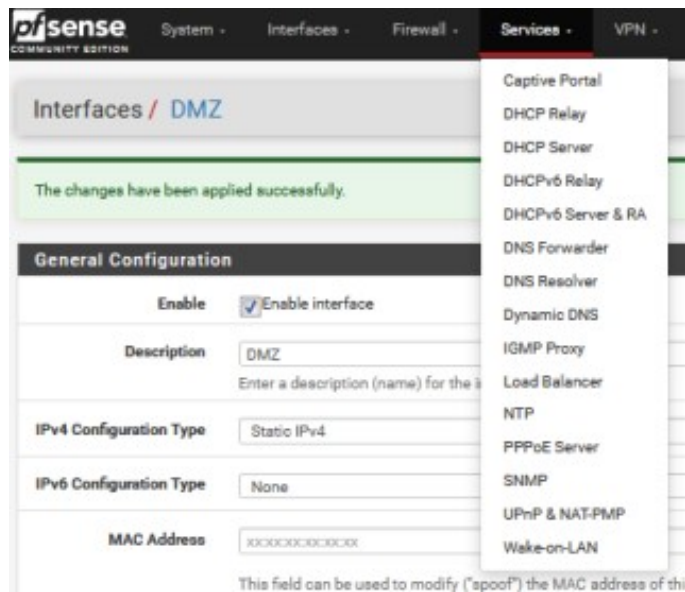
Interfaces / DMZ

The DMZ configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.

[✓ Apply Changes](#)

General Configuration

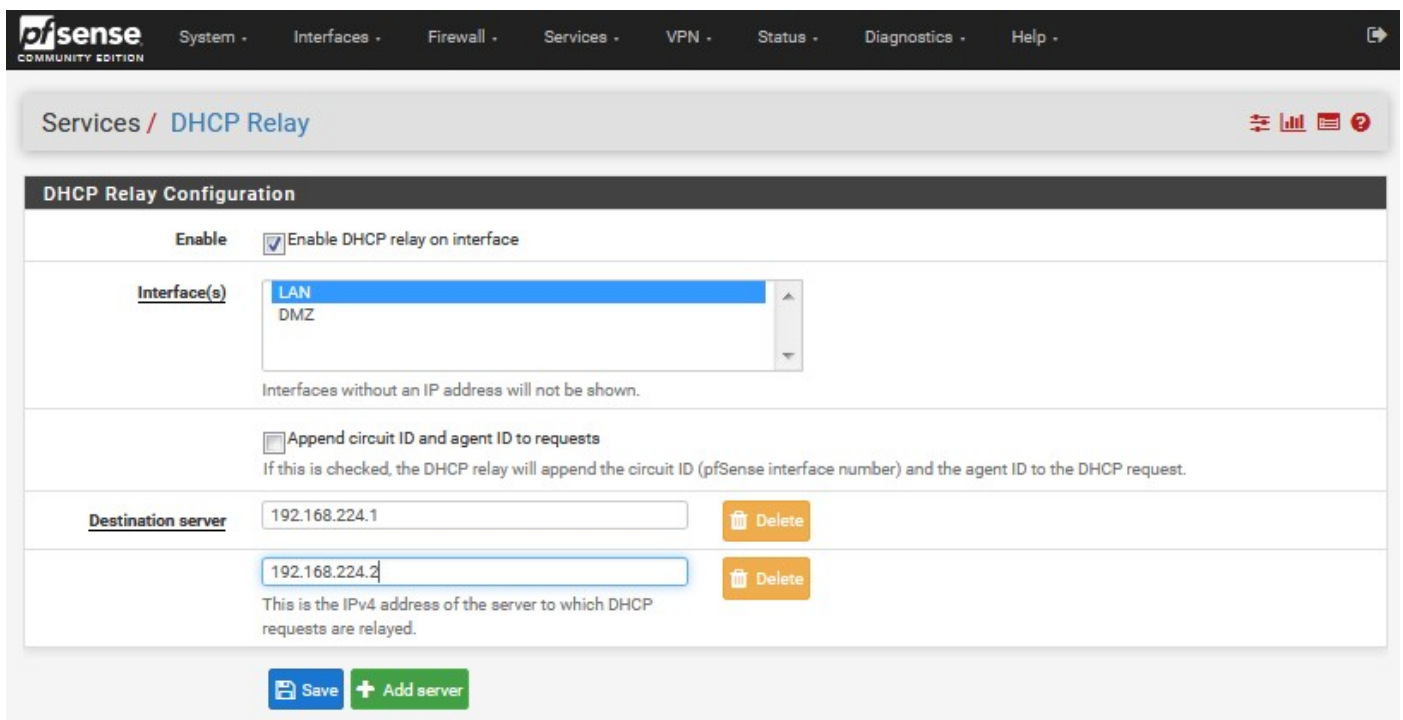
"Dhcp relay" et création de la route pour les VLAN

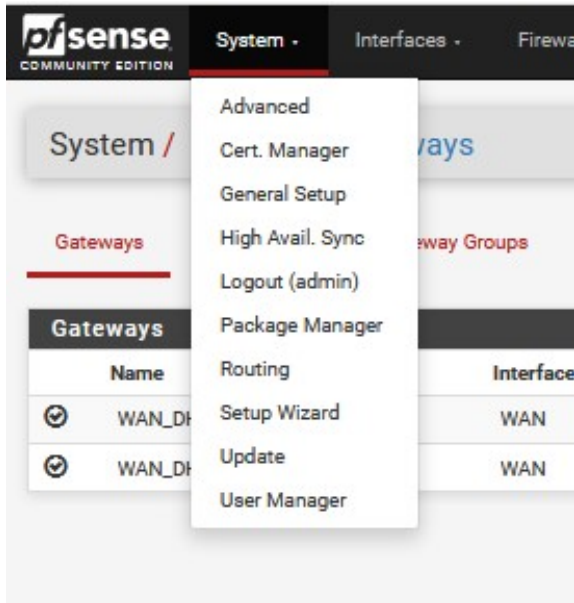


Aller dans Services / dhcp relay

Remplissez le formulaire de la même façon pour que le "DHCP relay" soit actif et que votre serveur DHCP et les clients puissent communiquer ensemble.

Cliquer sur "Add server" pour rentrer le deuxième AD.
Cliquer sur "Save" pour enregistrer votre paramétrage.





Aller dans system / routing / gateways

Cliquer sur "+add" pour ajouter

Remplissez le formulaire de la même façon

The screenshot shows the 'Edit Gateway' form in the pfSense web interface. The form is titled 'Edit Gateway' and has a 'Save' button at the bottom. The form contains several fields and checkboxes: 'Disabled' (checkbox), 'Interface' (dropdown menu set to 'LAN'), 'Address Family' (dropdown menu set to 'IPv4'), 'Name' (text field set to 'GatewayCisco'), 'Gateway' (text field set to '192.168.224.14'), 'Default Gateway' (checkbox), 'Gateway Monitoring' (checkbox), 'Gateway Action' (checkbox), 'Monitor IP' (text field), 'Force state' (checkbox), and 'Description' (text field). Each field has a small description below it. At the bottom of the form, there is a 'Display Advanced' button and a 'Save' button.

Cliquer sur "Save" pour enregistrer votre paramétrage.

Cliquer sur "Apply changes" pour appliquer les changements

System / Routing / Gateways

The gateway configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Gateways Static Routes Gateway Groups

Name	Interface	Gateway	Monitor IP	Description	Actions
GatewayCisco	LAN	192.168.224.14	192.168.224.14		
WAN_DHCP (default)	WAN	dynamic		Interface WAN_DHCP Gateway	
WAN_DHCP6 (default)	WAN	dynamic		Interface WAN_DHCP6 Gateway	

+ Add

Dans "static routes"
Puis ajouter une route statique en cliquant sur "+add"

System / Routing / Static Routes

Gateways Static Routes Gateway Groups

Network	Gateway	Interface	Description	Actions
---------	---------	-----------	-------------	---------

+ Add

Remplissez le formulaire de la même façon
Cliquez sur "Save" pour enregistrer votre paramétrage.

System / Routing / Static Routes / Edit

Edit Route Entry

Destination network: 192.168.224.16 / 28
Destination network for this static route

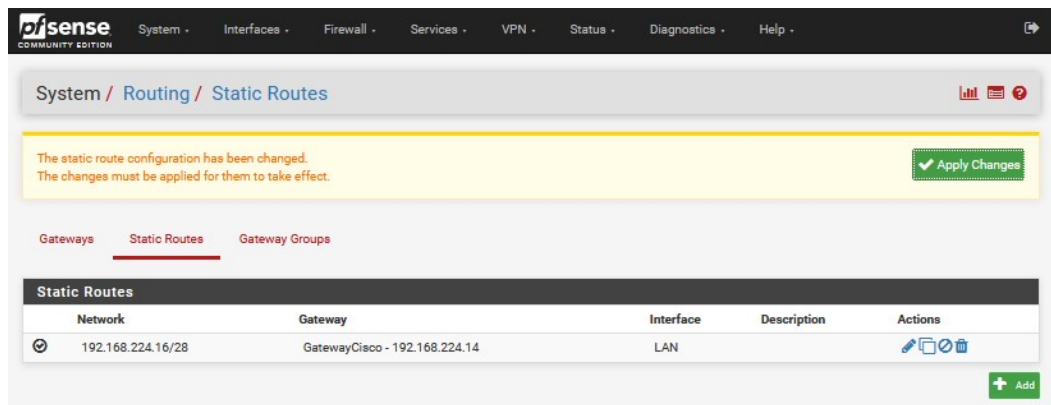
Gateway: GatewayCisco - 192.168.224.14
Choose which gateway this route applies to or add a new one first

Disabled: ☐ Disable this static route
Set this option to disable this static route without removing it from the list.

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

Save

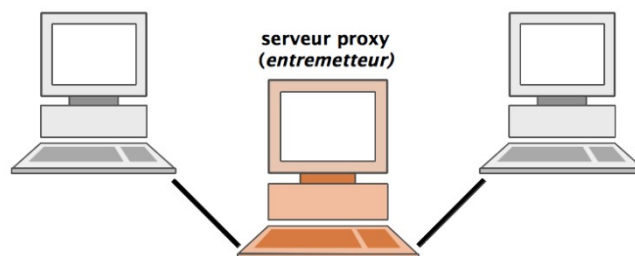
Cliquer sur "Apply changes" pour appliquer les changements

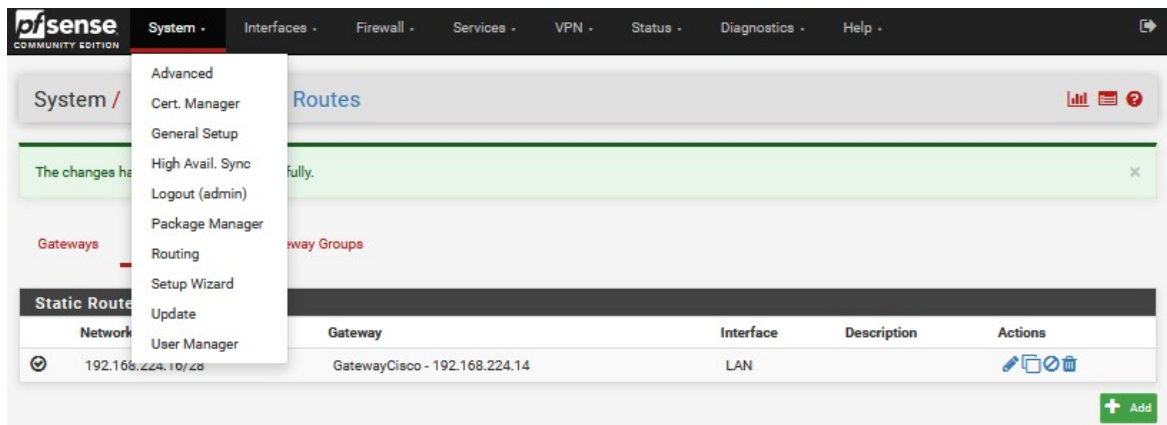


Proxy

Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.

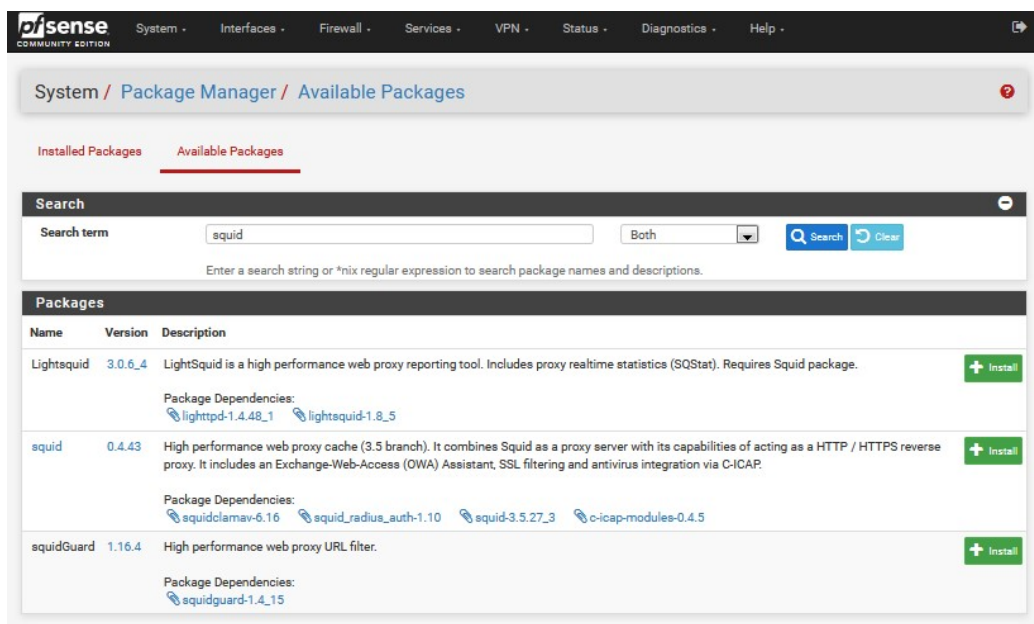
Dans le cadre plus précis des réseaux informatiques, un proxy est alors un programme servant d'intermédiaire pour accéder à un autre réseau, généralement internet. Par extension, on appelle aussi « proxy » un matériel comme un serveur mis en place pour assurer le fonctionnement de tels services.





System / package manager
Available package

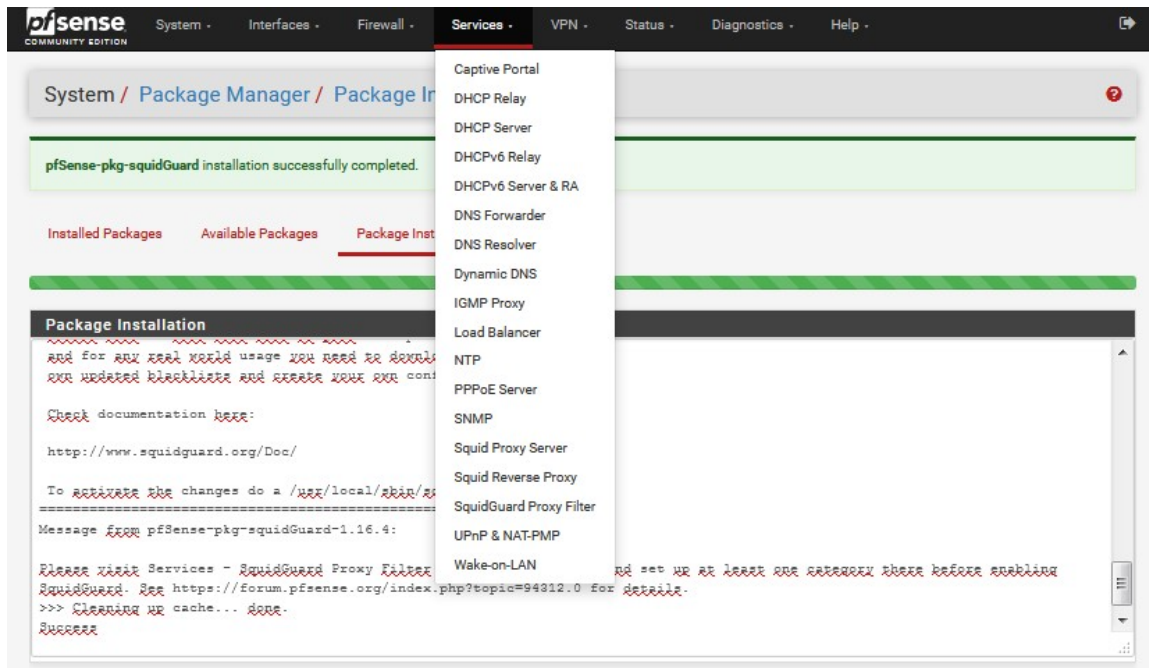
On va installer squidguard



Installer "squid" puis "squidguard"

- "Squid" est un serveur proxy
- "Squidguard" fait filtrage web

Aller dans : Service / squid proxy server



Remplissez le formulaire de la même façon

General	Remote Cache	Local Cache	Antivirus	ACLs	Traffic Mgmt	Authentication	Users	Real Time	Sync
Squid General Settings									
<p>Enable Squid Proxy <input checked="" type="checkbox"/> Check to enable the Squid proxy. Important: If unchecked, ALL Squid services will be disabled and stopped.</p>									
<p>Keep Settings/Data <input checked="" type="checkbox"/> If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls. Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.</p>									
<p>Proxy Interface(s) LAN DMZ WAN loopback <small>The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.</small></p>									
<p>Proxy Port <input type="text" value="3128"/> <small>This is the port the proxy server will listen on. Default: 3128</small></p>									
<p>ICP Port <input type="text"/> <small>This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.</small></p>									
<p>Allow Users on Interface <input checked="" type="checkbox"/> If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. <small>There will be no need to add the interface's subnet to the list of allowed subnets.</small></p>									
<p>Patch Captive Portal <small>This feature was removed - see Bug #5594 for details!</small></p>									
<p>Resolve DNS IPv4 First <input type="checkbox"/> Enable this to force DNS IPv4 lookup first. <small>This option is very useful if you have problems accessing HTTPS sites.</small></p>									
<p>Disable ICMP <input type="checkbox"/> Check this to disable Squid ICMP pinger helper.</p>									
<p>Use Alternate DNS Servers for the Proxy Server <input type="text"/> <small>To use DNS servers other than those configured in System > General Setup, enter the IP(s) here. Separate entries by semi-colons (;)</small></p>									
Transparent Proxy Settings									
<p>Transparent HTTP Proxy <input checked="" type="checkbox"/> Enable transparent mode to forward all requests for destination port 80 to the proxy server. <small>Transparent proxy mode works without any additional configuration being necessary on clients.</small> Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below. <small>Hint: In order to proxy both HTTP and HTTPS protocols without intercepting SSL connections, configure WPAD/PAC options on your DNS/DHCP servers.</small></p>									
<p>Transparent Proxy Interface(s) LAN DMZ WAN <small>The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.</small></p>									
<p>Bypass Proxy for Private Address Destination <input type="checkbox"/> Do not forward traffic to Private Address Space (RFC 1918) destinations. <small>Destinations in Private Address Space (RFC 1918) are passed directly through the firewall, not through the proxy server.</small></p>									
<p>Bypass Proxy for These Source IPs <input type="text"/> <small>Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall. Applies only to transparent mode. Separate entries by semi-colons (;)</small></p>									

Address Destination	Destinations in Private Address Space (RFC 1918) are passed directly through the firewall, not through the proxy server.
Bypass Proxy for These Source IPs	<input type="text"/> Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall. Applies only to transparent mode. Separate entries by semi-colons (;)
Bypass Proxy for These Destination IPs	<input type="text"/> Do not proxy traffic going to these destination IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall. Applies only to transparent mode. Separate entries by semi-colons (;)

SSL Man In the Middle Filtering

HTTPS/SSL Interception ☐ Enable SSL filtering.

SSL/MITM Mode
 The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled.
 Default: Splice Whitelist, Bump Otherwise. [Click Info for details.](#)

SSL Intercept Interface(s)
 The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.

SSL Proxy Port
 This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129

SSL Proxy Compatibility Mode
 The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. [Click Info for details.](#)

DHParams Key Size
 DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.

CA
 Select Certificate Authority to use when SSL interception is enabled.

SSL Certificate Daemon Children
 This is the number of SSL certificate daemon children to start. May need to be increased in busy environments. Default: 5

Remote Cert Checks
 Do not verify remote certificate
 Select remote SSL certificate checks to perform. Use CTRL + click to select multiple options.

Certificate Adapt
 Sets the 'Not Before' (setValidBefore)
 Sets CN property (setCommonName)
 See [sslproxy_cert_adapt directive documentation](#) and [Mimic original SSL server certificate wiki article](#) for details.

Logging Settings

Enable Access Logging ☒ This will enable the access log.
Warning: Do NOT enable if available disk space is low.

Log Store Directory
 The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs
Important: Do NOT include the trailing / when setting a custom location.

Rotate Logs
 Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Log Pages Denied by SquidGuard ☐ Makes it possible for SquidGuard denied log to be included on Squid logs.
[Click Info for detailed instructions.](#)

Headers Handling, Language and Other Customizations

Visible Hostname
 This is the hostname to be displayed in proxy server error messages.

Administrator's Email
 This is the email address displayed in error messages to the users.

Error Language
 Select the language in which the proxy server will display error messages to users.

X-Forwarded Header Mode
 Choose how to handle X-Forwarded-For headers. Default: on

Disable VIA Header ☐ If not set, Squid will include a Via header in requests and replies as required by RFC2616.

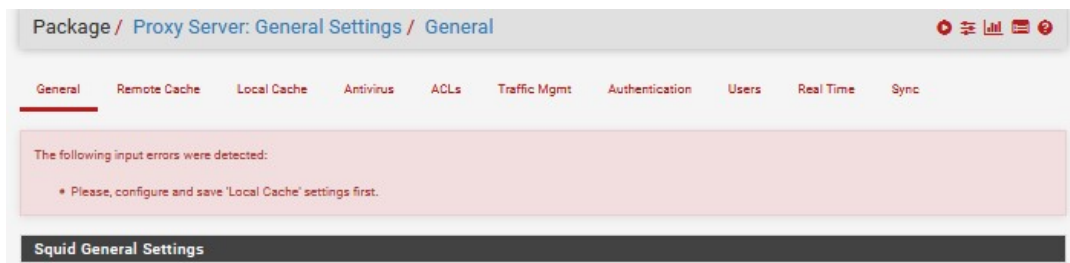
URI Whitespace Characters Handling
 Choose how to handle whitespace characters in URL. Default: strip

Suppress Squid Version ☐ Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

[Save](#) [Show Advanced Options](#)

Cliquer sur "Save" pour enregistrer votre paramétrage.

Un message d'erreur va apparaitre, c'est normal.

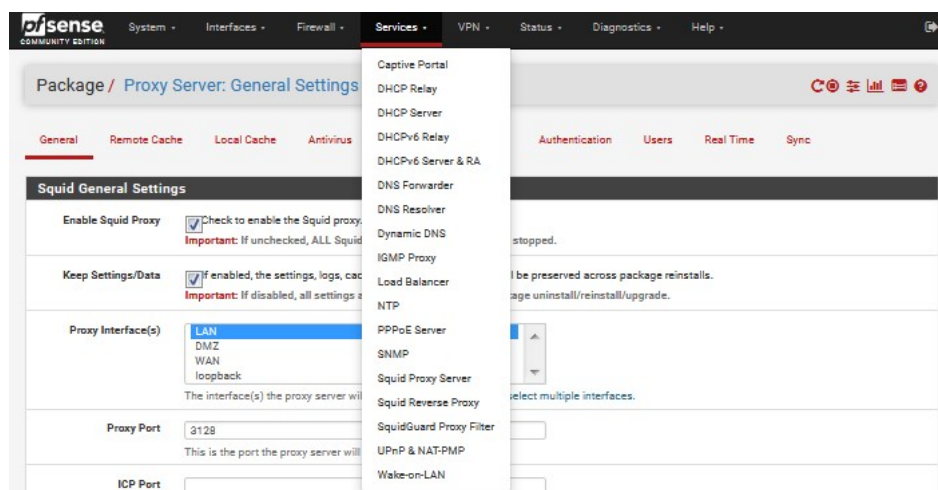


Aller dans "local cache"

Faire "save" tout en bas sans modifier les réglages.

Retourner sur "général" (vérifier bien que tout soit bien paramétrer car parfois la modification change) puis refait "save"

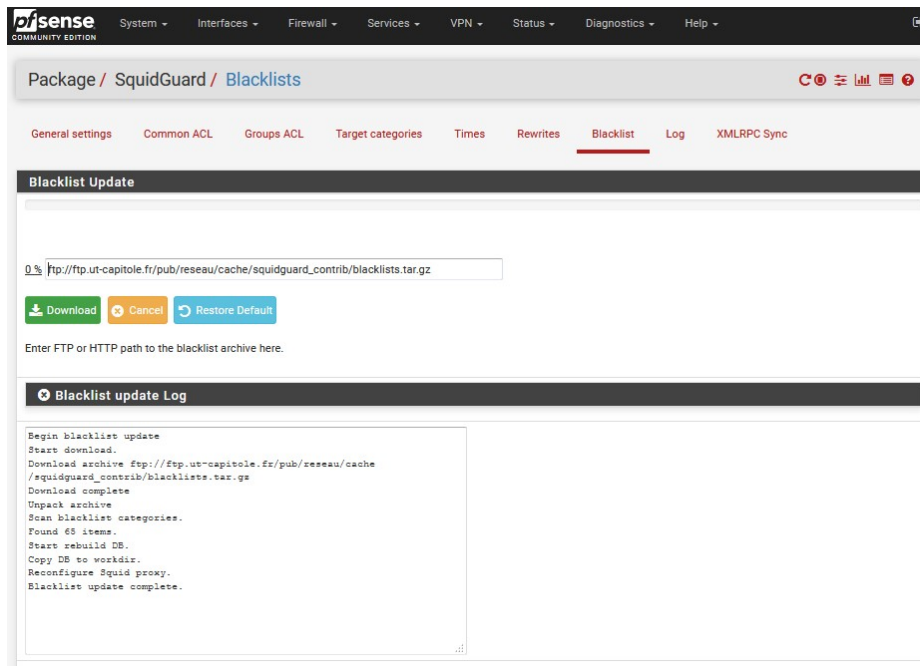
Aller dans service / squidguard proxy filter



Remplissez le formulaire de la même façon

Récupérer la blacklist de l'IUT de Toulouse et rentrer le lien dans "Blacklist url" :

ftp://ftp.ut-capitole.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz

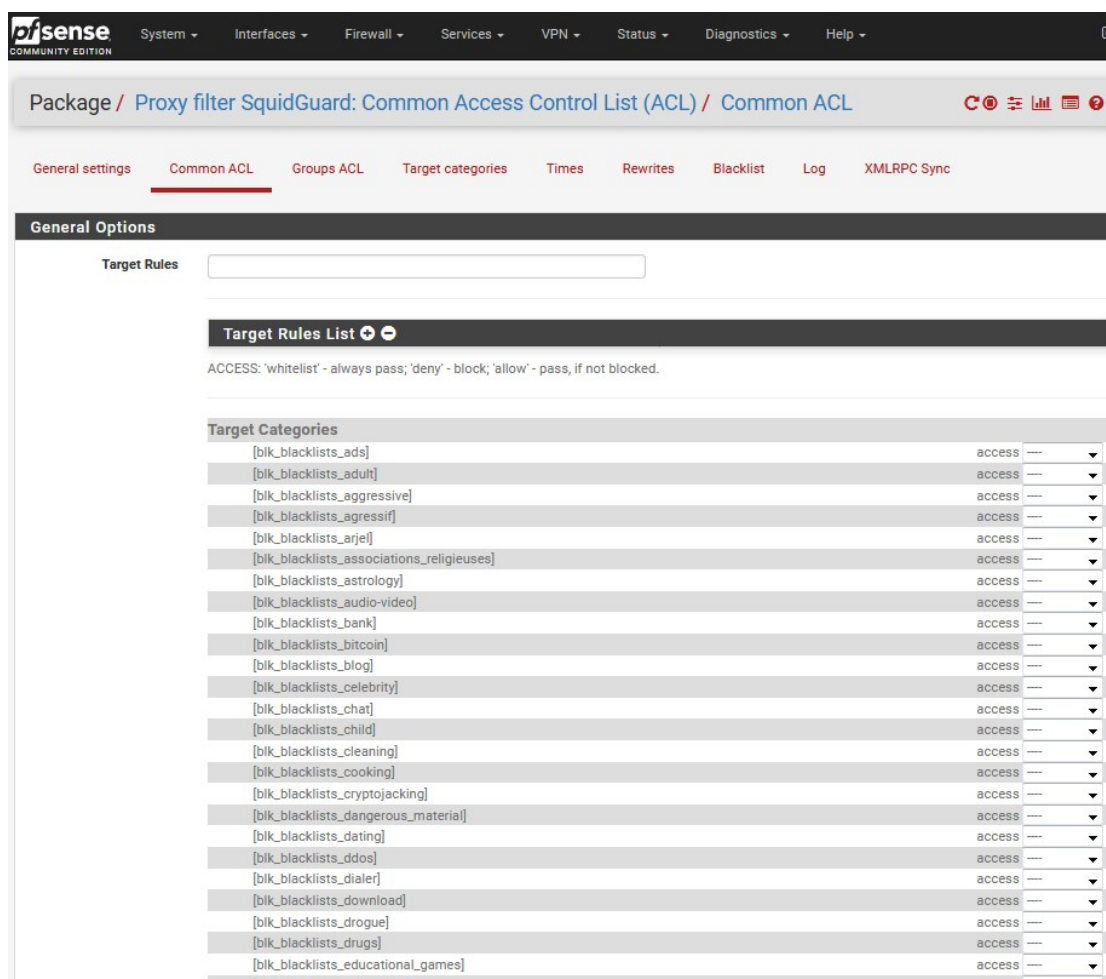


Dans l'onglet "common acl"

Cliquer sur +

Aller tout en bas et mettre "Default access [all]" sur "allow"

Puis choisir les catégorie a interdire en les mettant sur "deny"



[blk_blacklists_games]	access	---	▼
[blk_blacklists_hacking]	access	---	▼
[blk_blacklists_jobsearch]	access	---	▼
[blk_blacklists_lingerie]	access	---	▼
[blk_blacklists_liste_blanche]	access	---	▼
[blk_blacklists_liste_bu]	access	---	▼
[blk_blacklists_mail]	access	---	▼
[blk_blacklists_malware]	access	---	▼
[blk_blacklists_manga]	access	---	▼
[blk_blacklists_marketingware]	access	---	▼
[blk_blacklists_mixed_adult]	access	---	▼
[blk_blacklists_mobile-phone]	access	---	▼
[blk_blacklists_phishing]	access	---	▼
[blk_blacklists_porn]	access	---	▼
[blk_blacklists_press]	access	---	▼
[blk_blacklists_proxy]	access	---	▼
[blk_blacklists_publicite]	access	---	▼
[blk_blacklists_radio]	access	---	▼
[blk_blacklists_reeffected]	access	---	▼
[blk_blacklists_redirector]	access	---	▼
[blk_blacklists_remote-control]	access	---	▼
[blk_blacklists_sect]	access	---	▼
[blk_blacklists_sexual_education]	access	---	▼
[blk_blacklists_shopping]	access	---	▼
[blk_blacklists_shortener]	access	---	▼
[blk_blacklists_social_networks]	access	---	▼
[blk_blacklists_special]	access	---	▼
[blk_blacklists_sports]	access	---	▼
[blk_blacklists_strict_redirector]	access	---	▼
[blk_blacklists_strong_redirector]	access	---	▼
[blk_blacklists_translation]	access	---	▼
[blk_blacklists_tricheur]	access	---	▼
[blk_blacklists_update]	access	---	▼
[blk_blacklists_violence]	access	---	▼
[blk_blacklists_warez]	access	---	▼
[blk_blacklists_webmail]	access	---	▼
Default access [all]	access	allow	▼

Do not allow IP-Addresses in URL ☐ To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.

Proxy Denied Error

Et cliquer sur "Save"

Remplissez le formulaire de la même façon

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

General Options

Target Rules

Target Rules List

Do not allow IP-Addresses in URL
☐ To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.

Proxy Denied Error

The first part of the error message displayed to clients when access was denied. Defaults to "Request denied by \$g[product_name] proxy"

Redirect mode

Select redirect mode here.
Note: if you use 'transparent proxy', then 'int' redirect mode will not be accessible.
Options: [ext url err page](#), [ext url redirect](#), [ext url as 'move'](#), [ext url as 'found'](#).

Redirect info

Enter external redirection URL, error message or size (bytes) here.

Use SafeSearch engine
☒ Enable the protected mode of search engines to limit access to mature content.
At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search and Bing. Make sure that the search engines can be accessed. It is recommended to prohibit access to others.
Note: This option overrides 'Rewrite' setting.

Rewrite

Enter the rewrite condition name for this rule or leave it blank.

Log
☒ Check this option to enable logging for this ACL.

Save

Et cliquer sur "Save"

Ensuite dans "general settings"

Puis "Enable"

Puis "apply"

Package / Proxy filter SquidGuard: General settings / General settings

General settings Common 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](#).
The Save button at the bottom of this page must be clicked to save configuration changes.
To activate squidGuard configuration changes, **the Apply button must be clicked**.

SquidGuard service state: **STOPPED**

LDAP Options

Enable LDAP Filter ☐ Enable options for setup ldap connection to create filters with ldap search

LDAP DN
Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)

LDAP DN Password
Password must be initialize with letters (Ex: Change123), valid format: [a-zA-Z0-9/_\.\!\@\#\%\&*\+\?=\&]

Strip NT domain name ☐ Strip NT domain name component from user names (/ or \ separated).

Strip Kerberos Realm ☐ Strip Kerberos Realm component from user names (@ separated).

LDAP Version

Logging options

Enable GUI log ☒ Check this option to log the access to the Proxy Filter GUI.

Enable log ☒ Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.

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

Il va afficher des erreurs Blacklist, n'en tenez pas compte et faite "Save" tout en bas

The following input errors were detected:

- (B1) BLACKLIST 'blk_blacklists_agressif' error: file '/var/db/squidGuard/blk_blacklists_agressif' not found
- (B1) BLACKLIST 'blk_blacklists_drugs' error: file '/var/db/squidGuard/blk_blacklists_drugs' not found
- (B1) BLACKLIST 'blk_blacklists_mail' error: file '/var/db/squidGuard/blk_blacklists_mail' not found
- (B1) BLACKLIST 'blk_blacklists_porn' error: file '/var/db/squidGuard/blk_blacklists_porn' not found
- (B1) BLACKLIST 'blk_blacklists_publicite' error: file '/var/db/squidGuard/blk_blacklists_publicite' not found
- (B1) BLACKLIST 'blk_blacklists_redirector' error: file '/var/db/squidGuard/blk_blacklists_redirector' not found
- (B1) BLACKLIST 'blk_blacklists_violence' error: file '/var/db/squidGuard/blk_blacklists_violence' not found

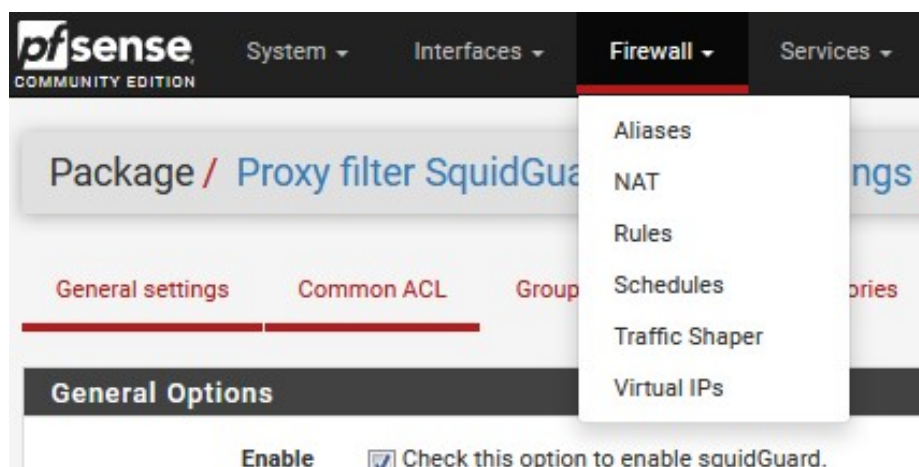
Maintenant le proxy est actif, il ne plus qu'à configurer les navigateurs.

En informatique, la répartition de charge (en anglais : load balancing) est un ensemble de techniques permettant de distribuer une charge de travail entre différents ordinateurs d'un groupe. Ces techniques permettent à la fois de répondre à une charge trop importante d'un service en la répartissant sur plusieurs serveurs, et de réduire l'indisponibilité potentielle de ce service que pourrait provoquer la panne logicielle ou matérielle d'un unique serveur.

Sources: Wikipedia

On commence par crée l'ip virtuel en 10.69.1.1

On va dans firewall / Virtual IP



On clique ensuite sur "+add"

Remplissez le formulaire de la même façon

A screenshot of the pfSense 'Edit Virtual IP' configuration form. The form is titled 'Edit Virtual IP' and has a breadcrumb trail 'Firewall / Virtual IPs / Edit'. It contains several sections: 'Type' with radio buttons for 'IP Alias' (selected), 'CARP', 'Proxy ARP', and 'Other'; 'Interface' with a dropdown menu showing 'DMZ'; 'Address type' with a dropdown menu showing 'Single address'; 'Address(es)' with a text input field containing '10.69.1.1' and a subnet mask dropdown showing '/ 32'; 'Virtual IP Password' with a password field and a 'Confirm' button; 'VHID Group' with a dropdown menu showing '1'; 'Advertising frequency' with two dropdown menus for 'Base' (showing '1') and 'Skew' (showing '0'); and 'Description' with a text input field containing 'VIP_DMZ'. A 'Save' button is at the bottom.

Cliquer sur "Apply changes" pour appliquer les changements

Firewall / Virtual IPs

The VIP configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes

Virtual IP Address	Interface	Type	Description	Actions
Virtual IP address	Interface	Type	Description	Actions
10.69.1.1/32	DMZ	IP Alias	VIP_DMZ	

+ Add



Maintenant allumer vos deux serveurs web

pfSense COMMUNITY EDITION

System - Interfaces - Firewall - Services - VPN -

Firewall / Virtual IPs

The changes have been applied successfully.

Virtual IP Address	Interface
10.69.1.1/32	DMZ

Services menu:

- Captive Portal
- DHCP Relay
- DHCP Server
- DHCPv6 Relay
- DHCPv6 Server & RA
- DNS Forwarder
- DNS Resolver
- Dynamic DNS
- IGMP Proxy
- Load Balancer
- NTP
- PPPoE Server
- SNMP
- Squid Proxy Server
- Squid Reverse Proxy
- SquidGuard Proxy Filter
- UPnP & NAT-PMP
- Wake-on-LAN

Aller dans : services / load balancer

pfSense COMMUNITY EDITION

System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help -

Services / Load Balancer / Pools / Edit

Add/Edit Load Balancer - Pool Entry

Name: servweb

Mode: Load Balance

Description:

Port: 80
This is the port the servers are listening on. A port alias listed in Firewall -> Aliases may also be specified here.

Retry: 3
Optionally specify how many times to retry checking a server before declaring it down.

Add Item to the Pool

Monitor: ICMP

Server IP Address: 10.69.1.12 + Add to pool

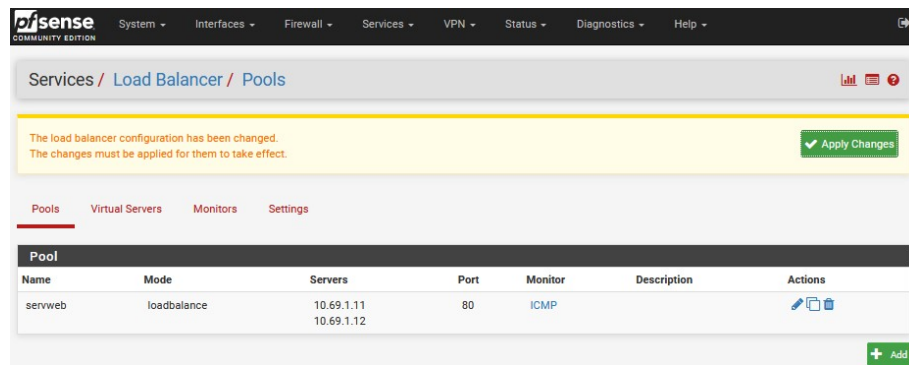
Current Pool Members

Members	Members
Disabled	Enabled (Default)

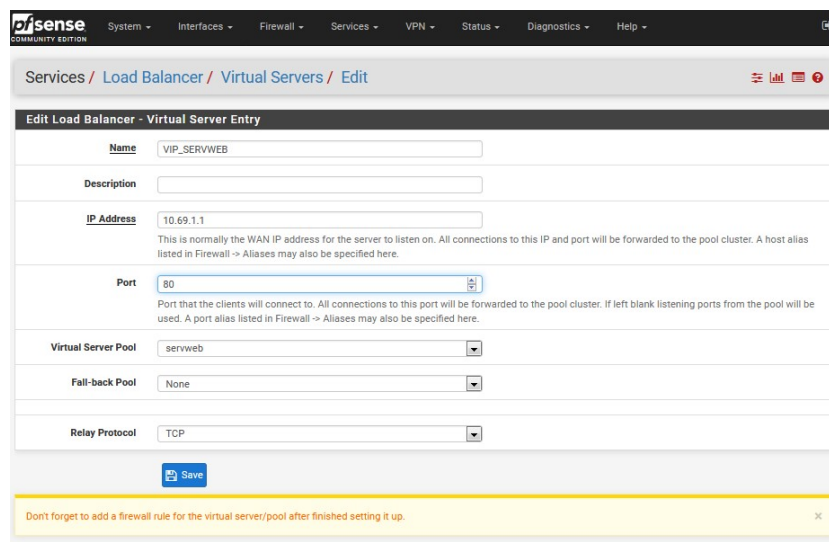
Save

- Aller dans : pools
- Puis faite : "+add"
- Remplissez le formulaire de la même façon
- Et cliquer sur "Save"

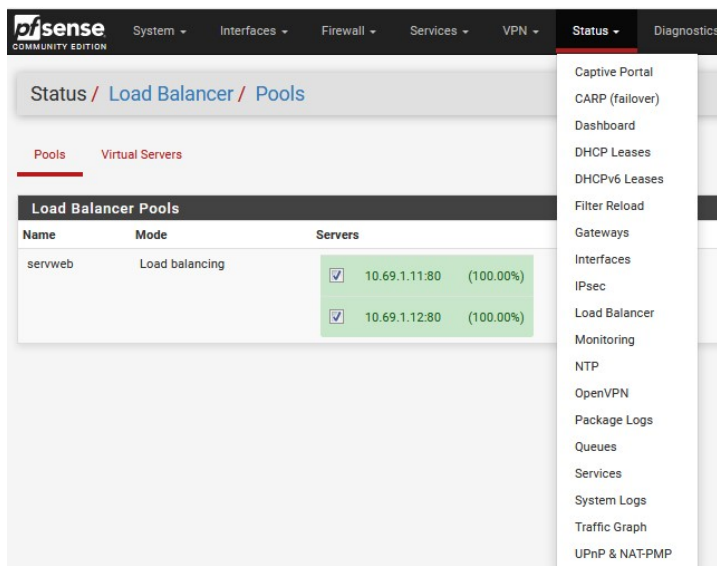
Cliquer sur "Apply changes" pour appliquer les changements



Aller dans l'onglet : "virtual server" puis "+add"



Puis cliquer sur "Apply changes" pour appliquer les changements



Aller dans status / load balancer

pfSense COMMUNITY EDITION

System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help

Status / Load Balancer / Pools

Pools Virtual Servers

Name	Mode	Servers	Monitor	Description
servweb	Load balancing	<input checked="" type="checkbox"/> 10.69.1.11:80 (100.00%)	ICMP	
		<input checked="" type="checkbox"/> 10.69.1.12:80 (100.00%)		

Save Reset

Nous pouvons voir que le load-balancing a bien été pris en compte sur les deux serveurs WEB.

Les deux serveurs sont en vert, ce qui signifie qu'ils sont bien connectés et ont chacun une charge de 100%.

On peut voir qu'il a bien identifié et pris en compte les 2 adresses des serveurs et leurs IP Virtuelle.

pfSense COMMUNITY EDITION

System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help

Status / Load Balancer / Virtual Servers

Pools Virtual Servers

Name	Address	Servers	Status	Description
VIP_SERVWEB	10.69.1.1:80	10.69.1.11 10.69.1.12	Active	

Test du load balancer

Pour tester le load balancer des serveurs web, on va couper l'un des deux serveurs web

- Couper l'un des deux serveurs WEB
- Aller dans status / load balancer grâce à votre interface WEB de pfSense

pfSense COMMUNITY EDITION

System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help

Status / Load Balancer / Pools

Pools Virtual Servers

Name	Mode	Servers	Monitor	Description
servweb	Load balancing	<input checked="" type="checkbox"/> 10.69.1.11:80 (95.00%)	ICMP	
		<input checked="" type="checkbox"/> 10.69.1.12:80 (100.00%)		

Save Reset

On peut voir que le serveur en 10.69.1.11 est tombé et que le load balancer a bien fonctionné.

Donc le serveur WEB en 10.69.1.12 a pris la charge de l'autre serveur automatiquement sans que personne ne s'en rende compte car les utilisateurs pointent vers l'IP virtuelle.