

PROJET : Cluster pfSense HA (Haute Disponibilité)

Le matériel nécessaire : 2 routeurs pfSense et deux machines clientes sous Windows 10 ou 11.

Les ressources indispensables pour installer correctement nos pfSense : 2 Gio de RAM, trois cartes réseau (WAN, LAN, SYNC). Il faut effectuer la même configuration sur le second pfSense. Prévoir également 10 Go de disque dur et 2 CPU.

L'objectif de ce TP est d'assurer la redondance entre deux pfSense, de réaliser la synchronisation entre le master et le backup, et de configurer une VIP (IP virtuelle) afin de garantir une **disponibilité constante des services et une transparence pour l'utilisateur.**

MASTER	BACKUP
10.10.11.168(WAN)	10.10.11.16G(WAN)
172.16.1.10(LAN)	172.16.1.11(LAN)

```
Writing configuration...done.
One moment while the settings are reloading... done!
UMware Virtual Machine - Netgate Device ID: 1366975ce7d281c537c0

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense-master ***

WAN (wan)   -> em0 -> v4/DHCP4: 10.10.11.168/24
LAN (lan)   -> em1 -> v4: 172.16.1.10/24
OPT1 (opt1) -> em2 ->

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                 10) Filter Logs
2) Set interface(s) IP address      11) Restart GUI
3) Reset admin account and 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:
Message from syslogd@pfSense at Apr 21 17:13:35 ...
php-fpm[424]: /index.php: Successful login for user 'admin' from: 172.16.1.1 (Local Database)
█
```

La console principale de pfSense (Master)

```

Starting CRON... done.
>>> Removing vital flag from php83...done.
pfSense 2.8.1-RELEASE amd64 20251215-1731
Bootup complete

FreeBSD/amd64 (pfSense-backup.home.arp) (ttyv0)

UMware Virtual Machine - Netgate Device ID: 8606e81a47ca9e4e6f54

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense-backup ***

WAN (wan) -> em0 -> v4/DHCP4: 10.10.11.169/24
LAN (lan) -> em1 -> v4: 172.16.1.11/24

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address      11) Restart GUI
3) Reset admin account and 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: █

```

La console du Backup après les modifications indispensables : désactivation du pare-feu et attribution d'une adresse IP statique à l'interface LAN.

Pour désactiver le pare-feu de pfSense : appuyer sur 8 pour entrer dans le shell, puis taper « pfctl -d ». Pour le relancer, utiliser « pfctl -e ».

Lorsque vous désactivez le pare-feu, celui-ci se relance à chaque modification de configuration que vous effectuez. Afin de le maintenir éteint, vous pouvez utiliser la commande suivante qui le désactive en boucle :

```
sh -c 'while true; do pfctl -d; sleep 5; done'
```

Pour revenir à l'interface de pfSense, il faut sortir du shell :

```
exit
```

Astuce :

DEBUG :

Si votre clavier n'est pas en français et que vous avez du mal à trouver certains caractères (notamment le « - »), copiez/collez la commande dans la VM en utilisant la fonctionnalité « coller » de VMware :

Menu VMware : Edit > Paste

Pour pouvoir mettre en œuvre le cluster HA, il faut dans un premier temps réaliser la synchronisation avec pfsync. Pour cela, il est nécessaire d'ajouter et de dédier une carte réseau sur chacune de nos VM, ainsi qu'une plage d'adressage dédiée et spécifique :

MASTER	BACKUP
SYNC : 10.180.0.100	SYNC : 10.180.0.200

Interfaces / Interface Assignments



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

Interface	Network port
WAN	em0 (00:0c:29:a3:4d:86)
LAN	em1 (00:0c:29:a3:4d:90) Delete
SYN	em2 (00:0c:29:a3:4d:9a) Delete

Save

Interfaces that are configured as members of a lagg(4) interface will not be shown.
Wireless interfaces must be created on the Wireless tab before they can be assigned.

Status / Dashboard



System Information

Name	pfSense-master.home.arpa
User	admin@172.16.1.1 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 1366975ce7d281c537c0
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020 Boot Method: BIOS
Version	2.8.1-RELEASE (amd64) built on Mon Dec 15 17:31:00 UTC 2025 FreeBSD 15.0-CURRENT The system is on the latest version. Version information updated at Tue Apr 21 17:13:42 UTC 2026
CPU Type	AMD Ryzen 7 Microsoft Surface (R) Edition 2 CPUs : 1 package(s) x 2 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	02 Hours 00 Minute 58 Seconds
Current date/time	Tue Apr 21 17:43:34 UTC 2026
DNS server(s)	• 127.0.0.1 • ::1 • 10.10.11.2
Last config change	Tue Apr 21 17:37:06 UTC 2026

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#).

Interfaces

WAN	↑	1000baseT <full-duplex>	10.10.11.168
LAN	↑	1000baseT <full-duplex>	172.16.1.10
SYN	↑	1000baseT <full-duplex>	10.180.0.100

À partir de là, nous pouvons aborder la configuration de la haute disponibilité :

The screenshot shows the pfSense web interface for High Availability configuration. The browser address bar indicates the URL is https://172.16.1.10/system_hasync.php. The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled "System / High Availability" and contains two sections: "State Synchronization Settings (pfsync)" and "Configuration Synchronization Settings (XMLRPC Sync)".

State Synchronization Settings (pfsync)

- Synchronize states:** pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)
- Synchronize Interface:** SYN. If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.
- Filter Host ID:** 81c537c0. Custom pf host identifier carried in state data to uniquely identify which host created a firewall state. Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01). Each node participating in state synchronization must have a different ID.
- pfsync Synchronize Peer IP:** 10.180.0.200. Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

- Synchronize Config to IP:** 10.180.0.200. Enter the IP address of the firewall to which the selected configuration sections should be synchronized. XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly! Do not use the Synchronize Config to IP and password option on backup cluster members!
- Remote System Username:** admin. Enter the webConfigurator username of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and username option on backup cluster members!
- Remote System Password:** *****. Enter the webConfigurator password of the system entered above for synchronizing the configuration. Confirm *****.

Sur la machine master, on accède à System / High Availability : depuis le master, il faut configurer les deux parties, à savoir pfsync et XMLRPC Sync.

pfsync : synchronisation des connexions en temps réel.

XMLRPC : synchronisation de la configuration.

Le pfsync doit être configuré sur les deux pfSense (bidirectionnel), tandis que le XMLRPC ne doit être configuré que sur le Master (unidirectionnel).

Remote System Username	<input type="text" value="admin"/>	
	Enter the webConfigurator username of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and username option on backup cluster members!	
Remote System Password	<input type="password" value="*****"/>	<input type="password" value="*****"/>
	Enter the webConfigurator password of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and password option on backup cluster members!	
Synchronize admin	<input type="checkbox"/> synchronize admin accounts and autoupdate sync password. By default, the admin account does not synchronize, and each node may have a different admin password. This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.	
Select options to sync	<ul style="list-style-type: none"><input checked="" type="checkbox"/> User manager users and groups<input checked="" type="checkbox"/> Authentication servers (e.g. LDAP, RADIUS)<input checked="" type="checkbox"/> Certificate Authorities, Certificates, and Certificate Revocation Lists<input checked="" type="checkbox"/> Firewall rules<input checked="" type="checkbox"/> Firewall schedules<input checked="" type="checkbox"/> Firewall aliases<input checked="" type="checkbox"/> NAT configuration<input checked="" type="checkbox"/> IPsec configuration<input checked="" type="checkbox"/> OpenVPN configuration (Implies CA/Cert/CRL Sync)<input checked="" type="checkbox"/> DHCP Server settings<input type="checkbox"/> DHCP Relay settings<input type="checkbox"/> DHCPv6 Relay settings<input checked="" type="checkbox"/> WoL Server settings<input checked="" type="checkbox"/> Static Route configuration<input checked="" type="checkbox"/> Virtual IPs<input checked="" type="checkbox"/> Traffic Shaper configuration<input checked="" type="checkbox"/> Traffic Shaper Limiters configuration<input checked="" type="checkbox"/> DNS Forwarder and DNS Resolver configurations<input checked="" type="checkbox"/> Captive Portal <input checked="" type="checkbox"/> Toggle All	
	<input type="button" value="Save"/>	

Ici, on renseigne les identifiants du backup et on active les paramètres que l'on souhaite synchroniser entre les deux routeurs.

L'étape suivante, obligatoire, consiste à créer une règle sur les deux pfSense, sur l'interface SYNC chargée d'effectuer la synchronisation.

Pour vérifier que tout fonctionne correctement, utiliser l'option « Filter Reload ».



Appuyer sur « Force Config Sync » pour forcer la synchronisation entre les deux routeurs.

Comme on le constate ici, les logs confirment que la synchronisation s'effectue correctement entre les deux pfSense. On peut également effectuer un test en créant un utilisateur sur le master, puis en vérifiant sur le backup si cet utilisateur a bien été créé.

L'étape de synchronisation est terminée. Nous passons maintenant à une autre partie du TP, en lien avec celle que nous venons de réaliser.

Pour simplifier la gestion de la Gateway, nous allons mettre en œuvre une VIP (Virtual IP) via le protocole CARP, afin de créer une carte réseau virtuelle et une adresse IP virtuelle. Cette adresse n'existe pas physiquement, n'est rattachée à aucune machine en particulier et peut basculer entre les deux pfSense.

Les étapes pour mettre en place la VIP (IP virtuelle) :

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type IP Alias CARP Proxy ARP Other

Interface LAN

Address type Single address

Address(es) 172.16.1.100 / 24
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password Confirm
Enter the VHID group password.

VHID Group 1
Enter the VHID group that the machines will share.

Advertising Frequency Base: 1 Skew: 0
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

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

Save

Dès que la configuration est effectuée sur le master, la réplication est automatiquement appliquée sur le backup, ce qui optimise et réduit la charge de travail.

Le mécanisme CARP utilise les paramètres Base et Skew pour déterminer la priorité des nœuds. Le nœud ayant la valeur la plus faible devient actif et envoie les messages de heartbeat.

La configuration a été répliquée sur le backup via le XMLRPC précédemment mis en place.

Ici, on constate que CARP distingue bien le master du backup. Pour tester le basculement, nous allons éteindre le master afin de vérifier si le backup prend effectivement le relais.

The image displays two screenshots from the pfSense web interface. The left screenshot shows the configuration page for the LAN (em1) interface. The right screenshot shows the CARP status page, which includes a table of interface and VHID information and a section for state synchronization status.

Left Screenshot: Interfaces / LAN (em1)

General Configuration

- Enable: Enable interface
- Description: LAN
- IPv4 Configuration Type: Static IPv4
- IPv6 Configuration Type: None
- MAC Address: xx:xx:xx:xx:xx:xx
- MTU: [empty]
- MSS: [empty]
- Speed and Duplex: Default (no preference, typically autoselect)

Static IPv4 Configuration

IPv4 Address: 172.16.1.10 / 24

Right Screenshot: Status / CARP

CARP Maintenance

- Buttons: [Temporarily Disable CARP](#), [Enter Persistent CARP Maintenance Mode](#)

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
LAN@1	172.16.1.100/24		MASTER

State Synchronization Status

State Creator Host IDs:

- 81c537c0
- 9e4e6f54 (This node)

When state synchronization is enabled and functioning properly the list of state creator host IDs will be identical on each node participating in state synchronization.

The state creator host ID for this node can be set to a custom value under System > High Avail Sync. If the state creator host ID has recently changed, the old ID will remain until all states using the old ID expire or are removed.

On constate bien que lorsque le master tombe en panne, le backup prend le rôle de master.

2. Déployer Squid Proxy et l'associer au serveur FreeRADIUS sur pfSense :

Configuration d'un Proxy Squid non transparent sur pfSense : Sans authentification, avec RADIUS et blocage de sites web

- I. **Configuration d'un Proxy Squid non transparent sur pfSense sans authentification, blocage de sites web**
 1. Télécharger Squid
 2. Activer le Cache Local du Proxy Squid
 3. Activer le Proxy Squid
 4. Ajouter les sites web à bloquer
 5. Créer une règle pour permettre aux utilisateurs du réseau LAN d'accéder à Internet via un proxy Squid.
 6. Désactiver le NAT OUTBOUND
 7. configuration manuelle du proxy sur le poste client du réseau LAN
 8. Tester la navigation sur internet
 9. Tester l'accès aux sites web bloqués

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: squid Both Search Clear

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

Packages

Name	Version	Description	
Lightsquid	3.0.7.5	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	+ install
Package Dependencies: lighttpd-1.4.76 lightsquid-1.8_5			
squid	0.5.3	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.	+ install
Package Dependencies: squidclamav-7.3_2 squid_radius_auth-1.10 squid-6.12_1 c-icap-modules-0.5.7_1			
squidGuard	1.16.23	High performance web proxy URL filter.	+ install
Package Dependencies: squidguard-1.4_15 pfSense-pkg-squid-0.5.3			

Installation du paquet Squid Proxy sur pfSense.

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

System / Package Manager / Package Installer

pfSense-pkg-squid installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation Auto-scroll

```

configuration file /usr/local/etc/squid/squid.conf.sample.

/usr/local/etc/squid/squid.conf.documented is a fully annotated
configuration file you can consult for further reference.

Additionally, you should check your configuration by calling
'squid -f /path/to/squid.conf -k parse' before starting Squid.
=====
Message from pfSense-pkg-squid-0.5.3:
--
Please visit Services - Squid Proxy Server menu to configure the package and enable the proxy.
>>> Cleaning up cache...done.
Success
  
```

L'installation du paquet est effectuée avec succès.

The screenshot displays the pfSense web interface for the 'Local Cache' configuration page. The breadcrumb trail at the top reads 'Package / Proxy Server: Cache Management / Local Cache'. Below this, a navigation menu includes 'General', 'Remote Cache', 'Local Cache' (which is highlighted with a red underline), 'Antivirus', 'ACLs', 'Traffic Mgmt', 'Authentication', 'Users', 'Real Time', 'Status', and 'Sync'. The main content area is titled 'Squid Cache General Settings' and contains several configuration sections:

- Disable Caching:** A checkbox labeled 'Disable caching completely.' is currently unchecked. A note below it states: 'This may be required if Squid is only used as a proxy to audit website access.'
- Cache Replacement Policy:** A dropdown menu is set to 'Heap LFUDA'. A descriptive note explains: 'The cache replacement policy decides which objects will remain in cache and which objects are replaced to create space for the new objects. Default: heap LFUDA'. An information icon is present.
- Low-Water Mark in %:** A text input field contains the value '90'. A note below it reads: 'The low-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm.' with an information icon.
- High-Water Mark in %:** A text input field contains the value '95'. A note below it reads: 'The high-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm.' with an information icon.
- Do Not Cache:** A large empty text area for listing domains or IP addresses. A note below it says: 'Enter domain(s) and/or IP address(es) that should never be cached. Put each entry on a separate line.'
- Enable Offline Mode:** A checkbox labeled 'Enable this option and the proxy server will never try to validate cached objects.' is unchecked. A note explains: 'Offline mode gives access to more cached information than normally allowed (e.g., expired cached versions where the origin server should have been contacted otherwise).'
- External Cache Managers:** An empty text input field. A note below it states: 'Enter the IPs for the external Cache Managers to be granted access to this proxy. Separate entries by semi-colons (;)'

Activation du cache de Squid Proxy.

Squid Access Control Lists

Allowed Subnets

Enter subnets that are allowed to use the proxy in CIDR format. All the other subnets won't be able to use the proxy.
Put each entry on a separate line.

When 'Allow Users on Interface' is checked on 'General' tab, there is no need to add the 'Proxy Interface(s)' subnet(s) to this list.

Unrestricted IPs

Enter unrestricted IP address(es) / network(s) in CIDR format. Configured entries will NOT be filtered out by the other access control directives set in this page.

Put each entry on a separate line. ⓘ

Banned Hosts Addresses

Enter IP address(es) / network(s) in CIDR format. Configured entries will NOT be allowed to use the proxy.
Put each entry on a separate line.

Whitelist

Destination domains that will be accessible to the users that are allowed to use the proxy.
Put each entry on a separate line. You can also use regular expressions.

Unrestricted IPs

Enter unrestricted IP address(es) / network(s) in CIDR format. Configured entries will NOT be filtered out by the other access control directives set in this page.

Put each entry on a separate line. [i](#)

Banned Hosts Addresses

Enter IP address(es) / network(s) in CIDR format. Configured entries will NOT be allowed to use the proxy.

Put each entry on a separate line.

Whitelist

Destination domains that will be accessible to the users that are allowed to use the proxy.

Put each entry on a separate line. You can also use regular expressions.

Blacklist

Destination domains that will be blocked for the users that are allowed to use the proxy.

Put each entry on a separate line. You can also use regular expressions.

Block User Agents

Enter user agents that will be blocked for the users that are allowed to use the proxy.

Put each entry on a separate line. You can also use regular expressions.

Dans l'onglet « Blacklist », on saisit les sites auxquels les utilisateurs ne doivent pas pouvoir accéder.

Put each entry on a separate line. You can also use regular expressions.

Blacklist

Destination domains that will be blocked for the users that are allowed to use the proxy.

Put each entry on a separate line. You can also use regular expressions.

Block User Agents

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾ 🔔 3 🔄

Package / Proxy Server: General Settings / General ▶ 📄 🗑️ ?

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Status Sync

Squid General Settings

Enable Squid Proxy	<input checked="" type="checkbox"/> Check to enable the Squid proxy. Important: If unchecked, ALL Squid services will be disabled and stopped.
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.
Listen IP Version	IPv4 Select the IP version Squid will use to select addresses for accepting client connections.
CARP Status VIP	none Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status. Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings synchronization.
Proxy Interface(s)	172.16.1.100 () WAN LAN SYN The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
Outgoing Network Interface	Default (auto) The interface the proxy server will use for outgoing connections.
Proxy Port	3128 This is the port the proxy server will listen on. Default: 3128
ICP Port	 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.
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.

Activation du proxy Squid.

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾ 🔔 3 🏠

Firewall / Rules / Edit 🔍 📄 📄 ?

Edit Firewall Rule

Action
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

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

Address Family
Select the Internet Protocol version this rule applies to.

Protocol
Choose which IP protocol this rule should match.

Source

Source Invert match /

[⚙️ Display Advanced](#)

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

Destination

Destination Invert match /

Destination Port Range
From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Activation d'une règle permettant aux utilisateurs du réseau LAN d'accéder à Internet via le proxy Squid.

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

Firewall / NAT / Outbound

Port Forward 1:1 **Outbound** NPT

Outbound NAT Mode

Mode	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
	Automatic outbound NAT rule generation. (IPsec passthrough included)	Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)	Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)	Disable Outbound NAT rule generation. (No Outbound NAT rules)

[Save](#)

Mappings

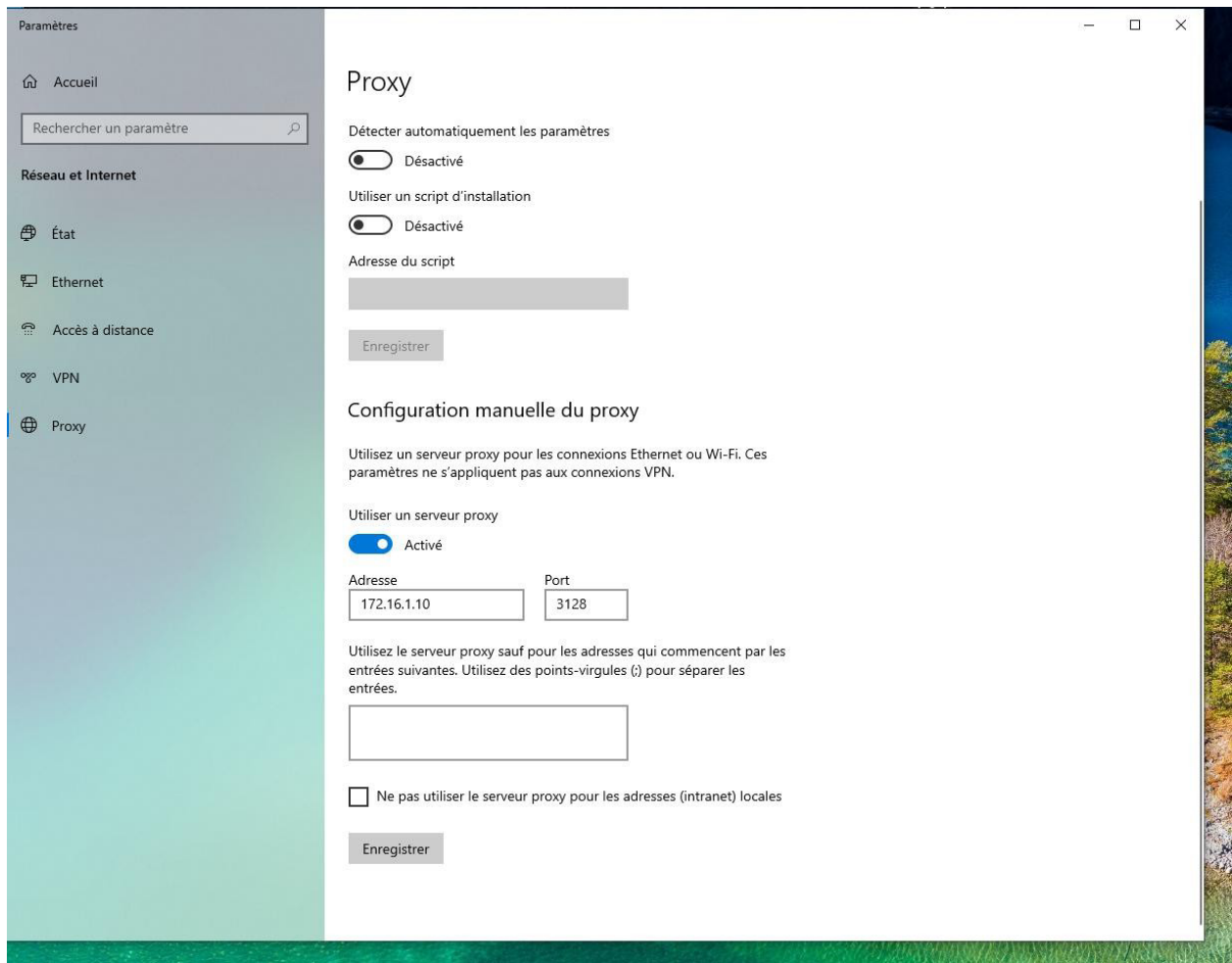
<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
										Add Add Delete Toggle Save

Automatic Rules

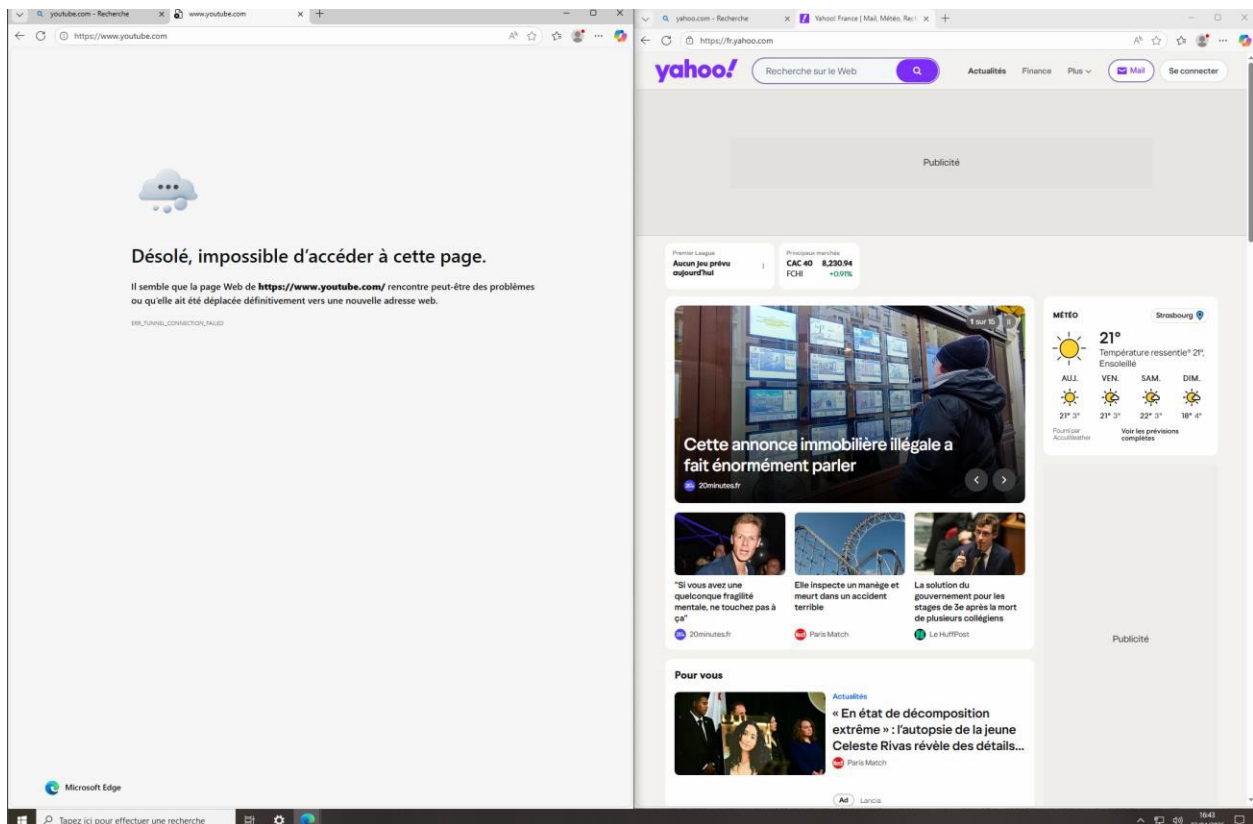
	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓	WAN	127.0.0.0/8 ::1/128 172.16.1.0/24 10.180.0.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓	WAN	127.0.0.0/8 ::1/128 172.16.1.0/24 10.180.0.0/24	*	*	*	WAN address	*	✗	Auto created rule

[?](#)

Désactivation du NAT OUTBOUND afin de forcer les utilisateurs à accéder à Internet via le proxy Squid, conformément à la règle définie précédemment.



Configuration manuelle du proxy sur le poste client du réseau LAN.



Les services fonctionnent correctement, conformément à ce qui était souhaité.

3. Configuration d'un proxy Squid non transparent sur pfSense avec authentification RADIUS

Les étapes indispensables pour associer l'authentification FreeRADIUS au proxy Squid :

- 1. Installer FreeRADIUS 3 ;**
- 2. Configurer le NAS/Client dans FreeRADIUS ;**
- 3. Configurer les interfaces de FreeRADIUS ;**
- 4. Définir FreeRADIUS comme méthode d'authentification sur le proxy ;**
- 5. Créer un compte utilisateur sur FreeRADIUS ;**
- 6. Ajouter RADIUS comme serveur d'authentification.**

pfSense COMMUNITY EDITION

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: freeradius Both Search Clear

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

Packages

Name	Version	Description
freeradius3	0.15.14	A free implementation of the RADIUS protocol. Supports MySQL, PostgreSQL, LDAP, Kerberos.

Package Dependencies:
[bash-5.2.37](#) [freeradius3-3.2.7](#) [python311-3.11.11](#)

+ Install

Installation de FreeRADIUS 3.

pfSense COMMUNITY EDITION

System / Package Manager / Package Installer

pfSense-pkg-freeradius3 installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation Auto-scroll

```
Useful configuration advice can be found in the FreeRADIUS Wiki at
http://wiki.freeradius.org
=====
Message from pfSense-pkg-freeradius3-0.15.14:

--

Please visit Services > FreeRADIUS menu to configure the package.

EAP certificate configuration is required before using the package.
Visit System > Cert. Manager and create a CA and a server certificate.
After that, visit Services > FreeRADIUS > EAP tab and complete
the 'Certificates for TLS' section (and, optionally, also the 'EAP-TLS' section.)
>>> Cleaning up cache...done.
Success
```

L'installation est terminée avec succès.

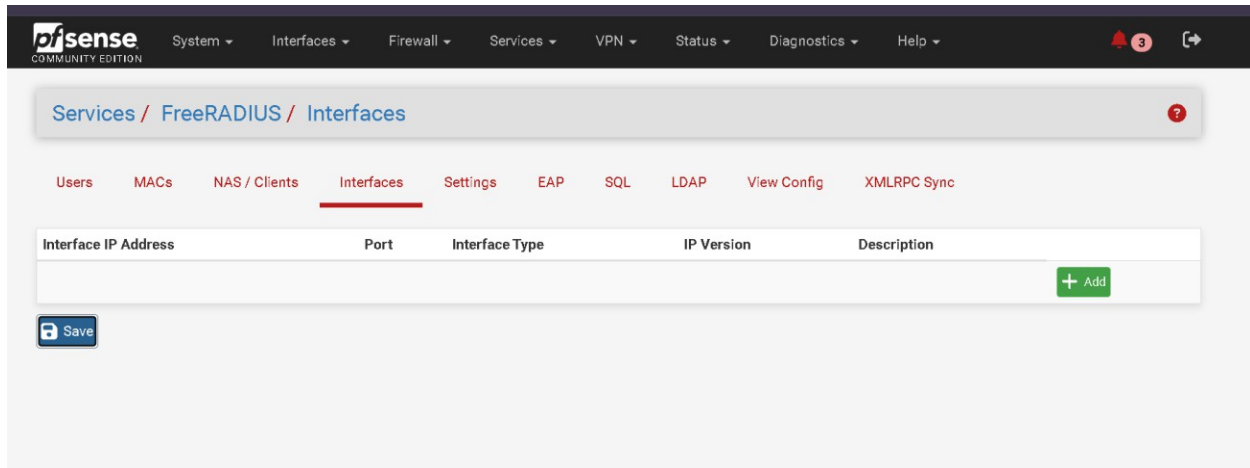
The screenshot shows the FreeRADIUS web interface. At the top, there is a breadcrumb trail: Services / FreeRADIUS / Edit / NAS / Clients. Below this is a navigation menu with options: Users, MACs, NAS / Clients (highlighted), Interfaces, Settings, EAP, SQL, LDAP, View Config, and XMLRPC Sync. The main content area is titled "General Configuration" and contains the following fields:

- Client IP Address:** 172.16.1.10. Description: Enter the IP address or network of the RADIUS client(s) in CIDR notation. This is the IP of the NAS (switch, access point, firewall, router, etc.).
- Client IP Version:** IPv4 (dropdown menu).
- Client Shortname:** lan. Description: Enter a short name for the client. This is generally the hostname of the NAS.
- Client Shared Secret:** [Redacted]. Description: Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch, accesspoint, etc.) needs to communicate with the RADIUS server. FreeRADIUS is limited to 31 characters for the shared secret. **Warning:** Single quotes in shared secret must be escaped with a backslash (\'). Backslash must be escaped by using two backslashes (\\).

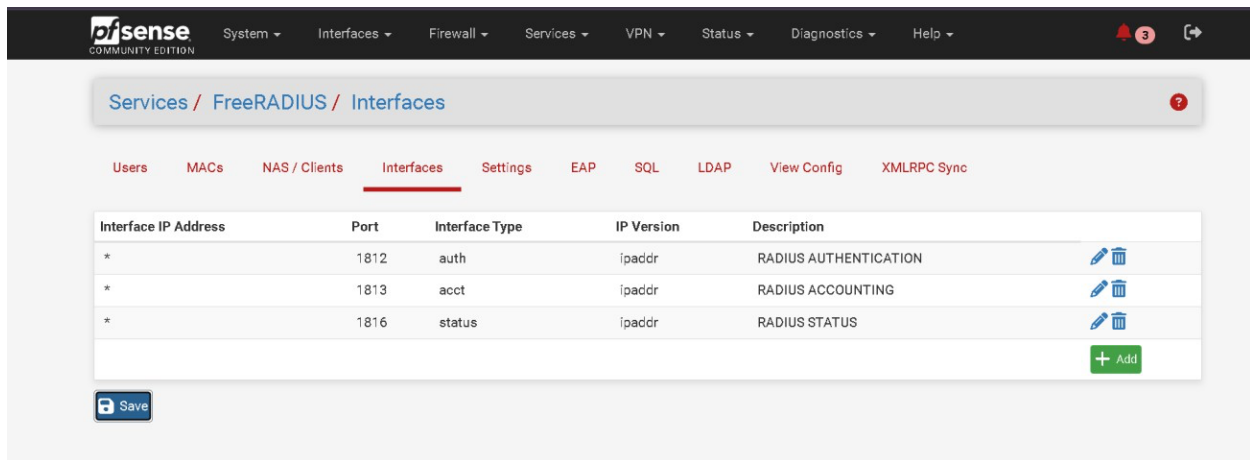
Below the "General Configuration" section is a "Miscellaneous Configuration" section.

Configuration du NAS/Client dans FreeRADIUS.

NAS/Client : il s'agit d'un service qui permet au proxy d'envoyer la demande ou la requête d'authentification au serveur RADIUS.




Ici, nous configurons les interfaces du serveur RADIUS, c'est-à-dire les interfaces sur lesquelles le serveur RADIUS va écouter.



Pourquoi 3 entrées dans FreeRADIUS ?

FreeRADIUS sépare les fonctions en 3 types de trafic :

1.  Authentication (auth) — Port 1812

➡ C'est le plus important.

- Sert à vérifier les identifiants (login / mot de passe).

Exemple :

- un utilisateur se connecte au Wi-Fi ;
- Le NAS (pfSense, switch, AP, etc.) envoie une requête à FreeRADIUS ;
- FreeRADIUS répond : ACCEPT ou REJECT.

2. Accounting (acct) – Port 1813

 Sert à enregistrer l'activité.

- Il enregistre :
 - l'heure de connexion ;
 - la durée de la session ;
 - le volume de données.

Exemple :

- utile pour le portail captif, la facturation et les journaux de sécurité.

3. Status – Port 1816

 Sert à vérifier si le serveur RADIUS fonctionne.

- C'est en quelque sorte un ping RADIUS.
 - le NAS peut tester si FreeRADIUS est disponible ;

- utilisé pour le monitoring ou la haute disponibilité (HA).

Package / Proxy Server: Authentication / Authentication

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt **Authentication** Users Real Time Status Sync

Squid Authentication General Settings

Authentication Method	RADIUS	Select an authentication method. This will allow users to be authenticated by local or external services.
Authentication Server	172.16.1.10	Enter the IP or hostname of the server that will perform the authentication here.
Authentication server port		Enter the port to use to connect to the authentication server here. Leave this field blank to use the authentication method's default port.
Authentication Prompt	Please enter your credentials to access the proxy	This string will be displayed at the top of the authentication request window.
Authentication Processes	5	The number of authenticator processes to spawn. If many authentications are expected within a short timeframe, increase this number accordingly.
Authentication TTL	5	This specifies for how long (in minutes) the proxy server assumes an externally validated username and password combination to be valid. When the Time To Live expires, the user will be prompted for credentials again. Default: 5
Authentication Max User IP Addresses		Enforces a limit to the number of unique IP addresses from which a single user can login. Attempts to login from additional IP addresses are denied until the Authentication TTL has expired. Default: none
Require Authentication for Unrestricted IPs	<input type="checkbox"/>	If enabled, even 'Unrestricted IPs' configured on the ACLs tab are required to authenticate to use the proxy.

Squid Authentication RADIUS Settings

RADIUS Secret	Enter the RADIUS secret for RADIUS authentication here.
---------------	-------	---

Save

Définir FreeRADIUS comme méthode d'authentification sur le proxy.

Services / FreeRADIUS / Edit / Users C O ?

Users MACs NAS / Clients Interfaces Settings EAP SQL LDAP View Config XMLRPC Sync

General Configuration

Username
 Enter the username. Whitespace is allowed.
 Note: May only contain a-z, A-Z, 0-9, underscore, period and hyphen when using OTP.

Password
 Enter the password for this username. Leave empty if you want to use custom options (such as OTP) instead of username/password.

Password Encryption
 Select the password encryption for this user. If the (pre-hashed) options are used, the password should already be hashed by the expected hash function. Note that not all authentication protocols are compatible with all types of hashed passwords. Default: Cleartext-Password

Création d'un compte utilisateur dans FreeRADIUS.

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help 3 ?

System / User Manager / Authentication Servers / Edit ?

Users Groups Settings Change Password Authentication Servers

Server Settings

Descriptive name

Type

RADIUS Server Settings

Protocol

Hostname or IP address

Shared Secret

Services offered

Authentication port

Accounting port

Authentication Timeout
 This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token.

RADIUS NAS IP Attribute
 Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests.
 Please note that this choice won't change the interface used for contacting the RADIUS server.

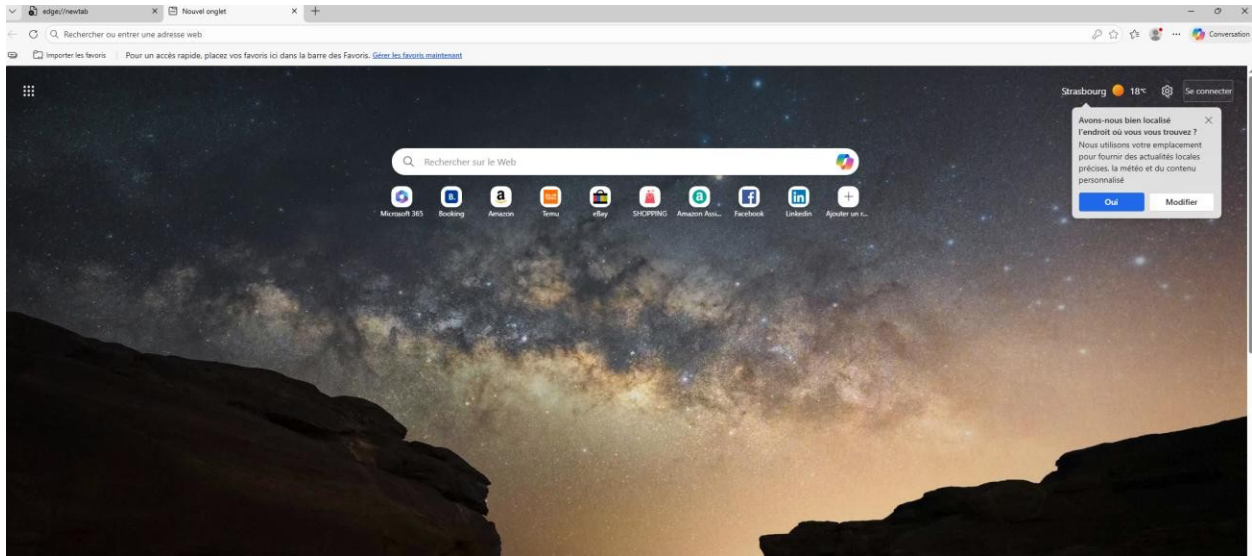
Ajout de RADIUS comme serveur d'authentification.

The screenshot shows the pfSense web interface. At the top, there is a navigation bar with the pfSense logo and menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A notification bell icon shows 3 alerts. Below the navigation bar, the breadcrumb path is "Diagnostics / Authentication". A green message box states: "User Ali authenticated successfully. This user is a member of groups:". Below this is the "Authentication Test" section, which includes a dropdown menu for "Authentication Server" set to "RADIUS", a text input for "Username" with "Ali", a password input for "Password", and a checkbox for "Debug" labeled "Set debug flag". A blue "Test" button is at the bottom of the form.

Test de l'authentification sur le serveur RADIUS.

The screenshot shows a web browser window with a login dialog box. The dialog box has the title "Se connecter pour accéder à ce site" and a warning: "Le proxy http://172.16.1.103:3128 requiert un nom d'utilisateur et un mot de passe. Votre connexion à ce site n'est pas sécurisée". It contains two input fields: "Nom d'utilisateur" with the value "Ali" and "Mot de passe" with masked characters. At the bottom of the dialog are two buttons: "Se connecter" and "Annuler".

Test sur la machine cliente : tout fonctionne correctement.



Après avoir saisi correctement les identifiants, l'accès à Internet est autorisé.

FIN DU PROJET

• Amir Tajik

