

Projet NovaResQ

BTS SIO 2025 Option SISR

Documentation Technique Situation Professionnelle 2

Table des matières

1) Préparation des routeurs.....	5
A) Initialisation de PfSense	5
2) Configuration des PfSense	25
A) Première connexion + changement de mot de passe.....	26
B) CARP LAN + High Availability	31
C) CARP WAN.....	48
3) OpenVPN RW	65
Documentation d'exploitation, L'utilisation et la gestion du Lot 1	107
Introduction :	108
Installation des rôles.....	109
Installation de l'Active Directory et DNS	117
2. Installation PRTG	126
3. Gestion Active Directory.....	132
Documentation d'installation Modoboa (Ubuntu).....	138
Introduction.....	138
Installation	140
1) Installation d'Asterisk.....	144
A) Mise à jour du serveur + installations des dépendances requises.....	144
B) Téléchargement et pré-installation de Asterisk	146
C) Compilation et installation de Asterisk	153
2) Configuration des utilisateurs SIP pour le softphone	163
3) Installation et configuration d'un client Softphone	168
4) Tests	187
1) Configuration de l'interface DMZ sur les routeurs	192
2) Configuration du serveur Ubuntu hébergeant eBrigade.....	203
A) Initialisation du serveur Ubuntu	203

B) Installation des dépendances requises	222
C) Téléchargement et déploiement de eBrigade	230

Configuration des routeurs PfSense

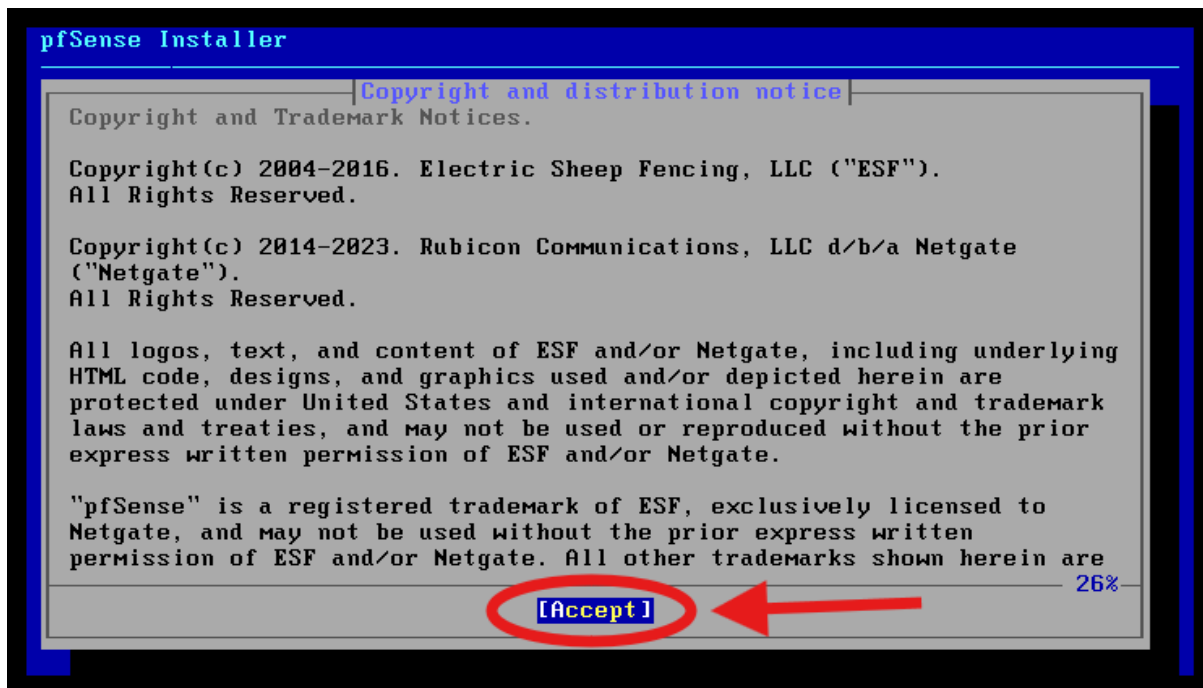


09/04/2025

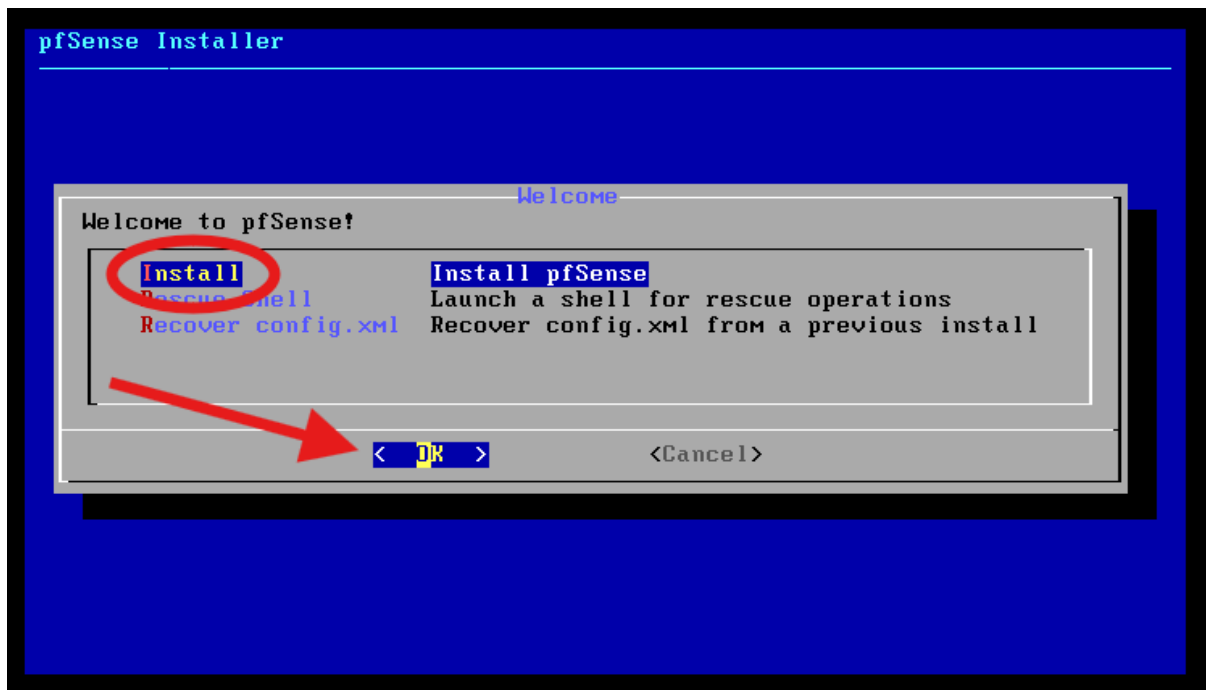
1) Préparation des routeurs

A) Initialisation de PfSense

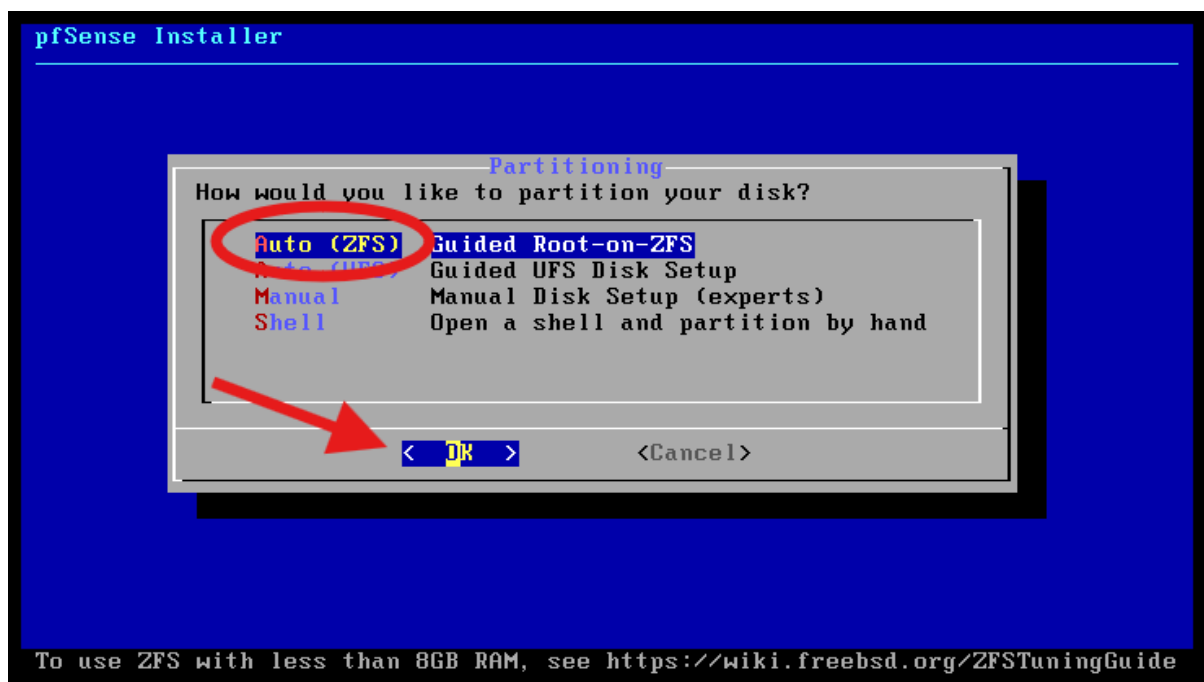
Cliquer sur Accept.



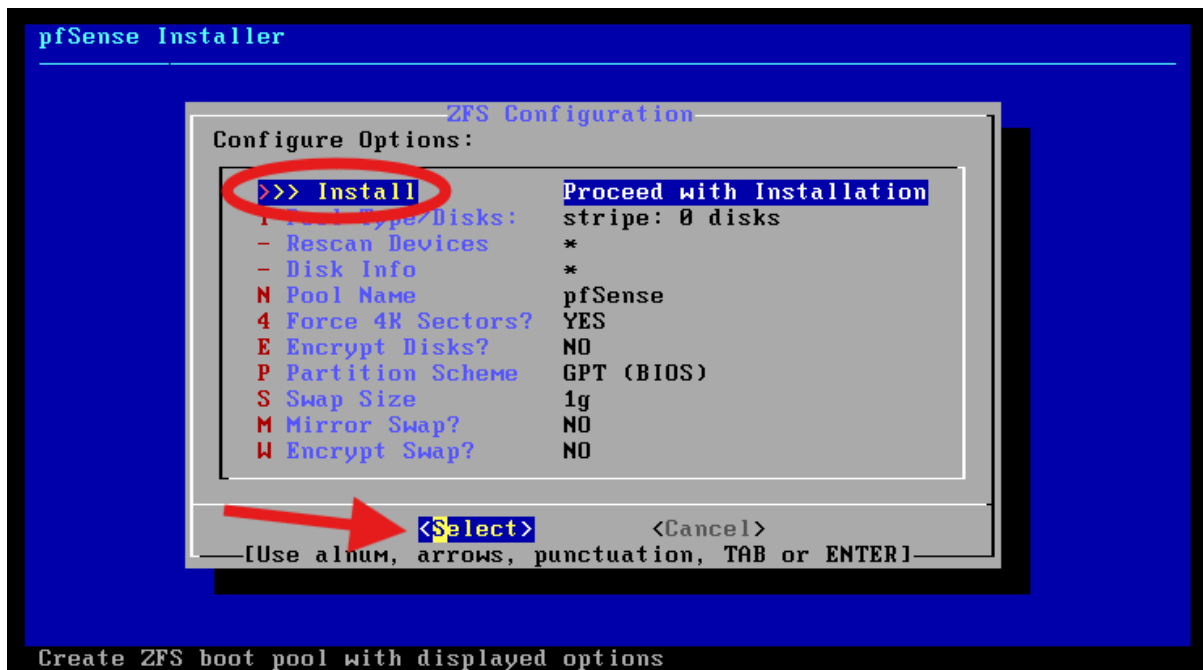
Choisir Install puis valider.



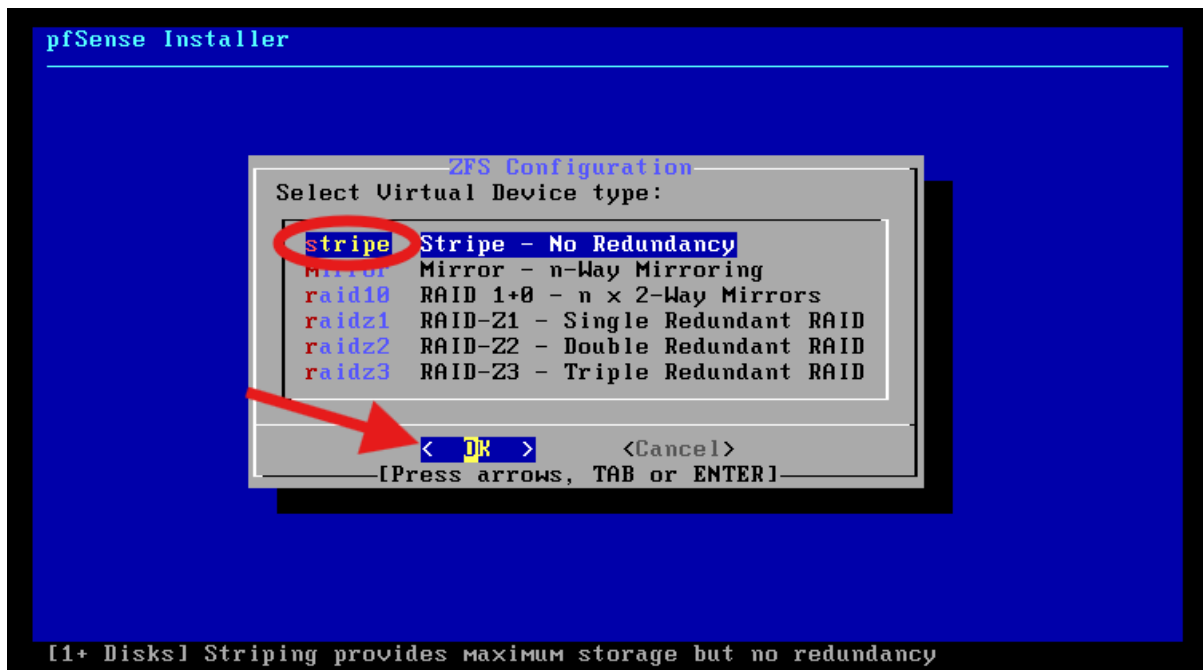
Choisir Auto (ZFS) puis valider.



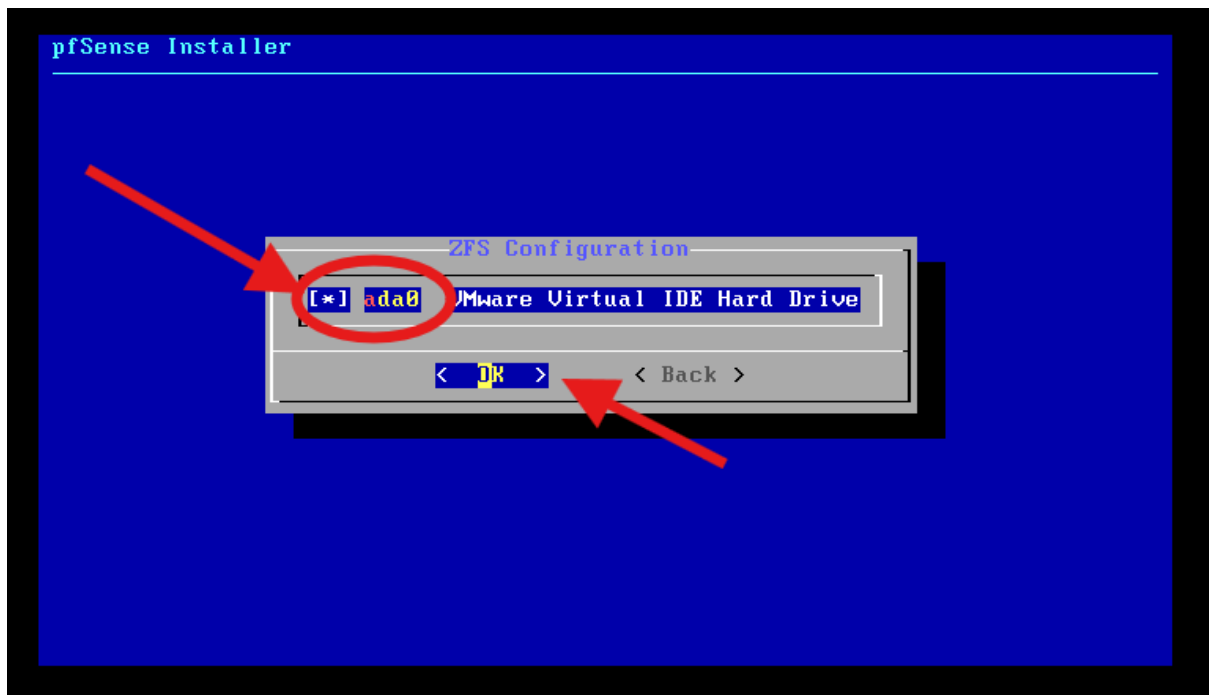
Sélectionner Install



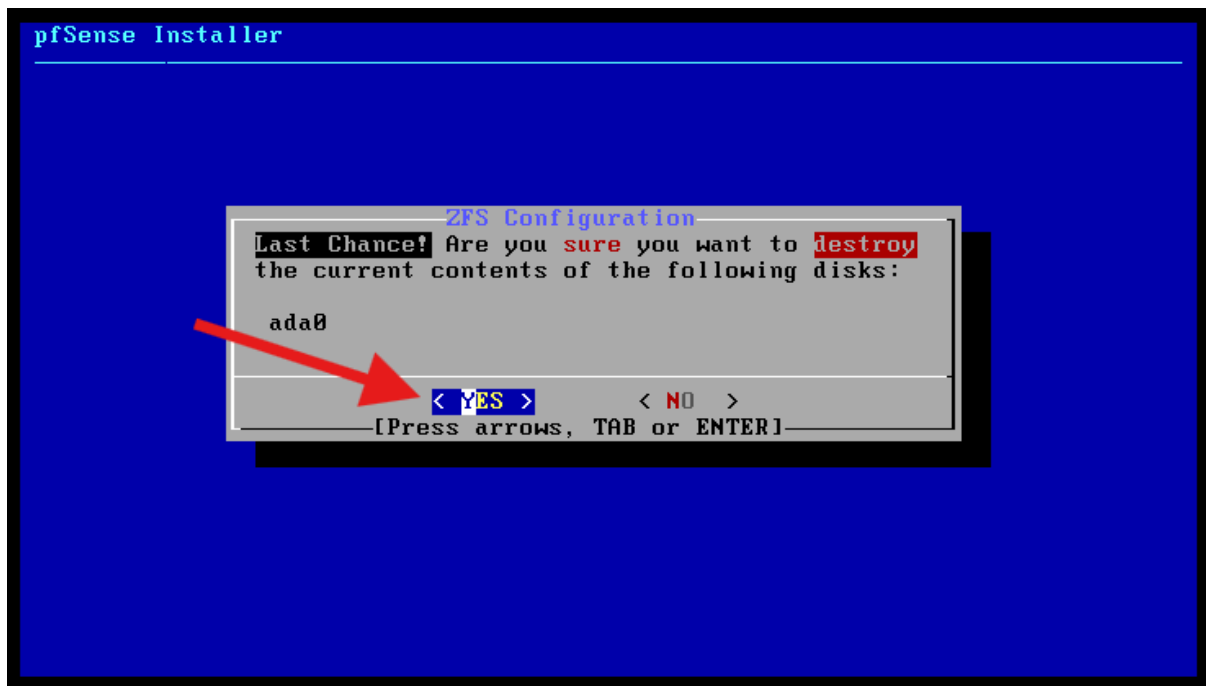
Choisir Stripe et valider.



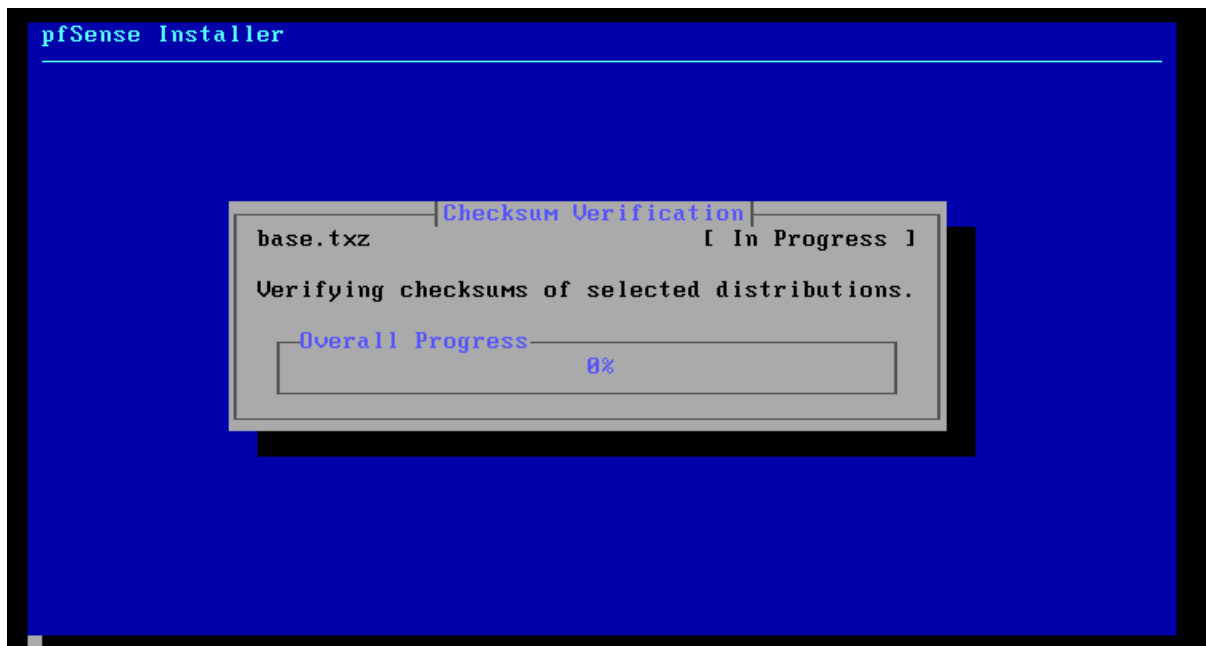
Choisir le disque et valider.



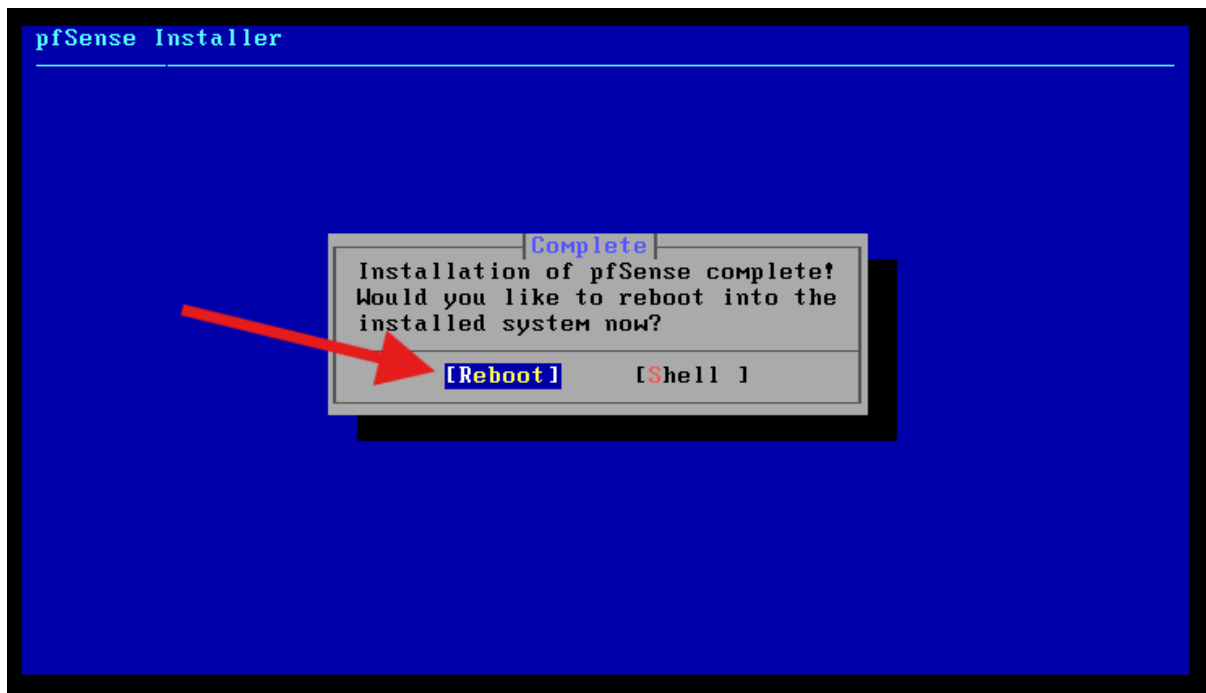
Cliquer sur OK pour valider.



Attendre la fin du téléchargement.



Cliquer sur Reboot pour redémarrer et finaliser l'installation. Attendre ensuite jusqu'à la prochaine étape.



Choisir le0 pour configurer le WAN.

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

Choisir ensuite le1 pour l'interface LAN.

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(le1 a or nothing if finished): le1
```

Valider en tapant y. Attendre ensuite la fin de la configuration.

```
The interfaces will be assigned as follows:  
  
WAN -> le0  
LAN -> le1  
  
Do you want to proceed [y/n]? y
```

Voici le menu de PfSense. Choisir 2 pour modifier les adresses IP des interfaces.

```
FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VMware Virtual Machine - Netgate Device ID: c285f019870b47b7fed9
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> le0      -> v4/DHCP4: 192.168.1.148/24
LAN (lan)      -> le1      -> v4: 192.168.1.1/24

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

Enter an option: 2
```

Sélectionner le LAN (2).

```
Available interfaces:
```

```
1 - WAN (le0 - dhcp, dhcp6)  
2 - LAN (le1 - static)
```

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

Choisir no.

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

Entrer la nouvelle adresse LAN puis sélectionner le port 24.

```
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 192.168.50.1  
  
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.  
e.g. 255.255.255.0 = 24  
     255.255.0.0   = 16  
     255.0.0.0     = 8  
  
Enter the new LAN IPv4 subnet bit count (1 to 32):  
> 24█
```

Appuyer sur la touche enter.

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

Choisir no et appuyer sur enter à la prochaine étape.

```
Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
> █
```

Choisir no aux 2 prochaines étapes.

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

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

Appuyer sur enter pour valider tous les changements.

```
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 192.168.50.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    https://192.168.50.1/

Press <ENTER> to continue. █
```

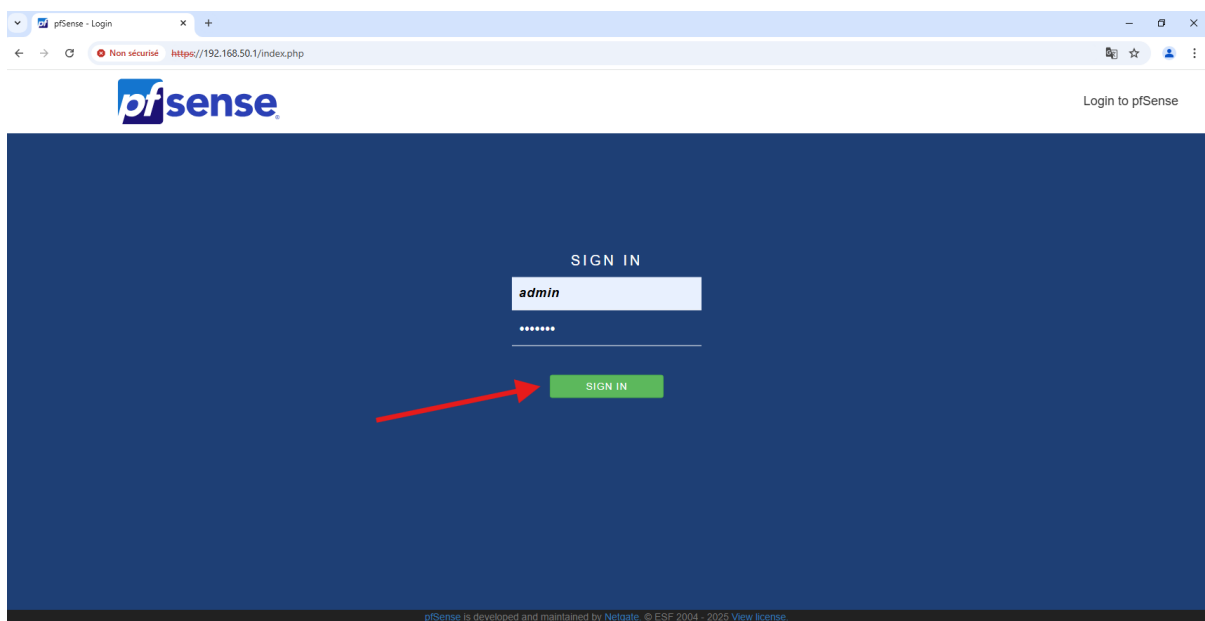
**! IL FAUT REALISER LE MEME PROCESSUS POUR LE 2EME ROUTEUR EN
REPLACANT L'ADRESSE LAN PAR UNE AUTRE (ex : 192.168.50.2). !**

2) Configuration des PfSense

A) Première connexion + changement de mot de passe

Accéder maintenant à l'interface web du PfSense Master (192.168.50.1) via un navigateur sur un poste client.

Rentrer l'identifiant "admin" avec le mot de passe de base "pfsense" puis cliquer sur sign in.



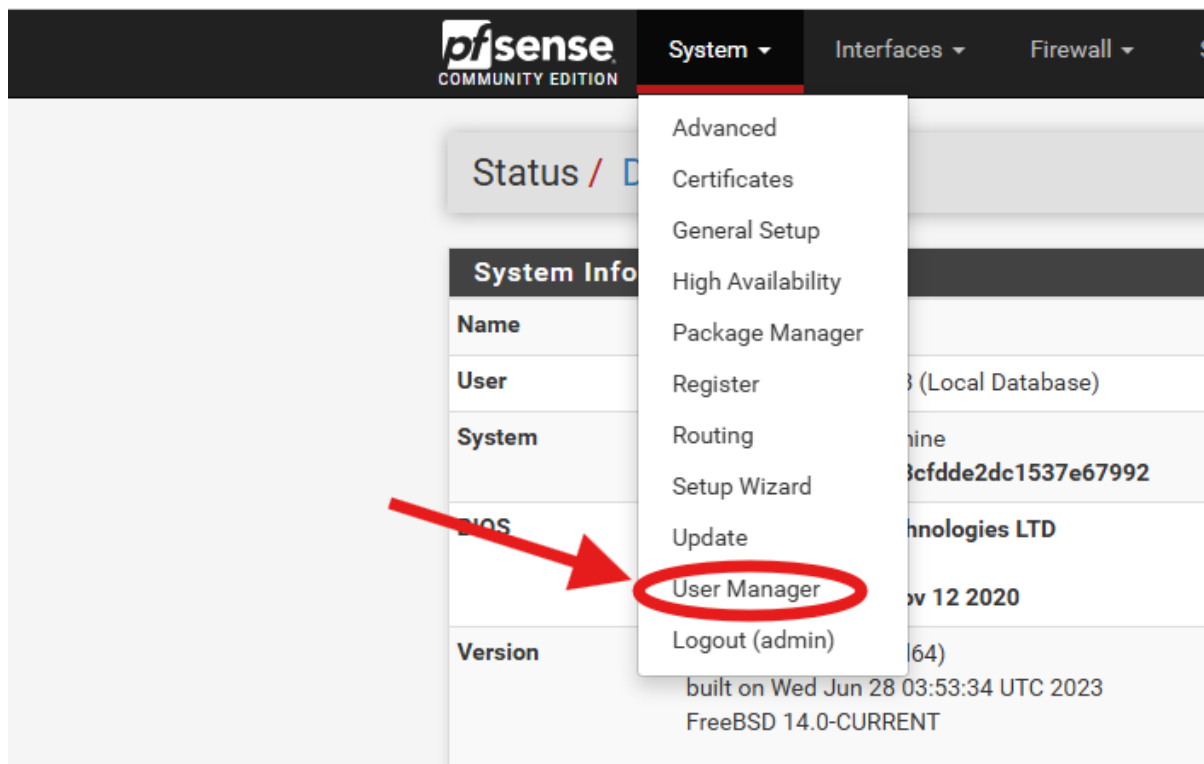
Voici la page d'accueil de PfSense. Nous allons maintenant changer le mot de passe de base pour accéder à PfSense en tant qu'admin.

The screenshot displays the pfSense Community Edition Status Dashboard. The left sidebar contains the following system information:

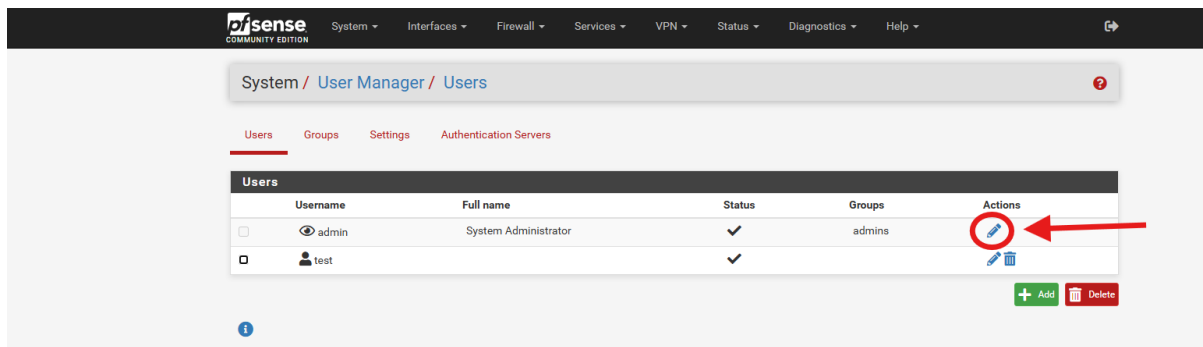
System Information	
Name	pfSense.home.arpa
User	admin@192.168.50.3 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 78cfdde2dc1537e67992
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.0-RELEASE (amd64) built on Wed Jun 28 03:53:34 UTC 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Wed Apr 9 17:12:25 UTC 2025
CPU Type	12th Gen Intel(R) Core(TM) i5-12450H 2 CPU(s): 2 package(s) x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 06 Minutes 12 Seconds
Current date/time	Wed Apr 9 17:16:45 UTC 2025

The right sidebar, titled "Netgate Services And Support", shows the contract type as "Community Support" and "Community Support Only". It includes a section for "NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES" with a detailed explanation of community support and links to various resources like the Netgate Resource Library, Upgrade Your Support, and Netgate Professional Services.

Aller dans System puis dans User Manager.



Cliquer sur l'icône du petit crayon pour accéder aux paramètres du compte admin de PfSense.



Entrer un nouveau mot de passe et confirmer le.

The screenshot shows the pfSense User Manager 'Users / Edit' page. The breadcrumb trail is 'System / User Manager / Users / Edit'. The 'Users' tab is selected in the top navigation bar. The 'User Properties' section contains the following fields:

- Defined by:** SYSTEM
- Disabled:** ☐ This user cannot login
- Username:** admin
- Password:** Password (highlighted with a red oval) and Confirm Password
- Full name:** System Administrator (with a subtext: 'User's full name, for administrative information only')
- Expiration date:** (with a subtext: '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 layout for this user.
- Group membership:** admins

Descendre tout en bas de la page et cliquer sur Save.

Name CA

+ Add

Keys

Authorized SSH Keys

Enter authorized SSH keys for this user

IPsec Pre-Shared Key

Shell Behavior

Keep Command History ☐ Keep shell command history between login sessions

If this user has shell access, this option preserves the last 1000 unique commands entered at a shell prompt between login sessions. The user can access history using the up and down arrows at an SSH or console shell prompt and search the history by typing a partial command and then using the up or down arrows.

Save

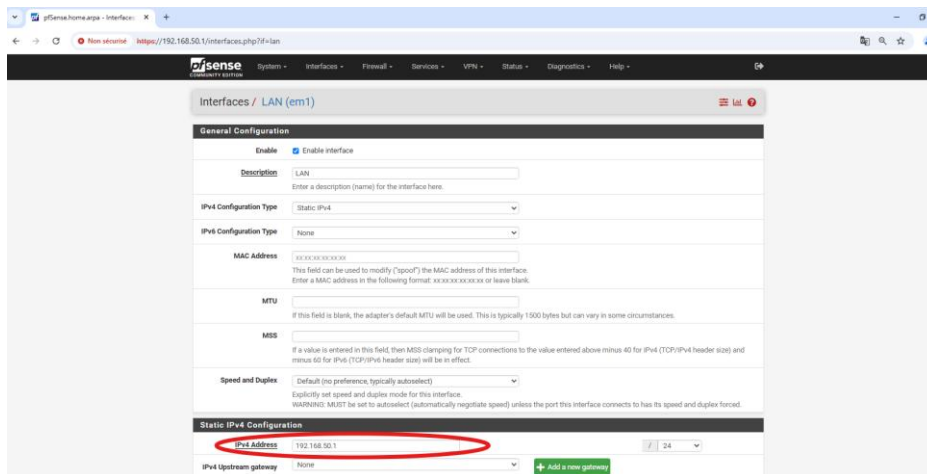
Une fois cette opération ayant été effectué, votre mot de passe a été changé.

! Cette opération est aussi à réaliser sur le deuxième PfSense en inscrivant le même mot de passe que sur le PfSense Master. !

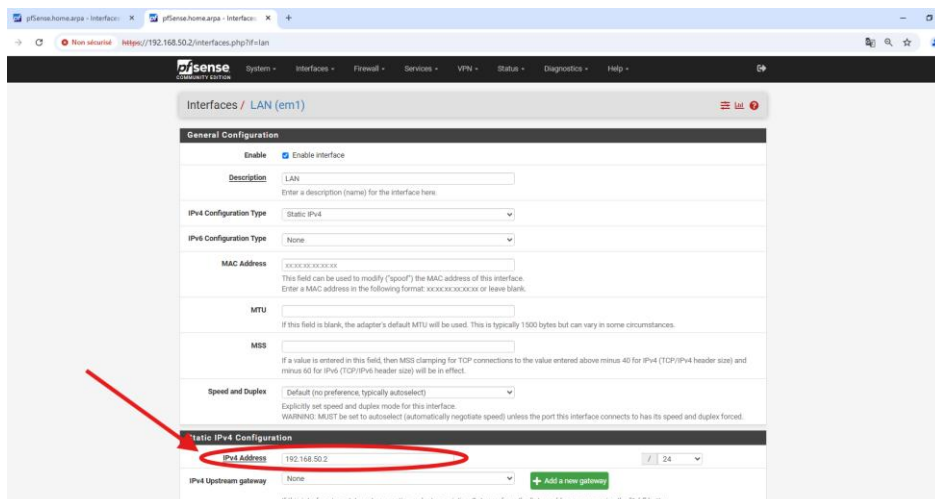
B) CARP LAN + High Availability

Avant de commencer cette étape, voici un rappel de la configuration des deux cartes LAN sur les 2 pfsense. On peut regarder ça en allant dans Interfaces, puis Assignements. Ensuite il faut cliquer sur em1 (LAN).

Voici la carte LAN sur le PfSense Master :



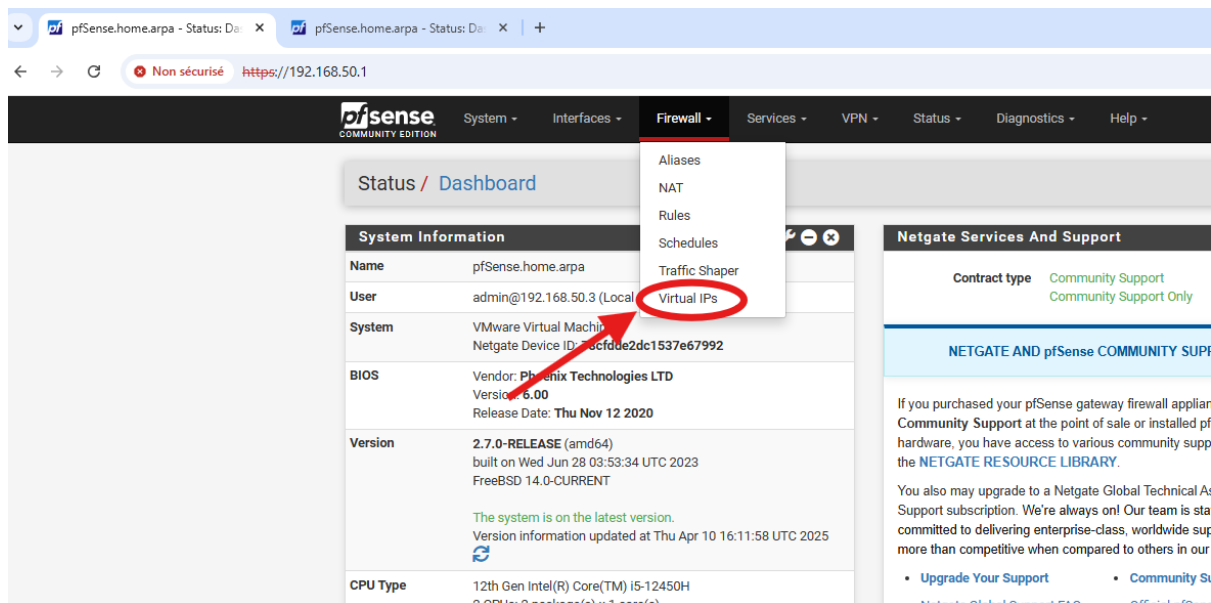
Voici la carte LAN sur le PfSense Backup :



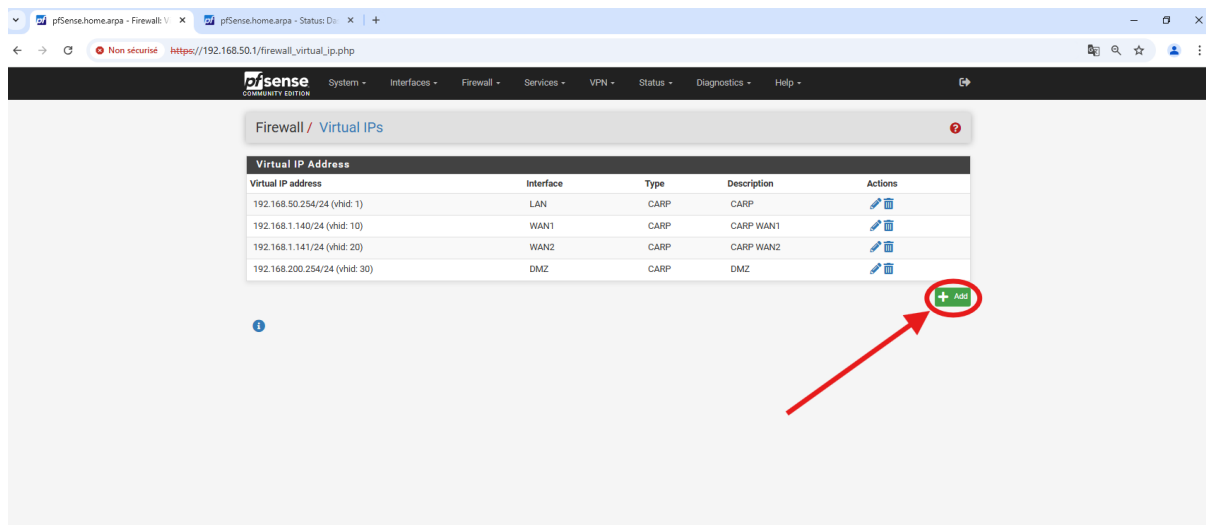
Ici, on peut voir que les deux cartes LAN sont sur la même plage d'adresse.

Pour créer notre CARP LAN, il faut d'abord configurer une IP virtuelle sur notre plage d'adresse.

Pour ce faire, aller dans Firewall puis Virtual IPs sur le PfSense Master.



Cliquer sur le bouton ADD.



Voici, dans mon cas, les paramètres à entrer (à adapter en fonction de la plage d'adresse IP du LAN).

Une fois les paramètres remplis, cliquer sur Save.

Cette opération est aussi à effectuer sur le PfSense Backup en remplaçant seulement Skew par 100 à la place de 0.

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type: ☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface: LAN

Address type: Single address

Address(es): 192.168.50.254 / 24
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password:
Enter the VHID group password. Confirm

VHID Group: 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: CARP LAN
A description may be entered here for administrative reference (not parsed).

[Save](#)

Cliquer ensuite sur Apply Changes pour appliquer les changements.

Firewall / Virtual IPs ?

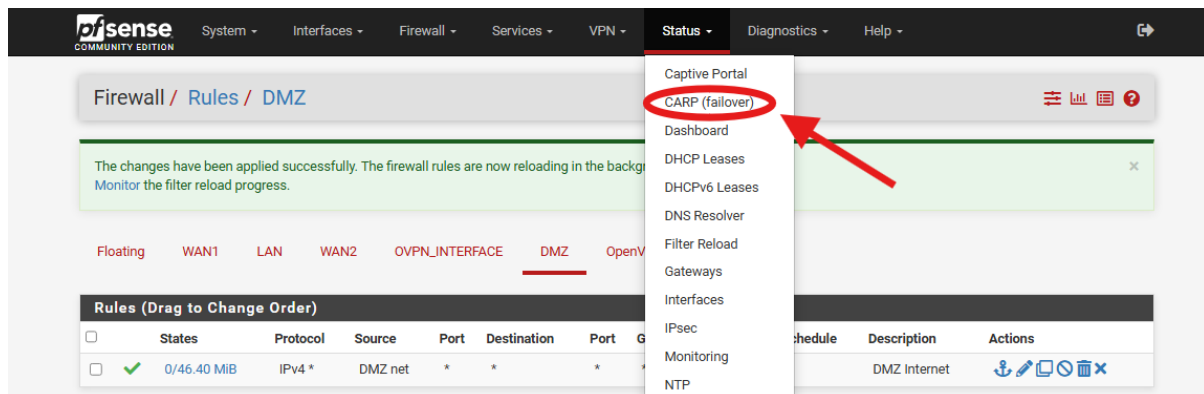
The VIP configuration has been changed.
The changes must be applied for them to take effect.

 ✓ Apply Changes

Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
192.168.50.254/24 (vhid: 1)	LAN	CARP	CARP	 
192.168.1.140/24 (vhid: 10)	WAN1	CARP	CARP WAN1	 
192.168.1.141/24 (vhid: 20)	WAN2	CARP	CARP WAN2	 
192.168.200.254/24 (vhid: 30)	DMZ	CARP	DMZ	 

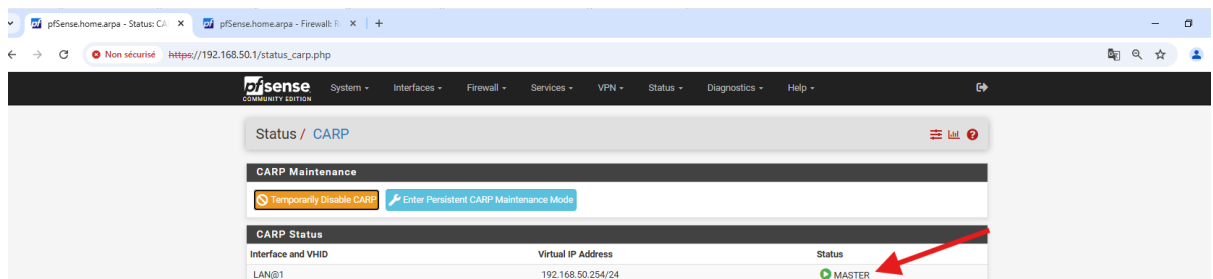
+ Add

Aller ensuite dans Status puis CARP (failover).

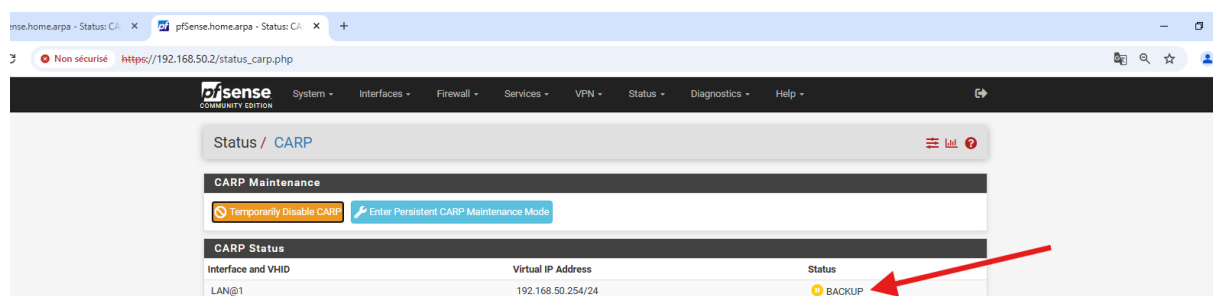


Si tout est normal, voici ce qui devrait s'afficher sur les deux PfSense.

- PfSense Master :

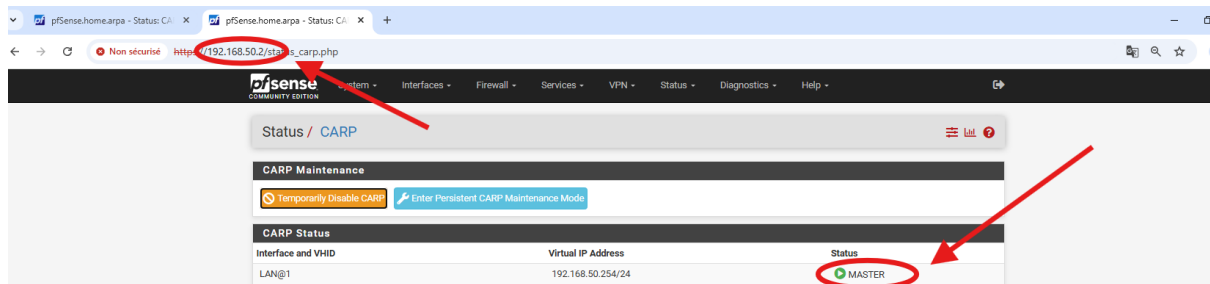


- PfSense Backup :



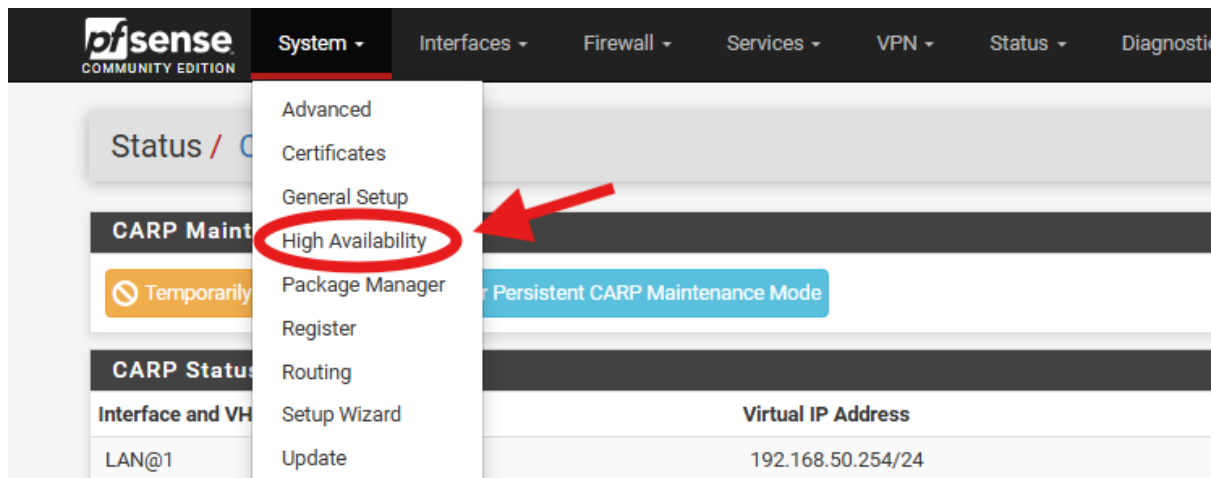
-> Explication : le routeur master (192.168.50.1) est pour l'instant actif. Si ce dernier tombe en panne, le routeur backup (192.168.50.2) prendra le relais en passant de backup à master.

Voici un exemple quand le routeur master est éteint.



Passons maintenant à la configuration de la High Availability afin que les paramètres effectués sur le PfSense Master soit aussi appliqués sur le Backup.

Aller dans System puis High Availability.



Voici les paramètres à rentrer dans le PfSense Master.

System / High Availability

State Synchronization Settings (pfsync)

Synchronize states

☒ pfsync transfers state insertion, update, and deletion messages between firewalls.
Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
This setting should be enabled on all members of a failover group.
Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface

LAN

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

37e67992

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

192.168.50.2

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

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP

192.168.50.2

Enter the IP address of the firewall to which the selected configuration sections should be synchronized.

XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username

admin

Enter the webConfigurator username of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password

Confirm

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

☒ synchronize admin accounts and autoupdate sync password.
By default, the admin account does not synchronize, and each node may have a different admin password.
This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

Select options to sync

☒ User manager users and groups
☒ Authentication servers (e.g. LDAP, RADIUS)
☒ Certificate Authorities, Certificates, and Certificate Revocation Lists
☒ Firewall rules
☒ Firewall schedules
☒ Firewall aliases
☒ NAT configuration
☒ IPsec configuration
☒ OpenVPN configuration (Implies CA/Cert/CRL Sync)
☒ DHCP Server settings
☒ DHCP Relay settings
☒ DHCPv6 Relay settings
☒ WoL Server settings
☒ Static Route configuration
☒ Virtual IPs
☒ Traffic Shaper configuration
☒ Traffic Shaper Limiters configuration
☒ DNS Forwarder and DNS Resolver configurations
☒ Captive Portal

☒ Toggle All

Save

Voici les paramètres à rentrer dans le PfSense Backup.

System / [High Availability](#) Lib ?

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 LAN
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 d1702440
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 192.168.50.1
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 IP Address **!!! NE PAS REMPLIR !!!**
Enter the IP address of the remote system. Only 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 ***** ***** **!!! ENTRER LE MEME MOT DE PASSE QUE SUR LE PFSense MASTER !!!**
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 ☒ synchronize admin accounts and autoupdate sync password.
By default, the admin account does not synchronize, and each node may have a different admin password.
This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

Select options to sync

- ☒ User manager users and groups
- ☒ Authentication servers (e.g. LDAP, RADIUS)
- ☒ Certificate Authorities, Certificates, and Certificate Revocation Lists
- ☒ Firewall rules
- ☒ Firewall schedules
- ☒ Firewall aliases
- ☒ NAT configuration
- ☒ IPsec configuration
- ☒ OpenVPN configuration (Implies CA/Cert/CRL Sync)
- ☒ DHCP Server settings
- ☒ DHCP Relay settings
- ☒ DHCPv6 Relay settings
- ☒ WoL Server settings
- ☒ Static Route configuration
- ☒ Virtual IPs
- ☒ Traffic Shaper configuration
- ☒ Traffic Shaper Limiters configuration
- ☒ DNS Forwarder and DNS Resolver configurations
- ☒ Captive Portal

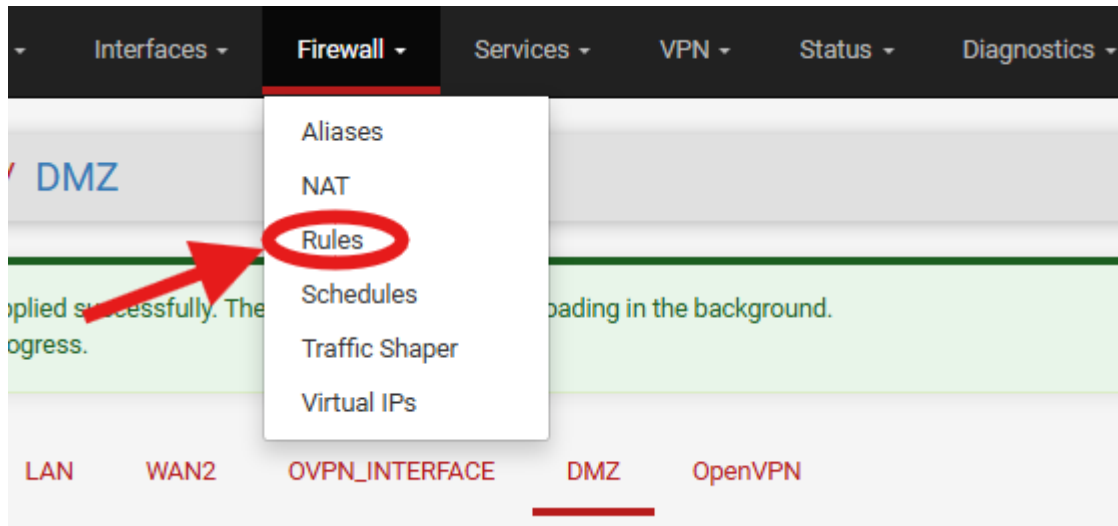
☒ [Toggle All](#)

[Save](#)

Cliquer sur Save pour valider les paramètres sur les deux PfSense. Une fois cela fait, les deux PfSense seront synchronisés.

Voici un test : Création d'une règle de pare-feu sur le PfSense Master qui va se répliquer sur le Backup.

Dans le PfSense Master, aller dans Firewall puis Rules.



Cliquer sur Add pour ajouter une nouvelle règle (pour l'exemple, création d'une règle dans le LAN ici).

Firewall / Rules / LAN

Floating WAN1 LAN WAN2 OVPN_INTERFACE DMZ OpenVPN

Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	18/639 KIB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
☐	2/44 KIB	IPv4 UDP	192.168.50.3	*	*	161 (SNMP)	*	none		PRTG	
☐	3/270 KIB	IPv4 *	*	*	*	*	*	none		PETIT POIX	
☐	0/0 B	IPv4 *	LAN net	*	*	*	WAN_FAILOVER	none		Default allow LAN to any rule	
☐	0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Descendre tout en bas, ajouter une description (Test dans l'exemple) et cliquer sur Save.

Extra Options

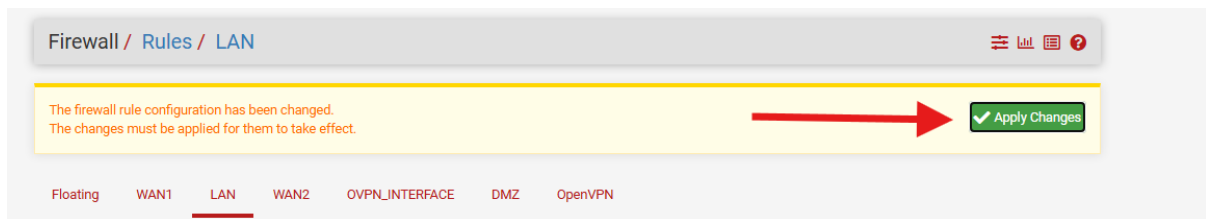
Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Log Settings](#) page)

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

[Save](#)

Cliquer sur Apply Changes.



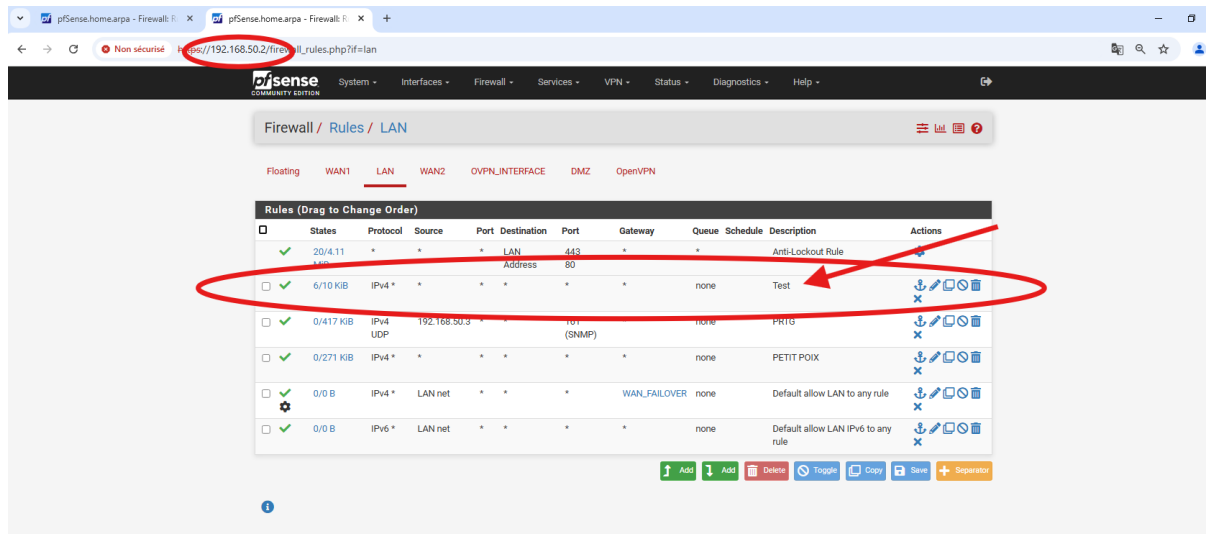
La nouvelle règle “Test” apparaît dans la liste des règles sur le LAN.

The screenshot shows the pfSense Firewall Rules configuration page for the LAN interface. A red circle highlights the 'Test' rule, and a red arrow points to its 'Actions' column.

Rules (Drag to Change Order)	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	✓	14/815 KIB	*	*	*	LAN Address	443	*	*	Anti-Lockout Rule	
☐	✓	0/0 B	IPv4 *	*	*	*	*	none		Test	
☐	✓	5/55 KIB	IPv4	UDP	164	(SNMP)	*	none			
☐	✓	3/351 KIB	IPv4 *	*	*	*	*	none		PETIT POIX	
☐	✓	0/0 B	IPv4 *	LAN net	*	*	WAN_FAILOVER	none		Default allow LAN to any rule	
☐	✓	0/0 B	IPv6 *	LAN net	*	*	*	none		Default allow LAN IPv6 to any rule	

Buttons: Add, Add, Delete, Toggle, Copy, Save, Separator

Si tout fonctionne, la règle apparaît aussi sur le PfSense Backup.



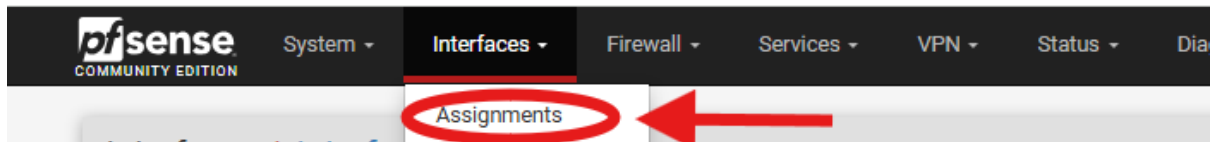
Vous pouvez ensuite supprimer la règle créée, c'était juste un exemple (elle va aussi se supprimer sur le PfSense Backup).

! ! Les règles appliquées sur le PfSense Master s'appliqueront aussi sur le Backup, mais cela ne marche pas inversement ! Seul le Pfsense Master peut influencer sur le Backup. ! !

C) CARP WAN

Pour cette partie, chaque PfSense devra disposer chacun de deux cartes WAN distinctes sur la même plage d'adresse. Dans mon cas, cette plage sera en 192.168.1.0.

Aller dans Interfaces puis Assignements.



Ici, en ayant ajouté une troisième carte réseau sur le PfSense Master avec les mêmes propriétés que celle déjà existante en WAN, nous pouvons voir que em2 est disponible à la configuration (il reste un assignement réseau à ajouter grâce à l'ajout de notre nouvelle carte réseau). Cet assignement sera le 2ème WAN.

Cliquer sur Add.



Une fois après avoir créé une nouvelle interface, celle-ci s'est automatiquement renommée en "OPT1".

Cliquer dessus pour modifier ses paramètres.

Interface	Network port	
WAN1	em0 (00:0c:29:43:e4:bb)	
LAN	em1 (00:0c:29:43:e4:c5)	Delete
OPT1	em2 (00:0c:29:43:e4:cf)	Delete

Cocher “Enable Interface”, renommer l’interface en “WAN2”, et changer la configuration IPv4 en DHCP (ou statique, même si l’adresse fourni en DHCP via PfSense ne changera jamais).

Interfaces / WAN2 (em2)   

General Configuration

Enable	☒ Enable interface
Description	WAN2 Enter a description (name) for the interface here.
IPv4 Configuration Type	DHCP 
IPv6 Configuration Type	None
MAC Address	xxxxxxxxxxxx This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxx:xxxx:xxxx or leave blank.
MTU	 If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	 If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) 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.

Descendre tout en bas et cliquer sur Save pour appliquer les changements sur l'interface.

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

Alias IPv4 address / 24 ▼
The value in this field is used as a fixed alias IPv4 address by the DHCP client.

Reject leases from
To have the DHCP client reject offers from specific DHCP servers, enter their IP addresses here (separate multiple entries with a comma). This is useful for rejecting leases from cable modems that offer private IP addresses when they lose upstream sync.

Reserved Networks

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

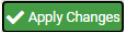
Block bogon networks ☐
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Cliquer sur Apply Changes.

Interfaces / WAN2 (em2) ≡ 📄 ?

The WAN2 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.

Voici la configuration qui apparaît sur le menu du routeur PfSense Master.

- WAN1 : 192.168.1.143
- WAN2 : 192.168.1.145

```
round-trip min/avg/max/stddev = 20.763/21.800/23.039/0.940 ms
Press ENTER to continue.
VMware Virtual Machine - Netgate Device ID: 7C-fdde2dc1537e67992
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***
WAN1 (wan)      -> em0      -> v4/DHCP4: 192.168.1.143/24
LAN (lan)       -> em1      -> v4: 192.168.50.1/24
WAN2 (opt1)     -> em2      -> v4/DHCP4: 192.168.1.145/24
OVPN_INTERFACE (opt2) -> ovpn1    ->
DMZ (opt3)      -> em3      -> v4: 192.168.200.251/24

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

Enter an option: █
```

Répéter le même processus sur le routeur Backup.

Voici la configuration qui apparaît sur le menu du routeur PfSense Backup.

- WAN1 : 192.168.1.144
- WAN2 : 192.168.1.146

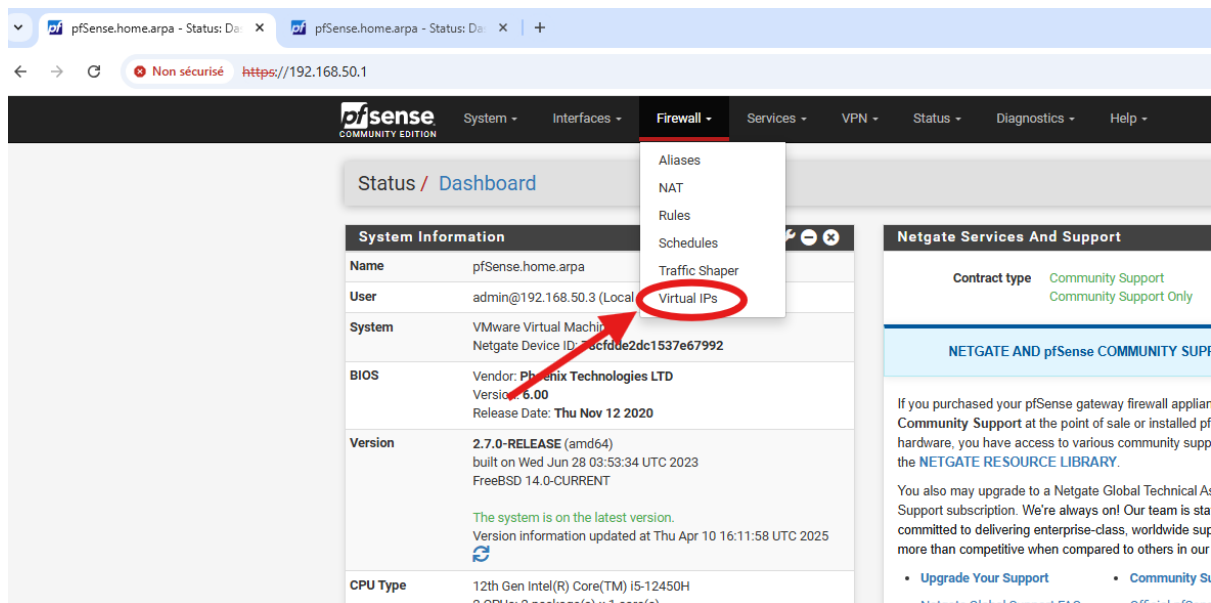
```
VMware Virtual Machine - Net4 - IP: c15e971628a2d1702440
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***
WAN1 (wan)      -> em0      -> v4/DHCP4: 192.168.1.144/24
LAN (lan)       -> em1      -> v4: 192.168.50.2/24
WAN2 (opt1)     -> em2      -> v4/DHCP4: 192.168.1.146/24
VPN_INTERFACE (opt2) -> ovpn1    ->
DMZ (opt3)      -> em3      -> v4: 192.168.200.252/24

0) Logout (SSH only)      9) priop
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

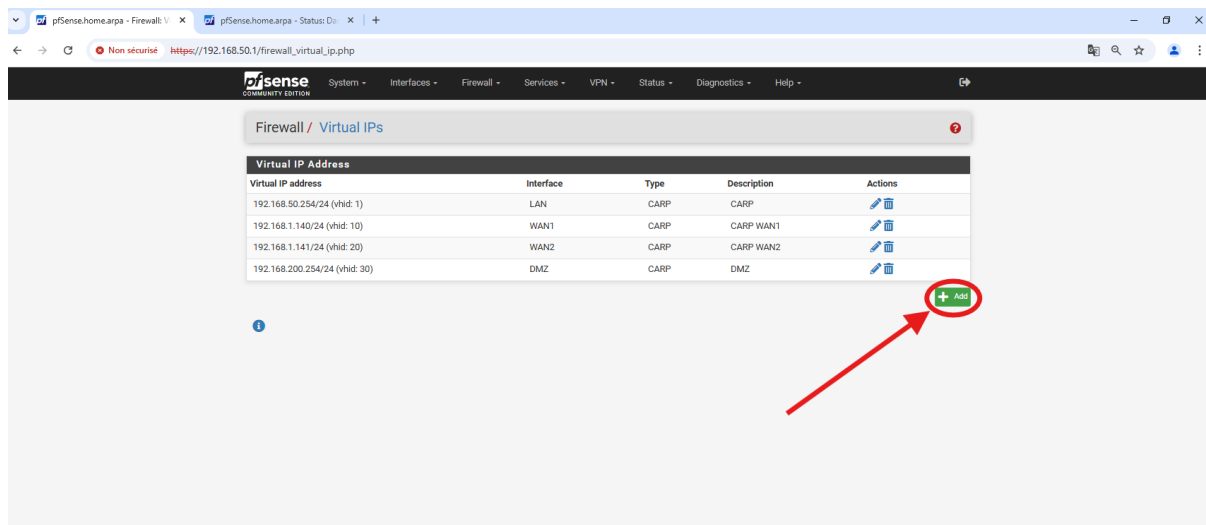
Enter an option: █
```

Nous allons maintenant créer 2 nouvelles IP virtuelles pour nos 2 CARP WAN.

Sur le PfSense Master, aller dans Firewall puis Virtual IPs.



Cliquer sur le bouton Add.



Voici, dans mon cas, les paramètres à entrer (à adapter en fonction de la plage d'adresse IP du WAN).

Il ne faut pas remettre le même VHID Group sur l'IP virtuelle LAN (j'ai mis 10 ici).

Une fois les paramètres remplis, cliquer sur Save.

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type ☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface WAN1

Address type Single address

Address(es) 192.168.1.140 / 24
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password
Enter the VHID group password.
Confirm

VHID Group 10
Enter the VHID group that the machines will share.

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 CARP WAN1
A description may be entered here for administrative reference (not parsed).

Save

Refaire la manipulation en créant une nouvelle IP virtuelle pour les 2ème WAN, tout en inscrivant un autre VHID Group comme pour le première IP virtuelle WAN (j'ai mis 20 ici).

Voici, dans mon cas, les paramètres à entrer.

Une fois les paramètres remplis, cliquer sur Save.

Firewall / Virtual IPs / Edit ?

Edit Virtual IP

Type

☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface

WAN2

Address type

Single address

Address(es)

192.168.1.141

/ 24

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password

Enter the VHID group password.

Confirm

VHID Group

20

Enter the VHID group that the machines will share.

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

CARP WAN2

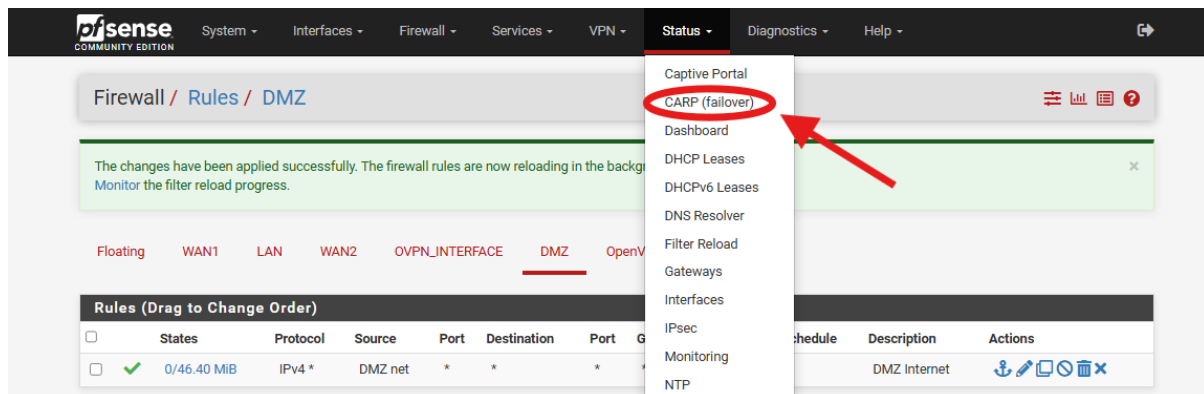
A description may be entered here for administrative reference (not parsed).

Save

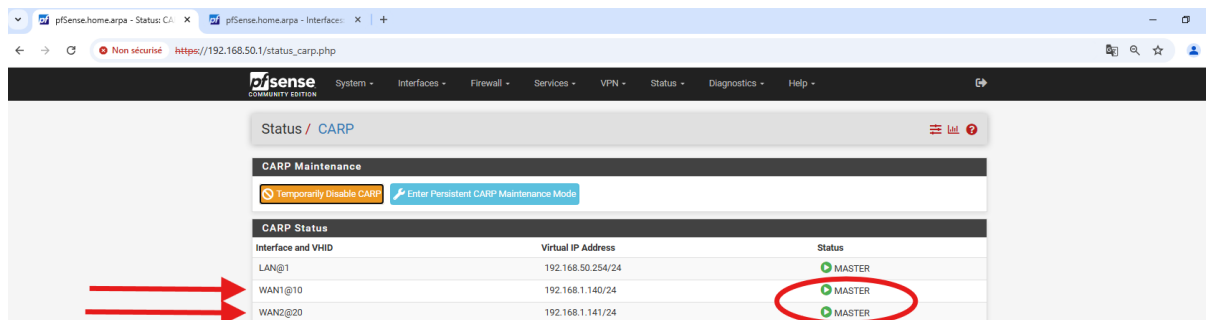
i

Cette opération n'est pas effectuée sur le Backup, grâce au High Availability, les paramètres se sont déjà répliqués.

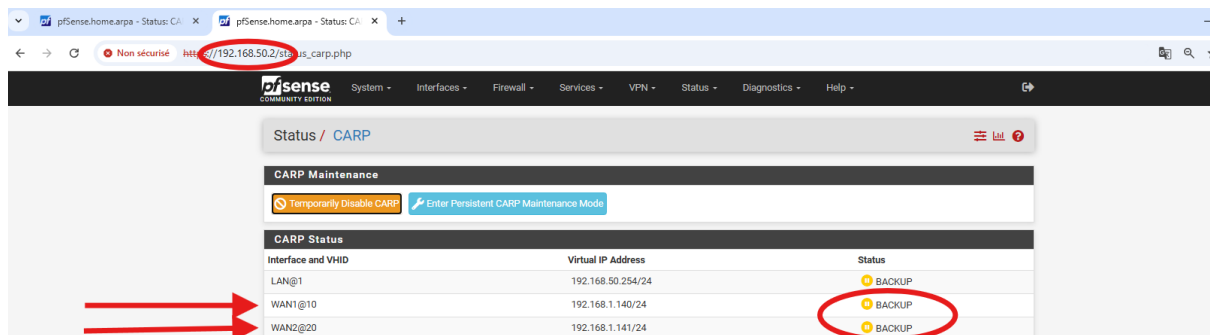
Sur le PfSense Master, retourner ensuite dans Status puis CARP (failover).



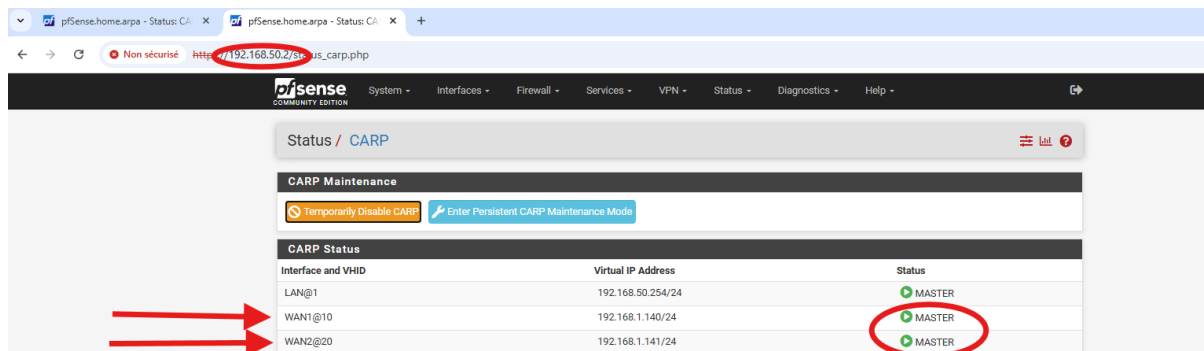
Les 2 CARP WAN sont bien présents en MASTER sur le PfSense Master.



Sur le PfSense Backup, les CARP WAN sont aussi présents mais en Backup.

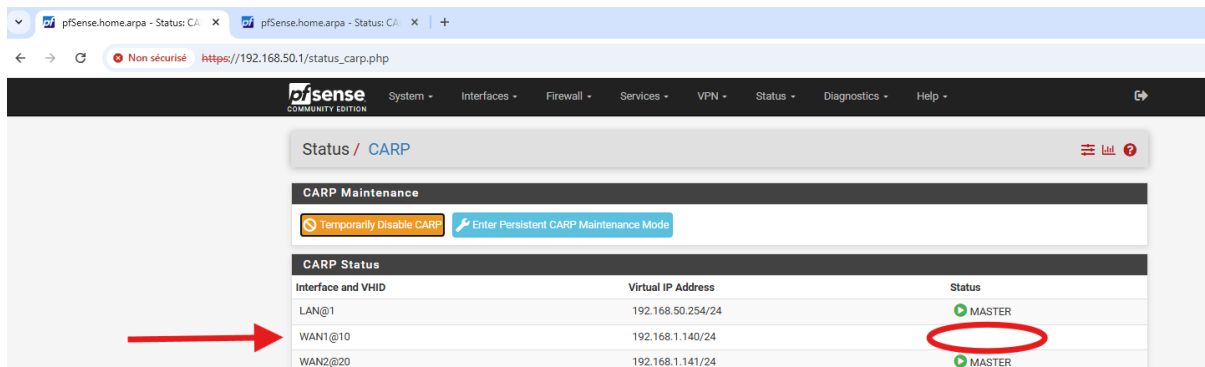


Si le routeur Master est en panne, le routeur Backup prend bien le relais.

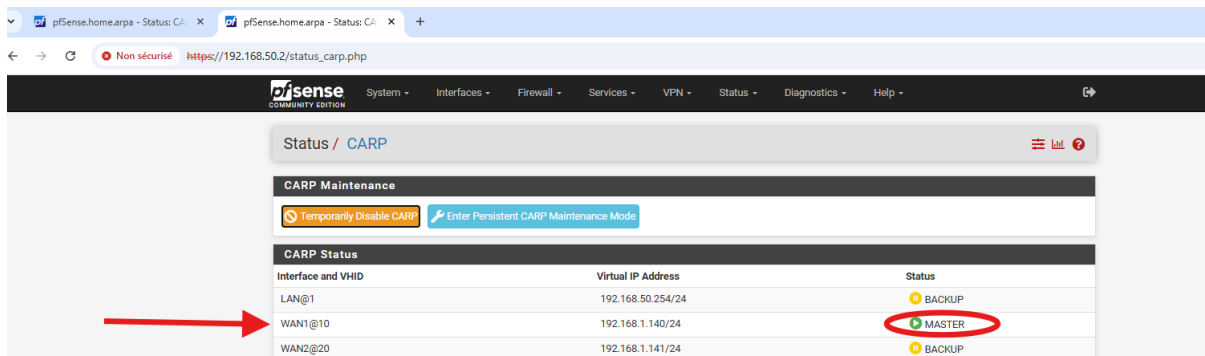


De même si l'on désactive une interface sur le PfSense Master (WAN1 ici), dans CARP (failover) WAN1 sera bien évidemment inactif sur le PfSense Master, et le WAN1 sur le PfSense Backup passera en MASTER.

- PfSense Master :



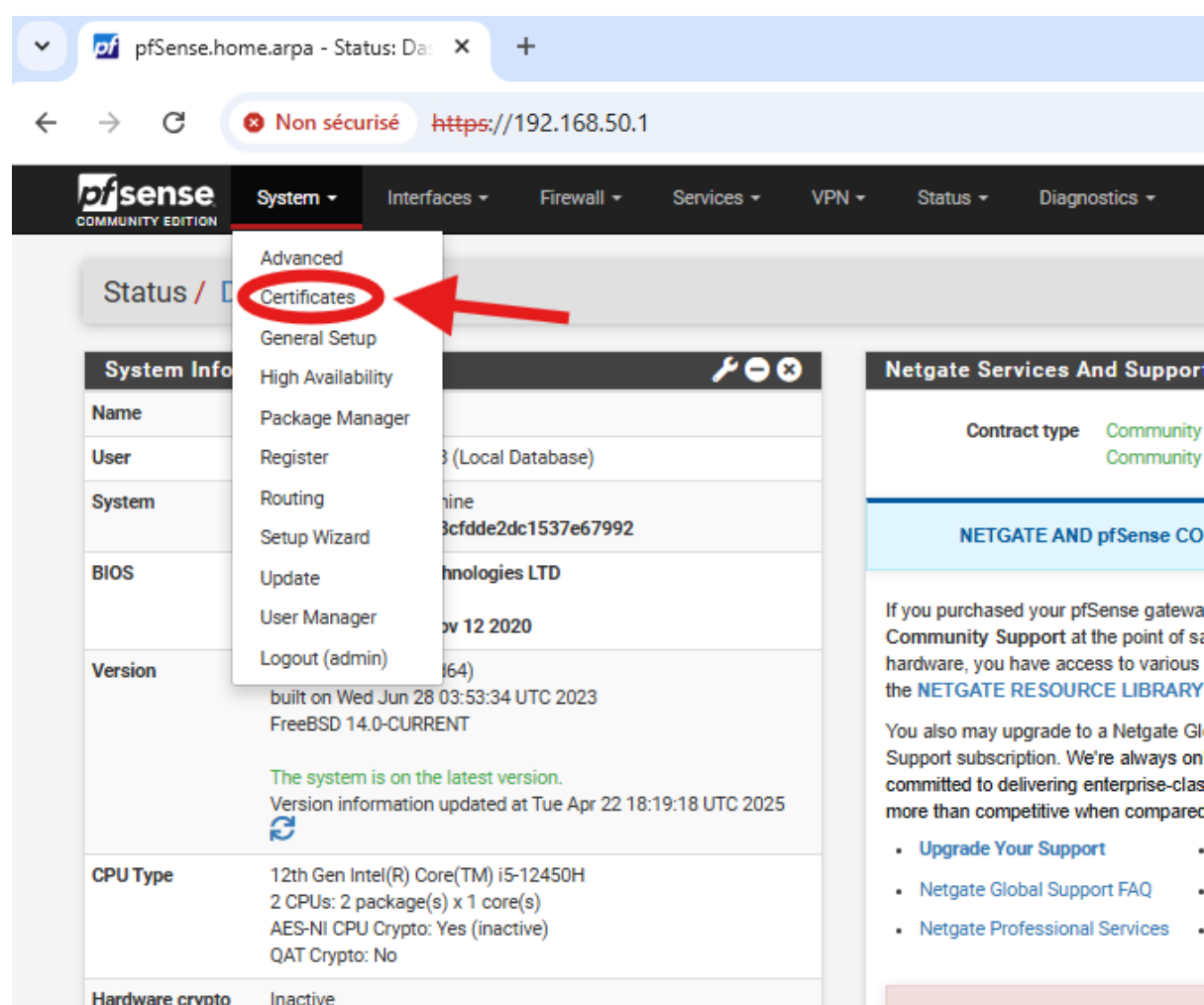
- PfSense Backup :



3) OpenVPN RW

! ! Cette partie est à réaliser seulement après avoir configuré ADDS sur le serveur Windows (voir doc associé) ! !

Il reste à configurer le VPN OpenVPN RW pour les clients distants. Premièrement, aller dans System puis Certificates.



Dans la partie Authorities, cliquer sur Add pour rajouter un certificat d'autorité.

System / Certificate / Authorities

Authorities Certificates Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
Openvpn_CA	✓	self-signed	1	CN=Openvpn_CA Valid From: Tue, 15 Apr 2025 07:10:05 +0000 Valid Until: Fri, 13 Apr 2035 07:10:05 +0000		

Add

Rentrer les mêmes paramètres et cliquer sur Save.

Create / Edit CA

Descriptive name

Openvpn_CA

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.

Method

Create an internal Certificate Authority

Trust Store

☒ Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial

☐ Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

Key type

RSA

1024

The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm

sha256

The digest method used when the CA is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

Lifetime (days)

Common Name

Openvpn_CA

The following certificate authority subject components are optional and may be left blank.

Country Code

None

State or Province

e.g. Texas

City

e.g. Austin

Organization

e.g. My Company Inc

Organizational Unit

e.g. My Department Name (optional)

Save

Aller ensuite dans Certificates puis cliquer sur Add/Sign pour ajouter un certificat.

Documentation situation professionnelle 2

68 sur 247

System / Certificates / Certificates

Authorities **Certificates** Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (67d58186ab106) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-67d58186ab106 Valid From: Sat, 15 Mar 2025 13:32:54 +0000 Valid Until: Fri, 17 Apr 2026 13:32:54 +0000	webConfigurator	
Cert Server Certificate CA: No Server: Yes	self-signed	CN=Cert Valid From: Sat, 15 Mar 2025 14:06:10 +0000 Valid Until: Fri, 17 Apr 2026 14:06:10 +0000		
OpenVPN_Server Server Certificate CA: No Server: Yes	external	CN=OpenVPN_Server Valid From: Mon, 17 Mar 2025 07:56:59 +0000 Valid Until: Thu, 15 Mar 2035 07:56:59 +0000		
test User Certificate CA: No Server: No	external	CN=Internal-CA Valid From: Thu, 20 Mar 2025 10:21:12 +0000 Valid Until: Sun, 18 Mar 2035 10:21:12 +0000	User Cert	
Openvpn_Cert Server Certificate CA: No Server: Yes	Openvpn_CA	CN=Openvpn_Cert Valid From: Tue, 15 Apr 2025 07:14:19 +0000 Valid Until: Wed, 15 Apr 2026 07:14:19 +0000	OpenVPN Server	

Rentrer ensuite ces paramètres.

Dans Certificate Authorities, sélectionner l'autorité de certificat créée avant (OpenVPN_CA).

System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an Internal Certificate

Descriptive name Openvpn_Cert
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: `~,~,~,~,~,~,~,~`

Internal Certificate

Certificate authority Openvpn_CA

Key type RSA

2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm sha256
The digest method used when the certificate is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days) 3650
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name e.g. www.example.com

Internal Certificate

Certificate authority Openvpn_CA

Key type RSA

2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm sha256
The digest method used when the certificate is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days) 365 1
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name e.g. www.example.com

The following certificate subject components are optional and may be left blank.

Country Code None

State or Province e.g. Texas

City e.g. Austin

Organization e.g. My Company Inc.

Organizational Unit e.g. My Department Name (optional)

Veiller à bien choisir Server Certificate et cliquer sur Save.

Certificate Attributes

Attribute Notes
The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.
For Internal Certificates, these attributes are added directly to the certificate as shown.

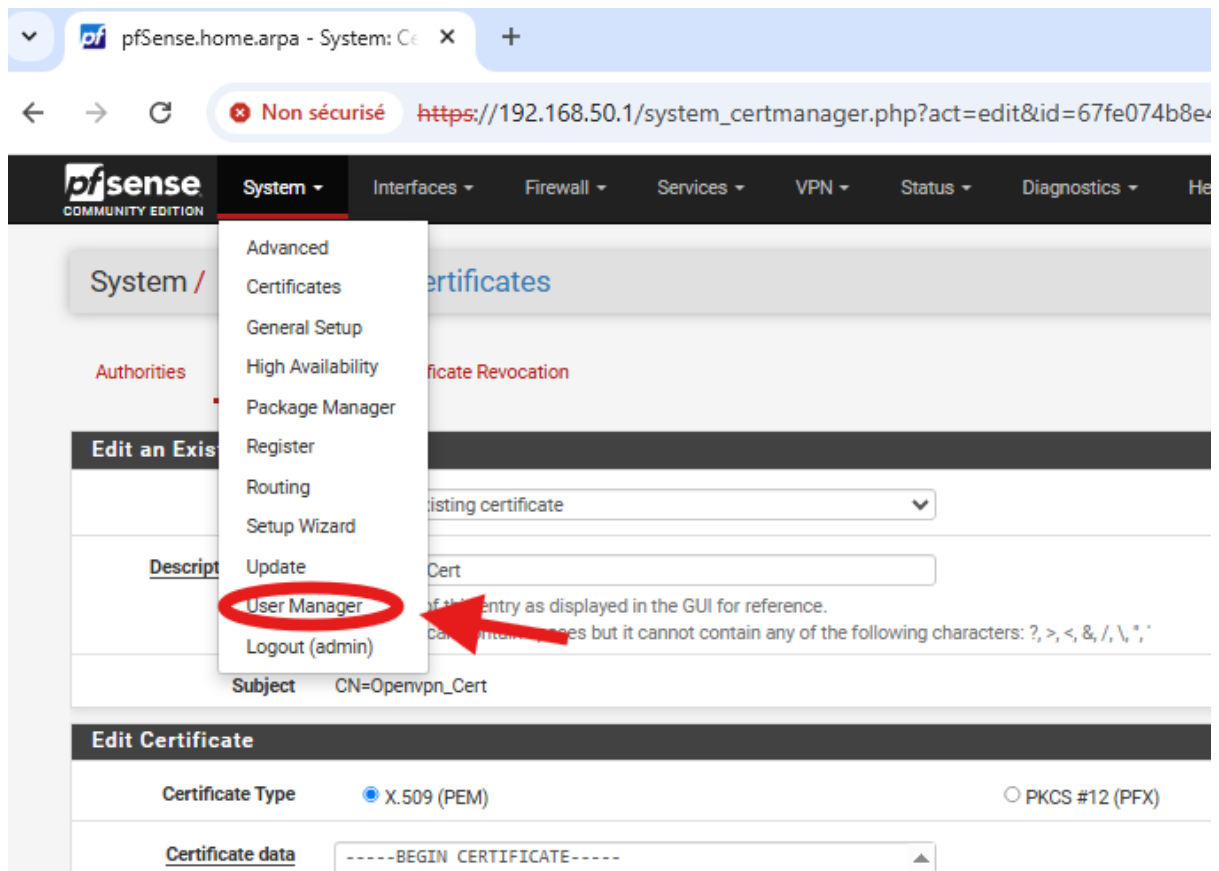
Certificate Type
Server Certificate

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 as an Alternative Name. The signing CA may ignore or change these values.

Add SAN Row
+ Add SAN Row

Save

Aller ensuite dans System puis User Manager.



Aller dans Authentification Servers et cliquer sur Add.

System / User Manager / Authentication Servers ?

Users Groups Settings **Authentication Servers**

Authentication Servers			
Server Name	Type	Host Name	Actions
Active Directory	LDAP	192.168.50.3	  
Local Database		pfSense	

 + Add

Entrer ces paramètres.

System / User Manager / Authentication Servers / Edit

Users Groups Settings Authentication Servers

Server Settings

Descriptive name Active Directory

Type LDAP

LDAP Server Settings

Hostname or IP address 192.168.50.3
NOTE: When using SSL/TLS or STARTTLS, this hostname must match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.

Port value 389

Transport Standard TCP

Peer Certificate Authority Openvpn_CA
This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.

Protocol version 3

Server Timeout 25
Timeout for LDAP operations (seconds)

Search scope Level
Entire Subtree

Base DN DC=securitecivile,DC=local

Authentication containers OU=Utilisateurs,DC=securitecivile,DC=local
Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component.
Example: CN=users,dc=example,dc=com or OU=Staff,OU=Freelancers

[Select a container](#)

Adresse IP du Serveur Windows avec ADDS (contrôleur de domaine)

Une fois les paramètres rentrés, cliquer sur Save.

Extended query ☐ Enable extended query

Bind anonymous ☐ Use anonymous binds to resolve distinguished names

Bind credentials

User naming attribute

Group naming attribute

Group member attribute

RFC 2307 Groups ☐ LDAP Server uses RFC 2307 style group membership
RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).

Group Object Class
Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".

Shell Authentication Group DN
If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login.
Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com

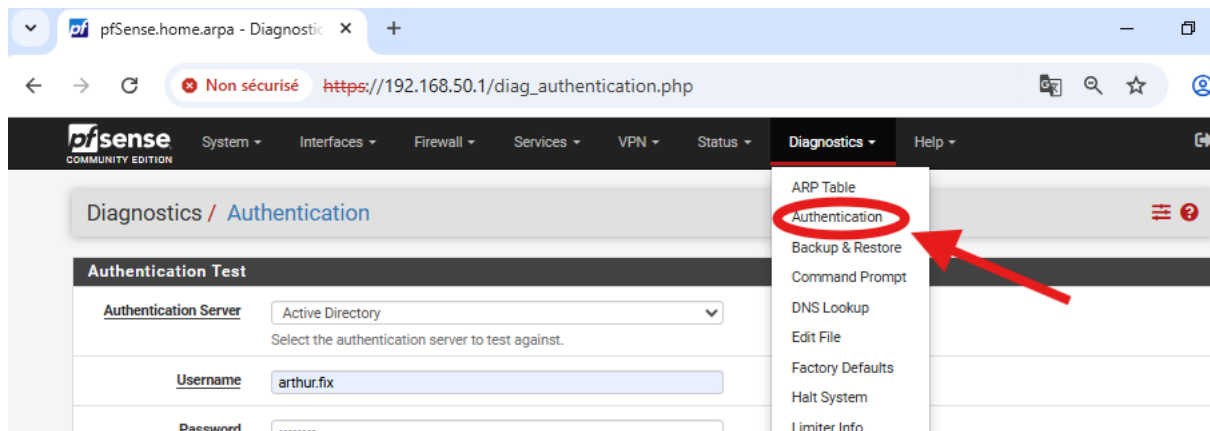
UTF8 Encode ☐ UTF8 encode LDAP parameters before sending them to the server.
Required to support international characters, but may not be supported by every LDAP server.

Username Alterations ☐ Do not strip away parts of the username after the @ symbol
e.g. user@host becomes user when unchecked.

Allow unauthenticated bind ☐ Allow unauthenticated bind
Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.

 Save

Pour tester si la connexion d'un utilisateur du domaine au PfSense fonctionne, aller dans Diagnostics puis Authentification.



Sélectionner le serveur Active Directory, rentrer les identifiants d'un utilisateur du domaine et cliquer sur Test.

Diagnostics / Authentication  

Authentication Test

Authentication Server	Active Directory 
Select the authentication server to test against.	
Username	arthur.fix
Password	*****
Debug	☐ Set debug flag Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).

Si ce message s'affiche, alors la configuration est correcte.

Diagnostics / Authentication  

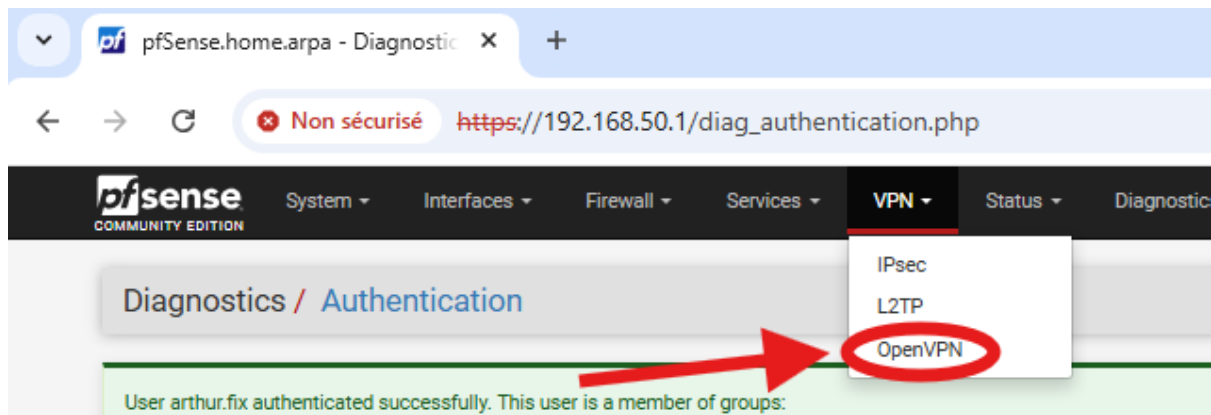
User arthur.fix authenticated successfully. This user is a member of groups:

Authentication Test

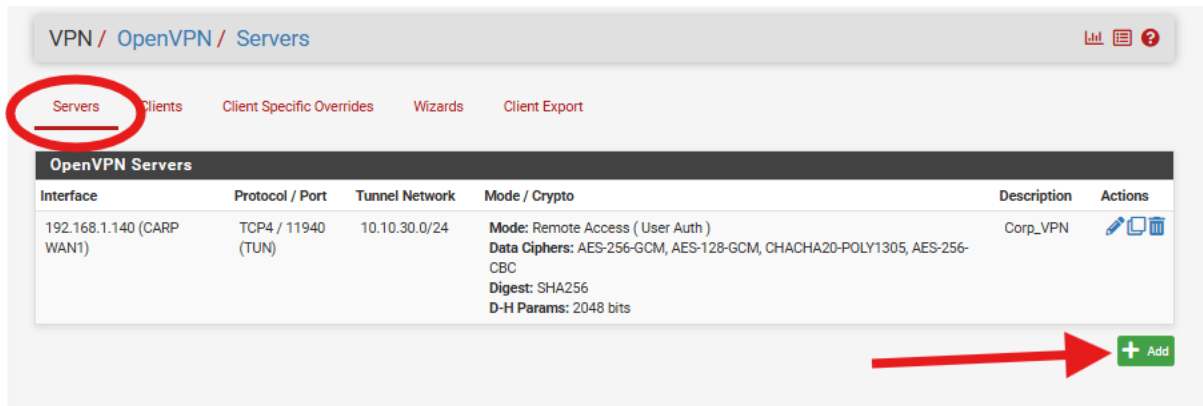
Authentication Server	Active Directory 
Select the authentication server to test against.	
Username	arthur.fix
Password	*****
Debug	☐ Set debug flag Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).

 Test

Aller dans VPN puis OpenVPN.



Dans la section Servers, cliquer sur Add.



VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards Client Export

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
192.168.1.140 (CARP WAN1)	TCP4 / 11940 (TUN)	10.10.30.0/24	Mode: Remote Access (User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	Corp_VPN	  

+ Add

Voici la configuration à rentrer.

VPN / OpenVPN / Servers / Edit

Servers

Clients

Client Specific Overrides

Wizards

Client Export

General Information

Description

corp_VPN

A description of this VPN for administrative reference.

Disabled

☐ Disable this server

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

Unique VPN ID

Server 1 (ovpn1)

Mode Configuration

Server mode

Remote Access (User Auth)

Backend for authentication

Active Directory

Local Database

Device mode

tun - Layer 3 Tunnel Mode

"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Endpoint Configuration

Protocol

TCP on IPv4 only

Interface

192.168.1.140 (CARP WAN1)

The interface or Virtual IP address where OpenVPN will receive client connections.

Local port

11940

The port used by OpenVPN to receive client connections.

Cryptographic Settings

TLS Configuration

☒ Use a TLS Key

A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

TLS Key

2048 bit OpenVPN static key

-----BEGIN OpenVPN Static key v1-----
cd3b30b8e159236a1bf515896bcac3c

Paste the TLS key here.
This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.

TLS Key Usage Mode

TLS Authentication

In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.

TLS keydir direction

Use default direction

The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.

Peer Certificate Authority

Openvpn_CA

Peer Certificate Revocation list

No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

OCSP Check

☐ Check client certificates with OCSP

Server certificate

Openvpn_Cert (Server: Yes, CA: Openvpn_CA, In Use)

DH Parameter Length

2048 bit

Diffie-Hellman (DH) parameter set used for key exchange. ⓘ

ECDH Curve

Use Default

The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

Data Encryption Algorithms

AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-OFB (128 bit key, 128 bit block)
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)

AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305

Fallback Data Encryption Algorithm	AES-256-CBC (256 bit key, 128 bit block) ▼
The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.	
Auth digest algorithm	SHA256 (256-bit) ▼
The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present. When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel. The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.	
Hardware Crypto	No Hardware Crypto Acceleration ▼
Certificate Depth	One (Client+Server) ▼
When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.	
Client Certificate Key Usage Validation	☒ Enforce key usage Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").
Tunnel Settings	
IPv4 Tunnel Network	10.10.30.0/24 This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients. A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.
IPv6 Tunnel Network	 This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
Redirect IPv4 Gateway	☐ Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	☐ Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)	192.168.50.254/24 IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. 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.
IPv6 Local network(s)	 IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. 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.
Concurrent connections	100

Allow Compression	Decompress incoming, do not compress outgoing (Asymmetric) ▼
Allow compression to be used with this VPN instance. Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack. Asymmetric compression allows an easier transition when connecting with older peers.	
Compression	Adaptive LZO Compression [Legacy style, comp-lzo adaptive] ▼
Deprecated. Compress tunnel packets using the LZO algorithm. Compression can potentially dangerous and insecure. See the note on the Allow Compression option above. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.	
Push Compression	☐ Push the selected Compression setting to connecting clients.
Type-of-Service	☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-client communication	☒ Allow communication between clients connected to this server
Duplicate Connection	☐ Allow multiple concurrent connections from the same user When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session. Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.
Client Settings	
Dynamic IP	☒ Allow connected clients to retain their connections if their IP address changes.
Topology	Subnet – One IP address per client in a common subnet ▼ 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".
Ping settings	
Inactive	300 Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device. Activity is based on the last incoming or outgoing tunnel packet. A value of 0 disables this feature. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.
Ping method	keepalive – Use keepalive helper to define ping configuration ▼ keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows: ping = interval

Interval	10
Timeout	60

Advanced Client Settings

DNS Default Domain	☒ Provide a default domain name to clients
DNS Default Domain	securitecivile.local
DNS Server enable	☒ Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	192.168.50.3
DNS Server 2	
DNS Server 3	
DNS Server 4	
Block Outside DNS	☐ Make Windows 10 Clients 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.
Force DNS cache update	☐ Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.
NTP Server enable	☐ Provide an NTP server list to clients
NetBIOS enable	☒ Enable NetBIOS over TCP/IP If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
Node Type	none Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast)
Scope ID	 A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID
WINS server enable	☐ Provide a WINS server list to clients

Une fois la configuration terminée, cliquer sur Save.

Advanced Configuration

Custom options

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
EXAMPLE: push "route 10.0.0.0 255.255.255.0"

Username as Common Name

☒ Use the authenticated client username instead of the certificate common name (CN).
When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate common name for purposes such as determining Client Specific Overrides.

Send/Receive Buffer

Default

Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.

Gateway creation

☐ Both ☒ IPv4 only ☐ IPv6 only

If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.

Verbosity level

default

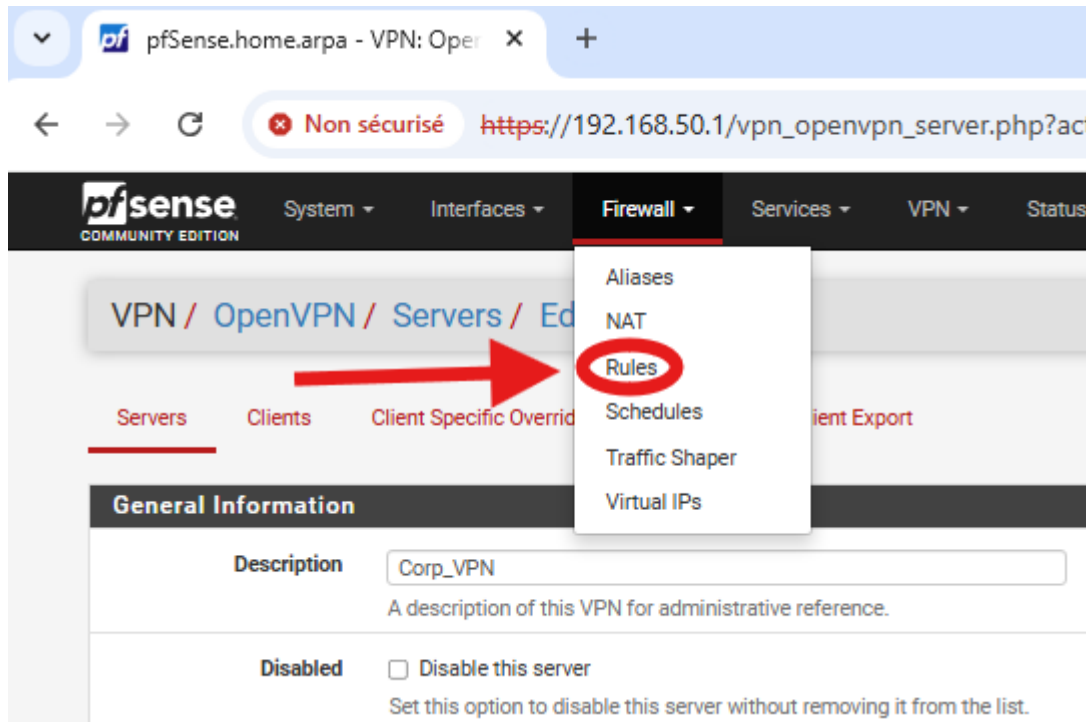
Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.

None: Only fatal errors
Default through 4: Normal usage range
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
6-11: Debug info range

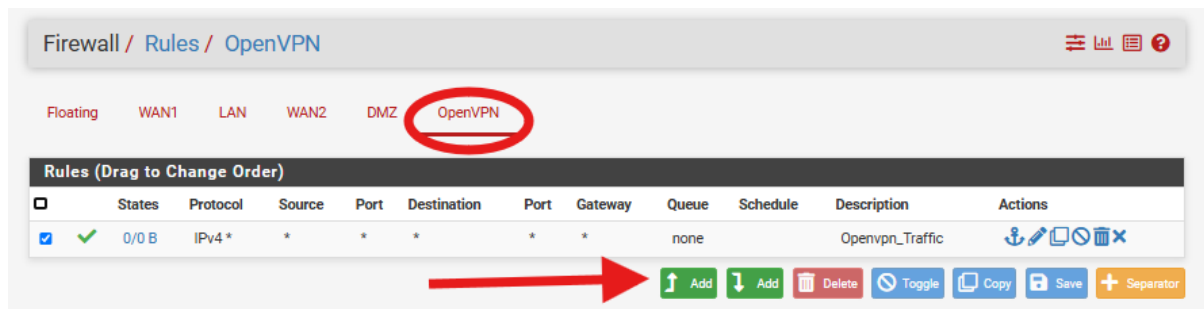
Save

Il faut maintenant créer des règles afin que les clients à distance puissent se connecter via OpenVPN.

Aller dans Firewall puis Rules.



Aller dans la section OpenVPN puis cliquer sur Add pour ajouter une nouvelle règle.



Sélectionner Pass pour Action, IPv4 pour la famille d'adresse, et Any pour Protocol.

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

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

OpenVPN

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

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

any

Source Address

/

Destination

Destination

☐ Invert match

any

Destination Address

/

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Openvpn_Traffic

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Ajouter une description à la règle et cliquer sur Save.

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Openvpn_Traffic

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Rule Information

Tracking ID	1744702773
Created	4/15/25 07:39:33 by admin@192.168.50.3 (Local Database)
Updated	4/15/25 07:39:33 by admin@192.168.50.3 (Local Database)

Save

Cliquer sur Apply Changes.

Firewall / Rules / OpenVPN

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

Apply Changes

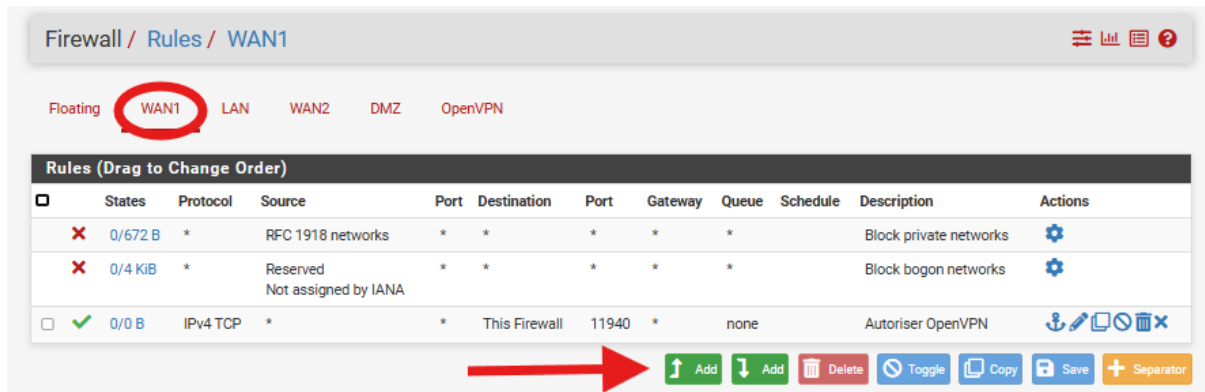
Floating WAN1 LAN WAN2 DMZ OpenVPN

Rules (Drag to Change Order)

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

 Add  Add  Delete  Toggle  Copy  Save  Separator

Aller ensuite sur l'interface WAN principale (WAN1) toujours dans les Rules. Cliquer sur Add pour ajouter une nouvelle règle.



Firewall / Rules / WAN1

Floating **WAN1** LAN WAN2 DMZ OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0/672 B	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	⚙️
✗ 0/4 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	⚙️
☐ ✓ 0/0 B	IPv4 TCP	*	*	This Firewall	11940	*	none		Autoriser OpenVPN	🔗 📄 🔄 🗑️

➡ Add ↓ Add 🗑️ Delete 🔄 Toggle 📄 Copy 💾 Save ➕ Separator

Choisir Pass en Action, IPv4 pour la famille d'adresse, TCP pour Protocol, et plus bas dans la section Destination, choisir le port 11940 pour le port de destination (celui que l'on a configuré et choisi avant dans la configuration de OpenVPN).

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
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 WAN1
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match any Source Address /
[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 This firewall (self) Destination Address /
Destination Port Range (other) 11940 (other) 11940
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [System Setup](#) page).

Ajouter une description et cliquer sur Save.

Extra Options

Log

☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Autoriser OpenVPN
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Rule Information

Tracking ID	1742198848
Created	3/17/25 08:07:28 by admin@192.168.50.10 (Local Database)
Updated	4/15/25 07:40:46 by admin@192.168.50.3 (Local Database)

Save

Cliquer sur Apply Changes.

Firewall / Rules / OpenVPN

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

Apply Changes

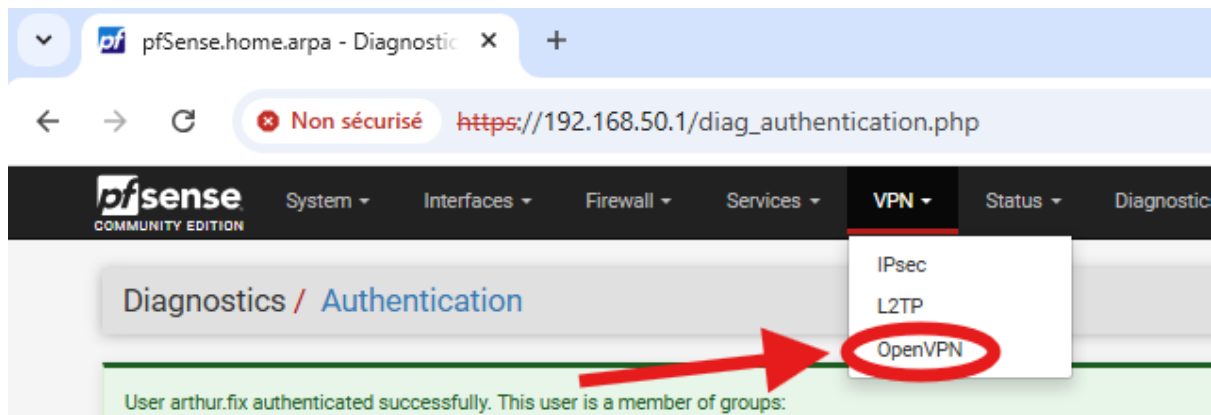
Floating WAN1 LAN WAN2 DMZ OpenVPN

Rules (Drag to Change Order)

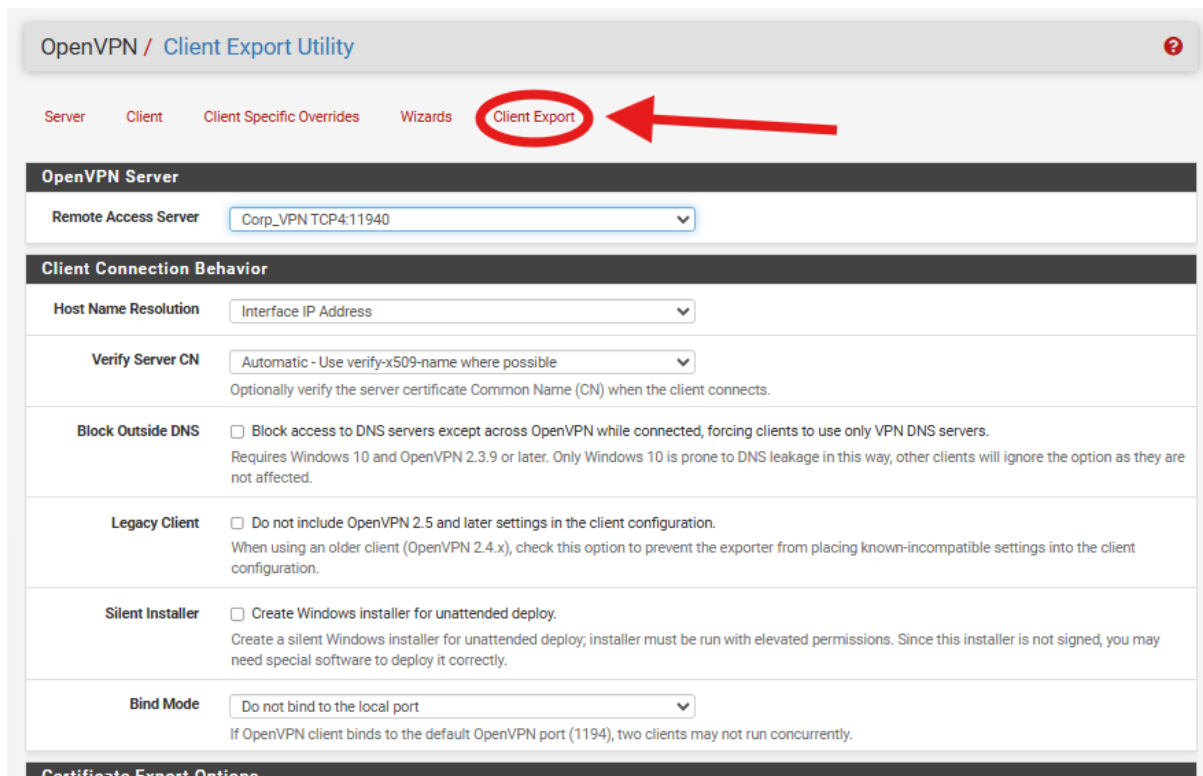
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0/0 B	IPv4 *	*	*	*	*	none		Openvpn_Traffic	    

 Add  Add  Delete  Toggle  Copy  Save  Separator

Retourner ensuite dans OpenVPN depuis la section VPN.



Aller sur Client Export.



OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards **Client Export**

OpenVPN Server

Remote Access Server Corp_VPN TCP4:11940

Client Connection Behavior

Host Name Resolution Interface IP Address

Verify Server CN Automatic - Use verify-x509-name where possible
Optionally verify the server certificate Common Name (CN) when the client connects.

Block 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.

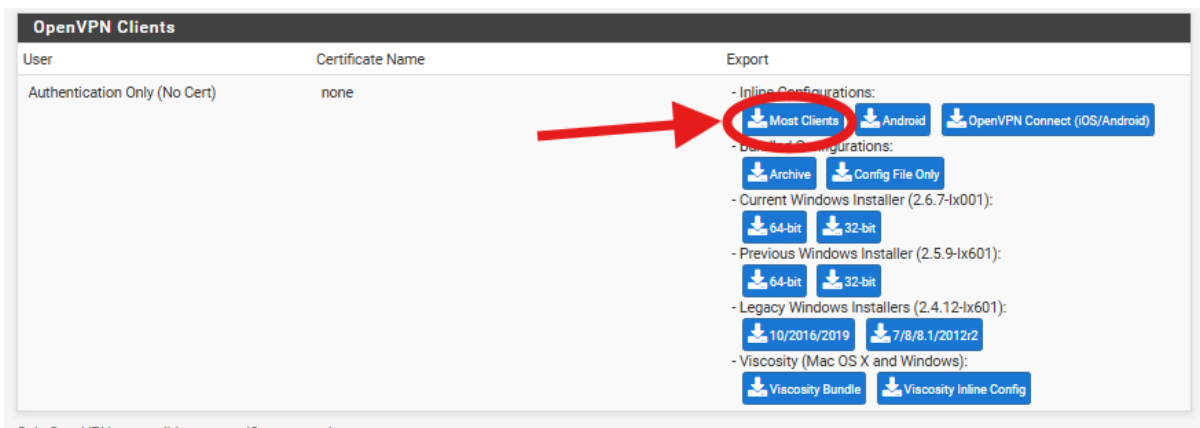
Legacy Client ☐ Do not include OpenVPN 2.5 and later settings in the client configuration.
When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.

Silent Installer ☐ Create Windows installer for unattended deploy.
Create a silent Windows installer for unattended deploy, installer must be run with elevated permissions. Since this installer is not signed, you may need special software to deploy it correctly.

Bind Mode Do not bind to the local port
If OpenVPN client binds to the default OpenVPN port (1194), two clients may not run concurrently.

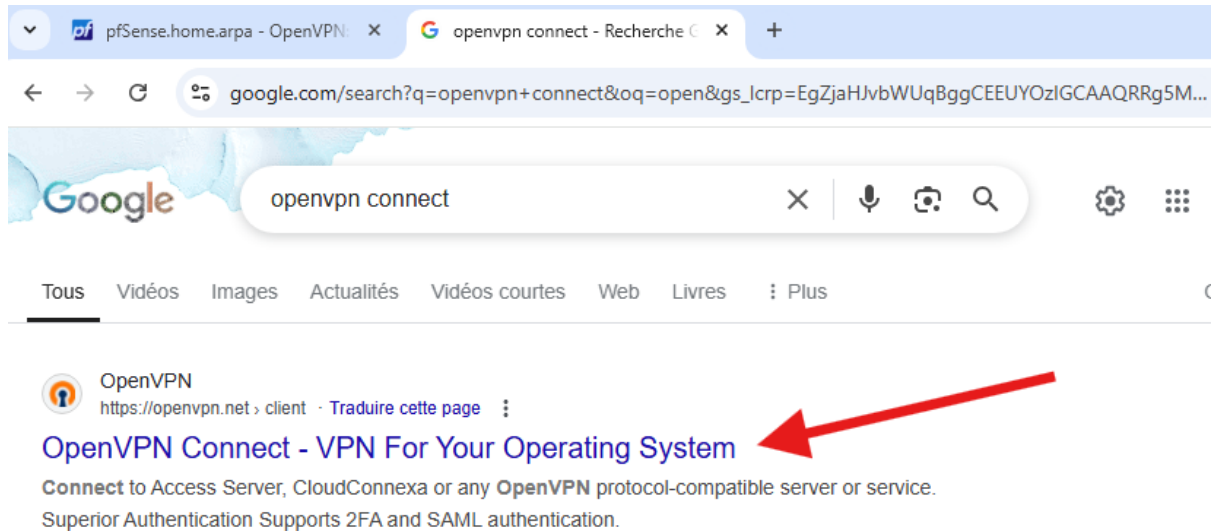
Certificate Export Options

Il n'y a aucun paramètre à changer, aller tout en bas et sélectionner Most Clients pour installer le fichier de configuration de OpenVPN.

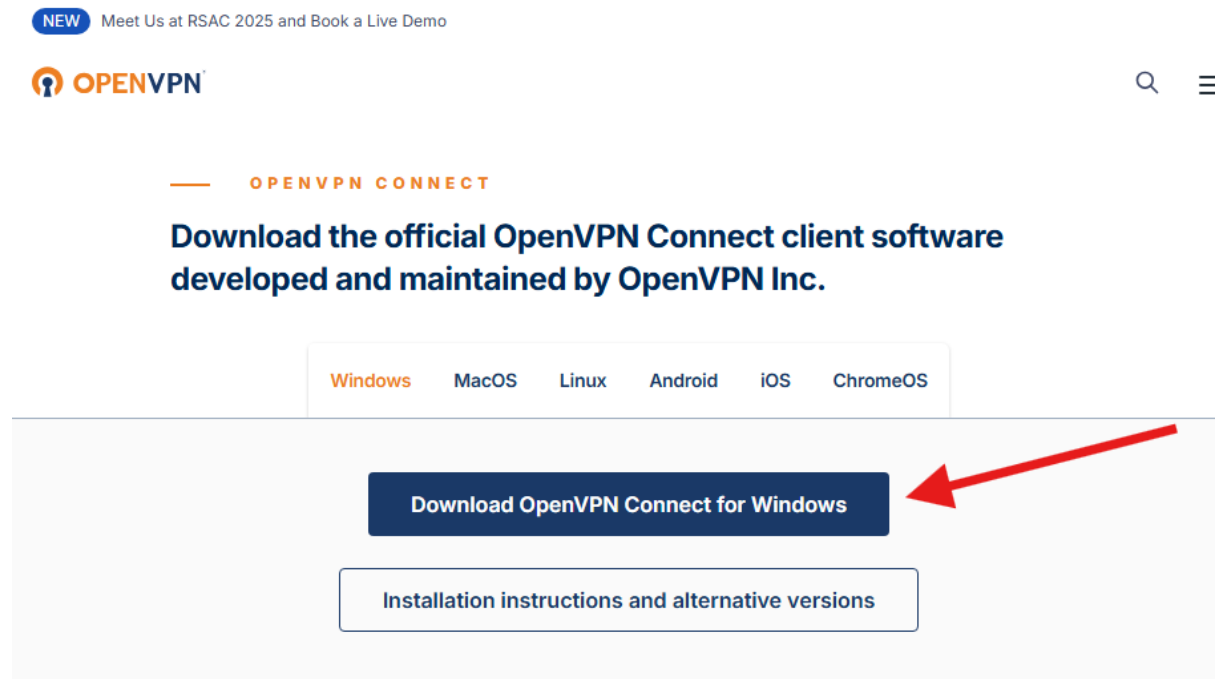


Il faut maintenant installer le client OpenVPN Connect pour tester si OpenVPN fonctionne (le client sera aussi à installer et à configurer sur les postes clients).

Sur le navigateur de recherche, rechercher openvpn connect et cliquer sur le premier lien.



Cliquer sur le bouton d'installation.



Une fois l'installation terminée, ouvrir l'installer et suivre les étapes d'installation.

Historique des téléchargements récents ✕



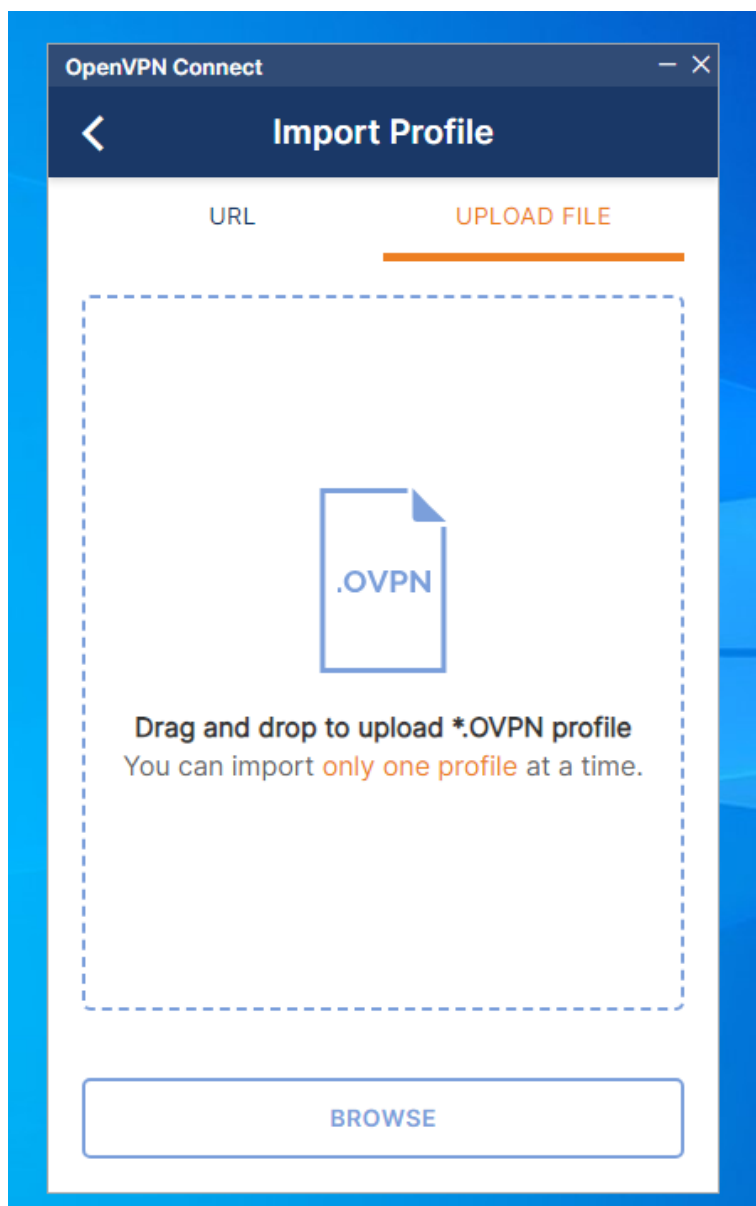
openvpn-connect-3.6.0.4074_signed (1).msi

↓ 51,6/98,2 Mo • 12 secondes restantes

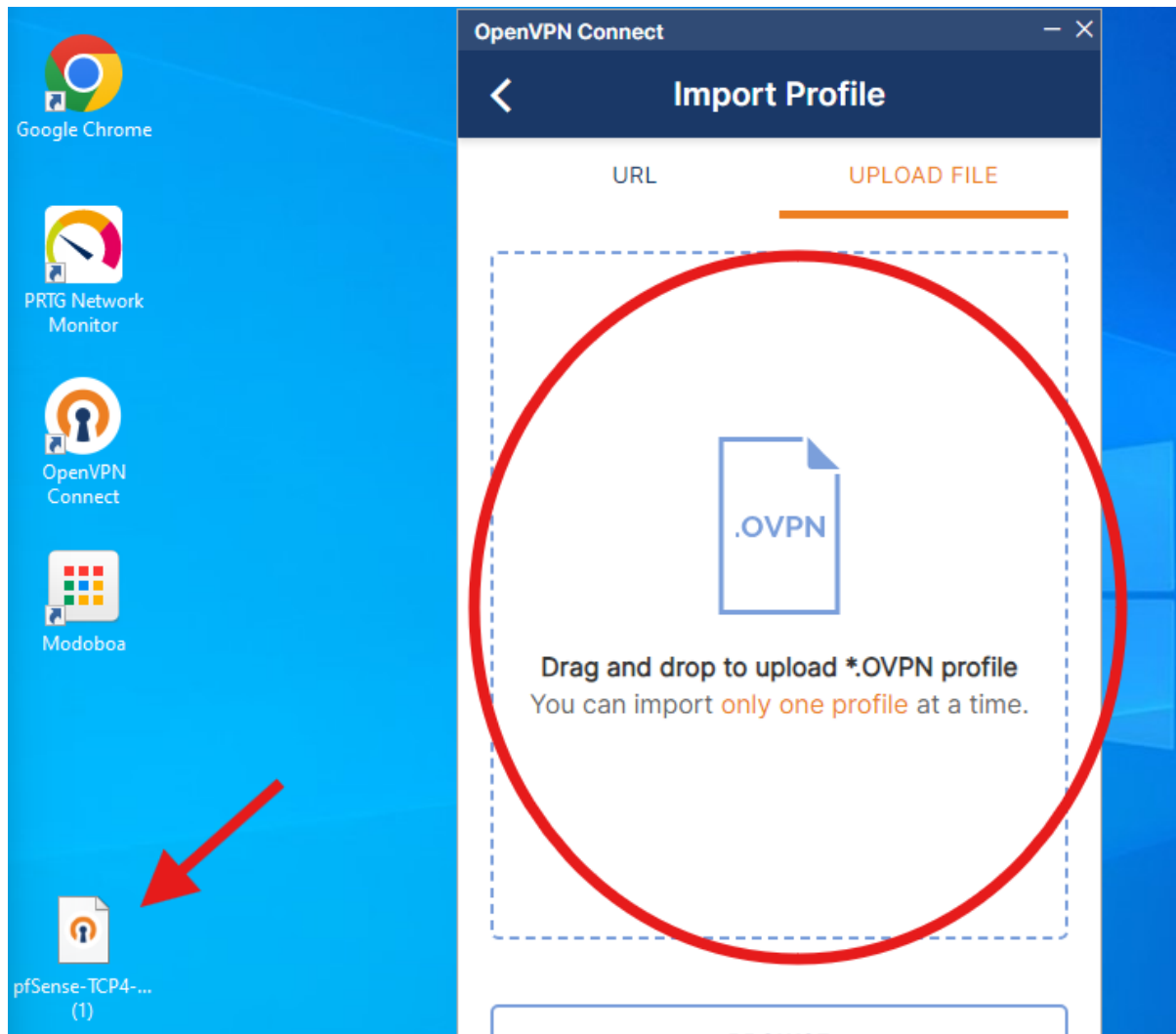
Historique complet des téléchargements



Ouvrir OpenVPN Connect.



Sélectionner le fichier de configuration de OpenVPN installé avant (se trouve sur mon bureau) et le glisser dans la zone d'upload de fichier de configuration sur OpenVPN Connect.



Entrer les paramètres suivants. Choisir 192.168.1.140 pour Server Hostname et utiliser les identifiants d'un utilisateur de l'AD pour se connecter.

A la fin de la configuration, cliquer sur Save en haut à droite.

OpenVPN Connect — ×

Edit Profile Save

Profile Name
Corp_VPN

Server Hostname (locked)
192.168.1.140

Server Override (optional)

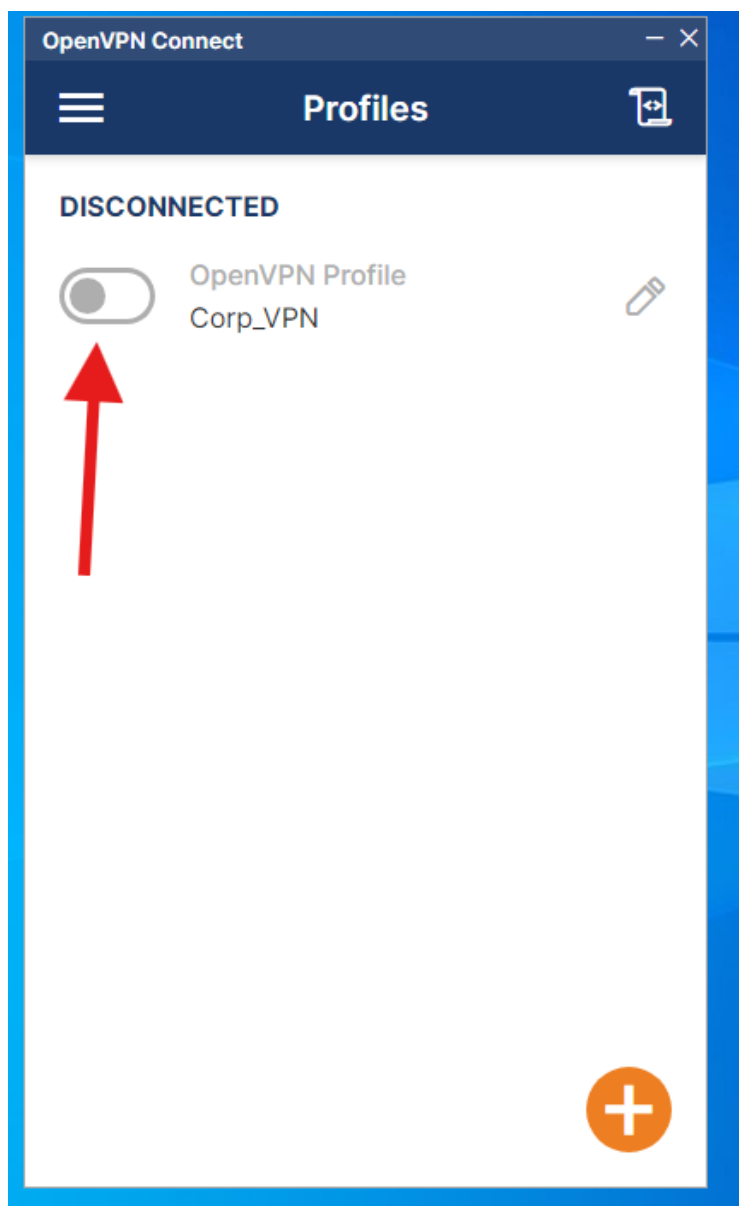
Username
arthur.fix

☒ Save password

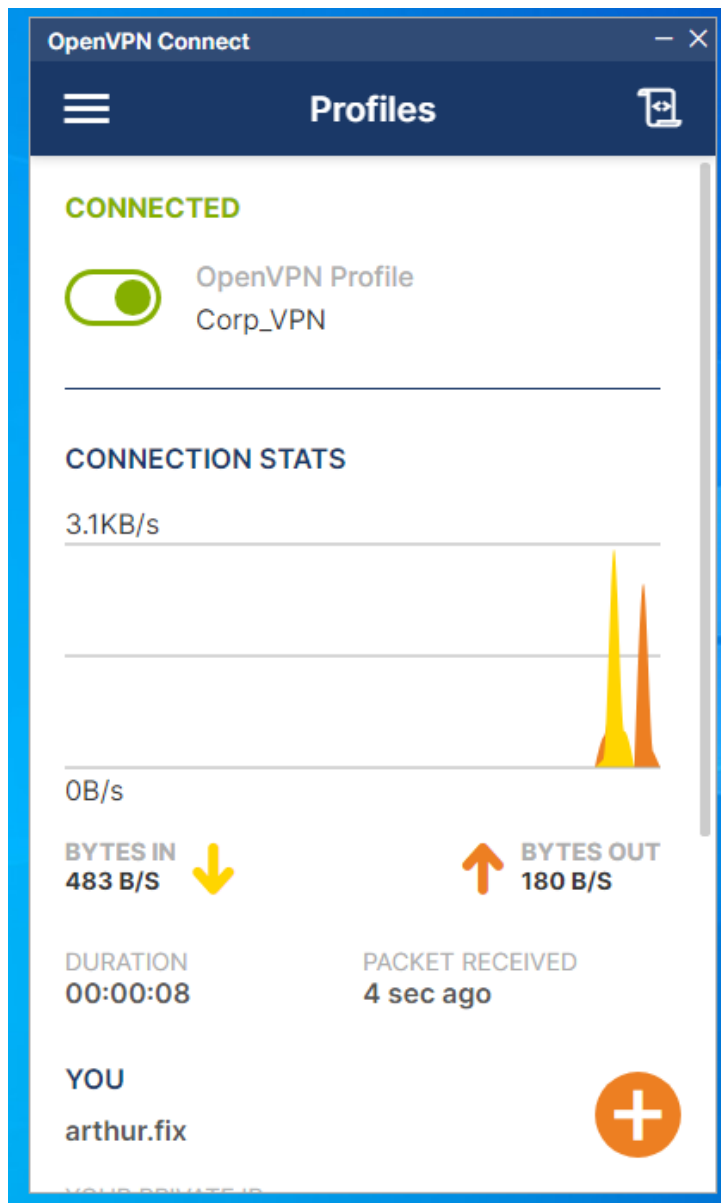
Password
.....

Profile ID
Unique identifier of this profile
1745067626075

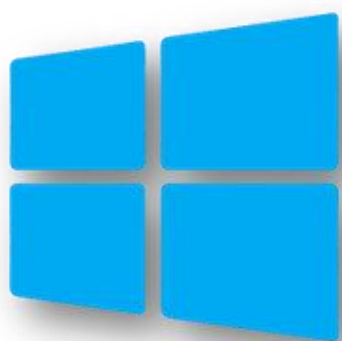
Cliquer ensuite sur le bouton de connexion.



Le VPN fonctionne.



Documentation d'exploitation, L'utilisation et la gestion
du Lot 1



Microsoft
Active Directory

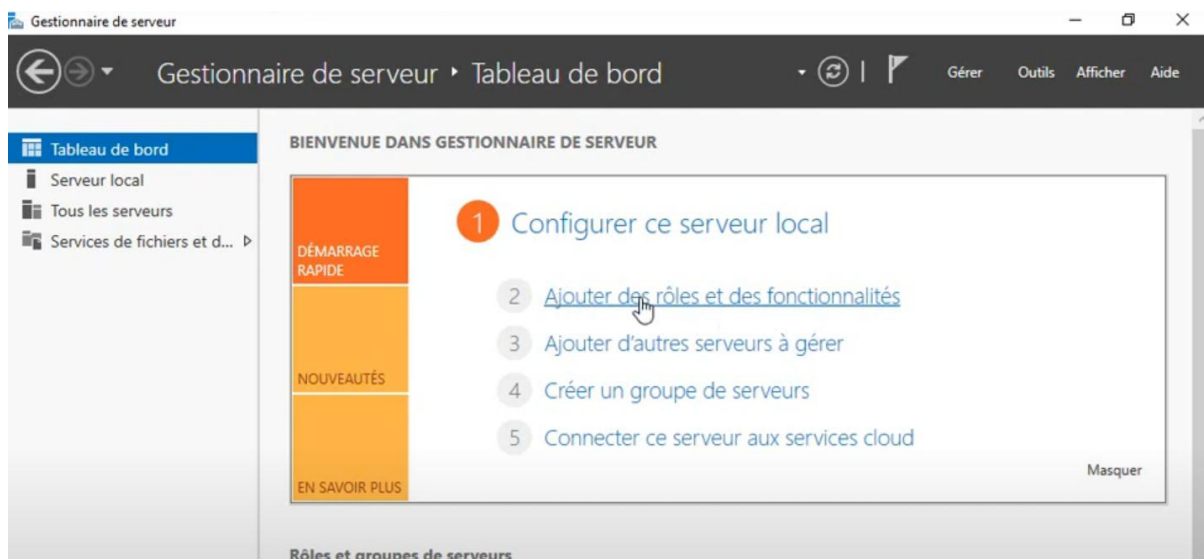
PRTG 
**NETWORK
MONITOR**

Introduction :

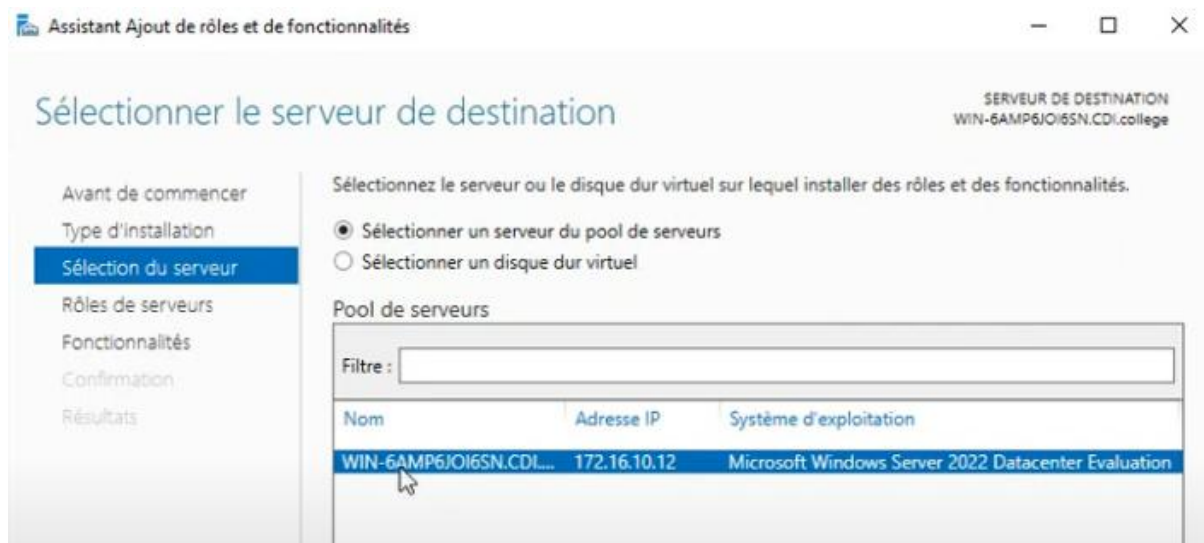
L'administration des réseaux informatiques repose sur des services essentiels qui assurent une gestion centralisée des utilisateurs, des ressources et des communications. Parmi ces services, Active Directory, DNS et DHCP jouent un rôle crucial. Active Directory permet de centraliser la gestion des comptes utilisateurs et des permissions, DNS assure la résolution des noms de domaine, tandis que DHCP automatise l'attribution des adresses IP dans le réseau. Ce document vous guidera à travers les étapes d'installation et d'utilisation de ces trois services fondamentaux, en mettant l'accent sur les bonnes pratiques pour garantir un fonctionnement optimal.

Installation des rôles

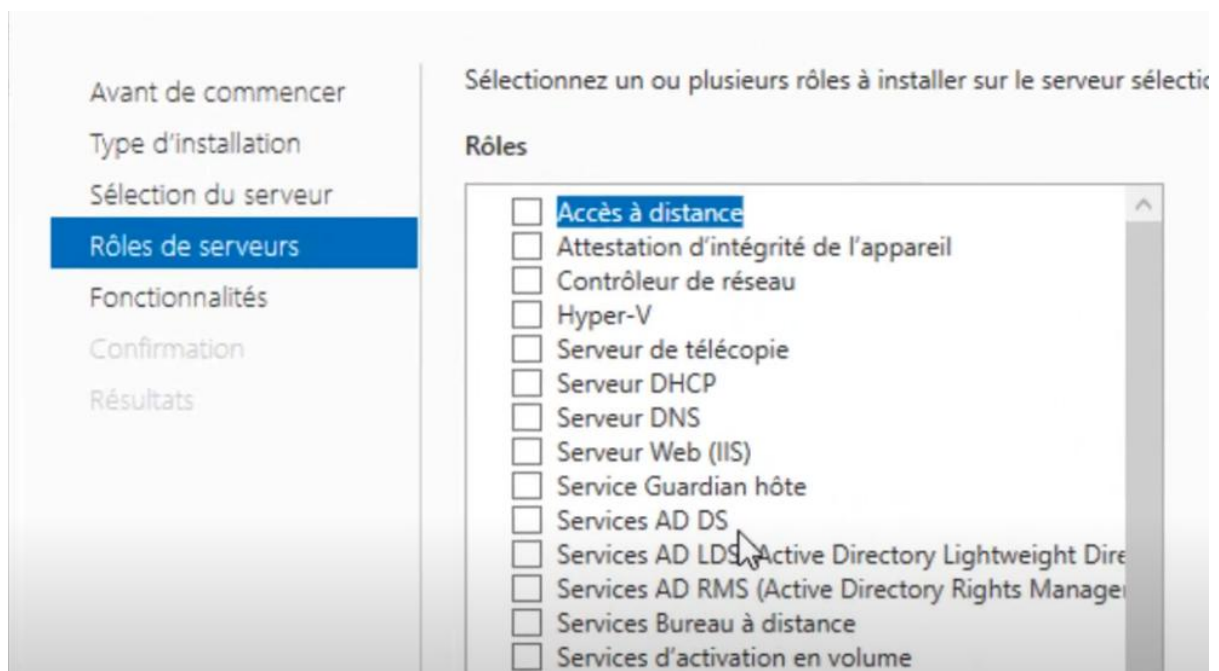
Lorsque vous allumez votre Windows Serveur cliquait sur Ajouter des rôles et des fonctionnalités.



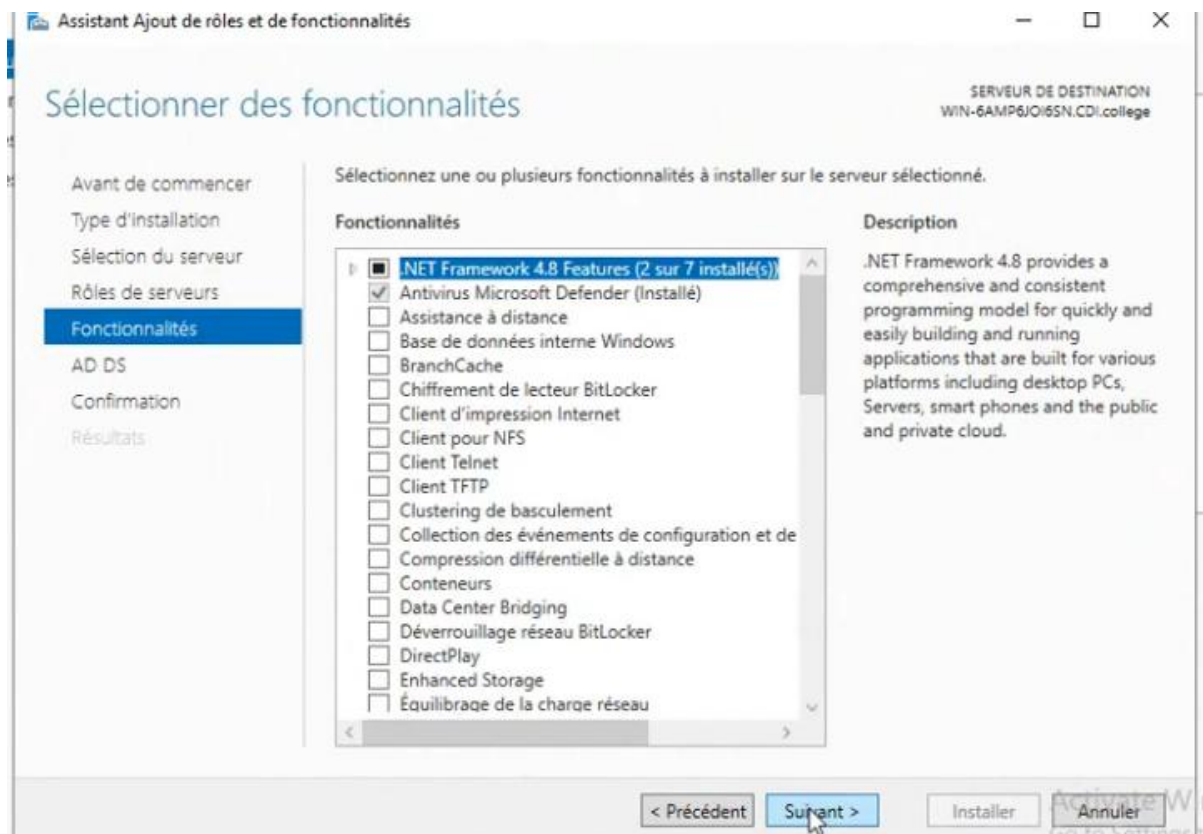
Cliquer deux fois sur suivant puis quand vous arrivez dans sélection du serveur sélectionnez votre serveur Windows.



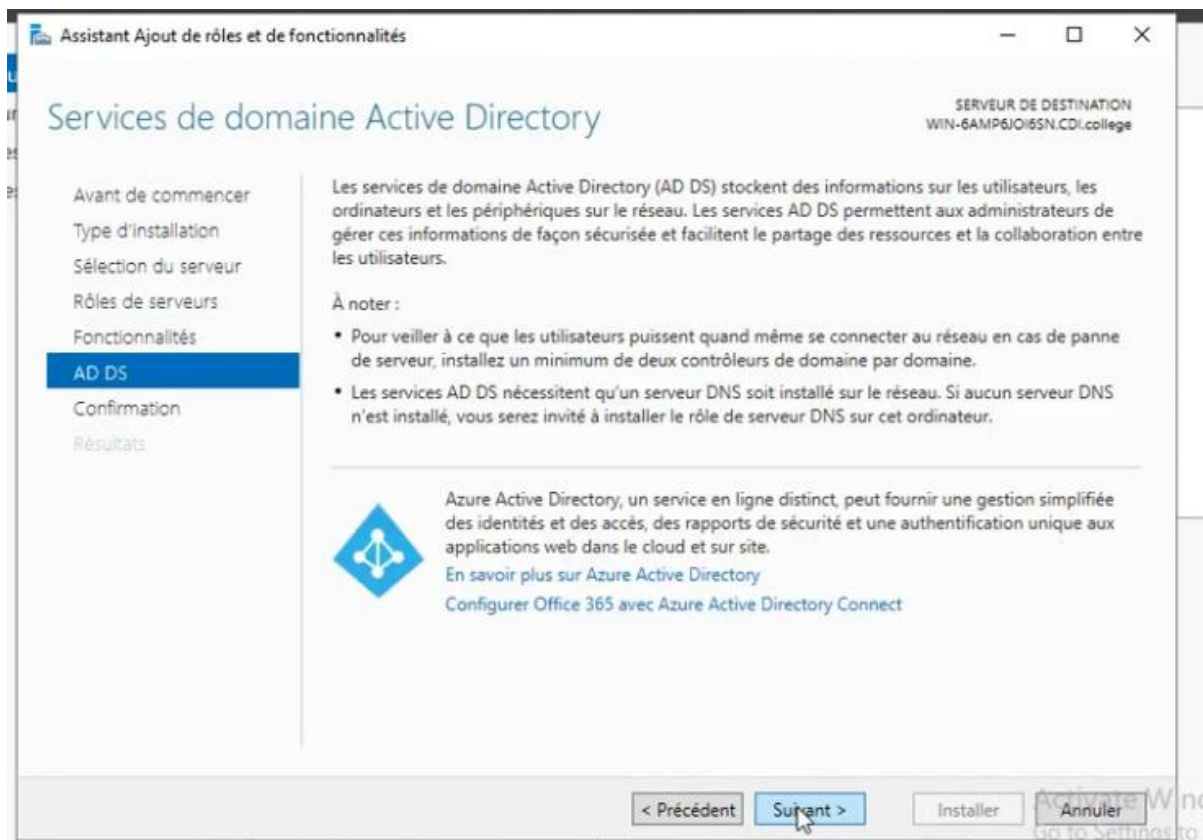
Dans rôles de serveurs sélectionnez les rôles Services AD DS et Serveur DHCP.



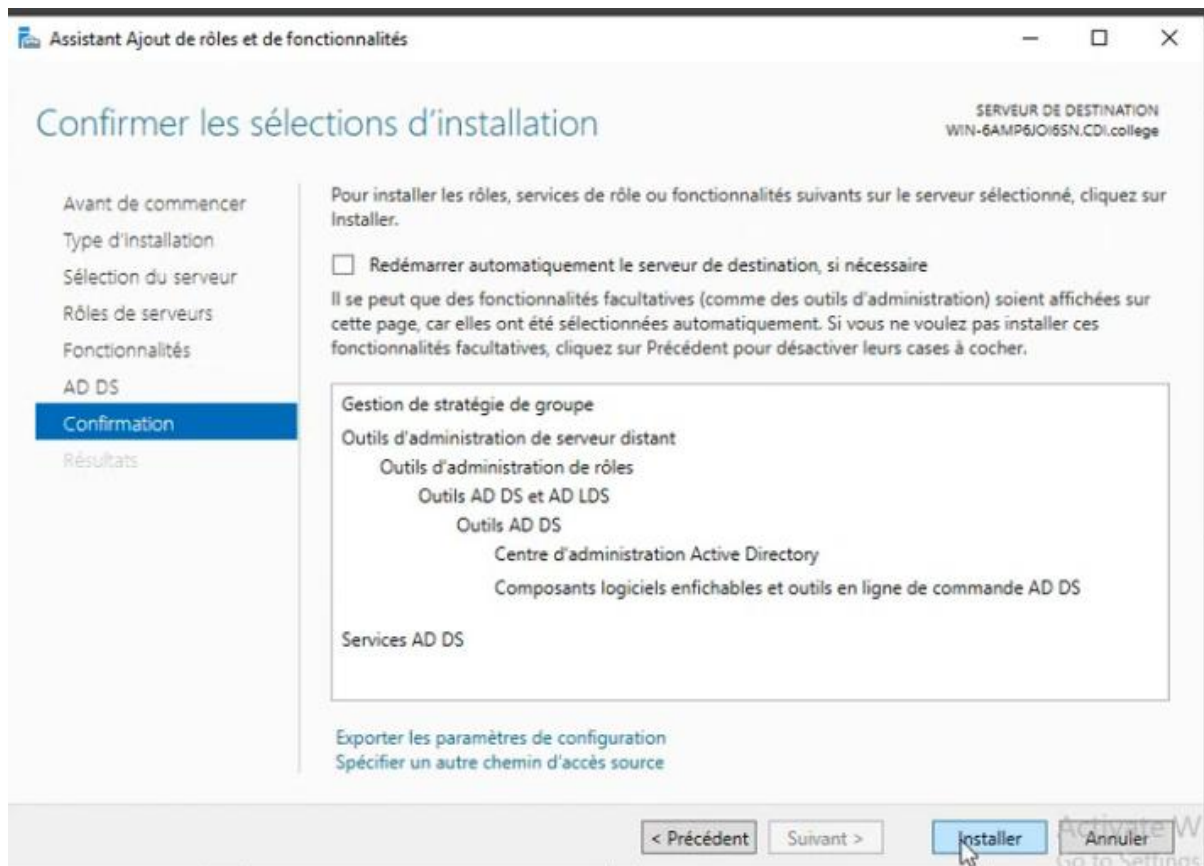
Cliquez sur suivant.



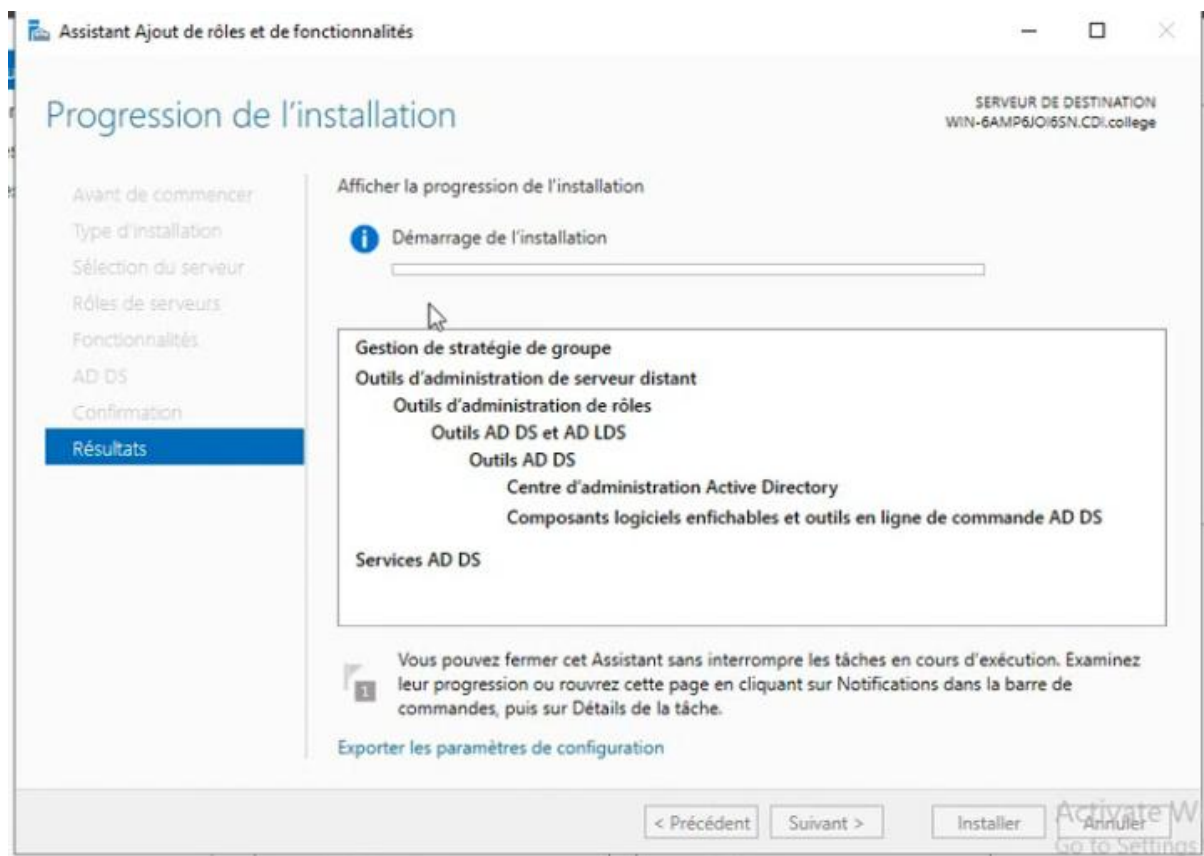
Cliquez sur suivant.



Cliquez sur installer.



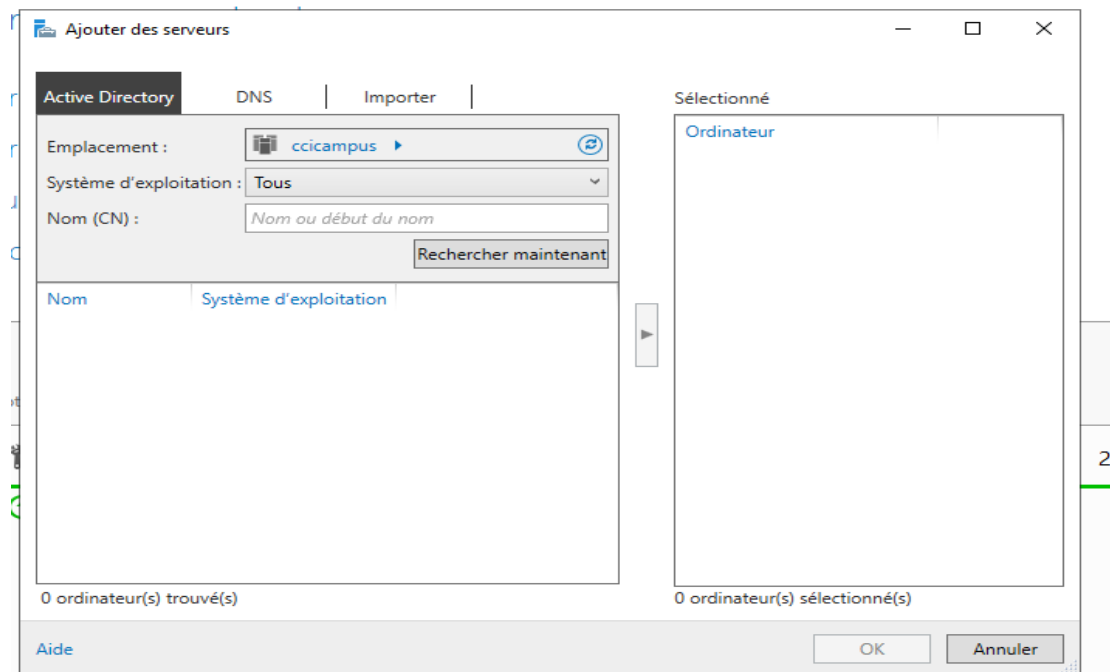
Attendez que l'installation se termine puis fermez la fenêtre lorsque c'est fini.



Pour installer des rôles sur un autre serveur (en l'occurrence le serveur secondaire en version core ici), cliquez sur "ajouter d'autres serveurs à gérer".

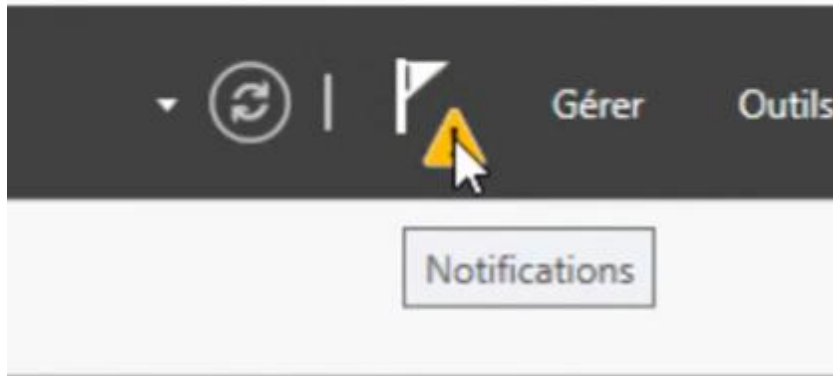


Recherchez ensuite le nom exact du serveur secondaire que vous voulez joindre et gérer à partir de votre serveur principal.



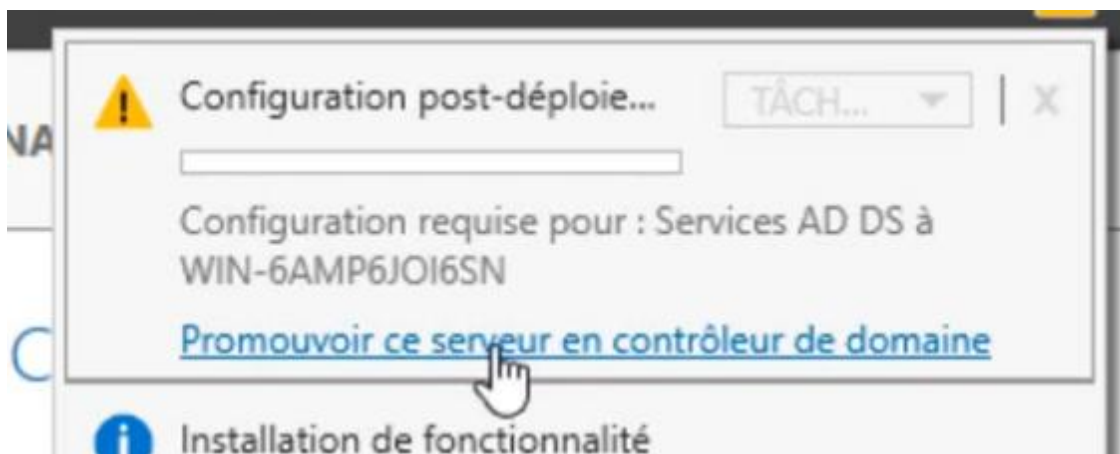
Installation de l'Active Directory et DNS

Cliquez sur le drapeau en haut.

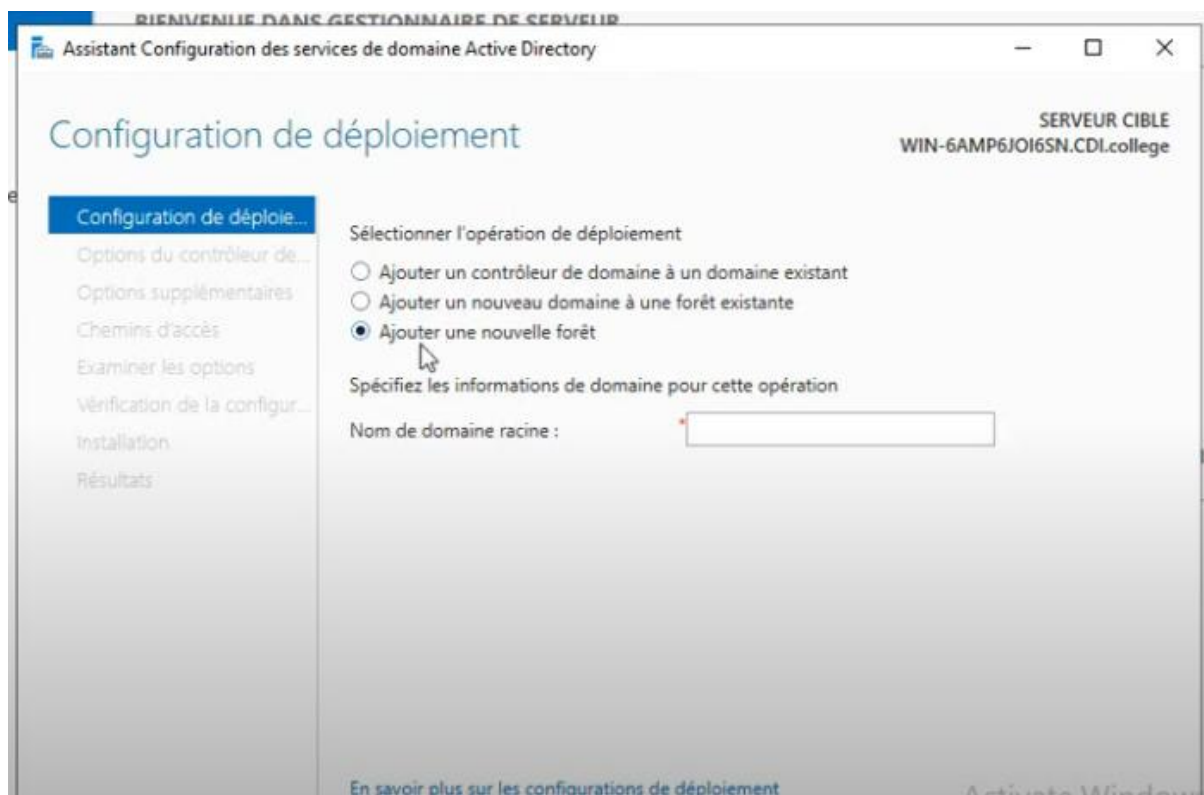


ur local

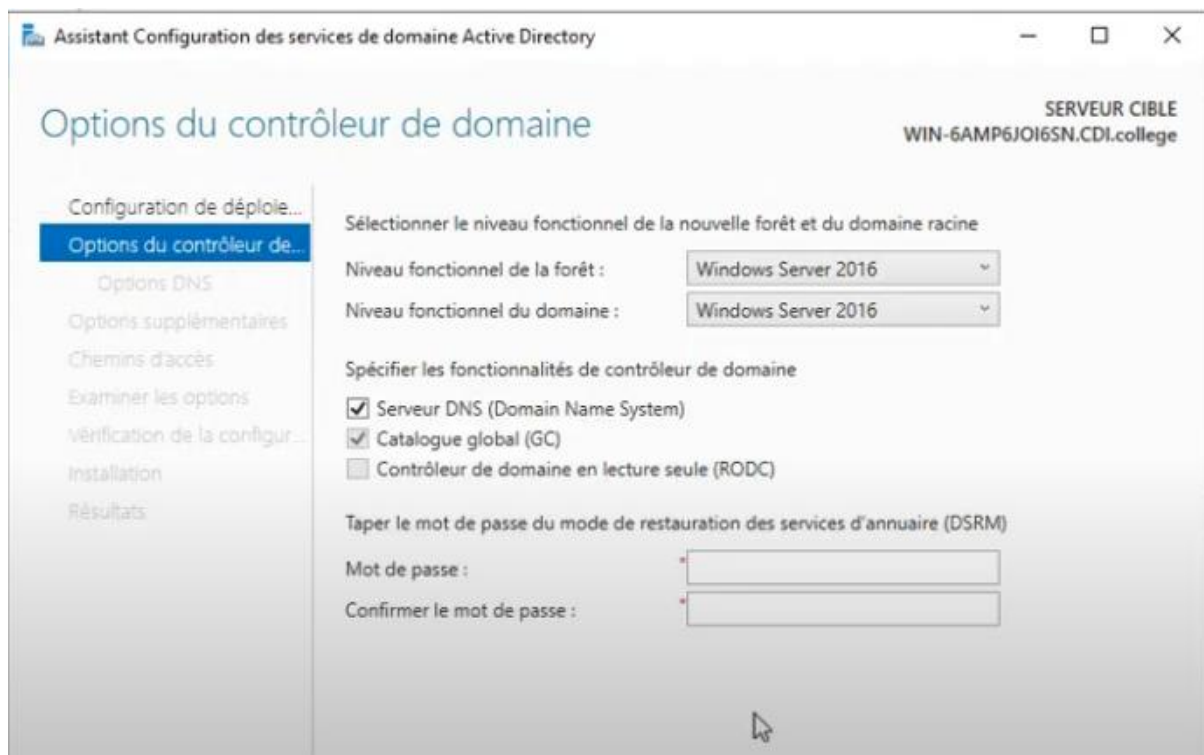
Cliquez sur promouvoir ce serveur en contrôleur de domaine.



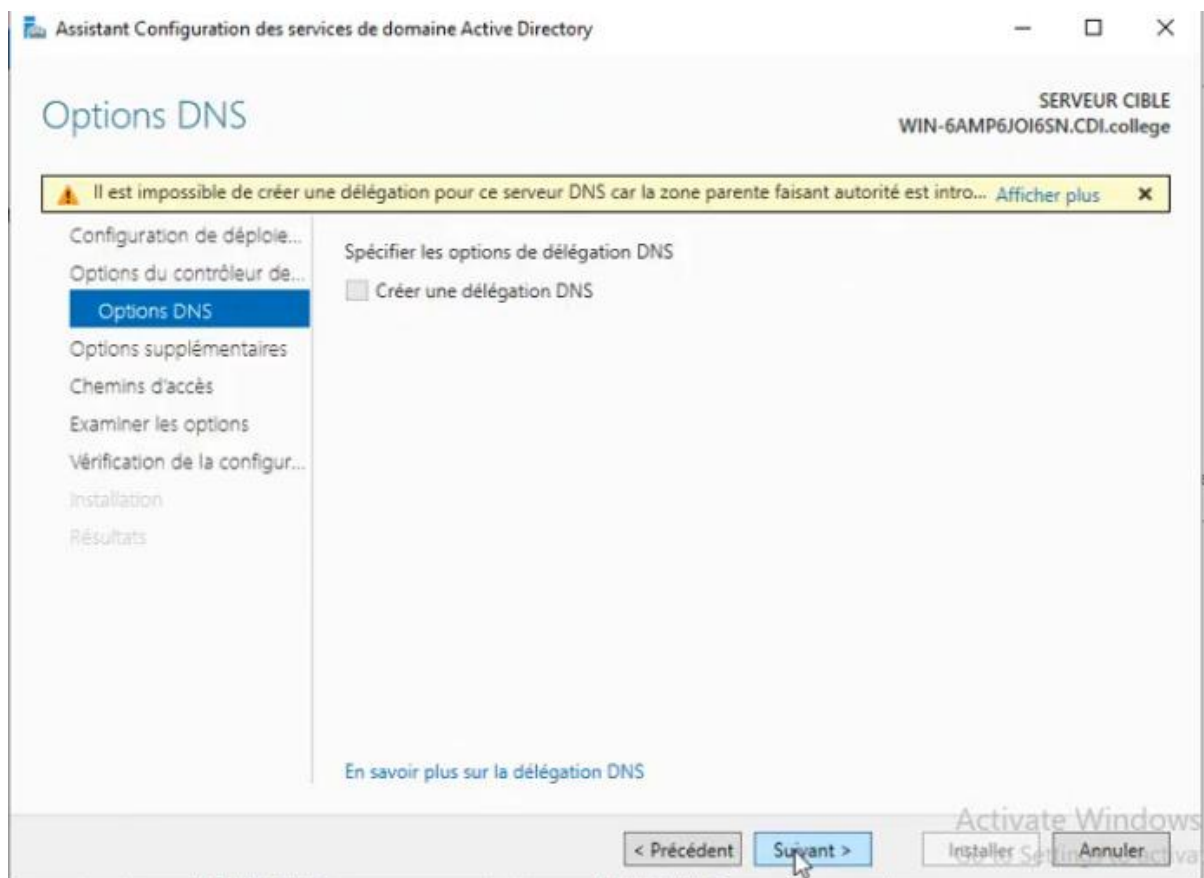
Sélectionnez Ajouter une nouvelle forêt puis entrez le nom de votre nouvelle forêt.



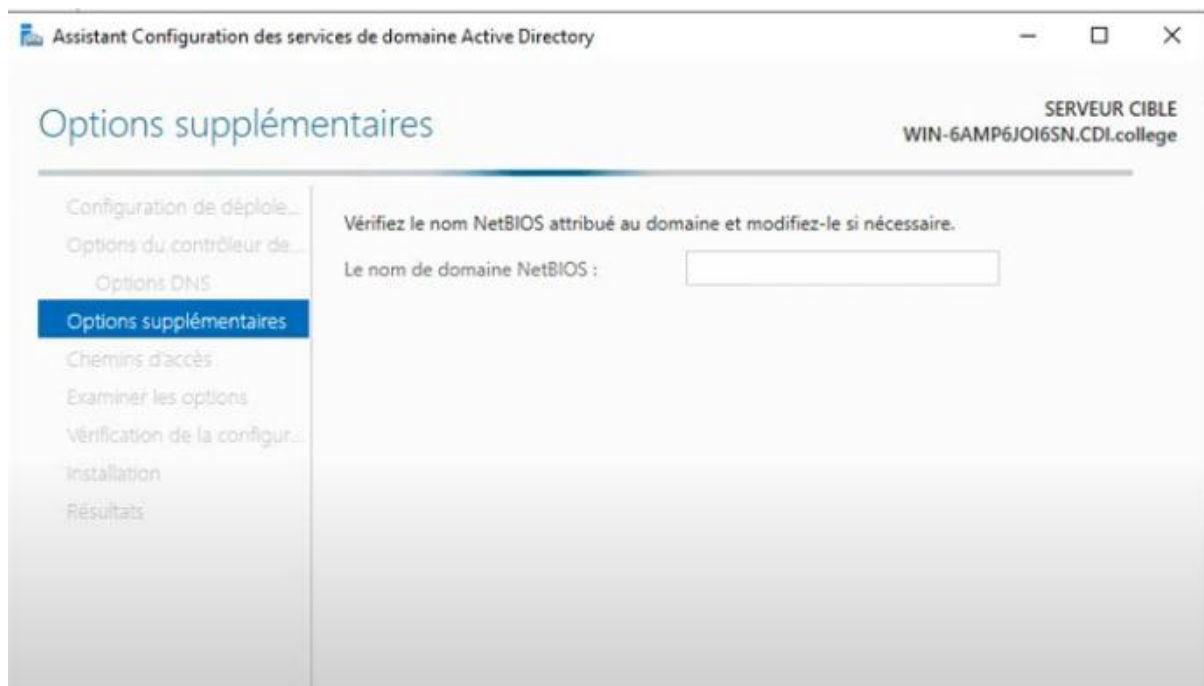
Mettez un mot de passe pour permettre de se connecter sur d'autres postes.



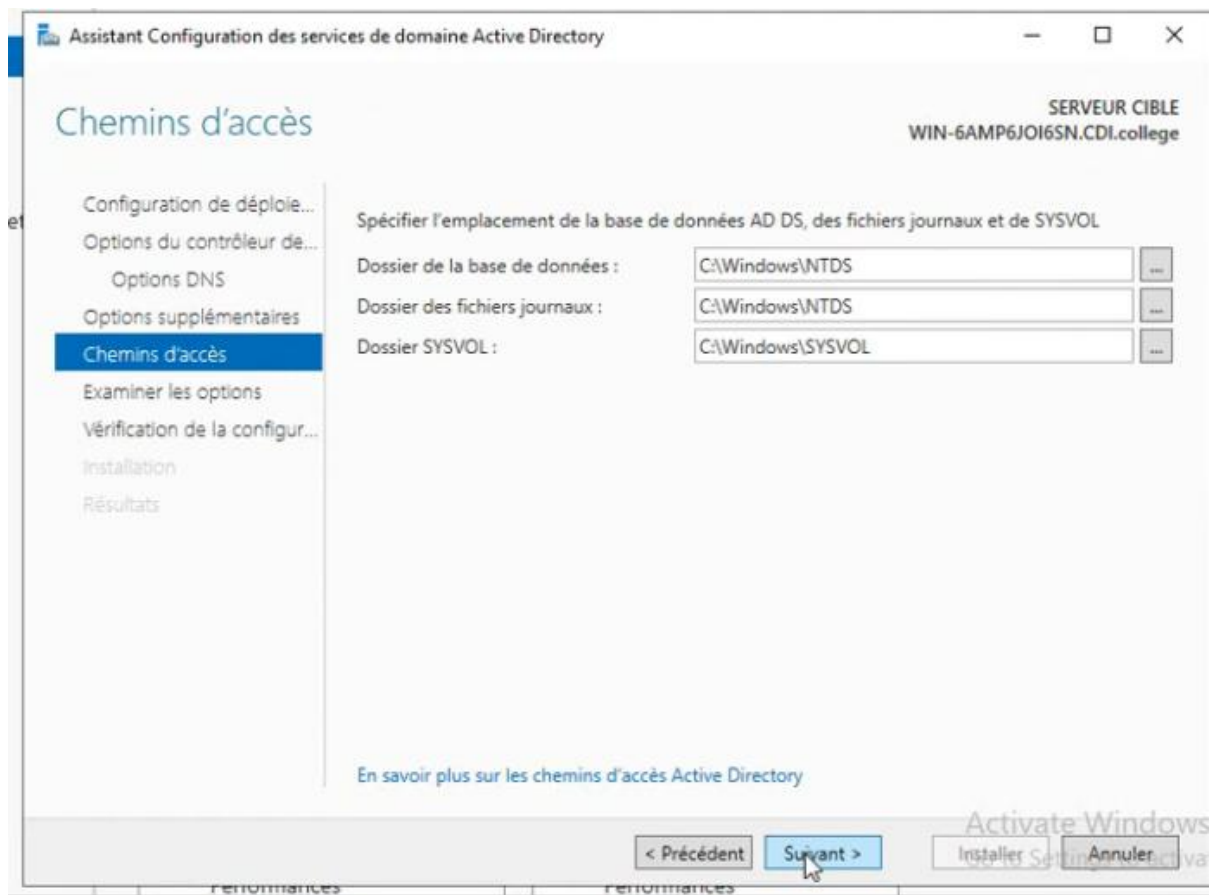
Cliquez sur suivant.



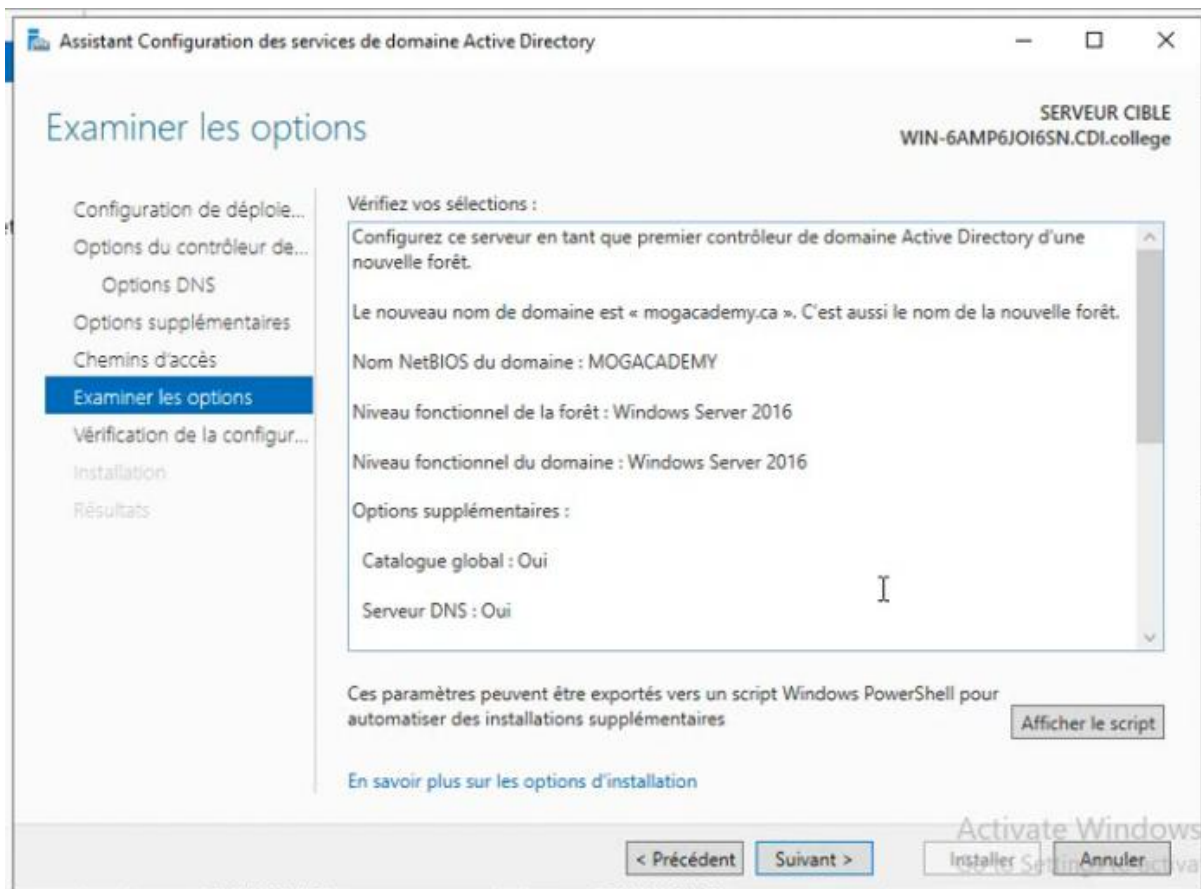
Attendez que Windows vous génère un nom de domaine.



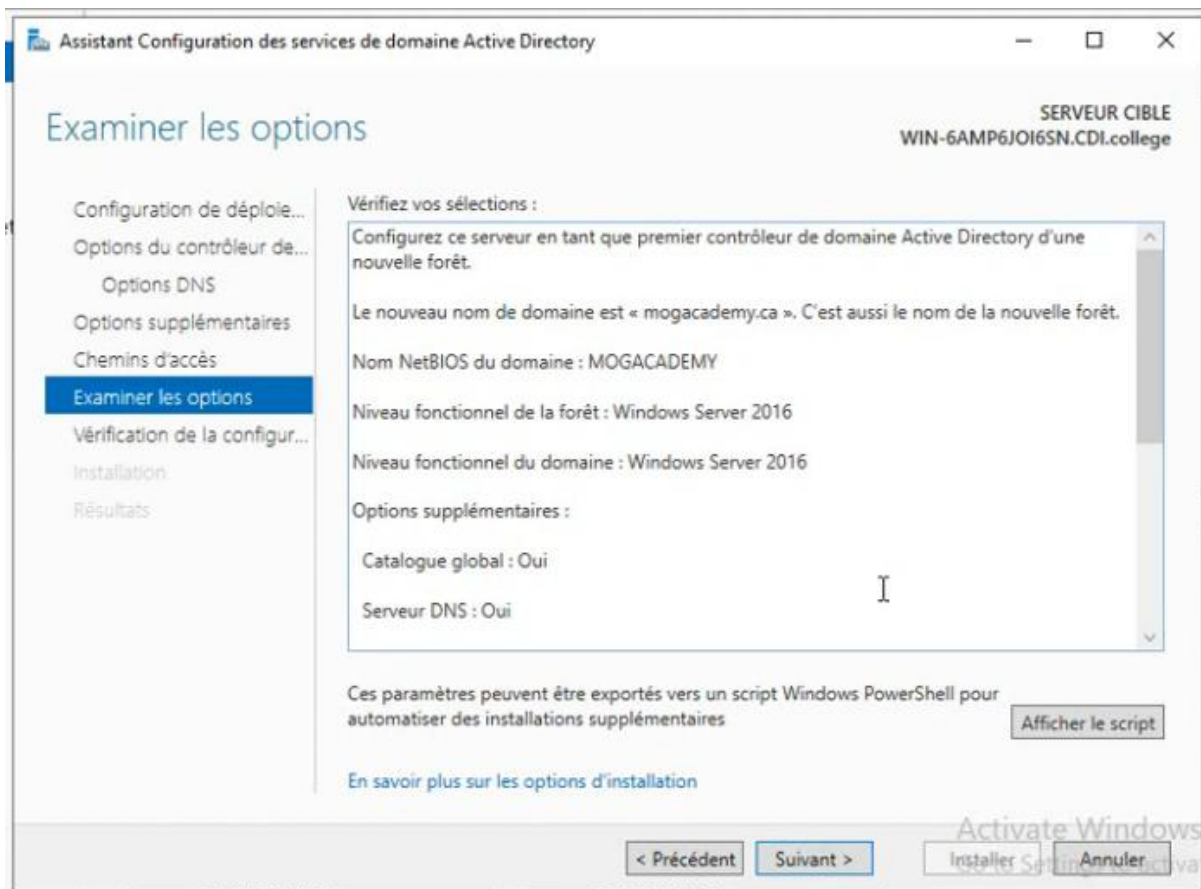
Cliquez sur suivant.



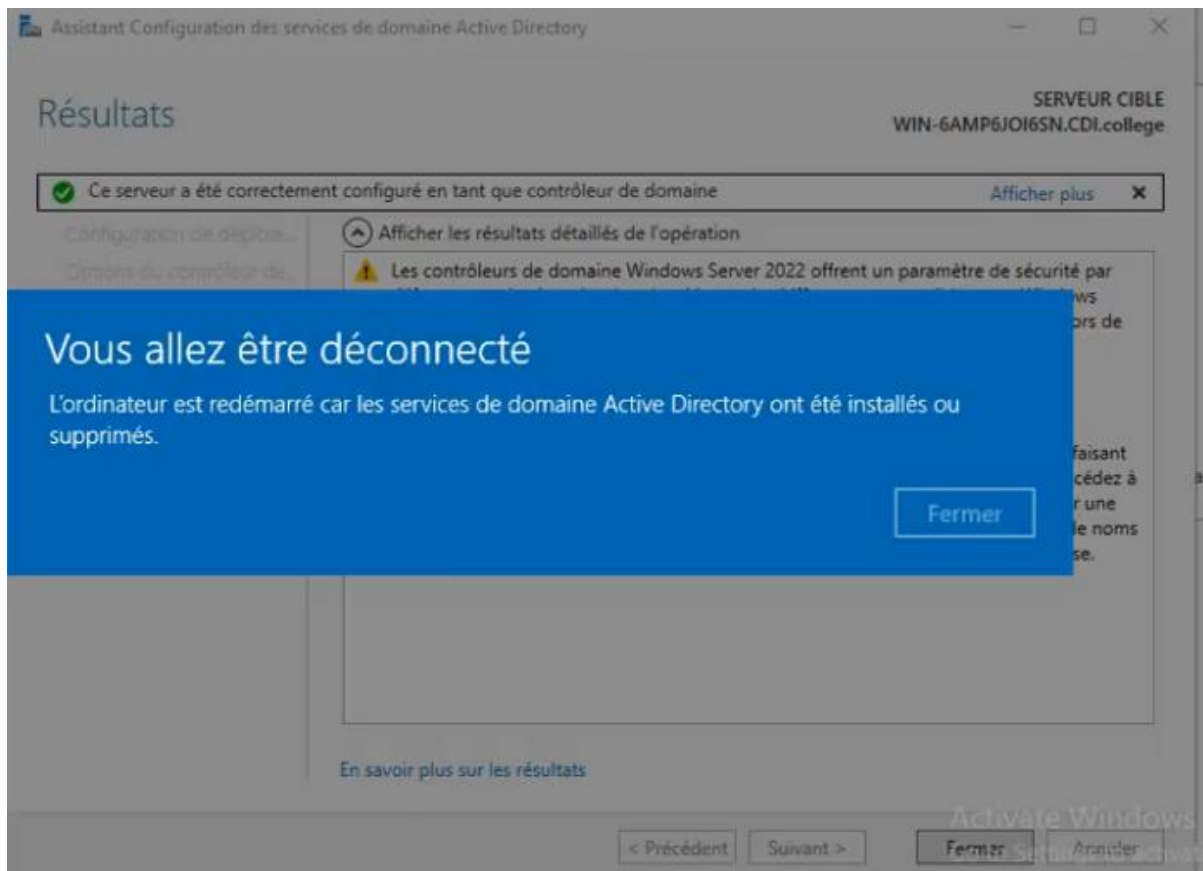
Cliquez sur suivant.



Puis cliquez sur suivant et Installer.



Attendez que ça s'installe puis fermer la fenêtre et redémarrez votre serveur.

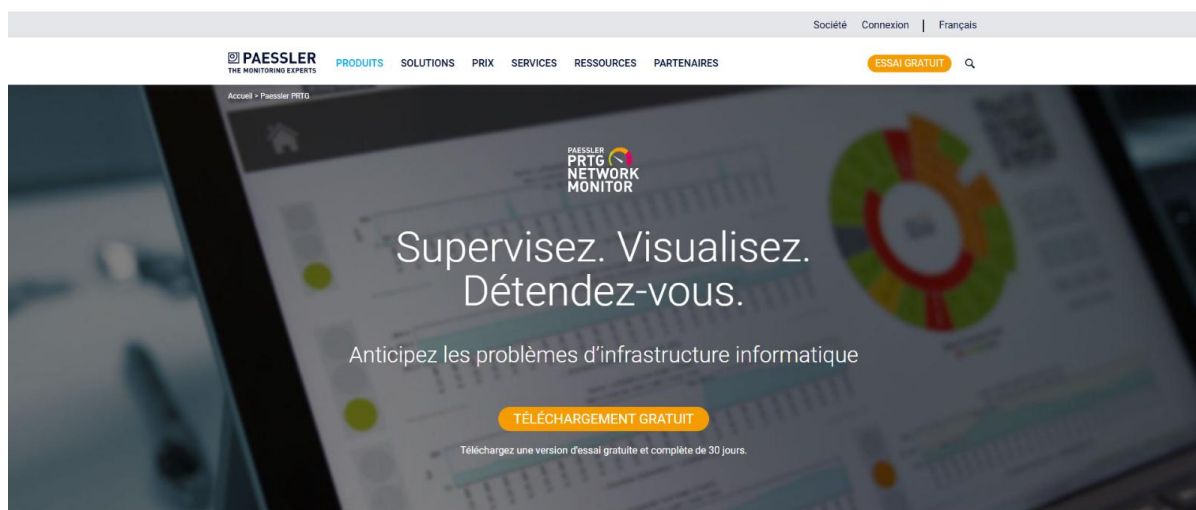


2. Installation PRTG

Aller sur le lien de téléchargement prtg:

<https://www.paessler.com/fr/prtg>

Cliquez ensuite sur “Téléchargement gratuit”:



Nos utilisateurs donnent les meilleures notes à la supervision avec Paessler PRTG

Laissez l'installateur PRTG se télécharger :

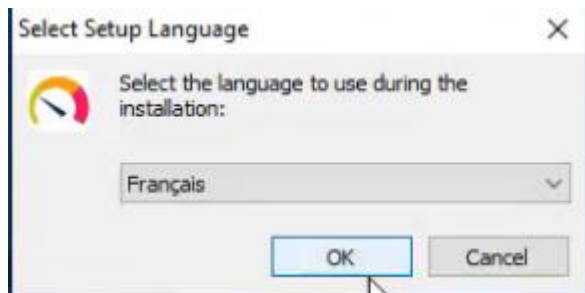


Cliquez sur l'installateur PRTG :

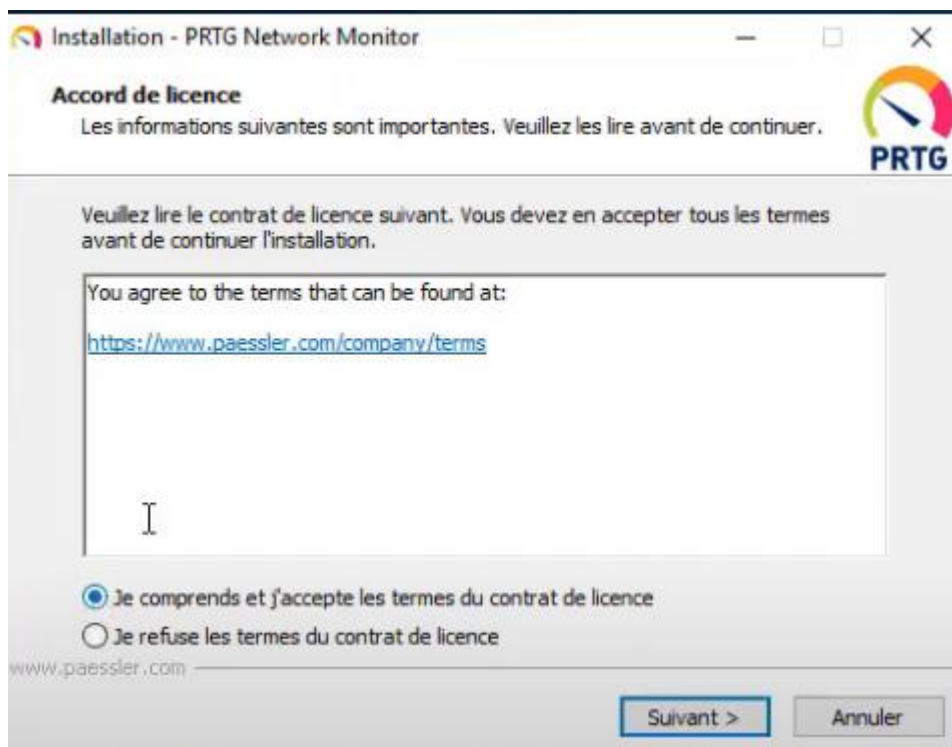
▼ Aujourd'hui

 prtg_installer_with_trial_key_000023-MEB...	12/04/2025 18:26	Application	359 425 Ko
---	------------------	-------------	------------

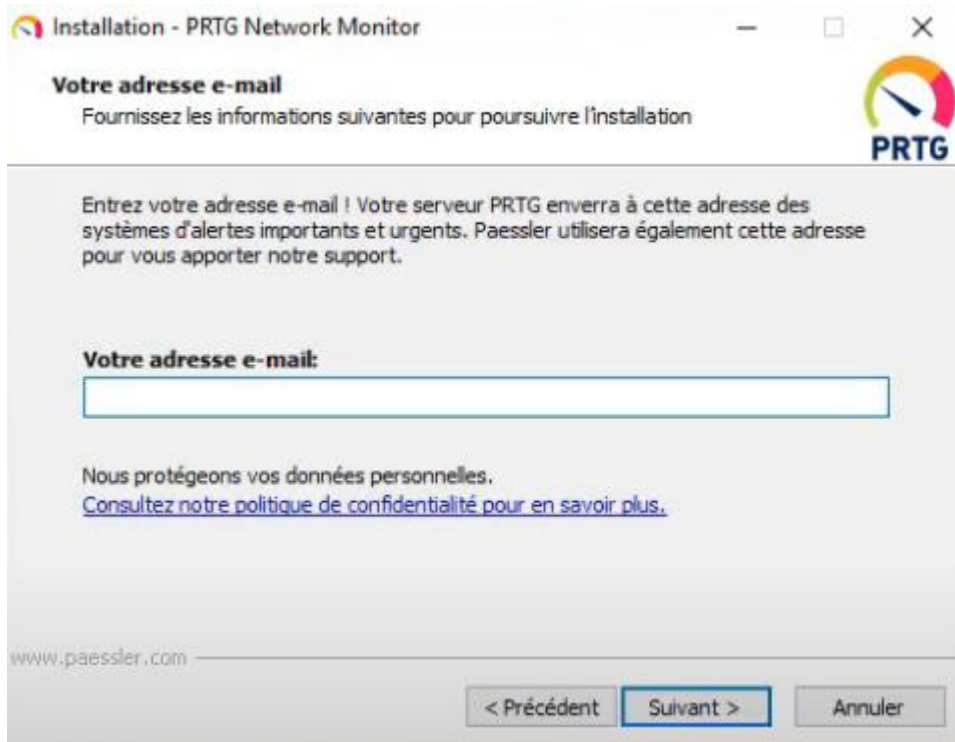
Choisissez votre langue en français :



Acceptez les termes puis cliquez sur Suivant.



Mettez votre adresse mail (optionnel) puis cliquez sur Suivant.



The screenshot shows the 'Installation - PRTG Network Monitor' window. The title bar includes the PRTG logo and standard window controls. The main content area is titled 'Votre adresse e-mail' and instructs the user to provide an email address for alerts and support. It includes a text input field and a 'Suivant >' button. A footer contains the website 'www.paessler.com' and navigation buttons '< Précédent', 'Suivant >', and 'Annuler'.

Installation - PRTG Network Monitor

Votre adresse e-mail
Fournissez les informations suivantes pour poursuivre l'installation

Entrez votre adresse e-mail ! Votre serveur PRTG enverra à cette adresse des systèmes d'alertes importants et urgents. Paessler utilisera également cette adresse pour vous apporter notre support.

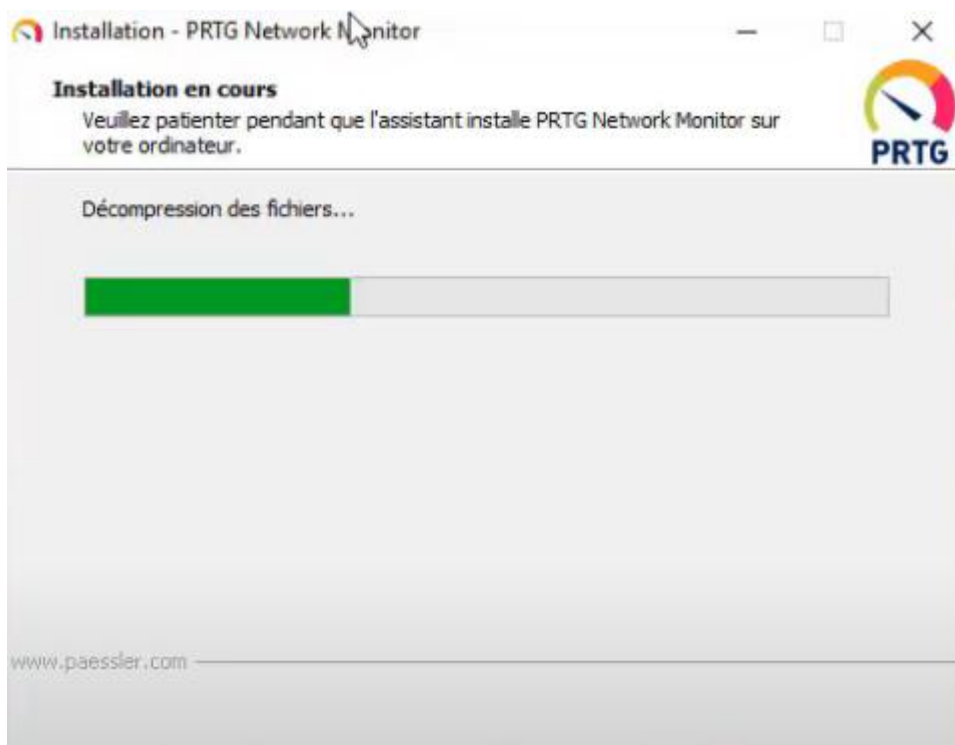
Votre adresse e-mail:

Nous protégeons vos données personnelles.
[Consultez notre politique de confidentialité pour en savoir plus.](#)

www.paessler.com

< Précédent **Suivant >** Annuler

Attendez que PRTG s'installe.



The screenshot shows the 'Installation - PRTG Network Monitor' window during the installation phase. The title bar is the same. The main content area is titled 'Installation en cours' and informs the user that the assistant is installing PRTG Network Monitor. It shows a progress bar for 'Décompression des fichiers...'. The footer remains the same with 'www.paessler.com' and navigation buttons.

Installation - PRTG Network Monitor

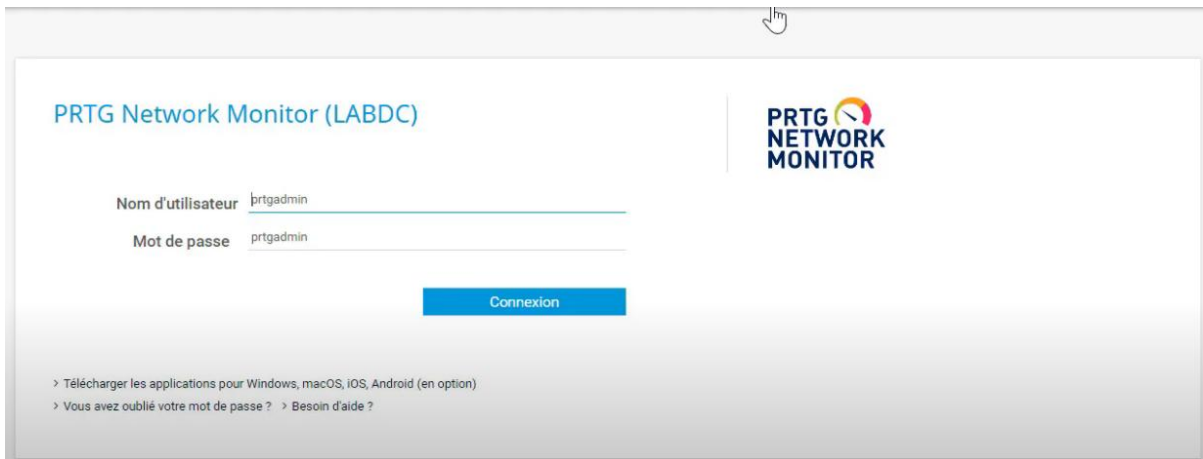
Installation en cours
Veuillez patienter pendant que l'assistant installe PRTG Network Monitor sur votre ordinateur.

Décompression des fichiers...

www.paessler.com

< Précédent **Suivant >** Annuler

Entrez votre adresse IP pour sur un navigateur web puis entrez vos identifiants admin (par défaut prtgadmin), puis cliquez sur Connexion.



Entrez votre licence qui apparaissez lors du téléchargement de l'installateur PRTG puis cliquez sur Activer la licence.

Nom de licence

prtgtrial

Clé de licence

000014-0R0KFM-8FFH20-U2G47P-U8BVFA-GCRUQJ-2D3JV8-QFDA3P-MFTJRM-RUJGM2

ÉTAPE 3 : Activer votre PRTG

Une connexion HTTPS au serveur d'activation Paessler (activation.paessler.com) est nécessaire. Vous pouvez utiliser un proxy HTTP pour la connexion.

Utiliser un serveur proxy

☒ Non, utiliser une connexion directe à Internet (par défaut)

☐ Oui, dans notre réseau un proxy est obligatoire

[Annuler](#) [Activer la licence](#)

Vous êtes sur la page d'accueil PRTG.

Page d'accueil Équipements Bibliothèques Capteurs Alertes Cartes Rapports Logs Tickets Configuration

Nouvelles entrées de log 2 11 Recherche...

Configuration Licence

Licence

État Log

Information sur la licence

État de la licence	La version d'essai a expiré.
Nom de licence	prtgtrial
Clé de licence	000014-0R0KFM-8FFH20-U2G47P-U8BVFA-GCRUQJ-2D3JV8-QFDA3P-MFTJRM-RUJGM2
ID de système	SYSTEMID-IOEMCCJO-PCIHPR05-IDZVDYKD-BB2DB7NL-Q2G5FWAA
Version sous licence	PRTG Freeware (Trial Expired) (expiré le 8/9/2019)
Dernière mise à jour	2/23/2021 2:53:18 AM
Nombre de capteurs	100 Avez-vous besoin de capteurs supplémentaires ? Cliquez ici pour effectuer la mise à niveau !

[Modifier la clé de licence](#) [Actualiser les informations](#)

Définir un mot de passe sécurisé

Le compte d'utilisateur de l'administrateur système de PRTG utilise le mot de passe par défaut « prtgadmin ». Modifiez-le pour sécuriser votre interface Web PRTG.

Ceci est absolument obligatoire si vous autorisez l'accès à votre interface Web PRTG depuis Internet (l'extérieur de votre pare-feu) !

[Modifier le mot de passe par défaut](#)

Activer SSL/TLS pour l'interface Web PRTG.

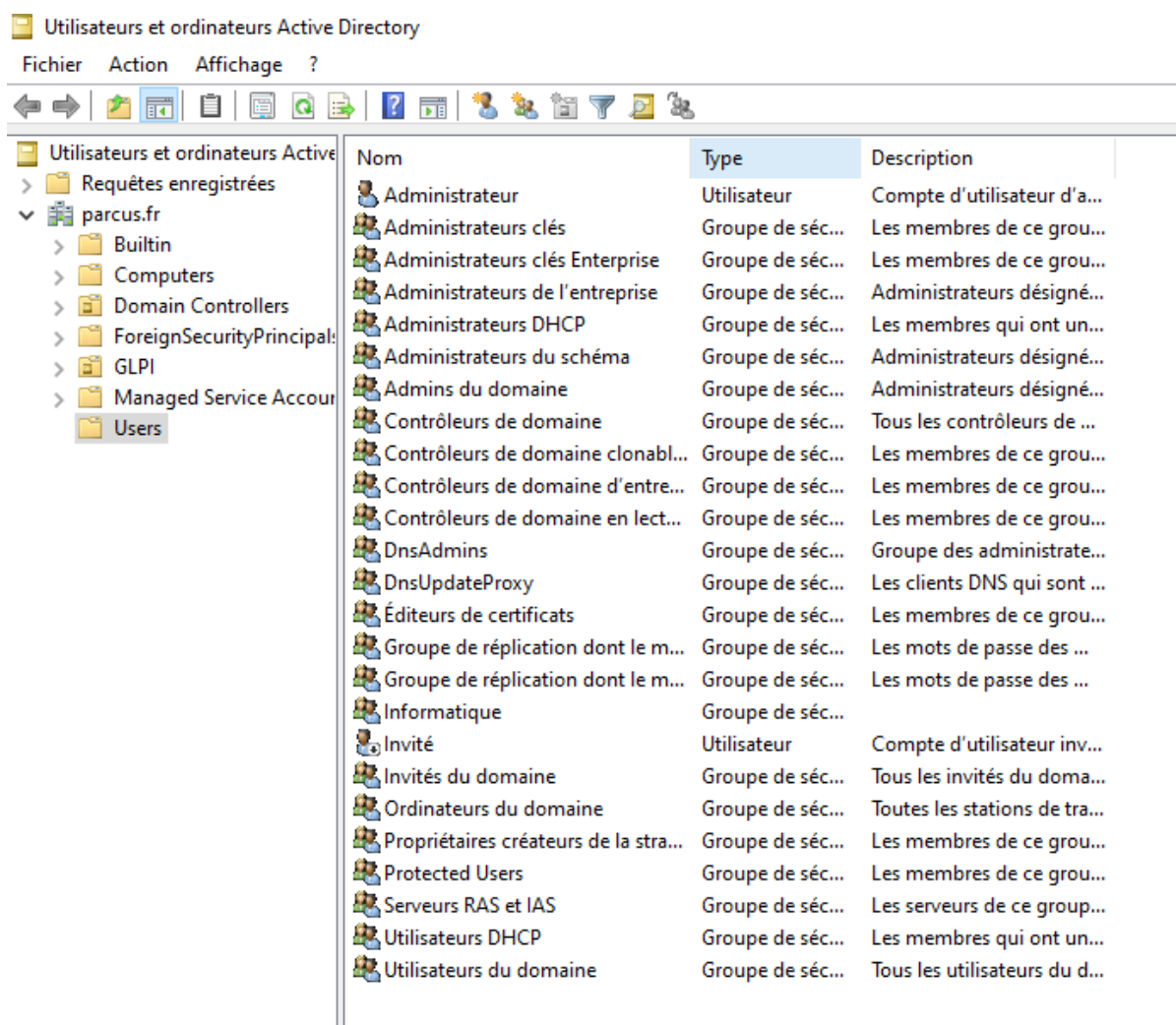
La connexion de votre navigateur à ce central serveur central PRTG n'est pas sécurisée par SSL/TLS.

Il est préférable de passer à SSL/TLS, particulièrement si votre interface Web PRTG est accessible depuis Internet (en dehors de votre pare-feu).

[Passer à SSL/TLS](#)

3. Gestion Active Directory

- Ouvrez "Utilisateurs et Ordinateurs Active Directory" (dsa.msc).
- Naviguez jusqu'à l'OU (Unité d'Organisation) où vous souhaitez créer l'utilisateur.



- Cliquez avec le bouton droit, sélectionnez "Nouveau" puis "Utilisateur".

- Remplissez les informations requises et suivez l'assistant pour créer le compte utilisateur.

Nouvel objet - Utilisateur

Créer dans : parcus.fr/Users

Prénom : Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur : @parcus.fr

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : PARCUS\

< Précédent Suivant > Annuler

- Les groupes sont utilisés pour simplifier la gestion des permissions.
- Pour créer un groupe, ouvrez "Utilisateurs et Ordinateurs Active Directory".
- Cliquez avec le bouton droit sur l'OU appropriée, sélectionnez "Nouveau" puis "Groupe".
- Nommez le groupe et définissez son type (Distribution ou Sécurité) et sa portée (Domaine local, Global, Universel).

Nouvel objet - Groupe ✕

 Créer dans : parcus.fr/Users

Nom du groupe :

Nom de groupe (antérieur à Windows 2000) :

Étendue du groupe ☐ Domaine local ☒ Globale ☐ Universelle	Type de groupe ☒ Sécurité ☐ Distribution
--	--

Ajout d'un Ordinateur au Domaine

- Sur le poste de travail ou le serveur à ajouter, accédez aux paramètres système.

Paramètres associés

[Gestionnaire de périphériques](#)

[Bureau à distance](#)

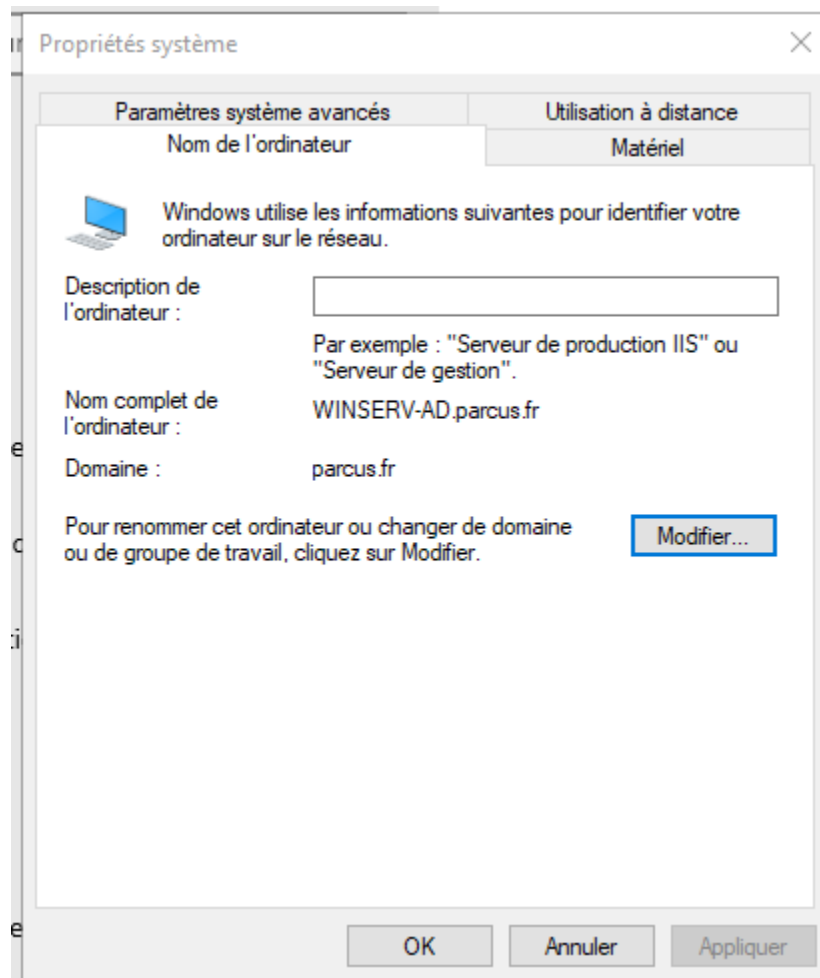
[Protection du système](#)

[Paramètres avancés du système](#)

[Renommer ce PC \(avancé\)](#)

[Paramètres graphiques](#)

- Cliquer sur "Renommer ce PC (avancé)".
- Sous "Nom de l'ordinateur", cliquez sur "Modifier".



- Sélectionnez "Domaine", entrez le nom de votre domaine, puis suivez les instructions pour redémarrer l'ordinateur.

Création et Gestion des OU

1. Les Unités d'Organisation permettent de structurer et de gérer les objets AD de manière hiérarchique.
2. Pour créer une OU, ouvrez "Utilisateurs et Ordinateurs Active Directory".
3. Cliquez avec le bouton droit sur le domaine ou l'OU existante, sélectionnez "Nouveau" puis "Unité d'Organisation".
4. Nommez l'OU et configurez les paramètres nécessaires.

Conclusion :

La mise en place et l'utilisation combinée d'Active Directory, DNS et DHCP renforcent la sécurité, la stabilité et l'efficacité des infrastructures réseau. Active Directory facilite la gestion centralisée des utilisateurs et des ressources, tandis que DNS et DHCP assurent respectivement une communication fiable et une configuration simplifiée des adresses IP. En suivant les étapes et les recommandations présentées dans ce guide, vous pourrez exploiter pleinement ces outils pour optimiser la gestion de votre réseau et améliorer l'expérience utilisateur.

Documentation d'installation Modoboa (Ubuntu)



Introduction

Modoboa est un serveur de messagerie 100% gratuit et open source. Il s'agit d'un serveur de messagerie Python hautement évolutif avec simplicité et vitesse à la base. Modoboa rassemble les meilleurs outils open source pour installer, configurer et sécuriser votre propre serveur de messagerie.

Installation

Installer python3:

```
root@mail:~# apt-get install python3-virtualenv python3-pip git curl gnupg2 -y
```

Installer le paquet Modoboa:

```
root@mail:~# git clone https://github.com/modoboa/modoboa-installer
```

Donner la permission au dossier modoboa-installer:

```
root@mail:~# chmod -R 777 modoboa-installer
```

Aller dans le dossier modoboa-installer:

```
root@mail:~# cd modoboa-installer
```

Créez un installeur modoboa:

```
root@mail:~/modoboa-installer# python3 ./run.py --stop-after-configfile-check yourdomain.com
Welcome to Modoboa installer!
Configuration file installer.cfg not found, creating new one.
```

Modifier le fichier d'installation créé :

```
root@mail:~/modoboa-installer# nano installer.cfg
```

```
[general]
hostname = mail.%(domain)s

[certificate]
generate = true
type = self-signed

[letsencrypt]
email = admin@example.com

[database]
engine = postgres
host = 127.0.0.1
install = true

[postgres]
user = postgres
password =

[mysql]
user = root
password = dnnUzG2BsM9RZ7PC
charset = utf8
collation = utf8_general_ci
```

Lancer l'installation de Modoboa:

```
root@mail:~/modoboa-installer# python3 ./run.py --interactive yourdomain.com
Welcome to Modoboa installer!

Warning:
Before you start the installation, please make sure the following DNS records exist for domain 'yourdomain.com':
    mail IN A      <IP ADDRESS OF YOUR SERVER>
          IN MX    mail.yourdomain.com.

Your mail server will be installed with the following components:
modoboa automx amavis clamav dovecot nginx razor postfix postwhite spamassassin uwsgi radicale opendkim
Do you confirm? (Y/n)
```

Vérifier si le site modoboa est en ligne:

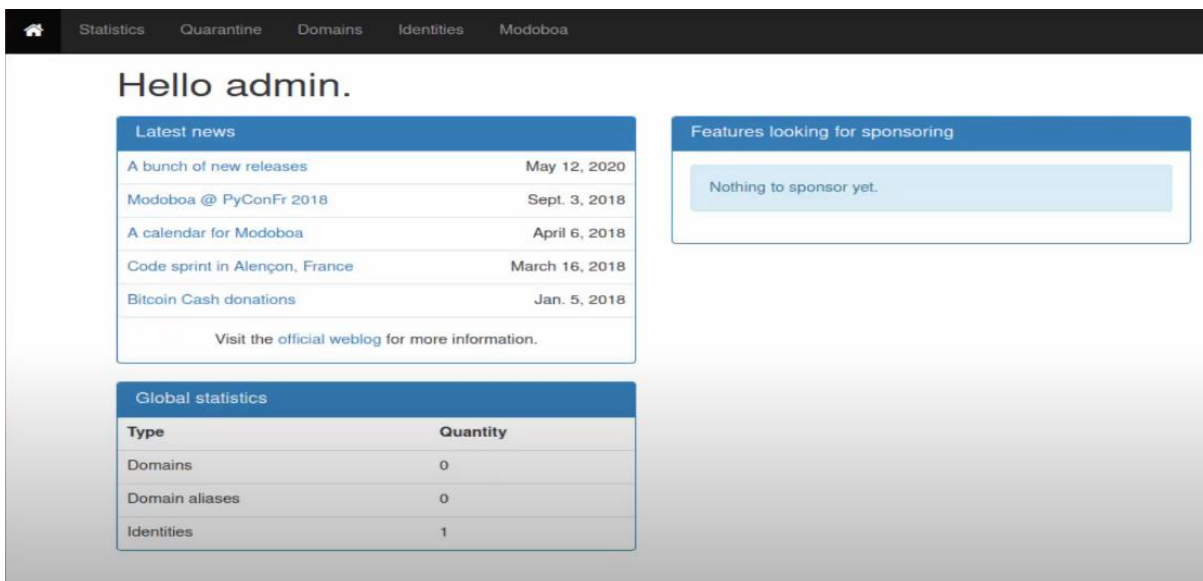
```
root@mail:~/modoboa-installer# systemctl restart nginx ; systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2022-02-07 18:47:35 PST; 7ms ago
     Docs: man:nginx(8)
   Process: 213638 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
   Process: 213640 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
   Main PID: 213641 (nginx)
    Tasks: 3 (limit: 4593)
   Memory: 3.4M
     CGroup: /system.slice/nginx.service
             └─213641 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
               └─213642 nginx: worker process
                 └─213643 nginx: worker process
```

Allez dans un navigateur web et entrez l'adresse ip du serveur modoboa puis entrez vos identifiants admin :



The image shows the Modoboa login page. At the top, the Modoboa logo (a lowercase 'm' inside a speech bubble) is next to the text 'modoboa' and 'mail hosting made simple'. Below this, there are two input fields: 'Username' and 'Password'. The 'Username' field has a cursor inside it. Below the 'Password' field is a checkbox labeled 'Remember me'. To the right of the 'Remember me' checkbox is a link that says 'Forgot password?'. At the bottom left, there is a blue button labeled 'Log in'.

Vous êtes maintenant dans Modoboa.



The image shows the Modoboa admin dashboard. At the top, there is a navigation bar with a home icon and links to 'Statistics', 'Quarantine', 'Domains', 'Identities', and 'Modoboa'. Below the navigation bar, the main content area starts with 'Hello admin.'. There are three main sections: 'Latest news', 'Global statistics', and 'Features looking for sponsoring'. The 'Latest news' section contains a table of recent news items. The 'Global statistics' section contains a table showing the quantity of domains, domain aliases, and identities. The 'Features looking for sponsoring' section contains a message that says 'Nothing to sponsor yet.'.

Type	Quantity
Domains	0
Domain aliases	0
Identities	1

Configuration d'Asterisk



09/04/2025

1) Installation d'Asterisk

L'installation et la configuration d'Asterisk se fera sur le même serveur ubuntu que Modoboa, donc pas besoin de montrer comment configurer le serveur.

A) Mise à jour du serveur + installations des dépendances requises

Mettre à jour le serveur avec cette commande.

```
hollo@hollo:~$ sudo apt update && sudo apt upgrade -y_
```

Installer les dépendances avec cette commande.

```
hollo@hollo:~$ sudo apt install build-essential git curl wget subversion libncurses5-dev libxml2-dev  
libsqlite3-dev uuid-dev libjansson-dev libssl-dev -y
```

B) Téléchargement et pré-installation de Asterisk

Accéder au répertoire `/usr/src`.

```
hollo@hollo:~$ cd /usr/src  
hollo@hollo:/usr/src$
```

Télécharger le paquet de Asterisk via le site web officiel.

```
hollo@hollo:/usr/src$ sudo wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-20-current.tar.gz
```

L'installation n'est pas très longue.

```
--2025-04-12 14:12:47-- http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-20-current.tar.gz
Resolving downloads.asterisk.org (downloads.asterisk.org)... 2604:a880:400:d0::14:9001, 165.22.184.19
Connecting to downloads.asterisk.org (downloads.asterisk.org)|2604:a880:400:d0::14:9001|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 28412463 (27M) [application/octet-stream]
Saving to: 'asterisk-20-current.tar.gz'

asterisk-20-current.tar. 22%[=====>] 6,05M 479KB/s eta 26s _
```

Extraire le paquet téléchargé dans le répertoire.

```
hollo@hollo:/usr/src$ sudo tar xvf asterisk-20-current.tar.gz
```

Accéder au répertoire de Asterisk.

```
hollo@hollo:/usr/src$ cd asterisk-20.13.0/
```

Démarrer la pré-installation de Asterisk en effectuant ces 2 commandes.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo contrib/scripts/install_prereq install
```

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo ./configure_
```

Effectuer cette commande.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo make menuselect
```

Une fois sur cette partie cliquer sur la touche S puis Q. Il n'y a aucune modification à apporter.

```
*****
Asterisk Module and Build Option Selection
*****

Press 'h' for help.

---> Add-ons (See README-addons.txt)
    Applications
    Bridging Modules
    Call Detail Recording
    Channel Event Logging
    Channel Drivers
    Codec Translators
    Format Interpreters
    Dialplan Functions
    PBX Modules
    Resource Modules
    Test Modules
    Compiler Flags
    Utilities
    AGI Samples
    Core Sound Packages
    Music On Hold File Packages
    Extras Sound Packages
```

C) Compilation et installation de Asterisk

Effectuer cette commande.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo make -j$(nproc)_
```

Lancer cette commande.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo make install
```

Lancer cette commande.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo make samples_
```

Effectuer cette commande.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo make config
```

Lancer cette commande pour terminer l'installation de Asterisk.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo ldconfig_
```

Démarrer Asterisk.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo systemctl start asterisk
```

Activer Asterisk.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo systemctl enable asterisk
```

Vérifier si Asterisk est bien actif.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo systemctl status asterisk
• asterisk.service - LSB: Asterisk PBX
   Loaded: loaded (/etc/init.d/asterisk; generated)
   Active: active (running) since Sat 2025-04-12 14:48:55 UTC; 49s ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 66 (limit: 4519)
   Memory: 38.9M
      CPU: 2.636s
   CGroup: /system.slice/asterisk.service
           └─59527 /usr/sbin/asterisk

avril 12 14:48:55 hollo systemd[1]: Starting LSB: Asterisk PBX...
avril 12 14:48:55 hollo asterisk[59514]: * Starting Asterisk PBX: asterisk
avril 12 14:48:55 hollo asterisk[59514]:    ...done.
avril 12 14:48:55 hollo systemd[1]: Started LSB: Asterisk PBX.
hollo@hollo:/usr/src/asterisk-20.13.0$ _
```

Accéder à la console de Asterisk pour voir si ça fonctionne.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo asterisk -rvv
```

Si ceci s'affiche, Asterisk s'est bien installé.

```
Asterisk 20.13.0, Copyright (C) 1999 - 2025, Sangoma Technologies Corporation and others.  
Created by Mark Spencer <markster@digium.com>  
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.  
This is free software, with components licensed under the GNU General Public  
License version 2 and other licenses; you are welcome to redistribute it under  
certain conditions. Type 'core show license' for details.  
=====
```

```
Connected to Asterisk 20.13.0 currently running on hollo (pid = 59527)  
hollo*CLI>
```

Faire exit pour quitter la console Asterisk.

```
hollo*CLI> exit
Asterisk cleanly ending (0).
Executing last minute cleanups
hollo@hollo:/usr/src/asterisk-20.13.0$ _
```

2) Configuration des utilisateurs SIP pour le softphone

Accéder au fichier de configuration pjsip.conf.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo nano /etc/asterisk/pjsip.conf
```

Chercher cette partie, il faut la modifier.

```
; Basic UDP transport
;
;[transport-udp]
;type=transport
;protocol=udp      ;udp,tcp,tls,ws,wss,flow
;bind=0.0.0.0
```

Voici le rendu final pour que le transport UDP fonctionne.

```
; Basic UDP transport
;
[transport-udp]
type=transport
protocol=udp      ;udp,tcp,tls,ws,wss,flow
bind=0.0.0.0
```

Descendre tout en bas du fichier pour ajouter un nouvel utilisateur SIP.

Voici un exemple de configuration pour un utilisateur (1001 ici).

```
[1001]
type=endpoint
context=internal
disallow=all
allow=ulaw
auth=auth1001
aors=1001

[auth1001]
type=auth
auth_type=userpass
username=1001
password=p@ssw0rd

[1001]
type=aor
max_contacts=1
```

Créer un deuxième utilisateur (1002 par exemple) afin de réaliser des tests plus tard.

Faire Ctrl + X, puis Y et Enter pour quitter et sauvegarder le fichier.

Accéder au fichier du plan de numérotation.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo nano /etc/asterisk/extensions.conf
```

Ajouter ces lignes à la fin du fichier puis quitter et sauvegarder.

```
[internal]
exten => 1001,1,Dial(PJSIP/1001)
exten => 1002,1,Dial(PJSIP/1002)
```

Redémarrer Asterisk.

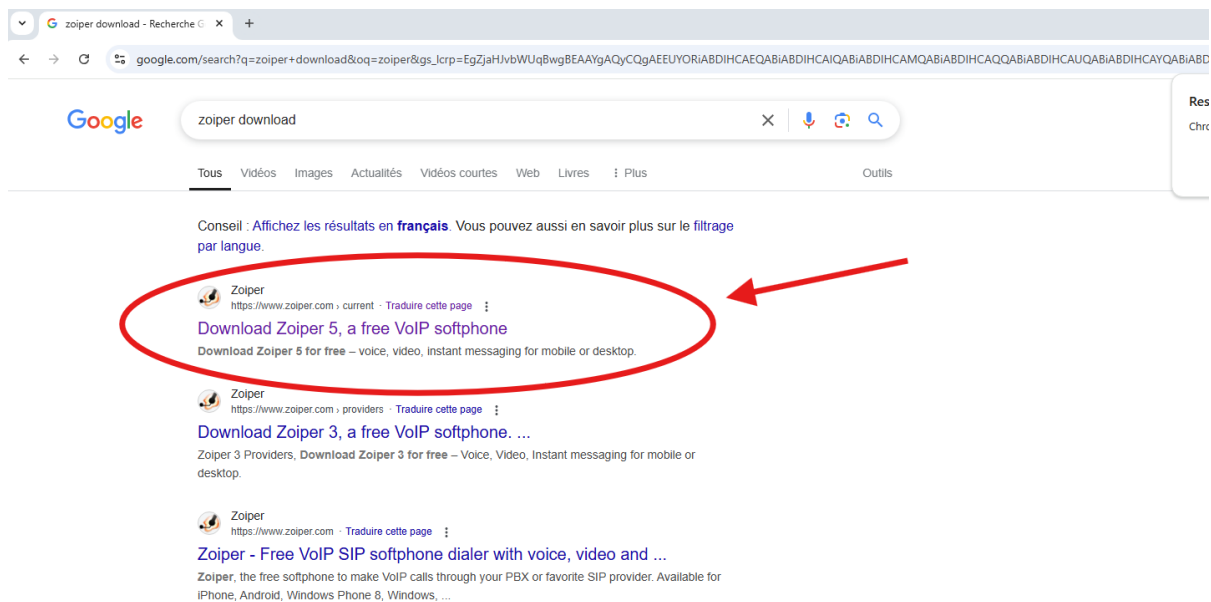
```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo systemctl restart asterisk
```

3) Installation et configuration d'un client Softphone

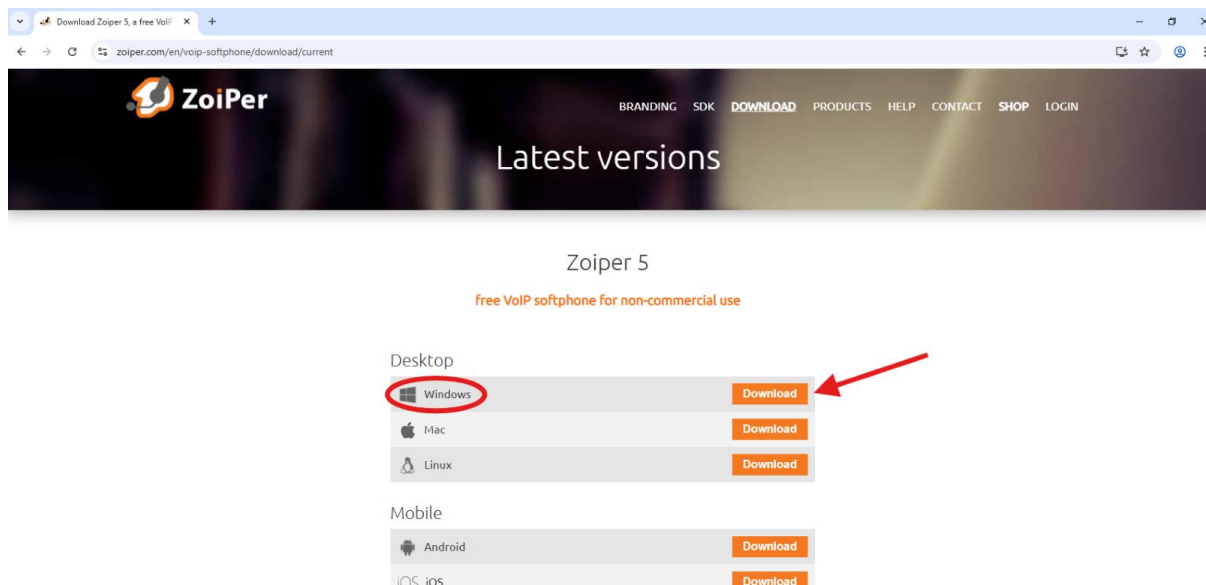
Accéder à une machine Windows Client connectée au domaine.

Nous allons installer Zoiper, un client Softphone très fiable et répandu.

Rechercher Zoiper download et accéder au premier lien.



Choisir la version Windows.

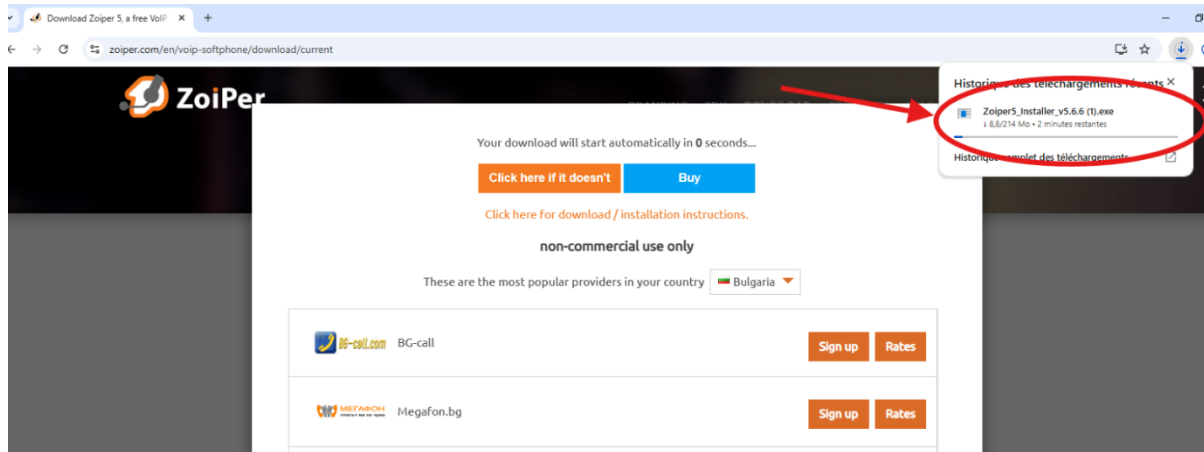


Dans le cadre du projet, choisir la version gratuite.

The screenshot shows the iPer pricing page with three plans. The 'Free' plan is highlighted with a red circle and arrow. The 'Premium' plan is highlighted with an orange border. The 'Custom' plan is highlighted with a light gray background.

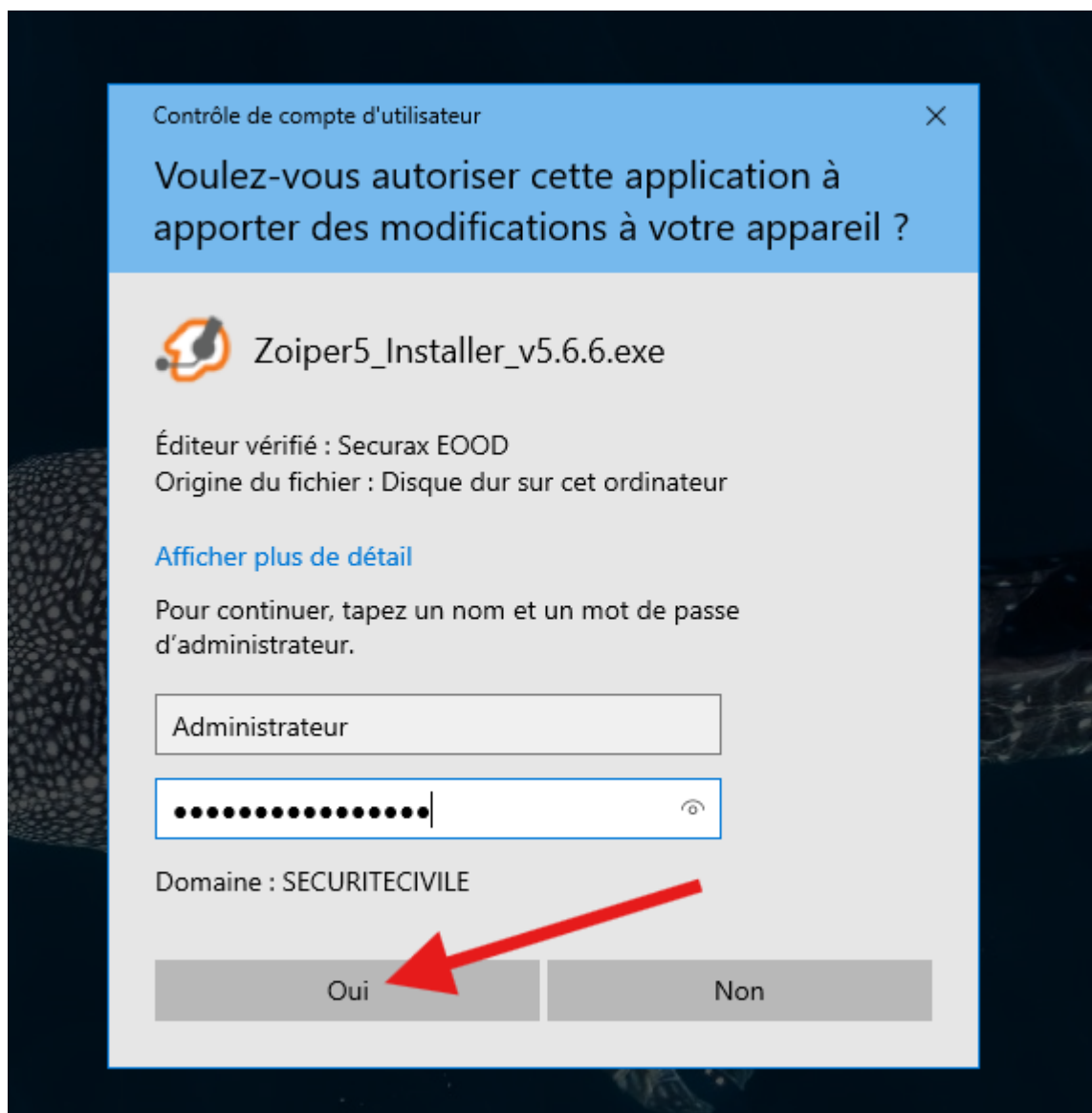
Free €0	Premium €59.95	Custom On demand
		
Download	Purchase	Contact us
Basic functionality for occasional use non-commercial use only • Basic functionality	Business functionality for the power user • Auto Provisioning • Contacts integration (Outlook, LDAP, Thunderbird, Mac OS X, Windows) • Browser integration (click to dial, open url) • Better quality/Lower bandwidth (G.729/H.264 codecs) • Business features (transfer, conferencing)	Fully customized solutions according to your specs • Your design • Your feature set • Locked to your service • Branded with your name and logo • Balance display

L'installation se lancera tout seul, attendre la fin.



Une fois installer, lancer le programme d'installation de Zoiper.

Entrer les droits admins puis cliquer sur OUI.



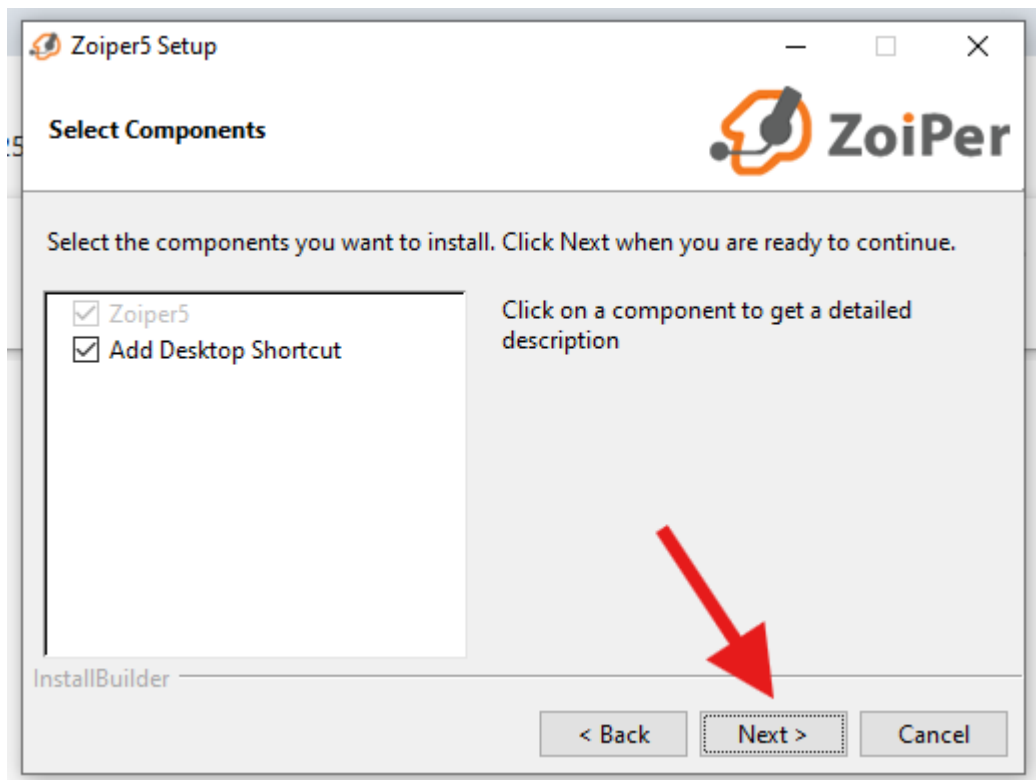
Cliquer sur Next.



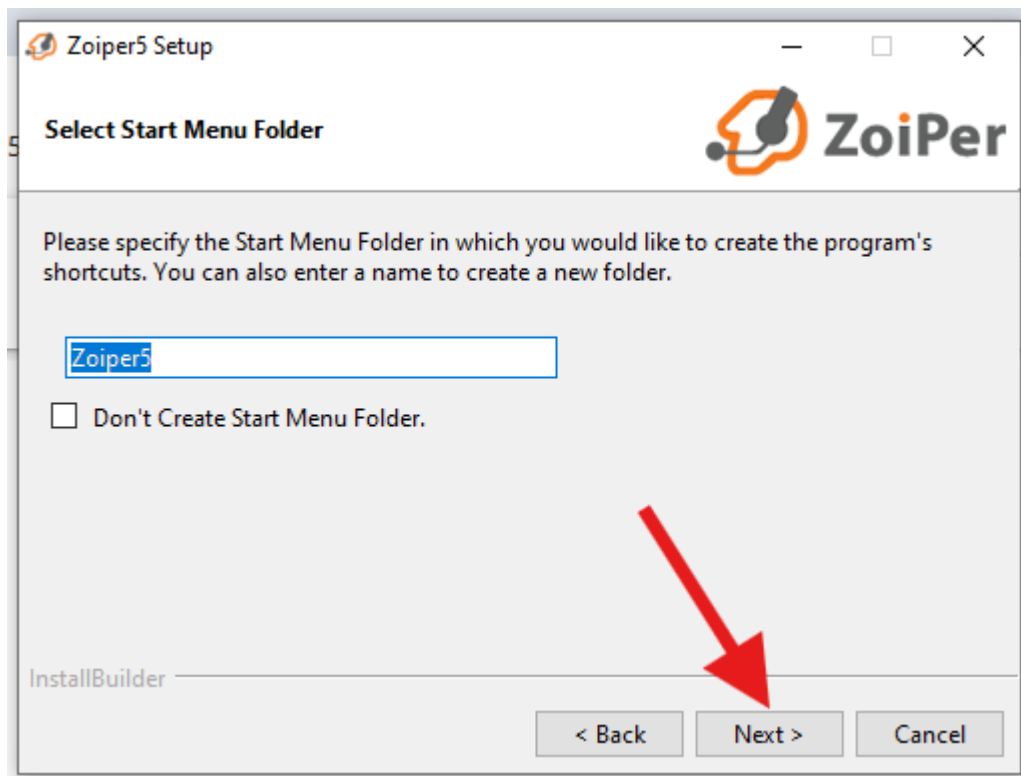
Accepter les termes de licence puis cliquer sur Next.



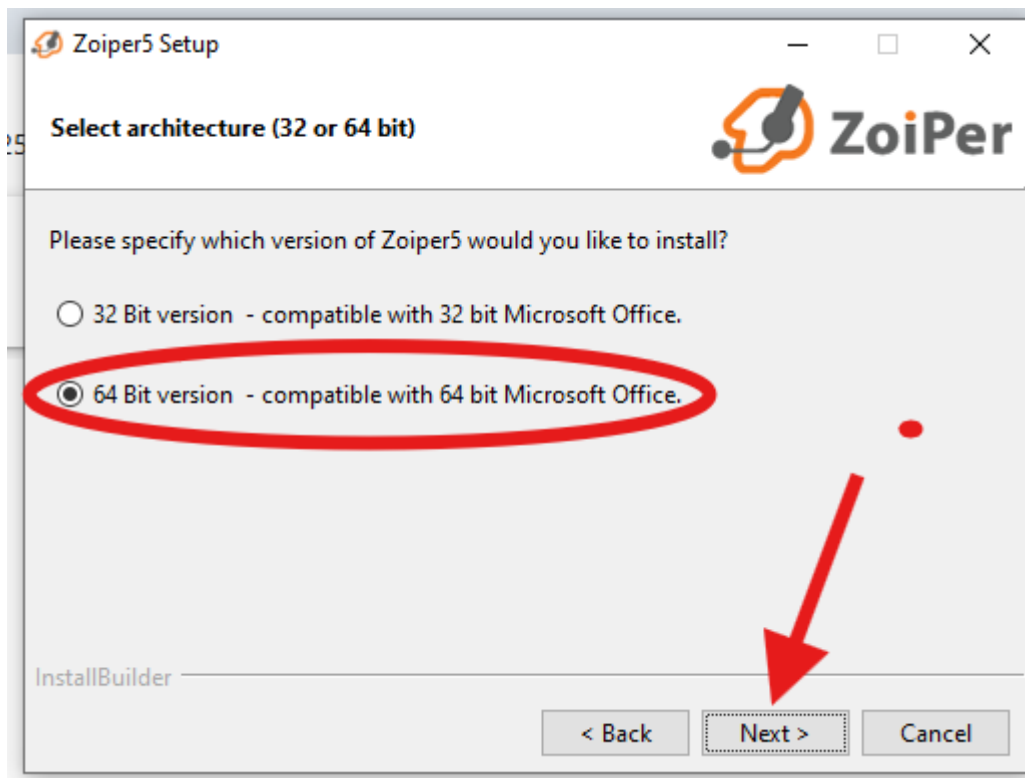
Cliquer sur Next.



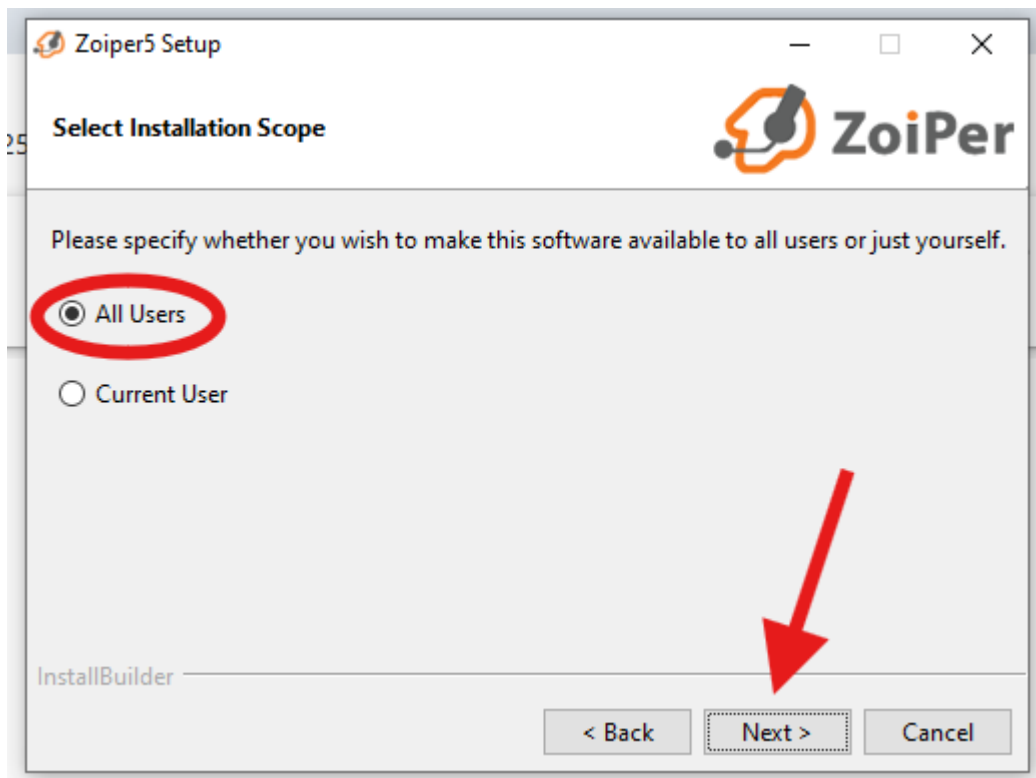
Cliquer sur Next.



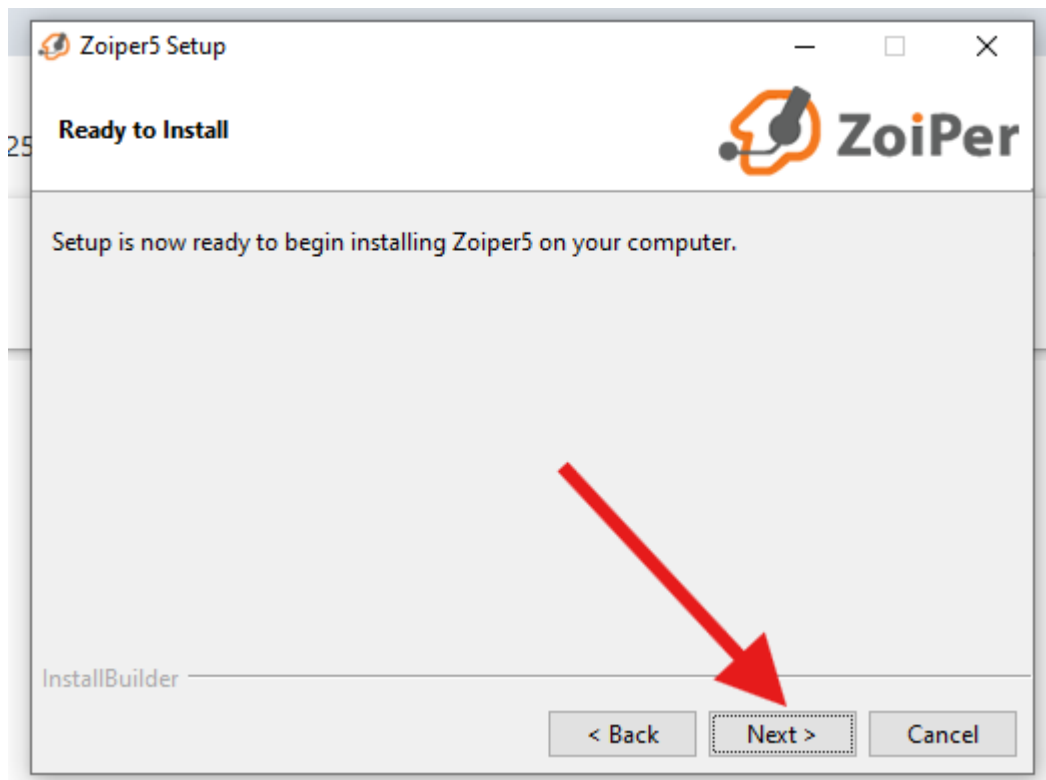
Sélectionner la version 64-bit et cliquer sur Next.



Sélectionner All Users et cliquer sur Next.



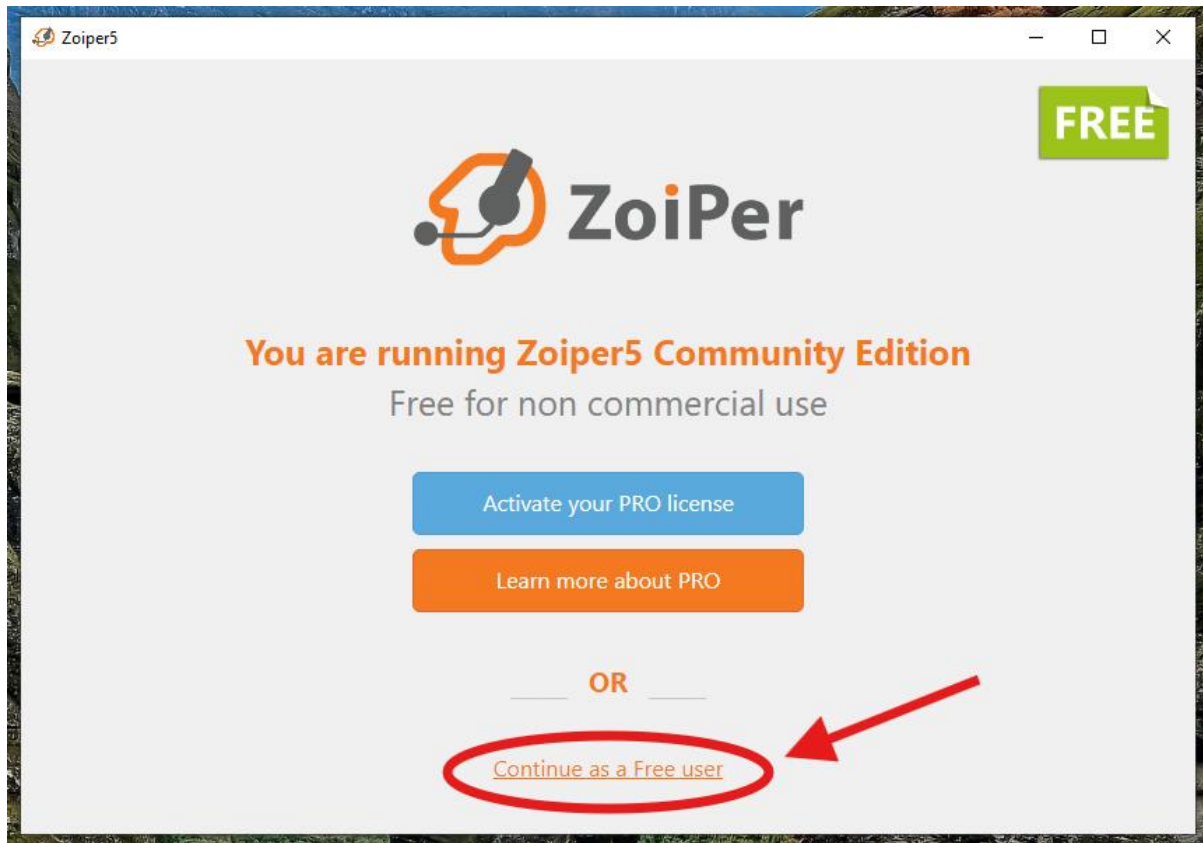
Cliquer sur Next.



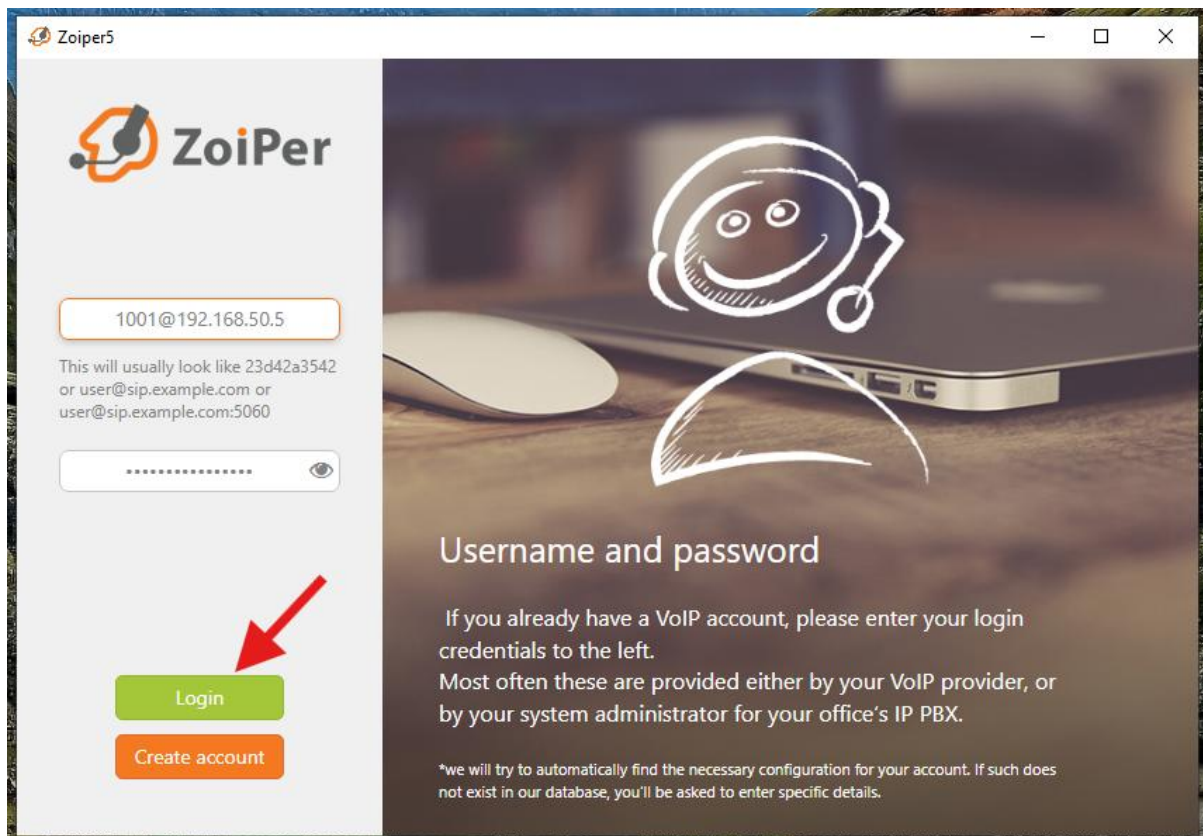
Attendre la fin de l'installation et cliquer sur Finish.



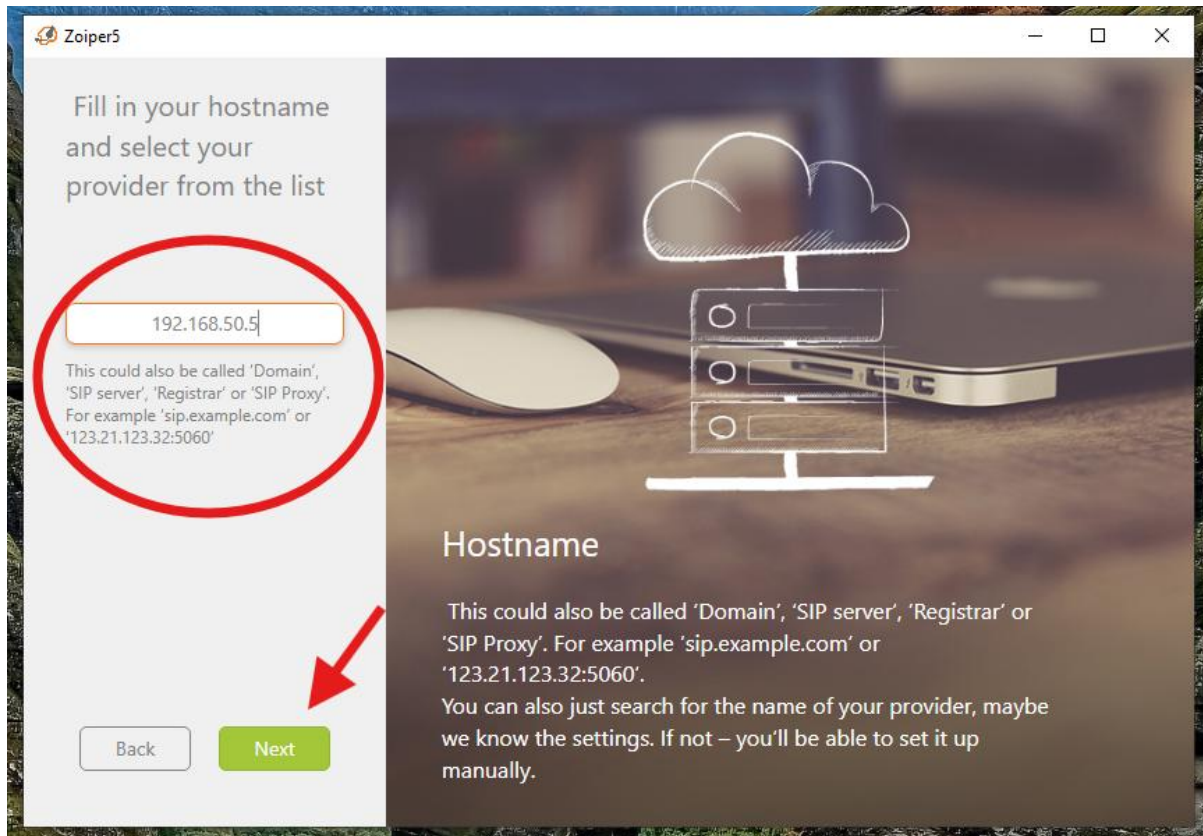
Ouvrir Zoiper et cliquer sur Continue as a Free user.



Se connecter en entrant le nom d'utilisateur (1001 par exemple) suivi de @192.168.50.5 (adresse IP du serveur Ubuntu). Rentrer aussi le mot de passe puis cliquer sur Login.

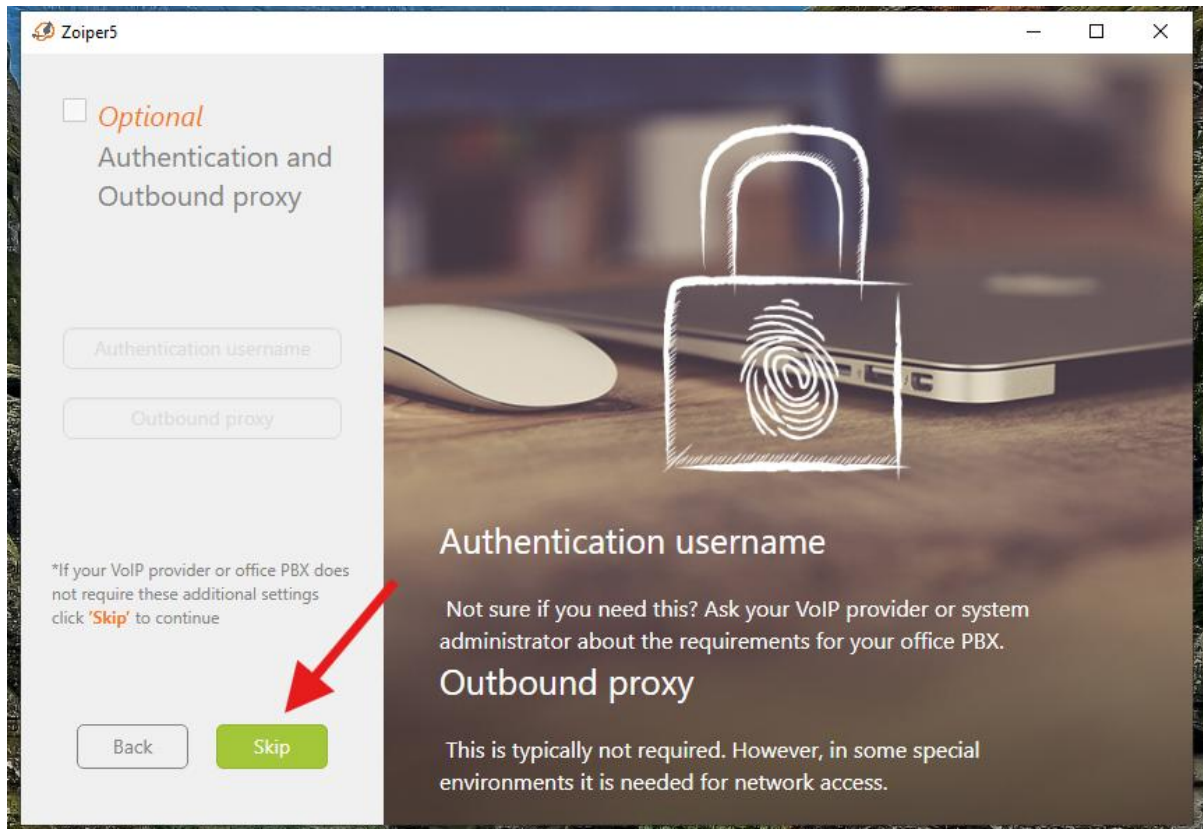


Rentrer à nouveau l'IP du serveur puis cliquer sur Next.

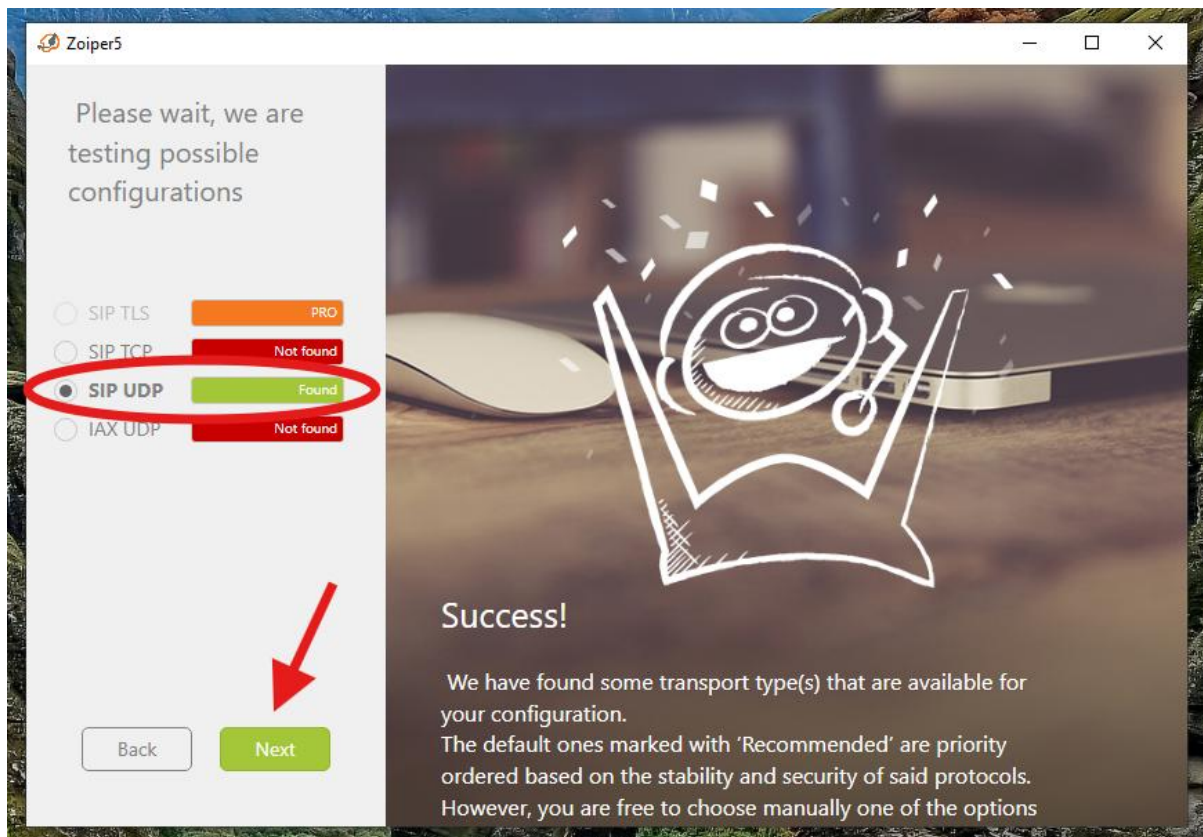


The screenshot shows the Zoiper5 installation window. On the left, a light gray sidebar contains the text "Fill in your hostname and select your provider from the list". Below this, a text input field contains "192.168.50.5" and is circled in red. Underneath the input field, smaller text explains: "This could also be called 'Domain', 'SIP server', 'Registrar' or 'SIP Proxy'. For example 'sip.example.com' or '123.21.123.32:5060'". At the bottom of the sidebar are "Back" and "Next" buttons. A red arrow points from the "Next" button towards the right panel. The right panel has a dark background with a white line-art illustration of a cloud connected to three server racks. Below the illustration, the heading "Hostname" is followed by the same explanatory text as in the sidebar. At the bottom of the right panel, it says: "You can also just search for the name of your provider, maybe we know the settings. If not – you'll be able to set it up manually."

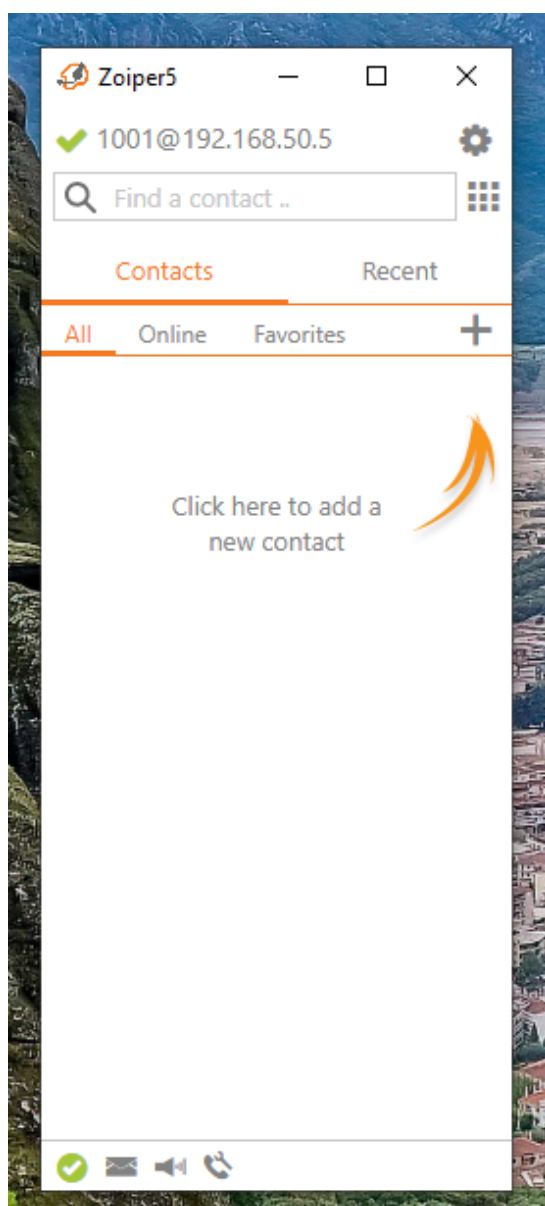
Cliquer sur Skip.



Sélectionner UDP pour le transfert et cliquer sur Next.



Nous avons réussi à nous connecter au compte SIP que l'on a créé avant.

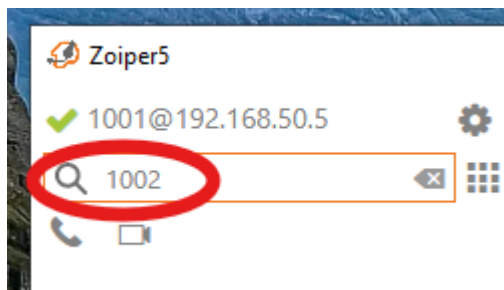


4) Tests

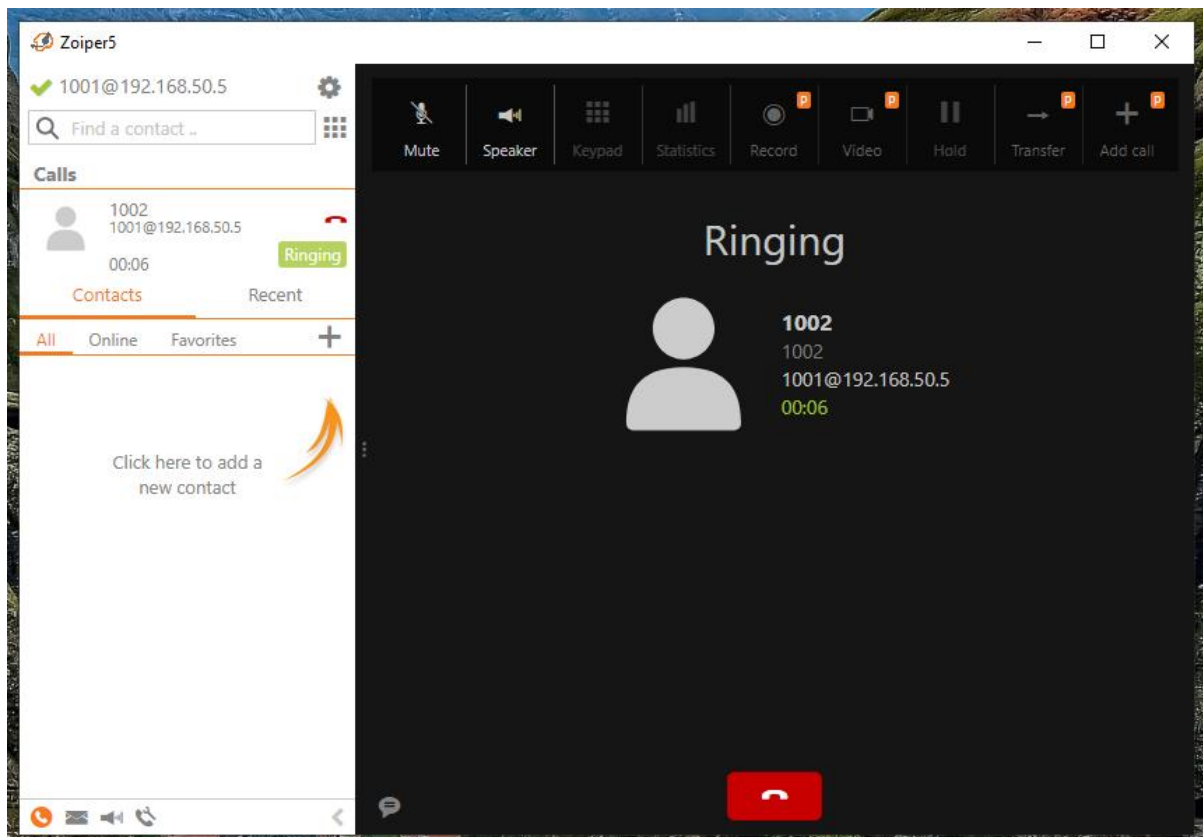
Sur un deuxième client Windows connecté au domaine, installer à nouveau Zoiper et se connecter avec le 2ème compte créé avant (1002 dans mon cas).

Essayer d'appeler 1002 sur le client Windows (sur le client Windows avec l'utilisateur 1001).

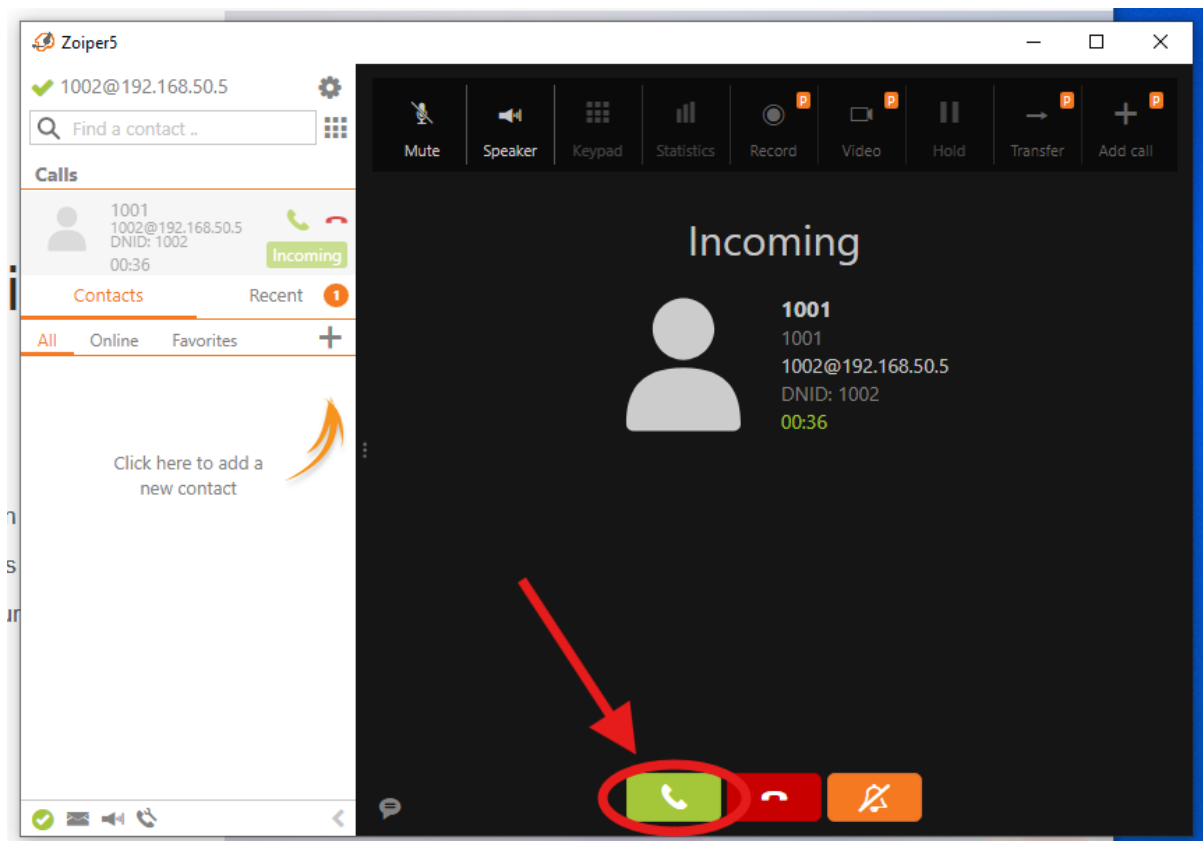
Rechercher 1002 puis cliquer sur Enter.



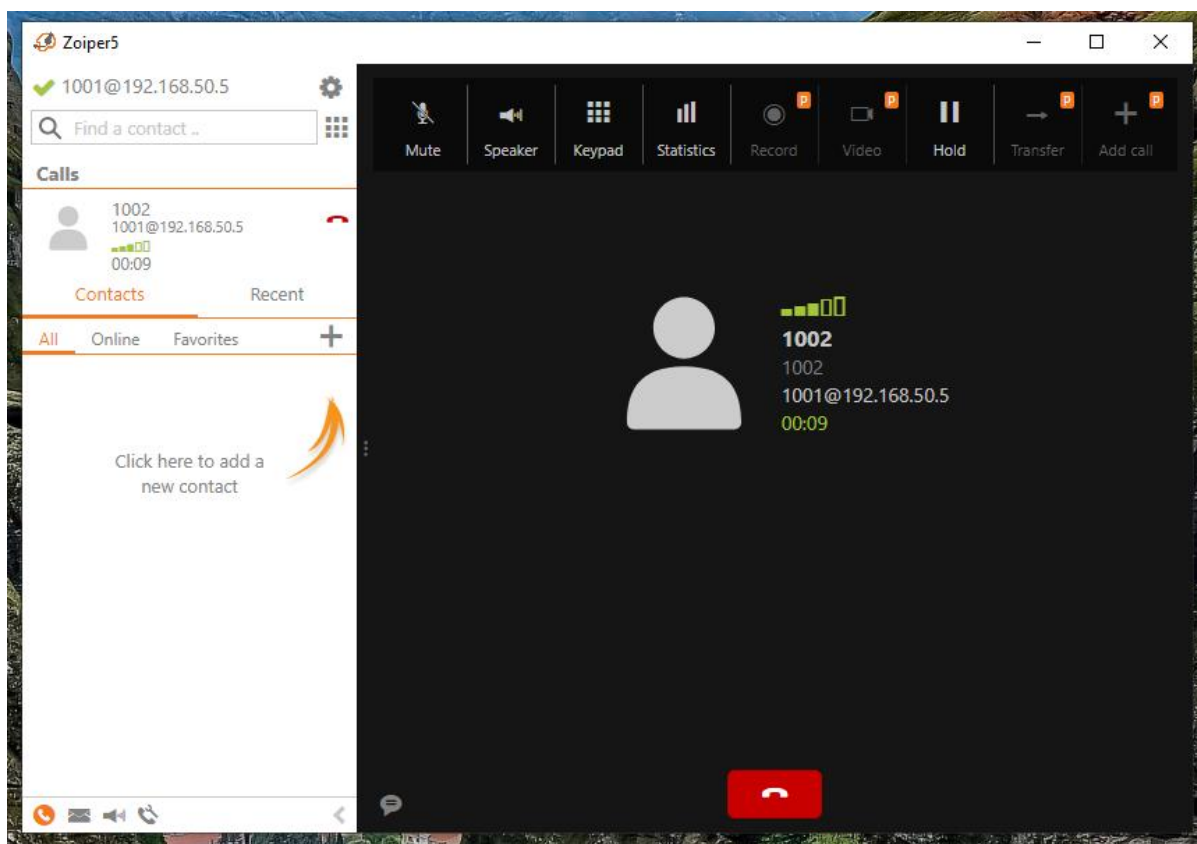
Le téléphone sonne bien.



Sur le deuxième client, décrocher en appuyant sur l'icône de téléphone vert.



Les appels fonctionnent.



Configuration de eBrigade + DMZ

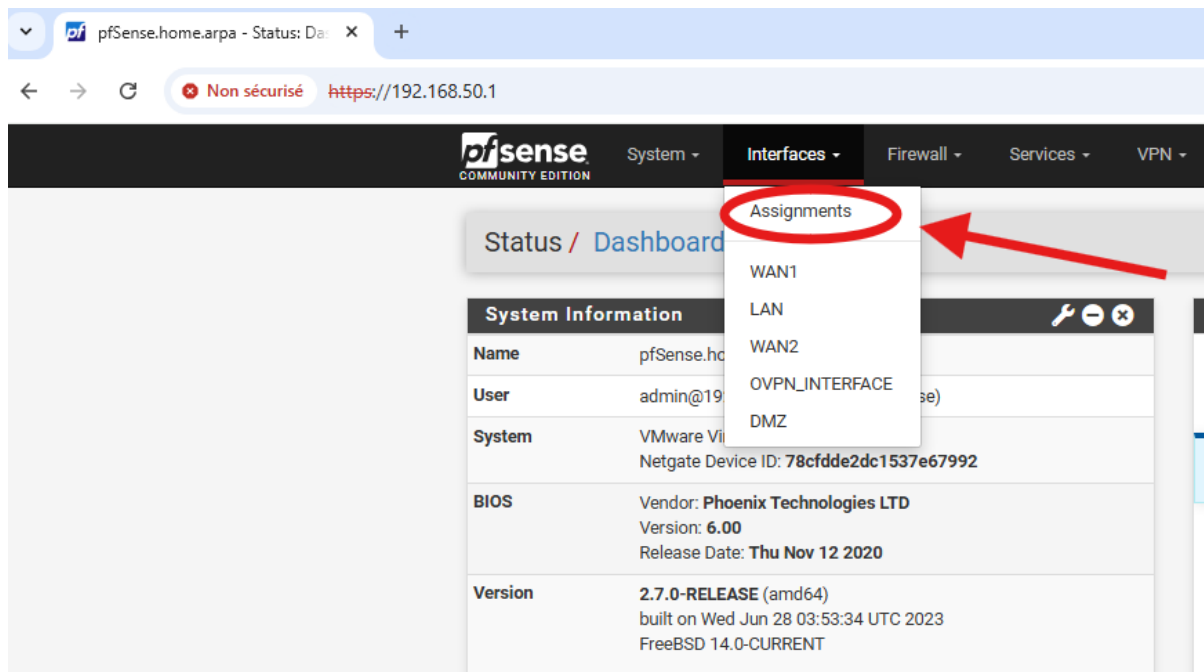


09/04/2025

1) Configuration de l'interface DMZ sur les routeurs

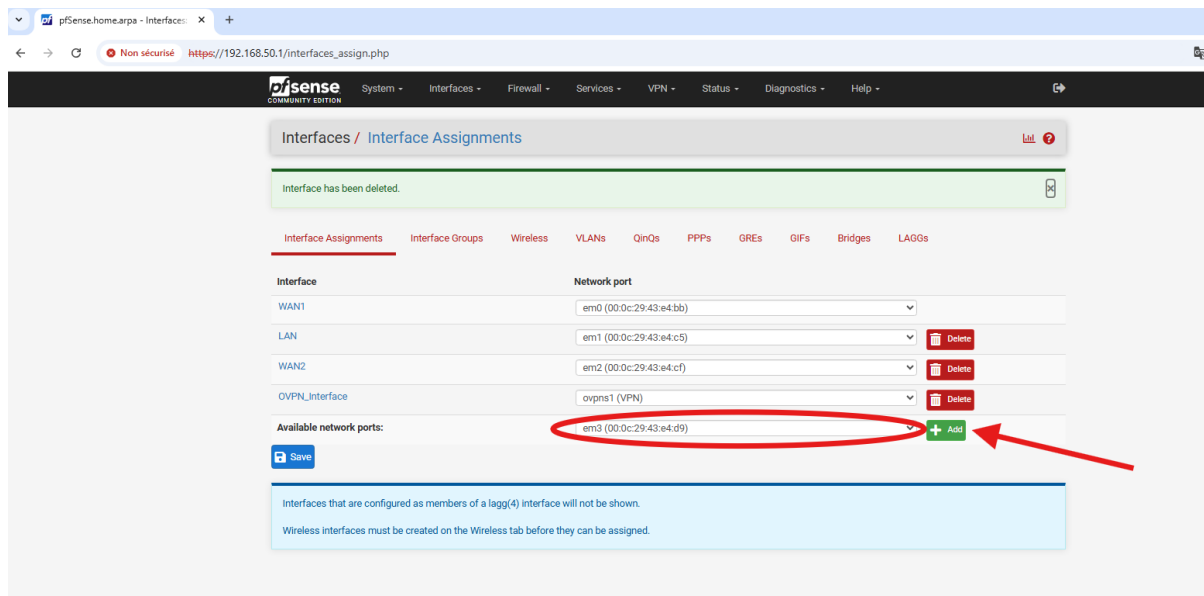
Après avoir ajouté une nouvelle carte réseau en host-only sur nos deux routeurs (avec une plage d'adresse différente de celle des LAN), on peut configurer l'interface DMZ.

Sur l'interface web de PfSense, aller dans Interfaces puis Assignments.



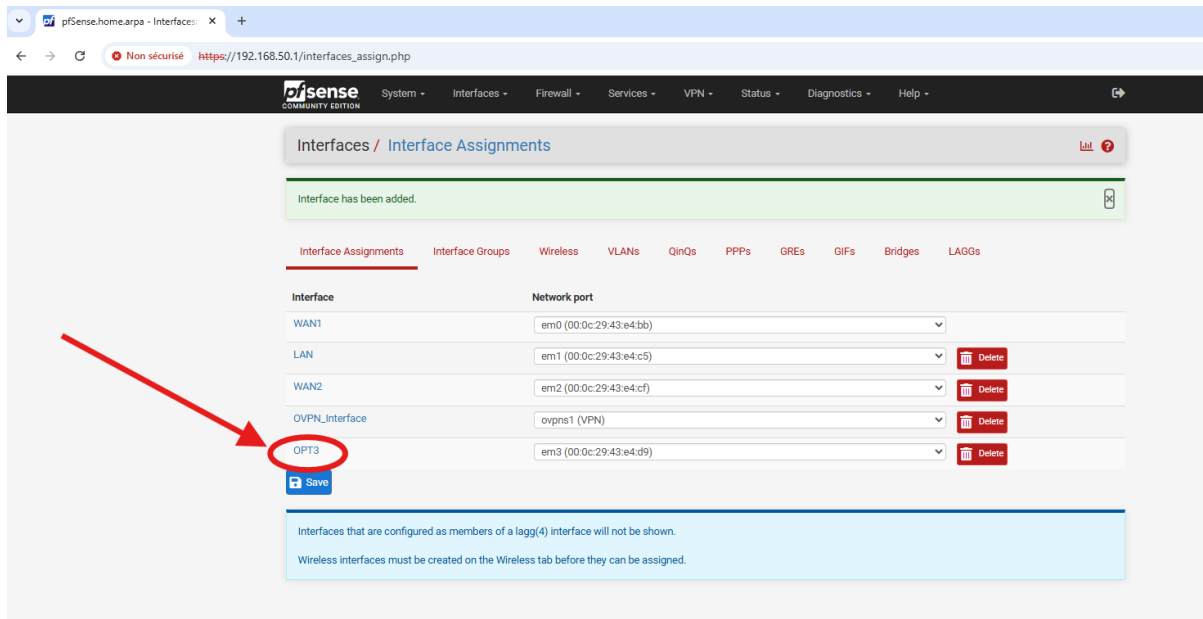
On peut voir qu'une interface est libre et prête à être configurée : c'est la carte réseau qui a été ajoutée.

Cliquer sur Add.



La nouvelle interface a été créée et s'appelle OPT3.

Cliquer dessus pour la configurer.



Activer l'interface en cochant enable, renommer l'interface en "DMZ", choisir Static IPv4 Pour la configuration IPv4, et entrer une adresse sur la plage de la nouvelle carte réseau (dans mon cas 192.168.200.0, j'ai mis 192.168.200.251).

Interfaces / OPT3 (em3)  

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: xxxxxxxxxx:xx:xx or leave blank.

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

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

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

Static IPv4 Configuration

IPv4 Address / 

IPv4 Upstream gateway 

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.

Une fois les paramètres rentrés, cliquer sur Save.

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

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).
Gateways can be managed by [clicking here](#).

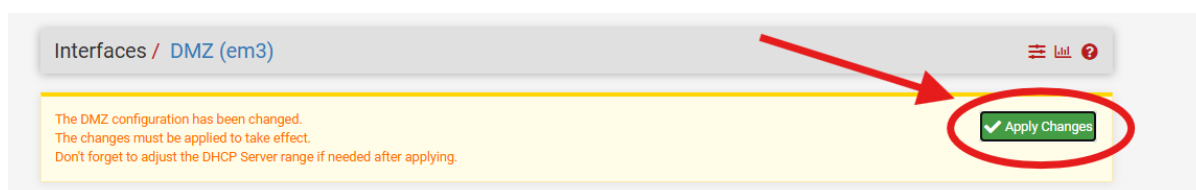
Reserved Networks

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

Block bogon networks ☐
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

[Save](#)

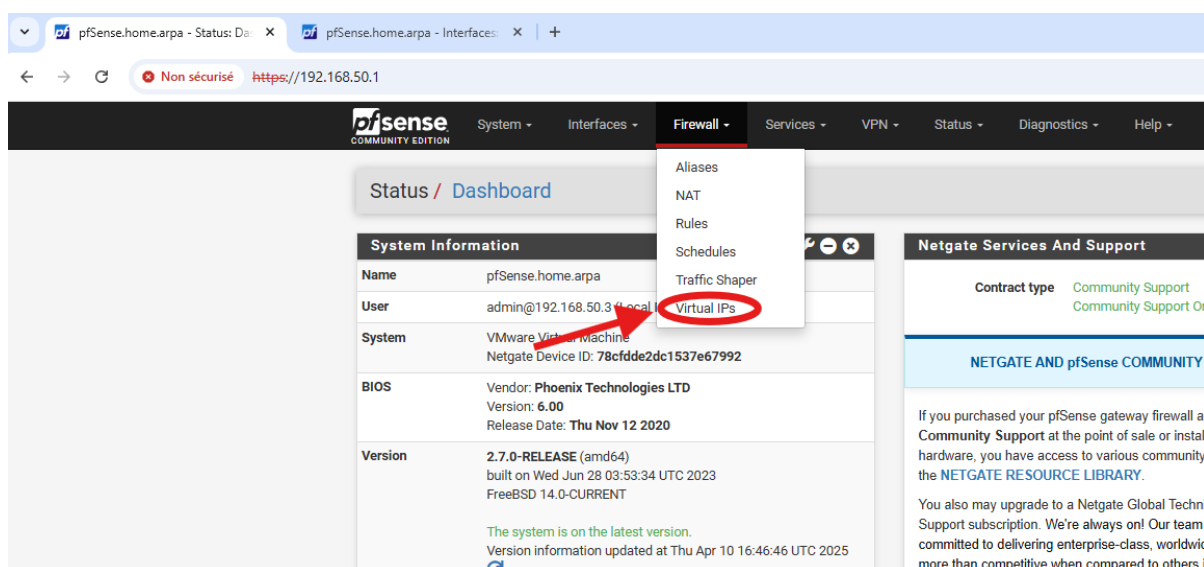
Cliquer sur Apply Changes pour appliquer les changements.



Il faut réaliser la même opération sur le PfSense Backup en rentrant une autre adresse IPv4 (192.168.200.252 dans mon cas).

Ensuite il faut configurer un CARP DMZ, de cette façon si le routeur Master tombe, notre DMZ sera toujours disponible via le routeur Backup.

Aller dans Firewall puis Virtual IPs.



Cliquer sur Add.

Firewall / Virtual IPs

Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
192.168.50.254/24 (vhid: 1)	LAN	CARP	CARP	 
192.168.1.140/24 (vhid: 10)	WAN1	CARP	CARP WAN1	 
192.168.1.141/24 (vhid: 20)	WAN2	CARP	CARP WAN2	 
192.168.200.254/24 (vhid: 30)	DMZ	CARP	DMZ	 

  Add

Voici les paramètres à rentrer (l'adresse est à ajuster en fonction de votre plage IP).
Mettre aussi un VHID Group différent des autres IP virtuelles déjà présentes.

Une fois tous les paramètres remplis cliquer sur Save.

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type ☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface DMZ

Address type Single address

Address(es) 192.168.200.254 / 24

Virtual IP Password Enter the VHID group password. Confirm

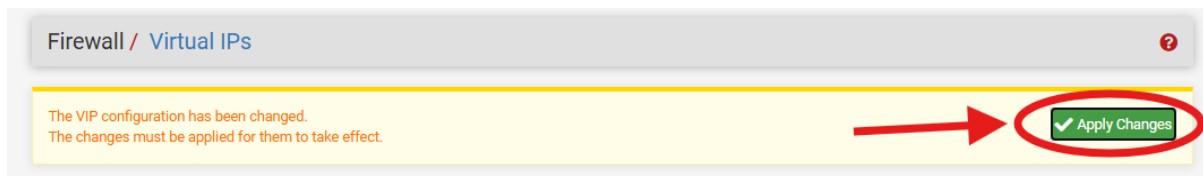
VHID Group 30

Advertising frequency Base: 1, Skew: 0

Description DMZ

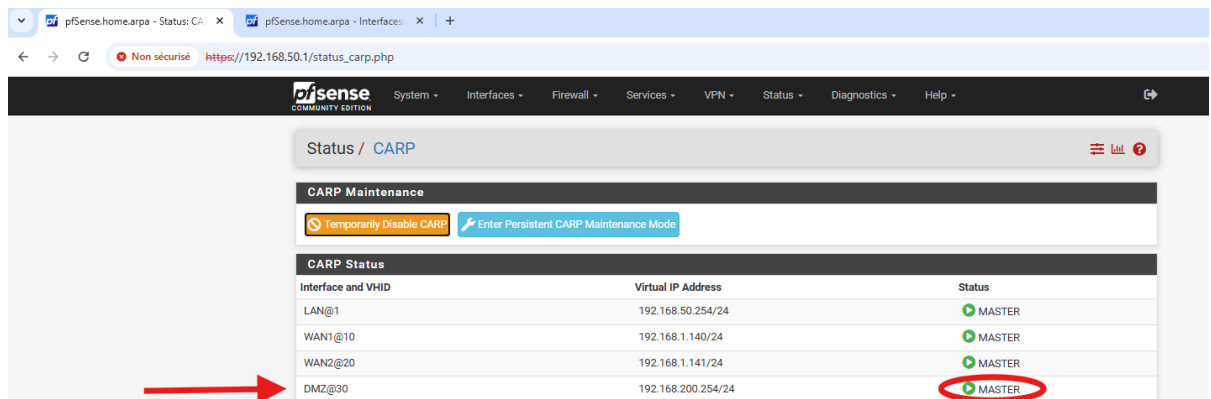
Save

Cliquer sur Apply Changes pour appliquer les changements.

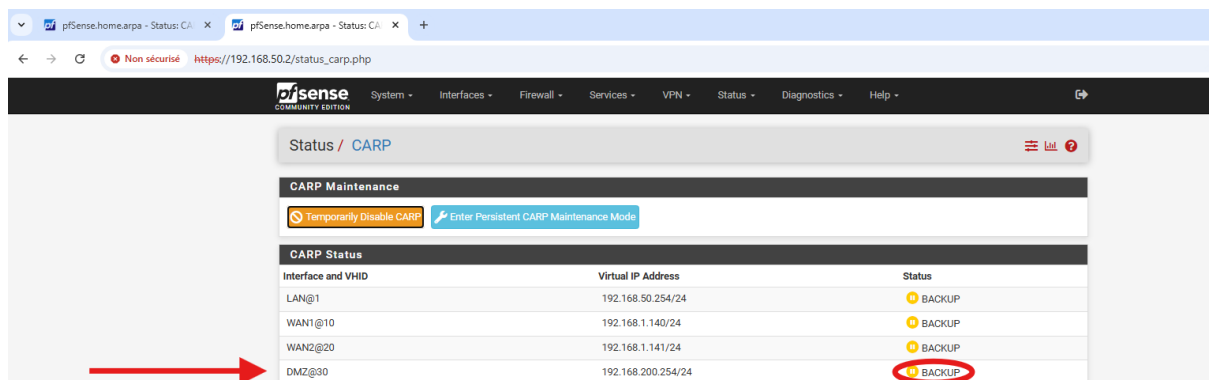


Si l'on va dans Status puis CARP (failover), on peut voir que :

- Sur le PfSense Master le CARP DMZ est bien en MASTER.



- Sur le PfSense Backup le CARP DMZ est bien en BACKUP.



La DMZ est bien configuré (nous reviendrons sur les règles de pare-feu plus tard).

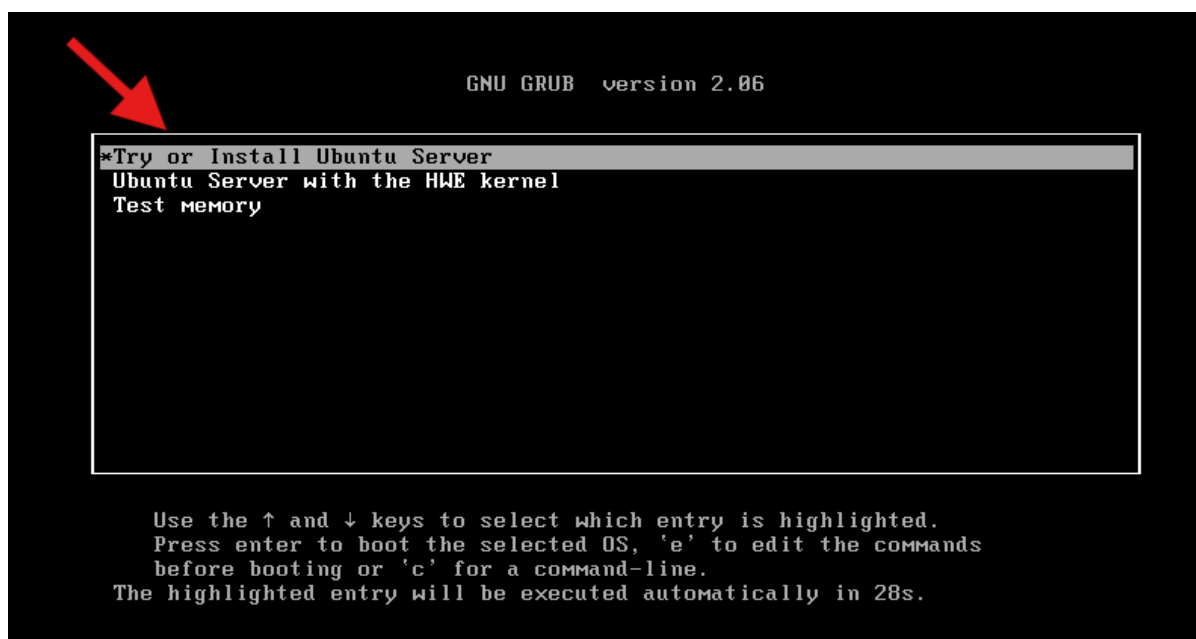
2) Configuration du serveur Ubuntu hébergeant eBrigade

A) Initialisation du serveur Ubuntu

L'installation et la configuration de eBrigade doit se faire sur un serveur différent de celui hébergeant déjà Modoboa et Asterisk.

Avant de lancer le serveur, configurer une carte réseau en host-only ayant la même plage IP que celle de l'interface DMZ sur les deux routeurs.

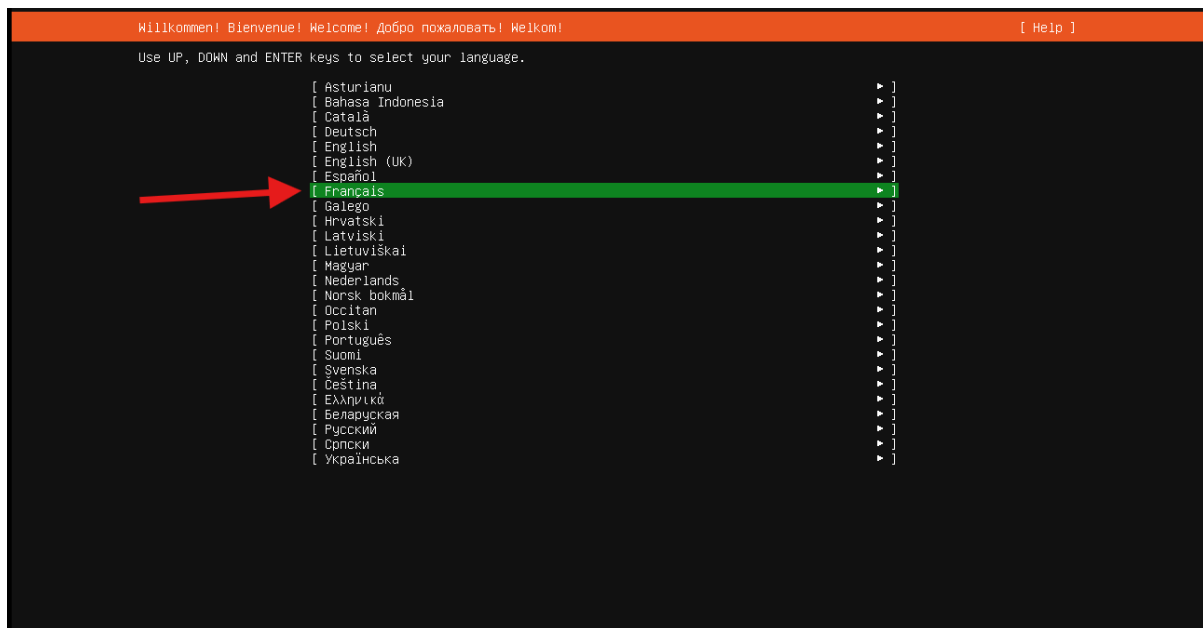
Une fois le serveur lancé, appuyer Enter sur l'option Try or Install Ubuntu Server.



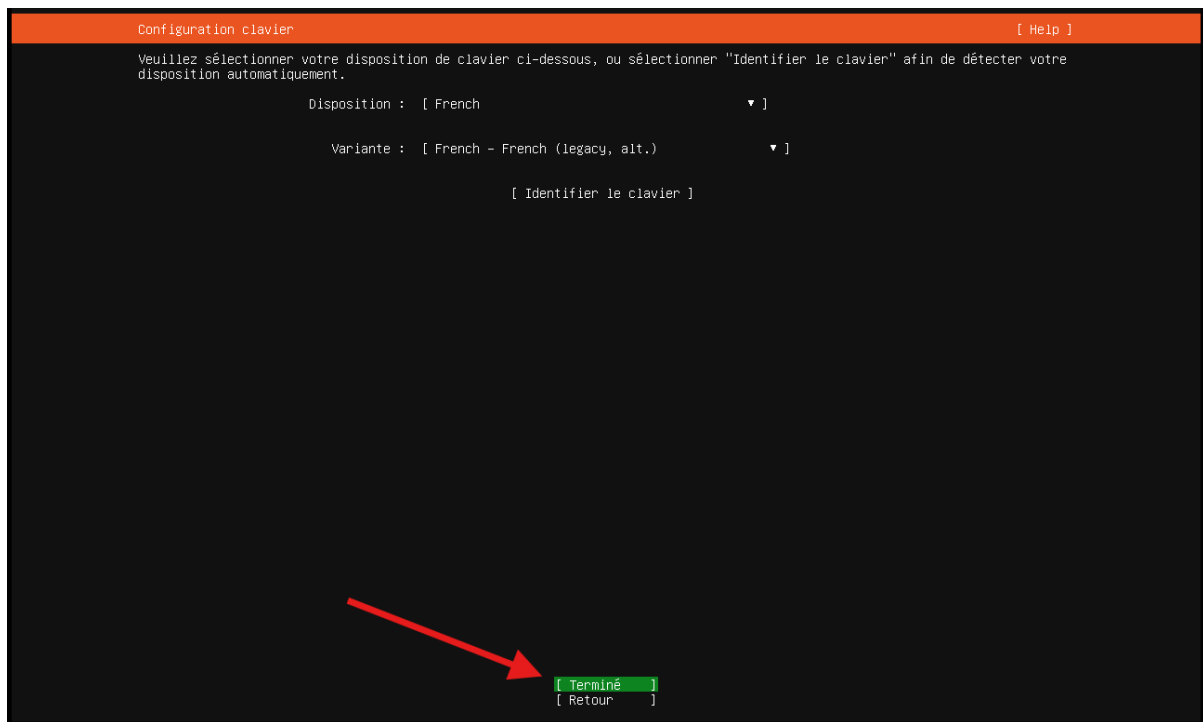
Attendre jusqu'à la prochaine étape.

```
[ OK ] Reached target Preparation for Remote File Systems.
[ OK ] Reached target Remote File Systems.
[ OK ] Finished Availability of block devices.
[ OK ] Listening on Socket activation for snappy daemon.
[ OK ] Reached target Socket Units.
[ OK ] Reached target Basic System.
      Starting LSB: automatic crash report generation...
[ OK ] Started Regular background program processing daemon.
[ OK ] Started D-Bus System Message Bus.
[ OK ] Started Save initial kernel messages after boot.
      Starting Remove Stale Online ext4 Metadata Check Snapshots...
[ OK ] Reached target Login Prompts.
[ OK ] Started irqbalance daemon.
      Starting Dispatcher daemon for systemd-networkd...
      Starting Authorization Manager...
      Starting Pollinate to seed the pseudo random number generator...
      Starting System Logging Service...
[ OK ] Reached target Preparation for Logins.
      Starting Snap Daemon...
      Starting User Login Management...
      Starting Permit User Sessions...
      Starting Disk Manager...
[ OK ] Started System Logging Service.
[ OK ] Finished Permit User Sessions.
      Starting Hold until boot process finishes up...
      Starting Terminate Plymouth Boot Screen...
[ OK ] Finished Hold until boot process finishes up.
      Starting Set console scheme...
[ OK ] Finished Terminate Plymouth Boot Screen.
[ OK ] Started LSB: automatic crash report generation.
[ OK ] Finished Set console scheme.
[ OK ] Started User Login Management.
[ OK ] Started Unattended Upgrades Shutdown.
[ OK ] Started Authorization Manager.
      Starting Modem Manager...
[ OK ] Started Dispatcher daemon for systemd-networkd.
[ OK ] Finished Remove Stale Online ext4 Metadata Check Snapshots.
[ OK ] Started Modem Manager.
[ OK ] Started Disk Manager.
[ OK ] Finished Pollinate to seed the pseudo random number generator.
      Starting OpenBSD Secure Shell server...
[ OK ] Started OpenBSD Secure Shell server.
[ OK ] Started Snap Daemon.
      Starting Holds Snappy daemon refresh...
      Starting Wait until snapd is fully seeded...
[ OK ] Finished Holds Snappy daemon refresh.
[ OK ] Started snap.lxd.hook.install.b978375a-a473-4a69-8155-dca9919d5f68.scope.
```

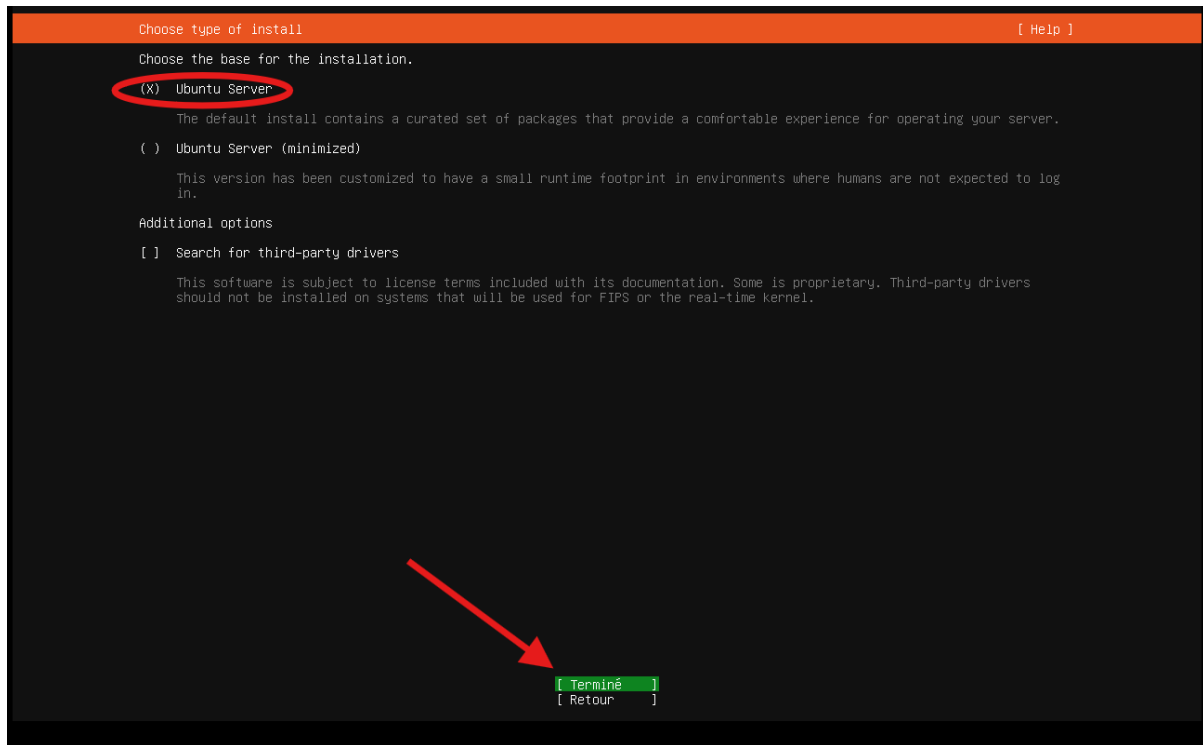
Sélectionner Français.



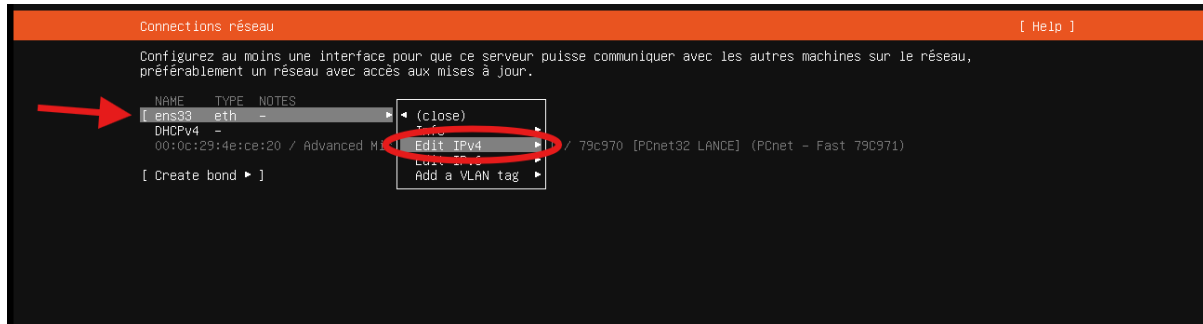
Appuyer sur Terminé.



Sélectionner Ubuntu Server et appuyer sur Terminé.



Une fois dans les paramètres réseaux, aller sur ens33 puis Edit IPv4.



Choisir Manuel.



Remplir avec ces paramètres (serveur DNS = le Windows Server GUI contrôleur de domaine). Cliquer ensuite sur Sauvegarder.

— Edit ens33 IPv4 configuration —

IPv4 Method: [Manuel ▼]

Masque de sous-réseau: 192.168.200.0/24

Adresse : 192.168.200.10

Passerelle : 192.168.200.254

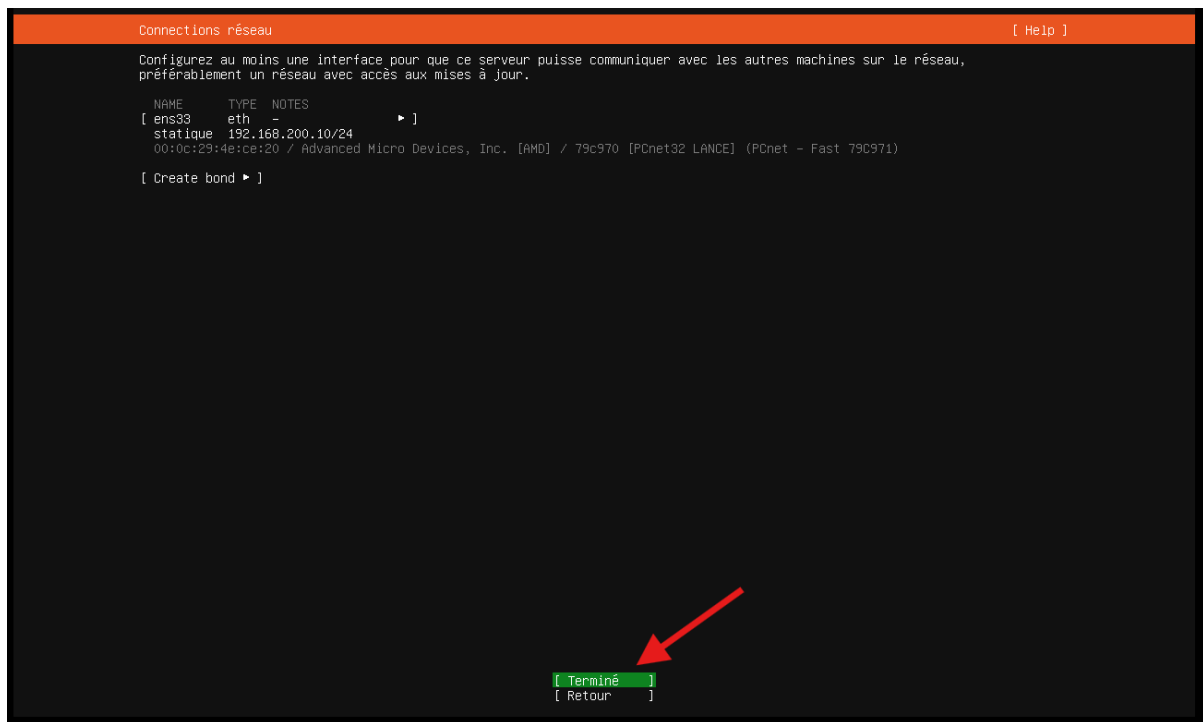
Serveurs DNS : 192.168.50.3
IP addresses, comma separated

Domaines de recherche : securitecivile.local
Domains, comma separated

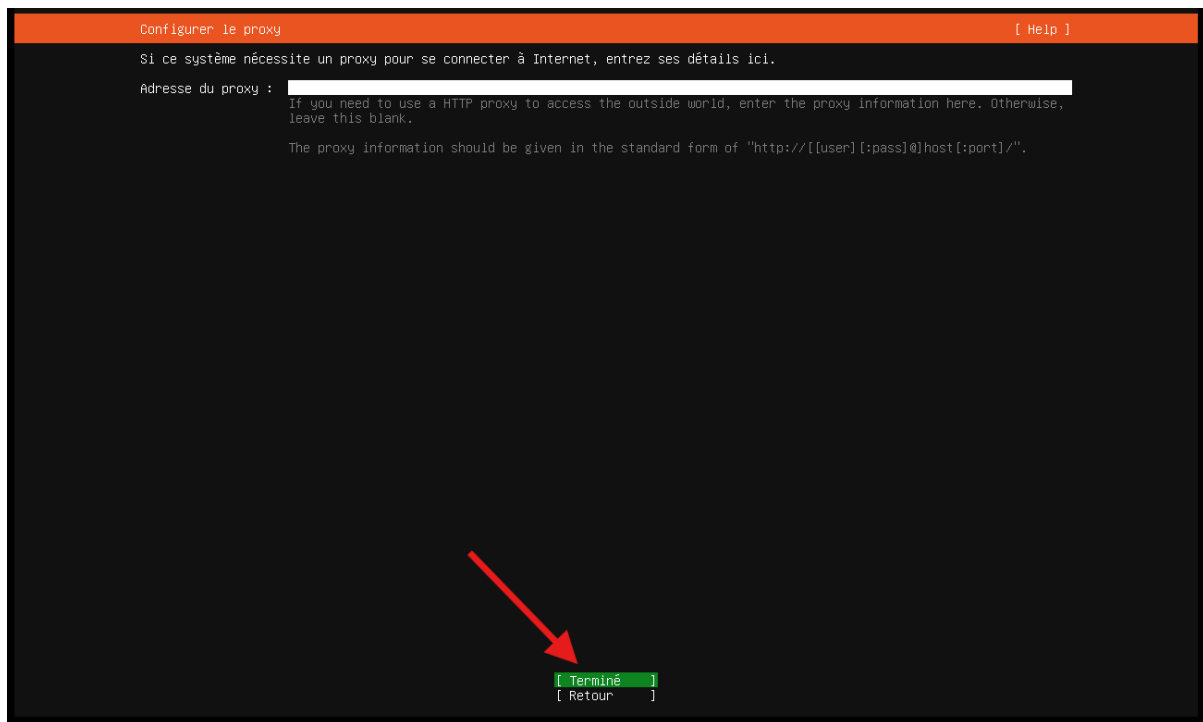
[Sauvegarder]
[Annuler]



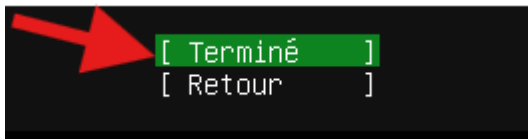
Attendre l'application des changements puis cliquer sur Terminé.



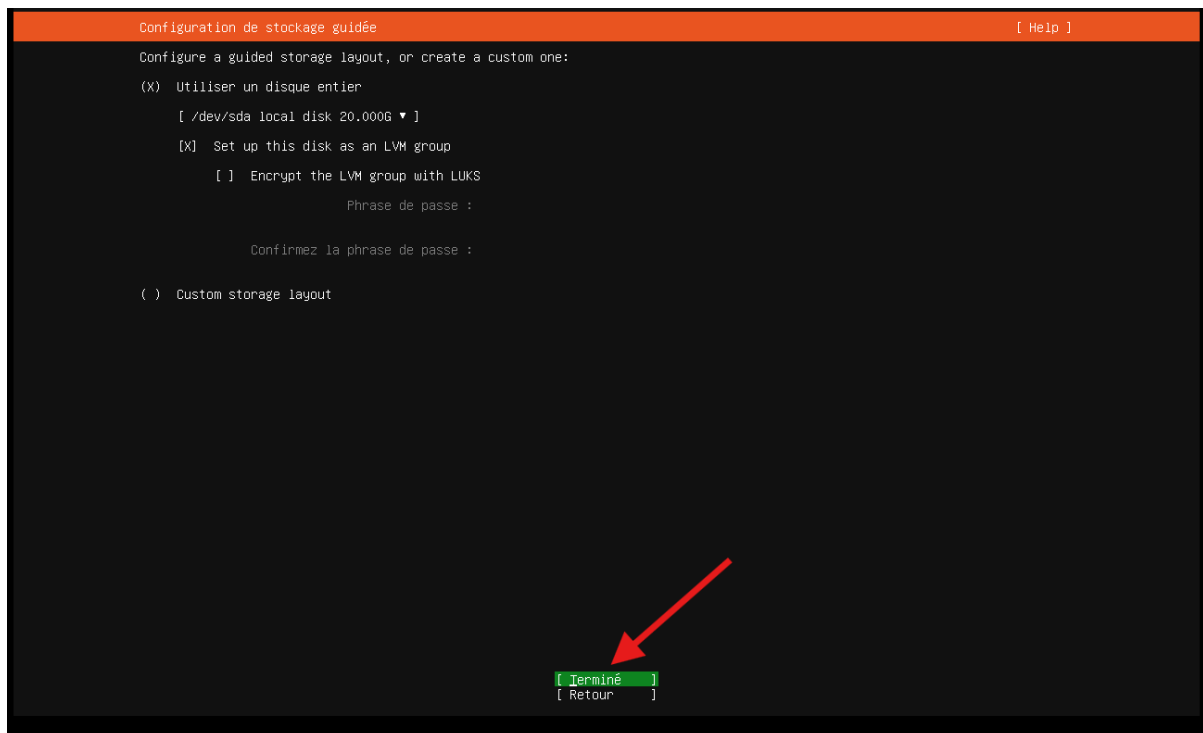
Appuyer sur Terminé.



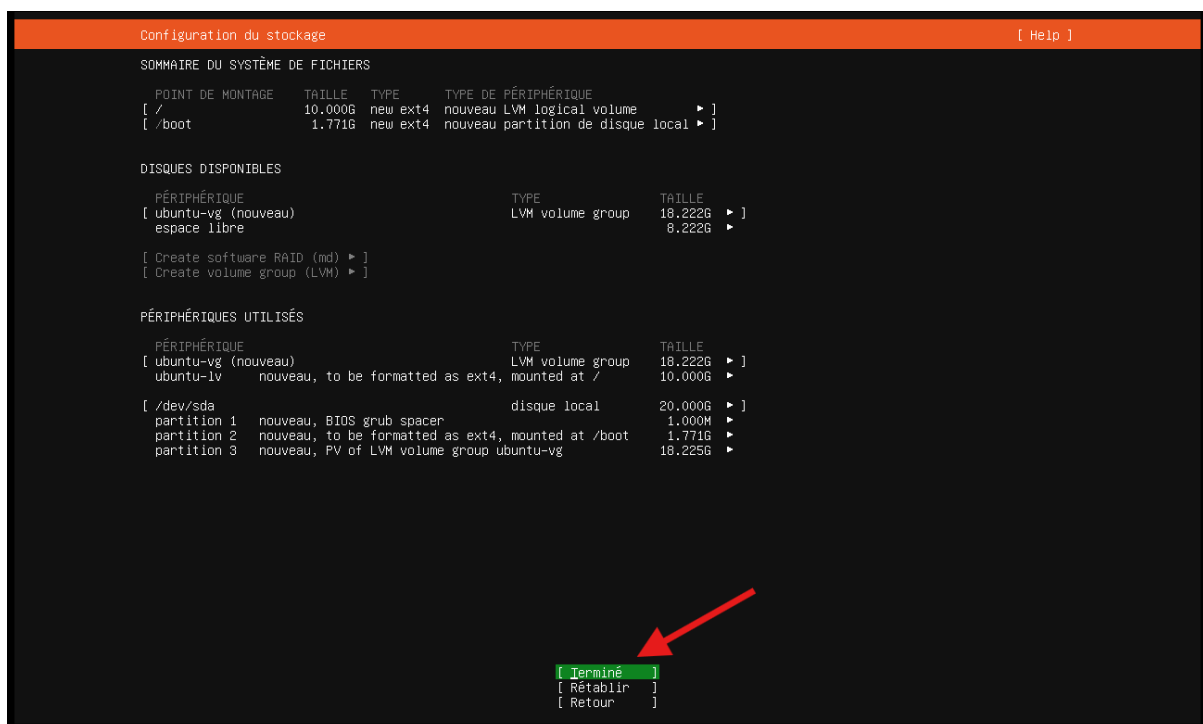
Attendre la fin du test miroir puis cliquer sur Terminé.



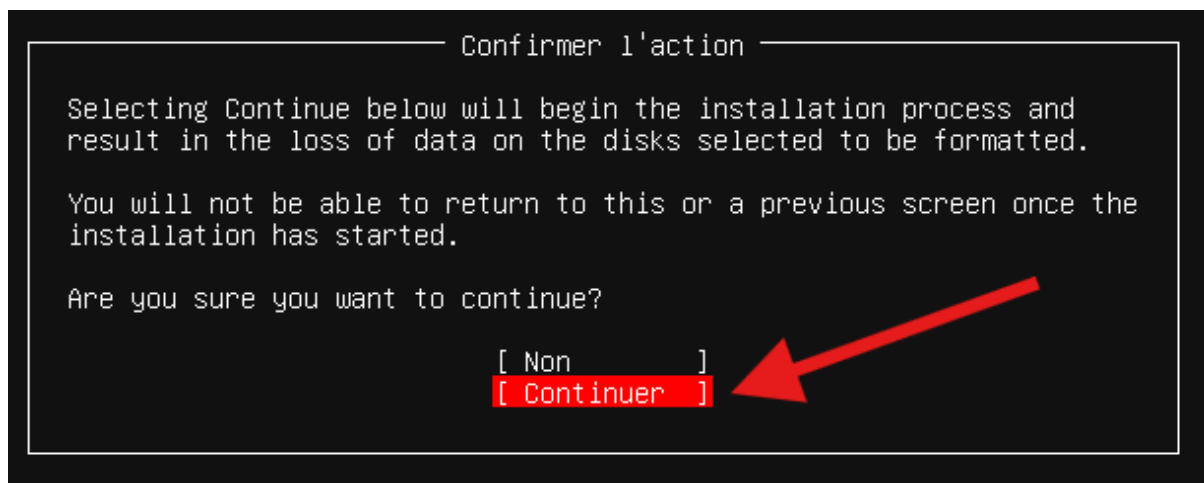
Appuyer sur Terminé.



Appuyer sur Terminé.



Sélectionner continuer.



Entrer les identifiants puis cliquer sur Terminé.

Configuration du profil [Help]

Enter the username and password you will use to log in to the system. You can configure SSH access on the next screen but a password is still needed for sudo.

Votre nom :

Le nom de cette machine:
The name it uses when it talks to other computers.

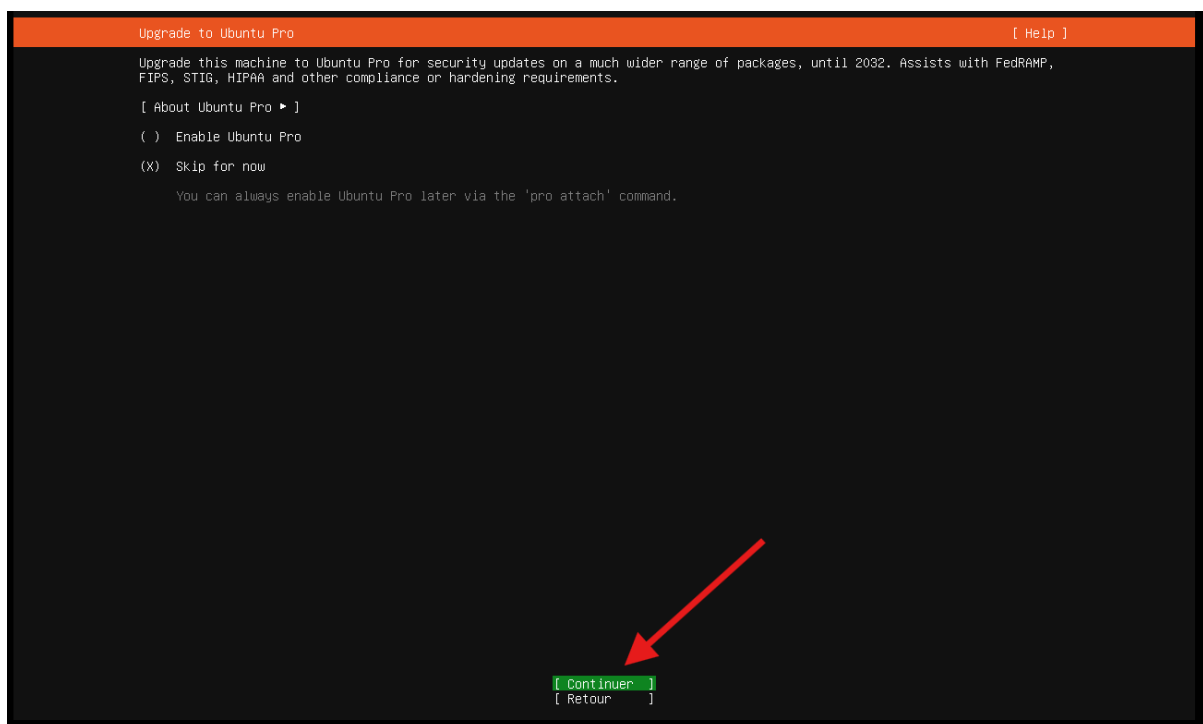
Choisir un nom d'utilisateur :

Choisir un mot de passe :

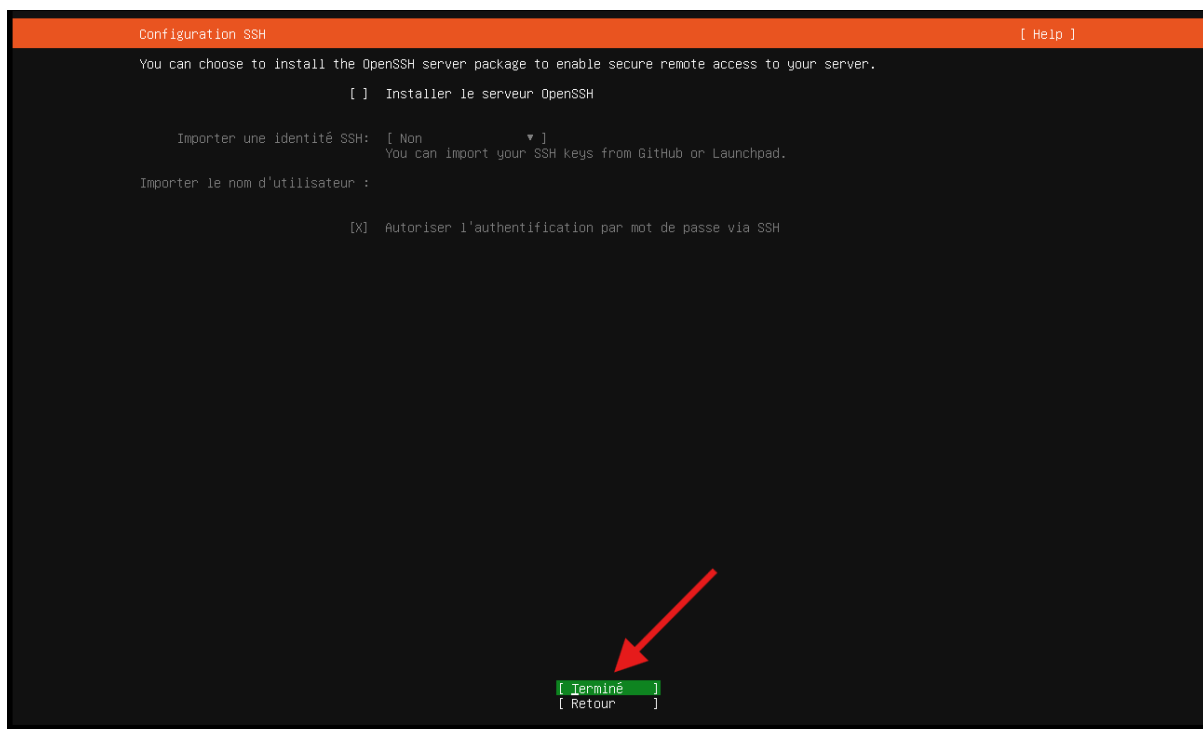
Confirmer votre mot de passe:

[Terminé]

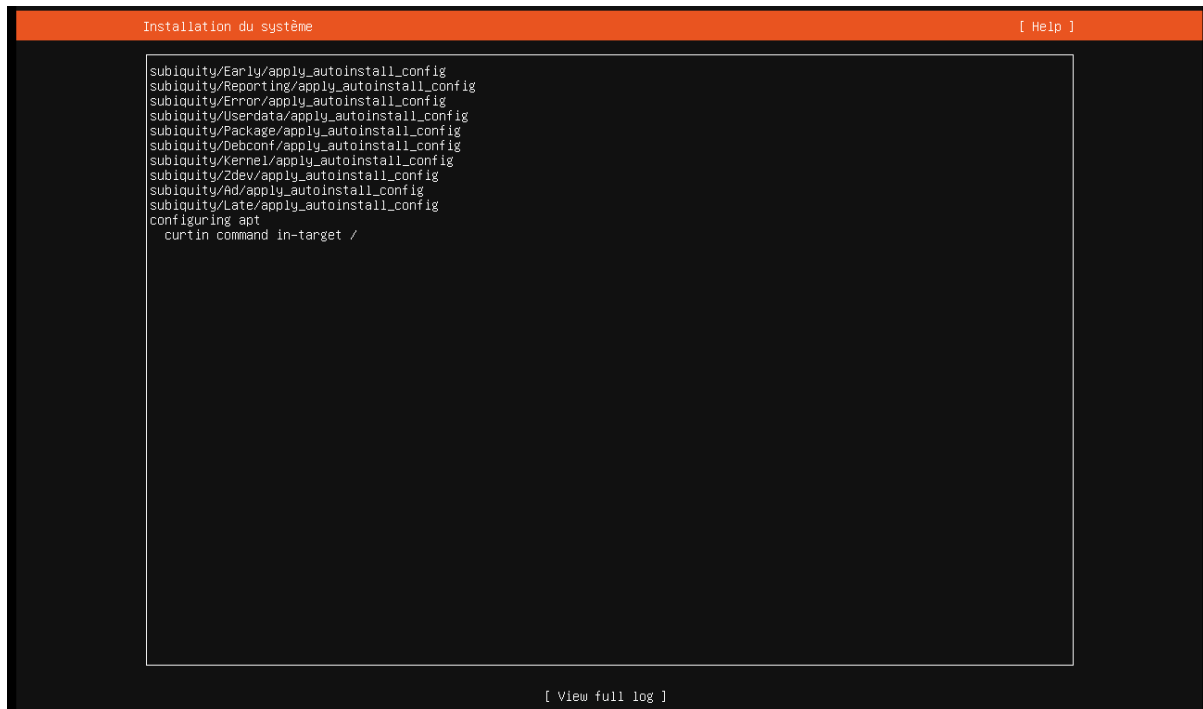
Sélectionner Continuer.



Appuyer sur Terminé, il n'y a pas besoin de OpenSSH.



Attendre la fin de l'installation.

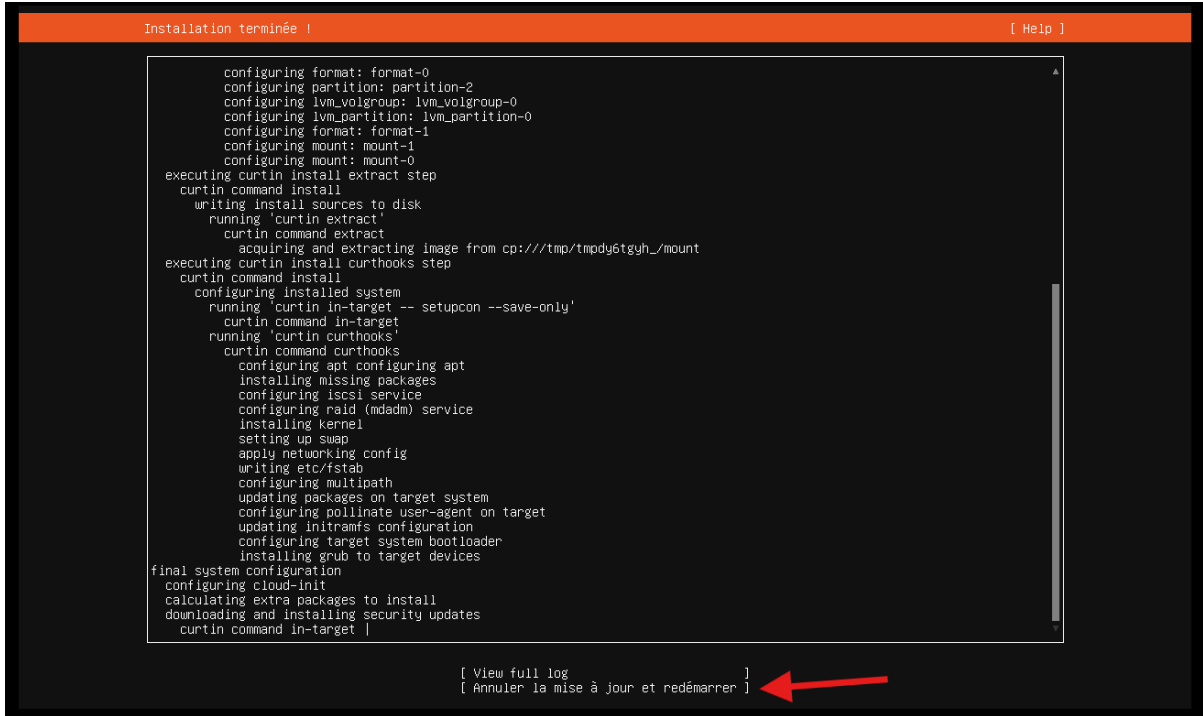


```
Installation du système [ Help ]

subiquity/Early/apply_autoinstall_config
subiquity/Reporting/apply_autoinstall_config
subiquity/Error/apply_autoinstall_config
subiquity/Userdata/apply_autoinstall_config
subiquity/Package/apply_autoinstall_config
subiquity/Debconf/apply_autoinstall_config
subiquity/kernel/apply_autoinstall_config
subiquity/Zdev/apply_autoinstall_config
subiquity/Ad/apply_autoinstall_config
subiquity/Late/apply_autoinstall_config
configuring apt
  curtin command in-target /

[ View full log ]
```

Après avoir attendu, sélectionner Annuler la mise à jour et redémarrer.



```
Installation terminée ! [ Help ]

configuring format: format-0
configuring partition: partition-2
configuring lvm_voigroup: lvm_voigroup-0
configuring lvm_partition: lvm_partition-0
configuring format: format-1
configuring mount: mount-1
configuring mount: mount-0
executing curtin install extract step
  curtin command install
    writing install sources to disk
    running 'curtin extract'
  curtin command extract
    acquiring and extracting image from cp:///tmp/tmpdy6tgyh_/mount
executing curtin install curthooks step
  curtin command install
    configuring installed system
    running 'curtin in-target -- setupcon --save-only'
    curtin command in-target
    running 'curtin curthooks'
    curtin command curthooks
      configuring apt configuring apt
      installing missing packages
      configuring iscsi service
      configuring raid (mdadm) service
      installing kernel
      setting up swap
      apply networking config
      writing etc/fstab
      configuring multipath
      updating packages on target system
      configuring pollinate user-agent on target
      updating initramfs configuration
      configuring target system bootloader
      installing grub to target devices
final system configuration
  configuring cloud-init
  calculating extra packages to install
  downloading and installing security updates
  curtin command in-target |

[ View full log ]
[ Annuler la mise à jour et redémarrer ]
```

Après s'être connecté avec les identifiants suite au redémarrage, mettre à jour le serveur avec cette commande.

```
hollo@dmz:~$ sudo apt update && sudo apt upgrade -y_
```

B) Installation des dépendances requises

Ajouter le dépôt PPA Ondřej en effectuant ces commandes (nous servira à installer la version 7.4 de php).

```
hollo@dmz:~$ sudo apt install software-properties-common -y
```

```
hollo@dmz:~$ sudo add-apt repository ppa:ondrej/php -y_
```

```
hollo@dmz:~$ sudo apt update_
```

Installer les dépendances avec cette commande.

```
hollo@dmz:~$ sudo apt install apache2 mariadb-server php7.4 libapache2-mod-php7.4 php7.4-mysql php7.4-xml php7.4-mbstring php7.4-curl php7.4-zip php7.4-gd unzip wget git -y
```

Activer les services apache2 et mariadb avec ces 2 commandes.

```
hollo@dmz:~$ sudo systemctl enable apache2
```

```
hollo@dmz:~$ sudo systemctl enable mariadb
```

Démarrer mariadb et apache2 avec cette commande.

```
hollo@dmz:~$ sudo systemctl start apache2 mariadb
```

(OPTIONNEL) Effectuer cette commande pour installer de manière sécurisé mariadb.

```
hollo@dmz:~$ sudo mysql_secure_installation
```

Effectuer cette commande pour entrer dans la console mariadb.

```
hollo@dmz:~$ sudo mysql -u root
```

Taper ces commandes à la suite pour créer la base de données ebrigade.

Créer la base de données.

```
MariaDB [(none)]> CREATE DATABASE ebrigade_db;_
```

Créer un utilisateur.

```
MariaDB [(none)]> CREATE USER 'arthur'@'localhost' IDENTIFIED BY 'Monsieursossou67';_
```

Accorder tous les privilèges au nouvel utilisateur créé.

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON ebrigade_db.* TO 'arthur'@'localhost';
```

Mettre à jour les privilèges.

```
MariaDB [(none)]> FLUSH PRIVILEGES;_
```

Quitter la base de données en rentrant EXIT; .

```
MariaDB [(none)]> EXIT;  
Bye  
hollo@dmz:~$
```

C) Téléchargement et déploiement de eBrigade

Télécharger le paquet de eBrigade avec cette commande.

```
hollo@dmz:~$ sudo wget https://ciscoursegoules.fr/wp-content/uploads/2022/08/ebrigade-5.3.2.zip_
```

Décompresser le paquet de eBrigade avec cette commande.

```
hollo@dmz:~$ unzip ebrigade-5.3.2.zip_
```

Copier le répertoire de eBrigade dans le répertoire web.

```
hollo@dmz:~$ sudo cp -r ~/ebrigade-5.3.2 /var/www/html/ebrigade_
```

Accorder les droits et les privilèges au répertoire de eBrigade avec ces 2 commandes.

```
hollo@dmz:~$ sudo chown -R www-data:www-data /var/www/html/ebrigade_
```

```
hollo@dmz:~$ sudo chmod -R 755 /var/www/html/ebrigade
```

Créer le fichier de configuration de eBrigade pour apache2.

```
hollo@dmz:~$ sudo nano /etc/apache2/sites-available/ebrigade.conf
```

Voici les paramètres à entrer (à adapter selon la configuration).

```
GNU nano 6.2 /etc/apache2/sites-available/ebrigade.conf
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html/ebrigade
    ServerName 192.168.200.10

    <Directory /var/www/html/ebrigade>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/ebrigade_error.log
    CustomLog ${APACHE_LOG_DIR}/ebrigade_access.log combined
</VirtualHost>
```

Faire CTRL + X, puis Y et Enter pour quitter et sauvegarder la configuration.

Activer le site en tapant ces commandes.

```
hollo@dmz:~$ sudo a2ensite ebrigade.conf_
```

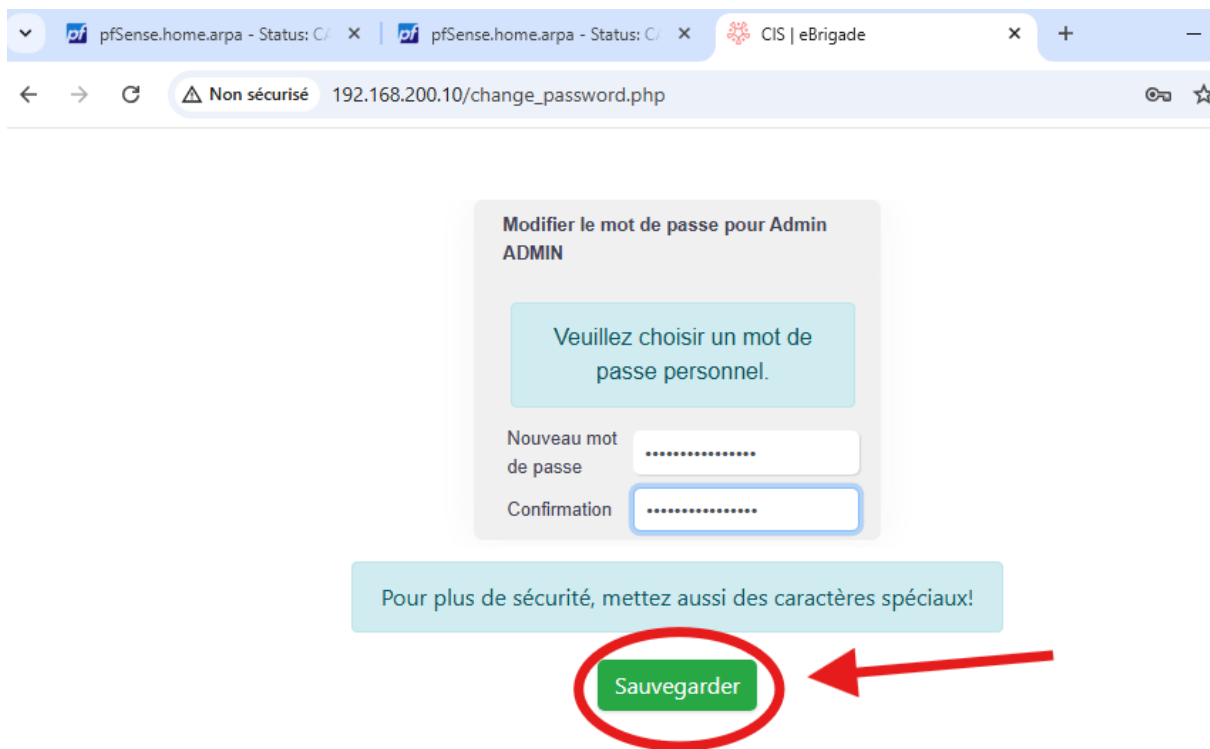
```
hollo@dmz:~$ sudo a2enmod rewrite_
```

```
hollo@dmz:~$ sudo systemctl reload apache2_
```

D) Première connexion à l'interface web de eBrigade

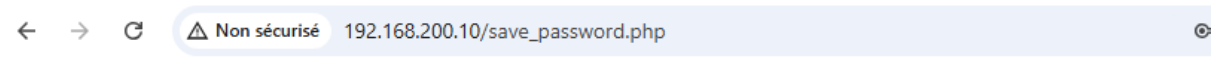
Depuis un client Windows, accéder à l'interface web de eBrigade via l'adresse IP du serveur (192.168.200.10 dans mon cas).

Entrer un nouveau mot de passe puis cliquer sur Sauvegarder.



The screenshot shows a web browser window with the address bar displaying "192.168.200.10/change_password.php". The page title is "Modifier le mot de passe pour Admin ADMIN". A light blue box contains the instruction "Veuillez choisir un mot de passe personnel." Below this, there are two input fields: "Nouveau mot de passe" and "Confirmation", both containing masked text (dots). A light blue box below the inputs contains the text "Pour plus de sécurité, mettez aussi des caractères spéciaux!". At the bottom, a green button labeled "Sauvegarder" is circled in red, with a red arrow pointing to it from the right.

Cliquer sur Continuer.



Voici les paramètres à entrer pour la configuration de eBrigade.

Ajouter l'adresse mail admin du serveur de messagerie Modoboa.

Cliquer ensuite sur Valider.



Configuration eBrigade

Type d'organisation *

Sans préconfiguration

Nom court de votre organisation *

SC

Nom long de votre organisation *

Sécurité civile

Adresse Web *

http://192.168.200.10

Votre adresse email *

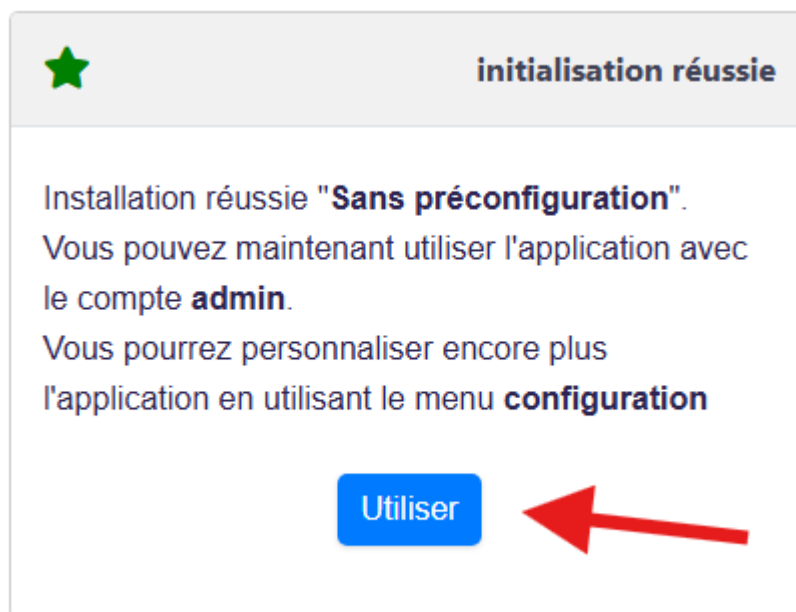
admin@securitecivile.local

Nom personnalisé de l'application *

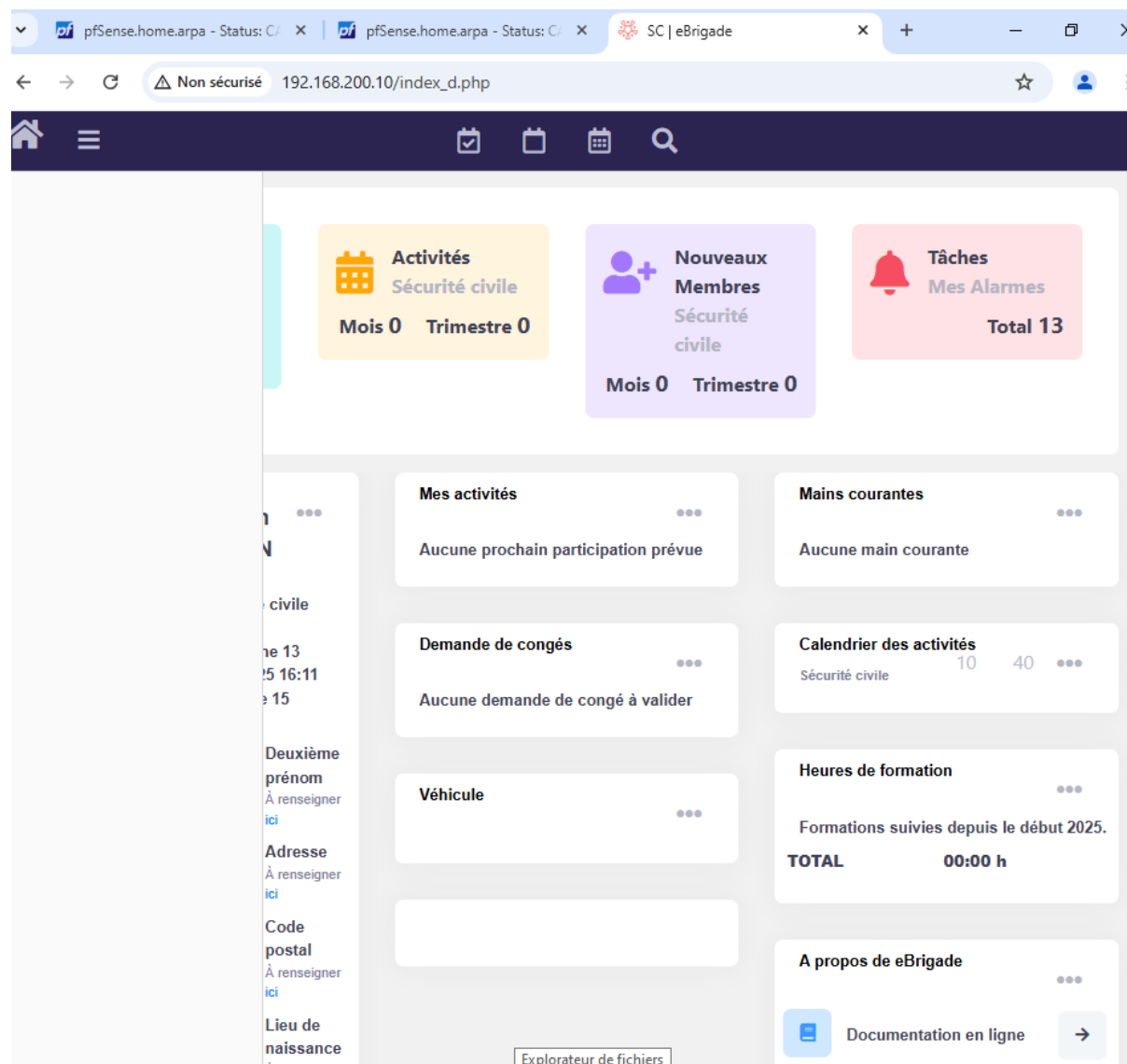
eBrigade

Valider

Cliquer sur Utiliser.

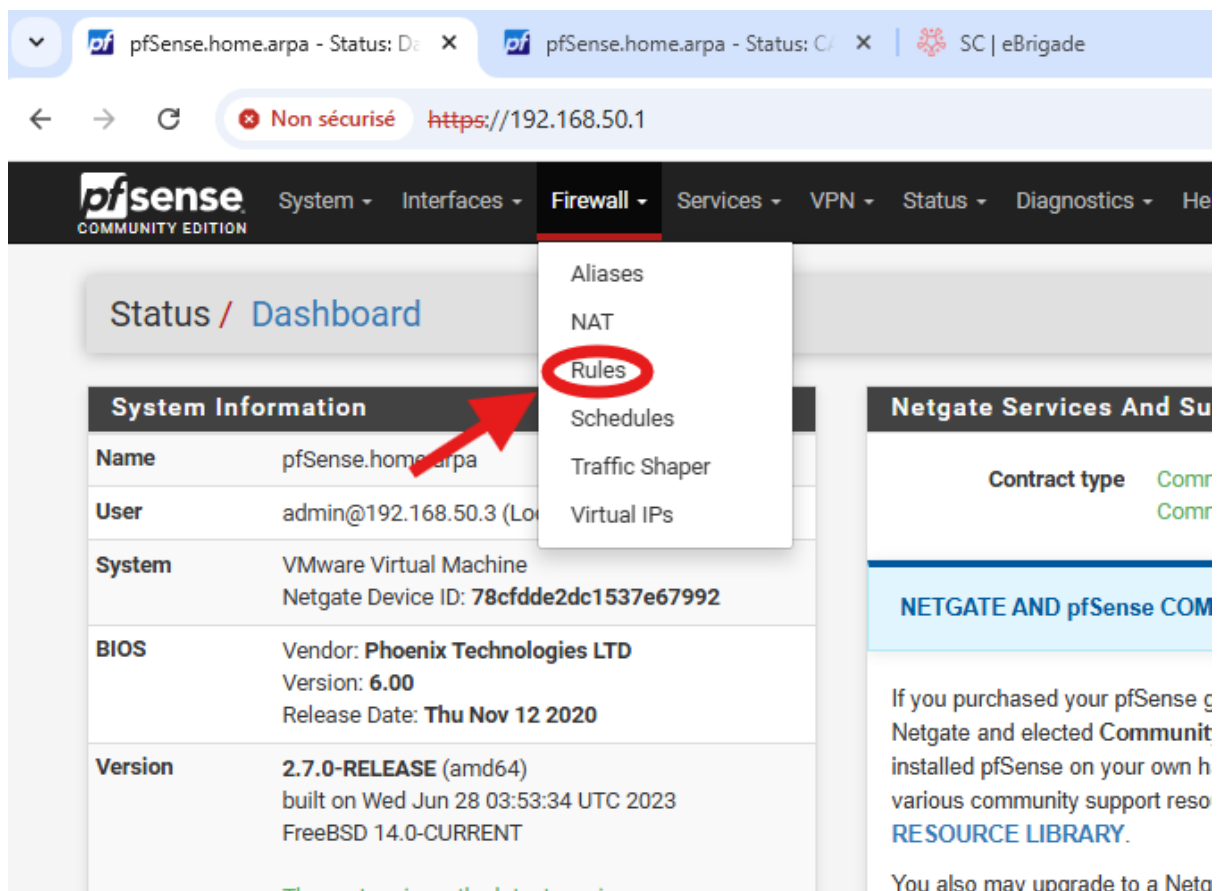


Nous sommes bien connectés à l'interface web de eBrigade.



3) Règles de pare-feu sur PfSense

Sur le PfSense Master, aller dans Firewall puis Rules.



Ajouter une règle d'accès depuis LAN vers DMZ.

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

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

Disabled

☐ Disable this rule

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

Interface

LAN

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

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

LAN net

Source Address

/

Destination

Destination

☐ Invert match

Single host or alias

192.168.200.10

/

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description

Accès eBrigade depuis LAN

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Rule Information

Ajouter une règle d'accès DMZ vers WAN.

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

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

DMZ

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

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

DMZ net

Source Address

/

Destination

Destination

☐ Invert match

any

Destination Address

/

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description

Accès Internet depuis DMZ

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Save

Microsoft Edge

Ajouter une règle d'accès Web à eBrigade depuis LAN.

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

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

DMZ

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

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

LAN net

Source Address

/

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

Single host or alias

192.168.200.10

/

Destination Port Range

HTTP (80)

From

Custom

To

HTTPS (443)

Custom

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

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Ajouter une règle vers Modoboa.

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

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

DMZ

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

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Single host or alias

192.168.200.10

/

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

Single host or alias

192.168.50.5

/

Destination Port Range

SMTP (25)

From

Custom

To

SMTP (25)

Custom

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

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status System Log Settings](#) page).

Ajouter une règle qui bloque DMZ > LAN.

Firewall / Rules / Edit

Edit Firewall Rule

Action

Block

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

Disabled

☐ Disable this rule

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

Interface

DMZ

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

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

DMZ net

Source Address

/

Destination

Destination

☐ Invert match

LAN net

Destination Address

/

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description

Bloquer DMZ vers LAN

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Save

Microsoft Edge

Voici un screen de la configuration des règles sur l'interface LAN.

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor the filter reload progress.](#)

Floating WAN1 **LAN** WAN2 OVPN_INTERFACE DMZ OpenVPN

Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	22/6.79 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
☐	0/22 KiB	IPv4 *	LAN net	*	192.168.200.10	*	*	none		Accès eBrigade depuis LAN	
☐	0/55 KiB	IPv4 UDP	192.168.50.3	*	*	161 (SNMP)	*	none		PRTG	
☐	0/0 B	IPv4 *	LAN net	*	*	*	WAN_FAILOVER	none		Default allow LAN to any rule	
☐	0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

Voici un screen de la configuration des règles sur l'interface DMZ.

Firewall / Rules / DMZ

Floating WAN1 LAN WAN2 OVPN_INTERFACE **DMZ** OpenVPN

Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	0/0 B	IPv4 TCP	192.168.200.10	*	192.168.50.5	25 (SMTP)	*	none		SMTP vers Modoboa	
☐	0/0 B	IPv4 TCP	LAN net	*	192.168.200.10	80 - 443	*	none		Web access à eBrigade	
☐	0/12 KiB	IPv4 *	DMZ net	*	*	*	*	none		Accès Internet depuis DMZ	
☐	0/553.08 MiB	IPv4 *	DMZ net	*	*	*	*	none		DMZ Internet	
☐	0/0 B	IPv4 *	DMZ net	*	LAN net	*	*	none		Bloquer DMZ vers LAN	

Add Add Delete Toggle Copy Save Separator