



1- Introduction

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

Prérequis pour une machine PfSense

	Configuration minimale	Configuration recommandée
Processeur	600 MHz	1 GHz
Mémoire vive	512 Mo	1 Go
Stockage	> 6 Go	

Il faut avoir en tout 5 interfaces réseaux avec la première interface en bridge:

The screenshot shows the 'Virtual Machine Settings' window with the 'Options' tab selected. A table lists the device configurations:

Device	Summary
Memory	2.0 GB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Using file E:\VM ISO\pfSense...
Network Adapter	Bridged (Automatic)
Network Adapter 2	LAN Segment
Network Adapter 3	LAN Segment
Network Adapter 4	LAN Segment
Network Adapter 5	LAN Segment
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Login et mdp pfsense : root/pfsense

Infrastructure

Pour notre projet :il nous faut 6 machines :

Nom du serveur PfSense : heimdall
Adresse IP : Dépends de votre réseau
Net masque : 255.255.255.0
Passerelle : 192.168.1.1
DNS : 192.168.100.2
DNS Secondaire : 192.168.100.3

Dans le réseau professionnel (Vlan 80) :

- **Une machine Windows :**
Adresse IP : DHCP

Dans le réseau visiteurs (Vlan 90) :

- **Une machine Windows :**
Adresse IP : DHCP

Dans le réseau Serveur (Vlan 100) :

- **Machine AD Primaire :**
Nom du serveur : SafetechDC
Adresse IP : 192.168.100.2
Net masque : 255.255.255.0
Passerelle : 192.168.100.254
DNS : 127.0.0.1
DNS Secondaire : 192.168.100.3
Nom de domaine DNS : **safetech.com**
- **Machine AD Secondaire :**
Nom du serveur : SafetechDC2
Adresse IP : 192.168.100.3
Net masque : 255.255.255.0
Passerelle : 192.168.100.254
DNS : 192.168.100.2
DNS Secondaire : 127.0.0.1
Nom de domaine DNS : **safetech.com**
- **1 Serveur de messagerie Zimbra :**
Nom du serveur : xmail
Adresse IP : 192.168.100.4
Net masque : 255.255.255.0
Passerelle : 192.168.100.254
DNS : 192.168.100.2
DNS Secondaire : 192.168.100.3
- **1 Serveur Debian avec GLPI et OCS :**
Nom du serveur : xmail
Adresse IP : 192.168.100.6

Net masque : 255.255.255.0
Passerelle : 192.168.100.254
DNS : 192.168.100.2
DNS Secondaire : 192.168.100.3

Dans le réseau Management (Vlan 110) :

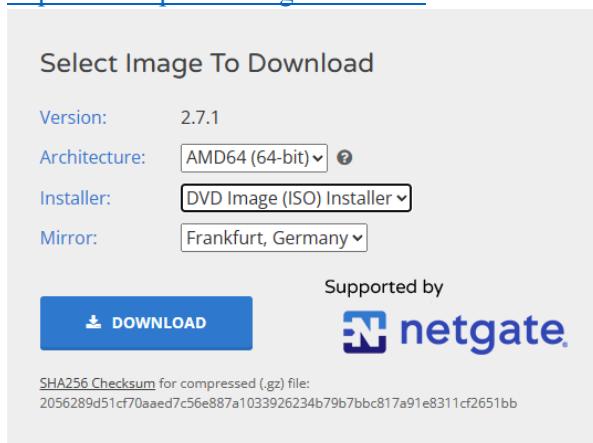
- **1 Serveur de supervision Nagios :**
 - Nom du serveur : Nagios
 - Adresse IP : 192.168.110.10
 - Net masque : 255.255.255.0
 - Passerelle : 192.168.110.254
 - DNS : 192.168.100.2
 - DNS Secondaire : 192.168.100.3

Network Adapter: Bridged
Network Adapter2: Vlan Visiteurs
Network Adapter3: Vlan Management
Network Adapter4: Vlan pro
Network Adapter5: Vlan Server

3- Installation de pfsense

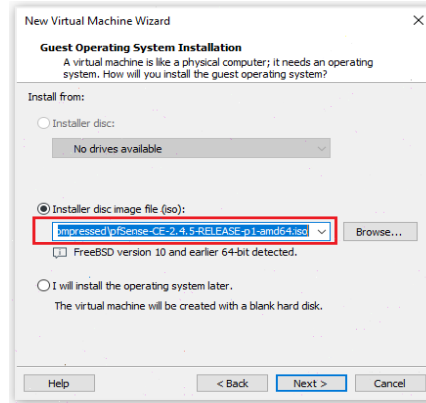
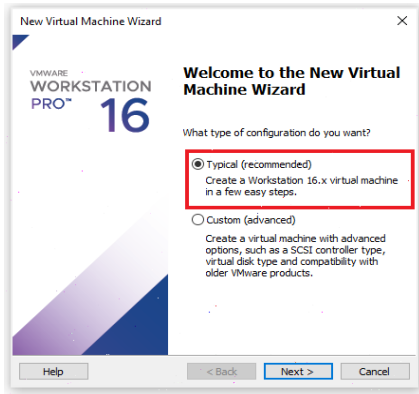
a- Téléchargement de pfsense

Pour installer pfSense il faut télécharger l'iso d'installation sur le site officiel à l'adresse :
<https://www.pfsense.org/download/>



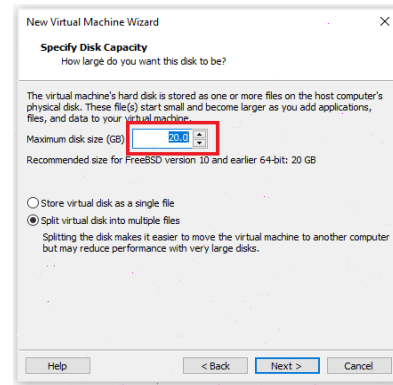
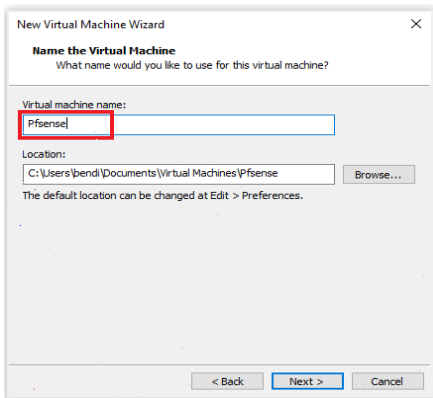
b- Lancement de l'installation

il faut maintenant dézipper notre fichier pour avoir l'iso et lancer l'installation sur vmware
On pointe vers le fichier iso de pfsense



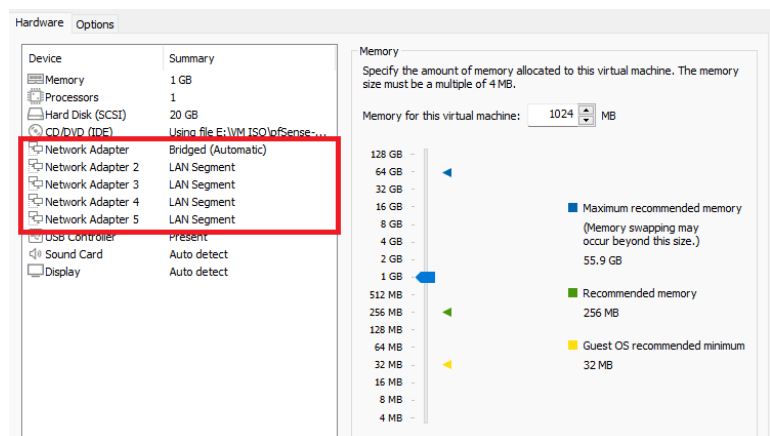
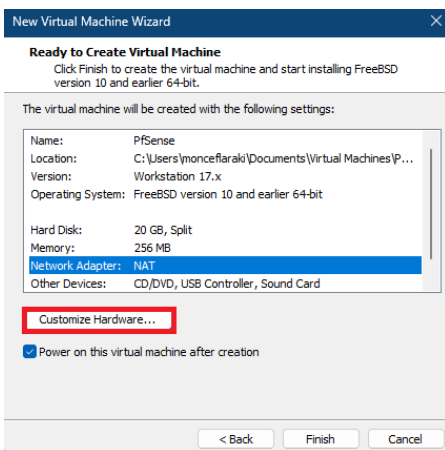
On choisit pfsense comme nom

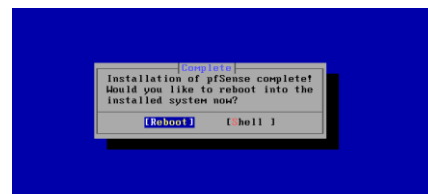
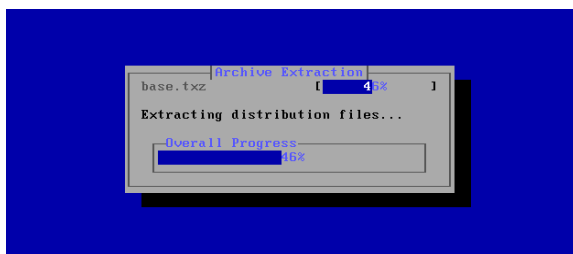
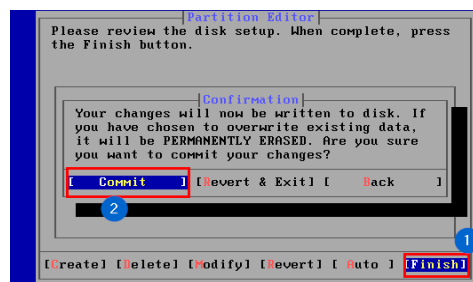
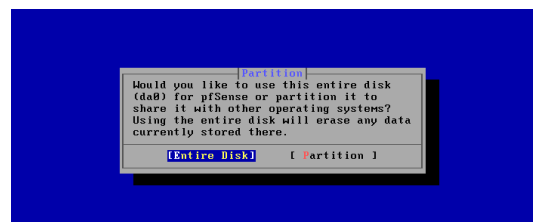
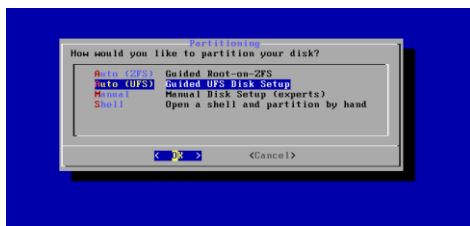
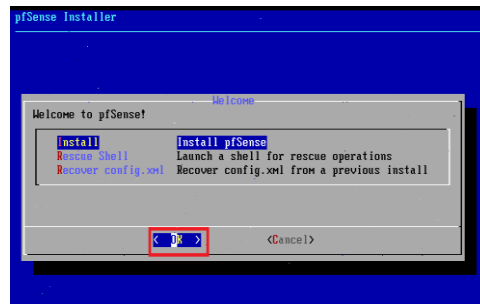
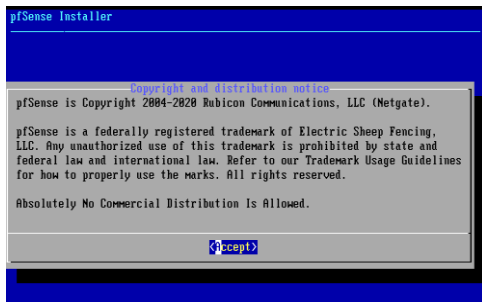
On laisse 20 gb par défaut



Pour cette étape On mettra en place 5 cartes

- Network Adapter en bridge -----→192.168.1.250/24
 - Network Adapter2 en Serveurs -----→192.168.100.254/24
 - Network Adapter3 en Management -----→192.168.110.254/24
 - Network Adapter4 en Professionnels -----→192.168.80.254/24
 - Network Adapter5 en Visiteurs -----→192.168.90.254/24
- La 1ere interface dépendra de la plage IP privée de votre réseau domestique.
On mettra 1GB de mémoire





Vous devez avoir un résultat comme ceci :

Si vous n'avez pas une adresse IPv6 ce n'est pas grave car nous allons la désactiver par la suite.

```
pfSense 2.7.1-RELEASE amd64 20231115-1706
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 729824a65f6c5652da0a

*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.140/24
                v6/DHCP6: 2a01:e0a:3cb:31b0:20c:29ff:fe32:6708
/64
LAN (lan)      -> em1      -> 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: █
```

4- Configuration post instalation

Manuellement on va mettre notre clavier en français mais temporairement car en redemarrant notre serveur le clavier redevient en qwerty ; on le configurera d'une façon permanente avec l'interface web: On choisit l'**option 8** pour demarrer le shell puis on tape la commande suivante :

```
[2.5.2-RELEASE][root@pfSense.home.arpa]/root: kbdcontrol -l fr
```

a- Déclaration des interfaces :

Maintenant on va déclarer nos 5 interfaces : Wan, professionnels, visiteurs, serveurs et management :

On choisit l'option 1

```
Enter an option: 1 █
```

```
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em3 em4 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode
(em1 em2 em3 em4 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 em3 em4 a or nothing if finished): em2

Enter the Optional 2 interface name or 'a' for auto-detection
(em3 em4 a or nothing if finished): em3

Enter the Optional 3 interface name or 'a' for auto-detection
(em4 a or nothing if finished): em4

The interfaces will be assigned as follows:

WAN -> em0
LAN -> em1
OPT1 -> em2
OPT2 -> em3
OPT3 -> em4

Do you want to proceed [y!n]? y
```

A la fin on doit avoir un résultat comme ça :

```
WAN (wan) -> em0 -> v4/DHCP4: 192.168.1.140/24
v6/DHCP6: 2a01:e0a:3cb:31b0:20c:29ff:fe32:6708
/64
LAN (lan) -> em1 -> v4: 192.168.1.1/24
OPT1 (opt1) -> em2 ->
OPT2 (opt2) -> em3 ->
OPT3 (opt3) -> em4 ->
```

Maintenant on va affecter les adresses IP à nos 5 interfaces,

- b- Assignement des adresses aux interfaces wan, lan, opt1, opt2 et opt3
• L'interface Wan :

Le choix de des adresses qu'on va affecter à cette interface dépend de la configuration de notre box internet c'est pour cela il faut faire une ipconfig /all sur la machine physique pour déterminer la passerelle et l'ID réseau utilisé :

```
Adresse IPv4. . . . . : 192.168.1.180(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0

Passerelle par défaut. . . . . :
192.168.1.254
```

Donc notre réseau est
Id réseau 192.168.1.0/24
DNS/Passerelle 192.168.1.254

On choisit l'option 2

Enter an option: 2

On met les choix suivants :

Adresse ip :192.168.1.250
Masque de sous réseau 255.255.255.0
Passerelle 192.168.1.254
Pas de DHCPv4
Pas de IPv6
Pas de DHCP6

```
2 - WAN (mt - static)
3 - OPT1 (en2)
4 - OPT2 (en3)
5 - OPT3 (en4)

Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.1.250

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 WAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.254

Should this gateway be set as the default gateway? (y/n) y
```

```
Configure IPv6 address WAN interface via DHCP6? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

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

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

The IPv4 WAN address has been set to 192.168.1.250/24

Press <ENTER> to continue.
```

L'interface lan :

@ip :192.168.100.254
Masque de sous réseau 255.255.255.0
Passerelle : non
DHCP IPv5 non
Pas de IPv6
Pas de DHCP IPV6


```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - static)
2 - LAN (em1 - static)
3 - OPT1 (em2 - static)
4 - OPT2 (em3 - static)
5 - OPT3 (em4 - static)

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

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.254

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

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

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

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

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

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

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

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

The IPv4 LAN address has been set to 192.168.100.254/24
You can now access the webConfigurator by opening the following URL in your web browser:
https://192.168.100.254/
```

- L'interface opt1 :

@ip :192.168.110.254
Masque de sous réseau 255.255.255.0
Passerelle : non
Pas de DHCP IPv5
Pas de IPv6
Pas de DHCP6

```
Enter the number of the interface you wish to configure: 3
Configure IPv4 address OPT1 interface via DHCP? (y/n) n
Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 192.168.110.254
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 OPT1 IPv4 subnet bit count (1 to 32):
> 24
For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
Configure IPv6 address OPT1 interface via DHCP6? (y/n) n
Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on OPT1? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
Please wait while the changes are saved to OPT1...
Reloading filter...
Reloading routing configuration...
DHCPD...
The IPv4 OPT1 address has been set to 192.168.110.254/24
You can now access the webConfigurator by opening the following URL in your web browser:
    https://192.168.110.254/
Press <ENTER> to continue.
```

- L'interface opt2 :

@ip :192.168.80.254
Masque de sous réseau 255.255.255.0
Passerelle : non
Pas de DHCP IPv5
Pas de IPv6
Pas de DHCP6

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - static)
2 - LAN (em1 - static)
3 - OPT1 (em2 - static)
4 - OPT2 (em3 - static)
5 - OPT3 (em4 - static)

Enter the number of the interface you wish to configure: 4

Configure IPv4 address OPT2 interface via DHCP? (y/n) n

Enter the new OPT2 IPv4 address. Press <ENTER> for none:
> 192.168.80.254

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 OPT2 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT2 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT2 interface via DHCP6? (y/n) n

Enter the new OPT2 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT2? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

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

Please wait while the changes are saved to OPT2...
Reloading filter...
```

- L'interface opt3 :

```
@ip :192.168.90.254
Masque de sous réseau 255.255.255.0
Passerelle : non
Pas de DHCP IPv5
Pas de IPv6
Pas de DHCP6
```

```
Enter an option: 2

Available interfaces:
1 - WAN (em0 - static)
2 - LAN (em1 - static)
3 - OPT1 (em2 - static)
4 - OPT2 (em3 - static)
5 - OPT3 (em4 - static)

Enter the number of the interface you wish to configure: 5

Configure IPv4 address OPT3 interface via DHCP? (y/n) n

Enter the new OPT3 IPv4 address. Press <ENTER> for none:
> 192.168.90.254

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 OPT3 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT3 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT3 interface via DHCP6? (y/n) n

Enter the new OPT3 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT3? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

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

Please wait while the changes are saved to OPT3...
Reloading filter...
```

Nos interfaces ressemblent donc à cela :

```
WAN (wan)      -> em0      -> v4: 192.168.1.250/24
LAN (lan)     -> em1      -> v4: 192.168.100.254/24
OPT1 (opt1)  -> em2      -> v4: 192.168.110.254/24
OPT2 (opt2)  -> em3      -> v4: 192.168.80.254/24
OPT3 (opt3)  -> em4      -> v4: 192.168.90.254/24
```

Nous allons maintenant accéder au WebGUI de PfSense depuis notre contrôleur de domaine : SafetechDC :

Taper l'adresse suivante sur le navigateur : <https://192.168.100.254>. Le navigateur va nous afficher la fenêtre suivante. Il faut appuyer sur continuer :



Votre connexion n'est pas privée

Les utilisateurs malveillants essaient peut-être de voler vos informations de **192.168.100.254** (par exemple, les mots de passe, les messages ou les cartes de crédit).

NET::ERR_CERT_AUTHORITY_INVALID

Masquer les éléments avancés

Retour

Ce serveur n'a pas pu prouver qu'il s'agit de **192.168.100.254**. Son certificat de sécurité n'est pas approuvé par le système d'exploitation de votre ordinateur. Cela peut être dû à une mauvaise configuration ou à un utilisateur malveillant qui intercepte votre connexion.

[Continuer vers 192.168.100.254 \(non sécurisé\)](#)

Nous arrivons ensuite dans la fenêtre de connexion de PfSense :



Login to pfSense

SIGN IN

Username

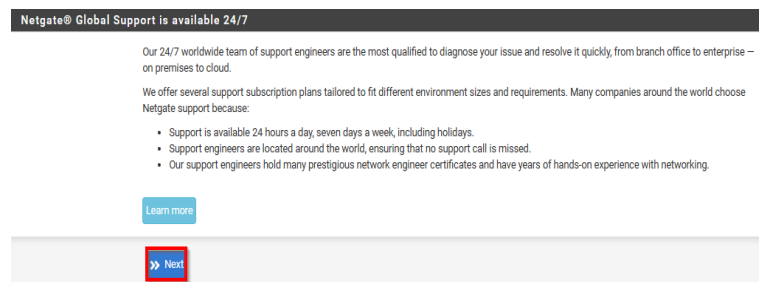
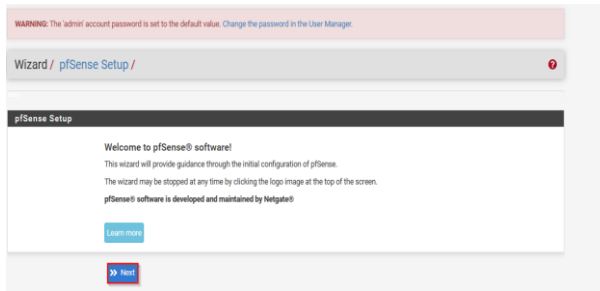
Password

SIGN IN

Connectez-vous avec les identifiants suivants :

Login : **admin**
Password : **pfsense**

Execution du Wizard de la configuration de base :



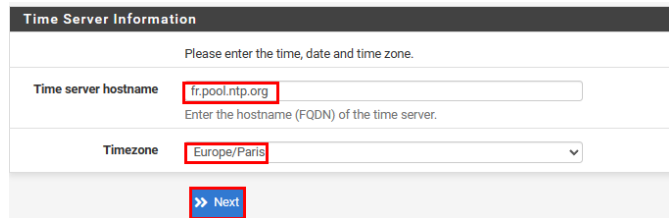
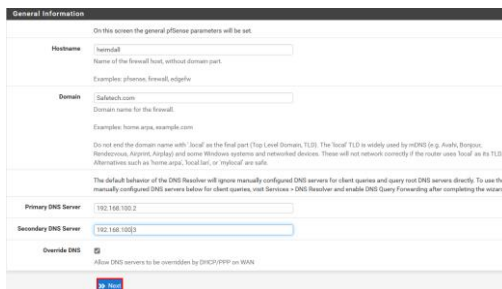
Le Wizard a 9 étapes qui vont s'exécuter par défaut. Les premières étapes sont des informations d'ordre générales traitant le SAV Netgate.

On rentre notre nom du serveur heimdall

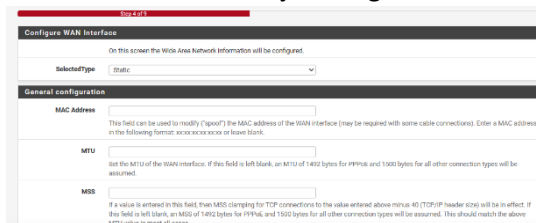
On configure le serveur NTP sur fr.pool.ntp.org

Le nom de domaine est safetech.com

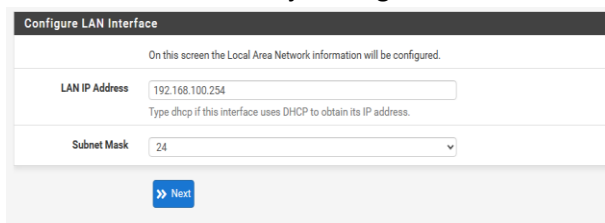
On change la Timezone en Europe/Paris



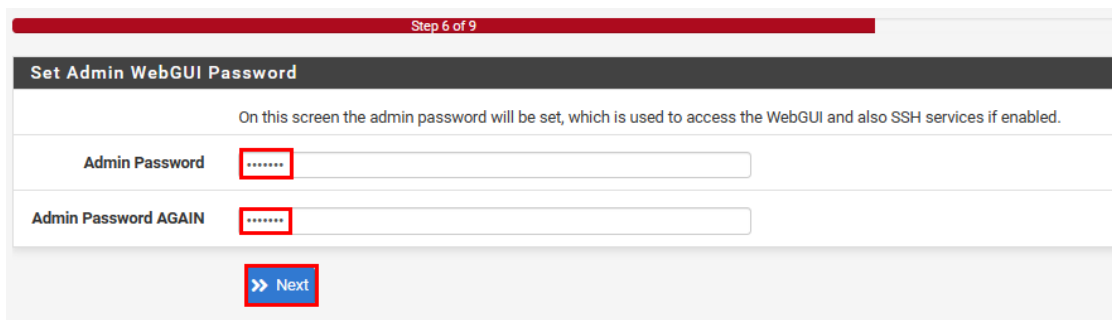
L'interface WAN est déjà configurée



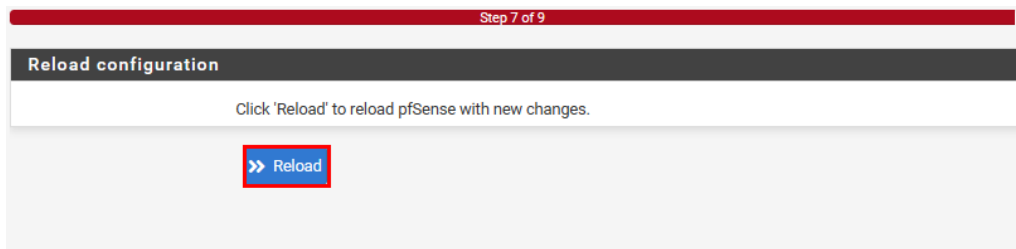
L'interface LAN est déjà configurée



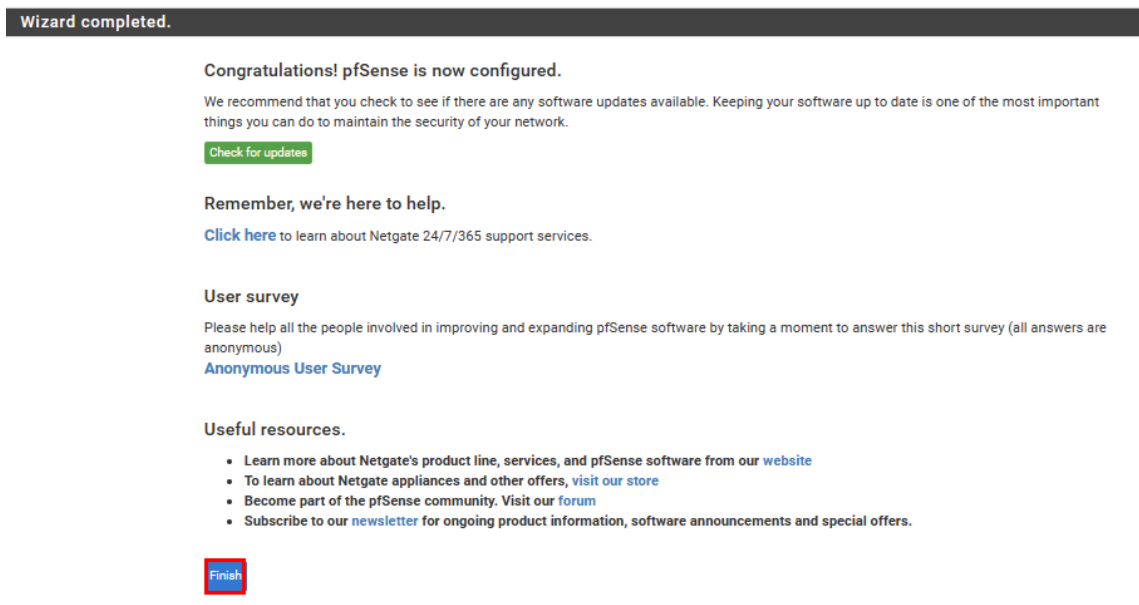
On change le mot de passe admin par défaut, ici nous avons mis Azerty1



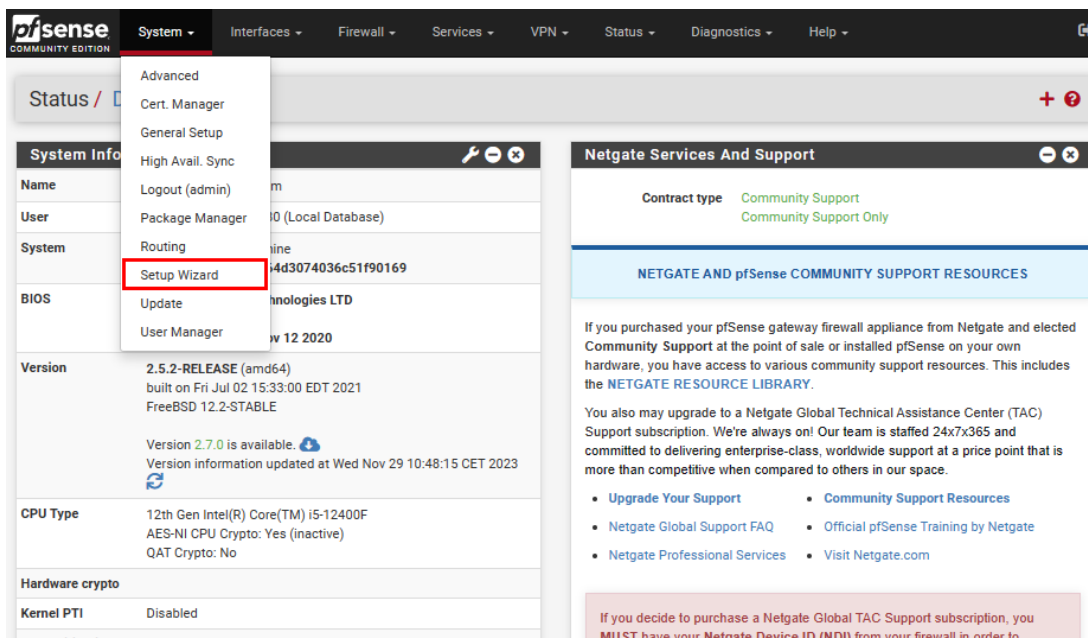
Appliquer la configuration en appuyant sur Reload :



On clique sur Finish pour finir la configuration :



En cas d'erreurs nous pouvons relancer le Wizard :

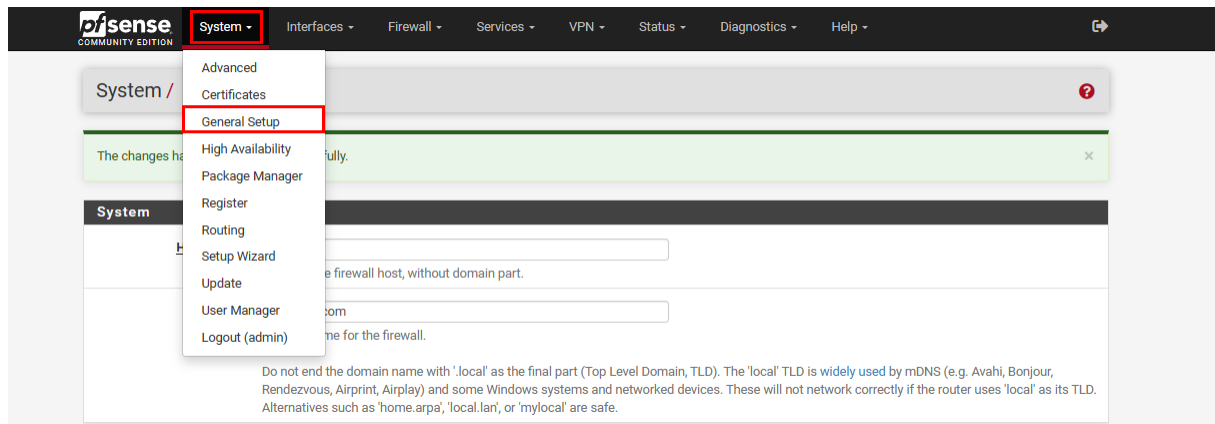


Configuration du Service DNS de PfSense :

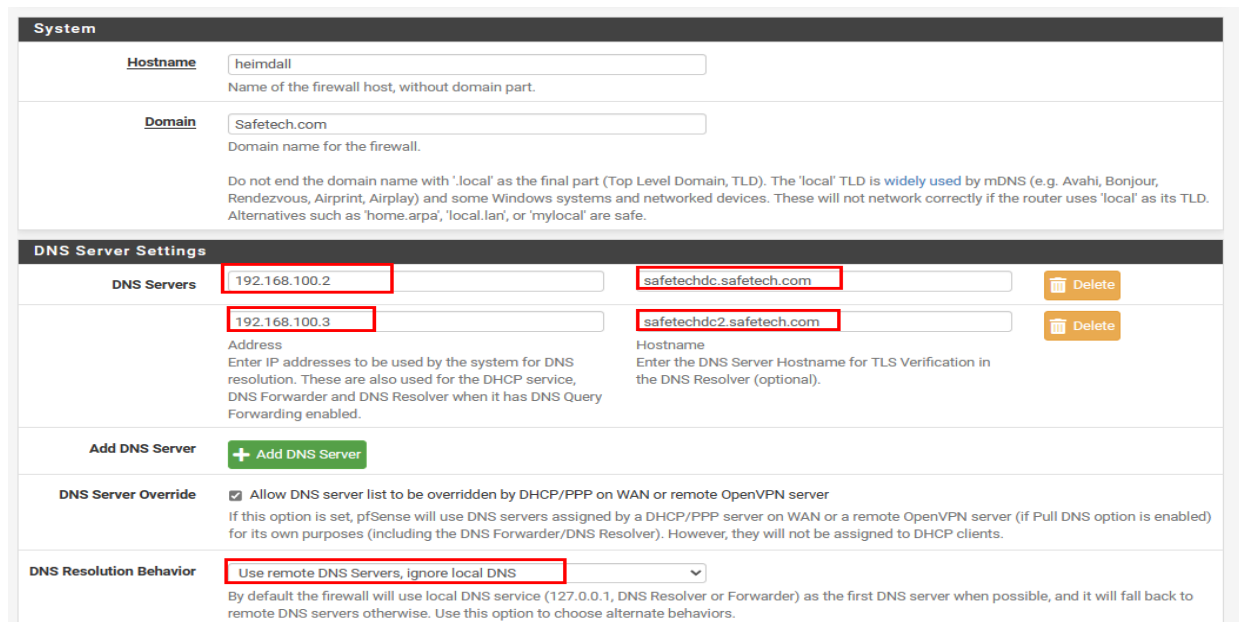
Par défaut, PfSense effectue en premier lieu des requêtes vers son propre serveur DNS avant de consulter les autres serveurs DNS distants. Nous souhaitons apporter une modification à cette configuration, car nous n'avons pas configuré pour assumer le rôle de serveur DNS. Cette

modification est nécessaire afin d'éviter des requêtes inutiles vers le serveur DNS local et d'améliorer ainsi les performances globales du système.

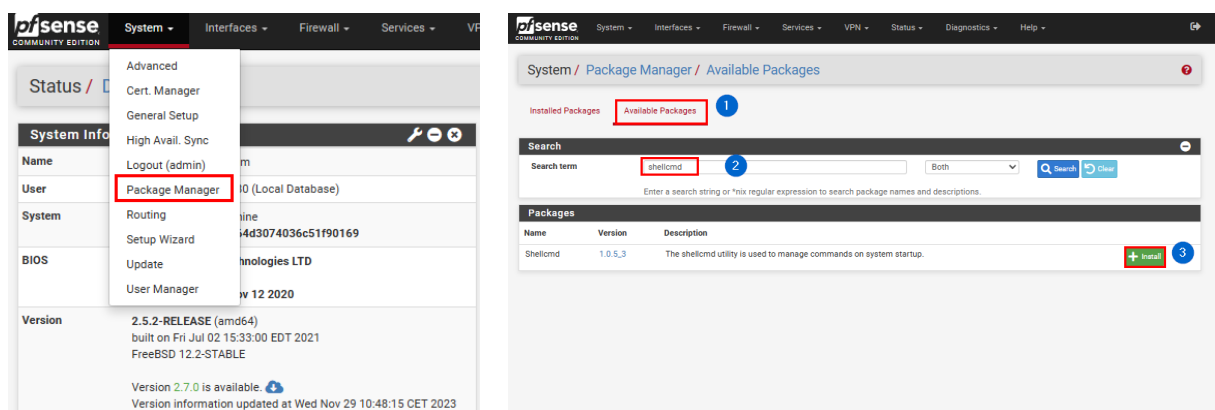
Pour ce faire nous allons dans la rebrique :

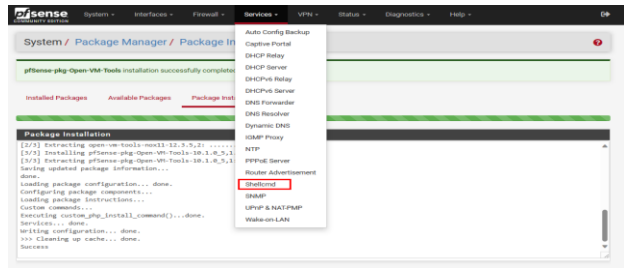
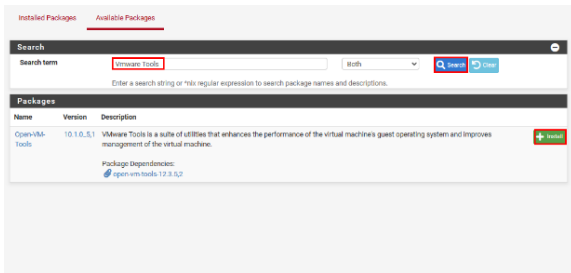


Ensuite nous allons appliquer les paramètres suivants :

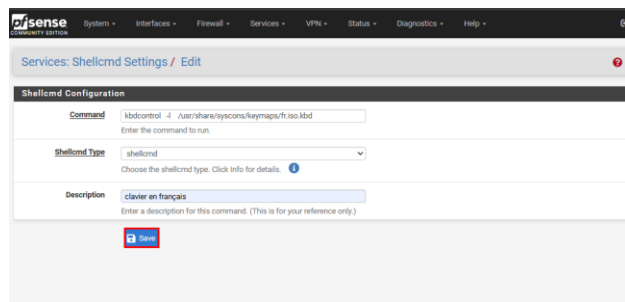
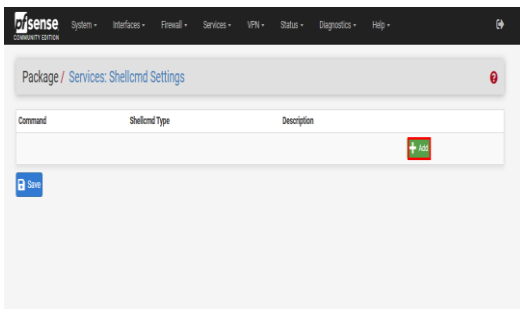


La mise en place de la configuration du clavier en français de façon permanente et installation de VMware Tools :

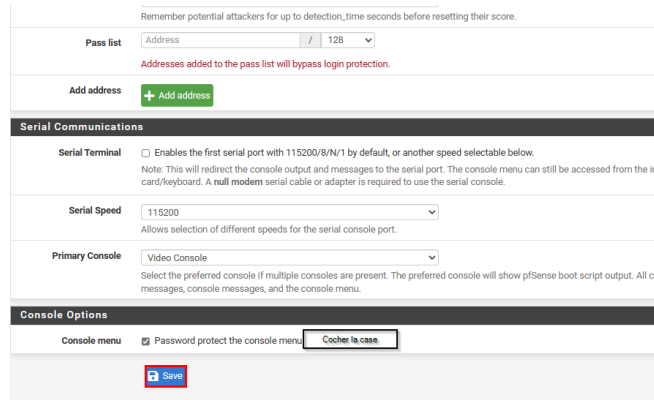
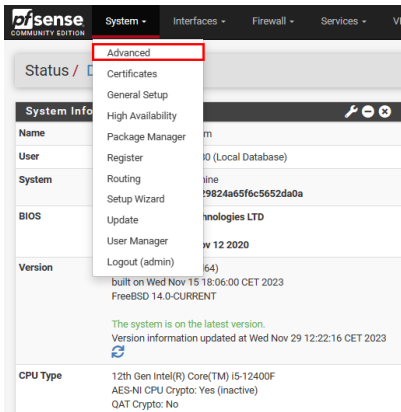




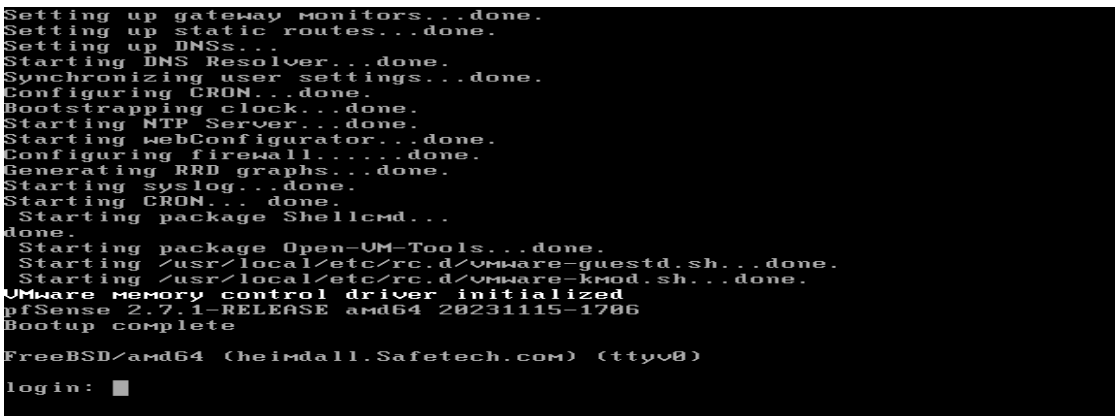
Tapez cette commande `kbdcontrol -l /usr/share/syscons/keymaps/fr.iso.kbd` dans le champ commande puis redémarrer votre machine pfSense et vérifiez que le clavier est en AZERTY



Securisation de la console PfSense :



On constate que la console nous demande le login :



Création de VLAN :

Interfaces / VLANs / Edit ☰ 📄 ?

VLAN Configuration

Parent Interface	em1 (00:0c:29:32:67:12) - lan
	Only VLAN capable interfaces will be shown.
VLAN Tag	100
	802.1Q VLAN tag (between 1 and 4094).
VLAN Priority	0
	802.1Q VLAN Priority (between 0 and 7).
Description	Vlan Server
	A group description may be entered here for administrative reference (not parsed).

[Save](#)

VLAN Configuration

Parent Interface	em2 (00:0c:29:32:67:1c) - opt1
	Only VLAN capable interfaces will be shown.
VLAN Tag	110
	802.1Q VLAN tag (between 1 and 4094).
VLAN Priority	0
	802.1Q VLAN Priority (between 0 and 7).
Description	Management
	A group description may be entered here for administrative reference (not parsed).

[Save](#)

VLAN Configuration

Parent Interface	em3 (00:0c:29:32:67:26) - opt2
	Only VLAN capable interfaces will be shown.
VLAN Tag	80
	802.1Q VLAN tag (between 1 and 4094).
VLAN Priority	0
	802.1Q VLAN Priority (between 0 and 7).
Description	Professionels
	A group description may be entered here for administrative reference (not parsed).

[Save](#)

VLAN Configuration

Parent Interface	em4 (00:0c:29:32:67:30) - opt3
	Only VLAN capable interfaces will be shown.
VLAN Tag	90
	802.1Q VLAN tag (between 1 and 4094).
VLAN Priority	0
	802.1Q VLAN Priority (between 0 and 7).
Description	Visiteurs
	A group description may be entered here for administrative reference (not parsed).

[Save](#)

Sécurisation de l'accès par SSH depuis le réseau WAN:

SSH nous permettra d'accéder à la console de PfSense de manière sécurisée. Nous allons changer le port par défaut du protocole SSH en (2121). Nous pouvons également faire une authentification par clés privé/publique au lieu d'une authentification par mot de passe :

The left screenshot shows the PfSense 'System' menu with 'Advanced' highlighted. The right screenshot shows the 'Secure Shell' configuration page with the following settings: 'Enable Secure Shell' checked, 'SSH Key Only' set to 'Password or Public Key', 'Allow Agent Forwarding' checked, and 'SSH port' set to 2121.

N'oubliez pas de sauvegarder les changements.

Maintenant il faut une règle autorisant ssh sur l'interface **Wan** on va dans le menu **Firewall** >rules>WAN>add :

The screenshot shows the PfSense Firewall Rules configuration page. The 'Firewall' menu is highlighted, and the 'Rules' sub-menu is open. The 'WAN' interface is selected. The 'Add' button is highlighted.

On rentre les choix ci-dessous après il ne faut pas oublier d'enregistrer et d'appliquer les changements comme indiqué dans ces captures d'écrans.

The screenshot shows the 'Edit Firewall Rule' form with the following settings: 'Action' set to 'Pass', 'Interface' set to 'WAN', 'Address Family' set to 'IPv4', and 'Protocol' set to 'TCP'.

Destination

Destination Invert match **WAN address** Destination Address /

Destination Port Range (other) **2121** (other) **2121**

From Custom To Custom

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

Extra Options

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

Description **autoriser SSH**
 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

on applique les changements :



On essaye maintenant d'y acceder en SSH depuis notre machine dans le VLAN Management :

Le serveur PfSense nous donne ici son empreinte numérique de sa clé publique

```

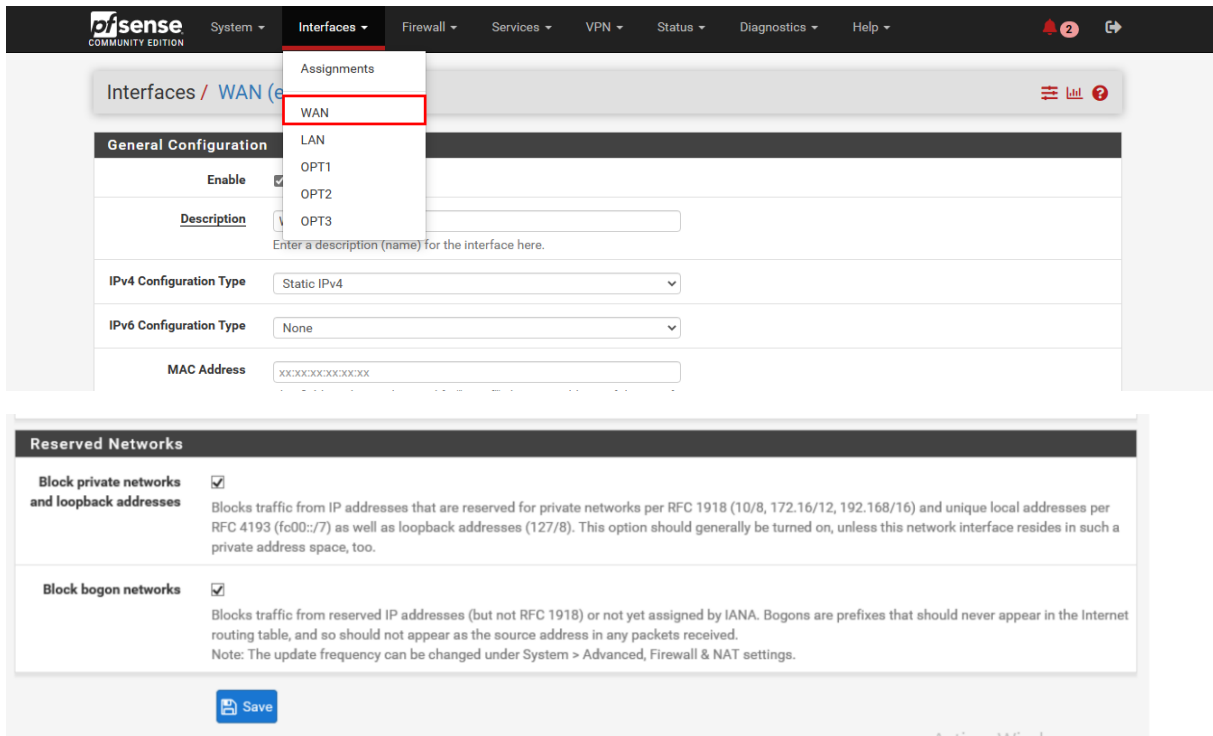
C:\Users\Administrateur> ssh admin@192.168.100.254 -p 2121
The authenticity of host '192.168.100.254 (192.168.100.254):2121)' can't be established.
ED25519 key fingerprint is SHA256:nUIHdeReX3exdlxGE2uMMeKN/FTFN7bLQFh9Vn9OAJQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.100.254:2121' (ED25519) to the list of known hosts.
Password for admin@heimdall.safetech.com:
VMware Virtual Machine - Netgate Device ID: 729824a65f6c5652da0a
*** Welcome to pfSense 2.7.1-RELEASE (amd64) on heimdall ***
WAN (wan)      -> em0      -> v4: 192.168.1.250/24
LAN (lan)      -> em1      -> v4: 192.168.100.254/24
OPT1 (opt1)   -> em2      -> v4: 192.168.110.254/24
OPT2 (opt2)   -> em3      -> v4: 192.168.00.254/24
OPT3 (opt3)   -> em4      -> v4: 192.168.90.254/24
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) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option:

```

On peut vérifier si l'empreinte numérique sur le serveur ssh est la même que celle envoyée par le serveur j'affiche le contenu détaillé du répertoire /etc/ssh après je génère l'empreinte numérique de la clé publique **ssh_host_ed25519_key.pub**.

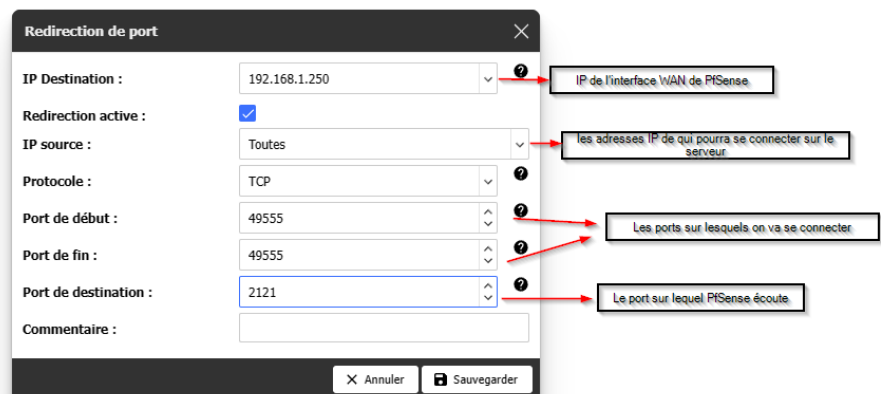
La clé correspond bien :



Maintenant pour accéder à notre serveur PfSense depuis l'extérieur en utilisant notre adresse publique.

Il faut tout d'abord :

- 1- Accéder à la boîte internet et ouvrir le port 22 en créant une redirection de port :



- 2- Déterminer notre adresse publique avec le site <http://www.whatismyip.com>.

- 3- Se connecter sur un serveur VPN et se connecter en SSH sur votre adresse IP publique avec le port configurée:



```
C:\Users\monceflaraki>ssh admin@ -p 49555
(admin@) | Password for admin@heimdall.Safetech.com:
VMware Virtual Machine - Netgate Device ID: 729824a65f6c5652da8a

*** Welcome to pfSense 2.7.1-RELEASE (amd64) on heimdall ***

WAN (wan)   -> em0     -> v4: 192.168.1.250/24
LAN (lan)   -> em1     -> v4: 192.168.110.254/24
OPT1 (opt1) -> em2     -> v4: 192.168.100.254/24
OPT2 (opt2) -> em3     -> v4: 192.168.80.254/24
OPT3 (opt3) -> em4     -> v4: 192.168.90.254/24

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) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

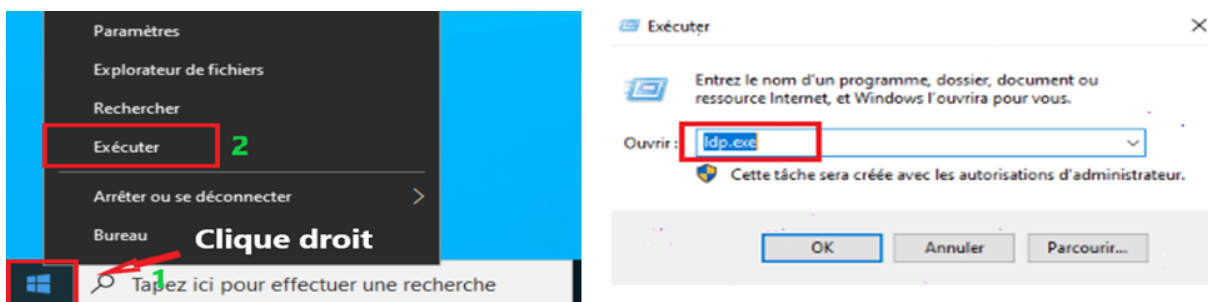
Enter an option: |
```

Nous pouvons désormais nous connecter sur notre serveur PfSense depuis n'importe où dans le monde.

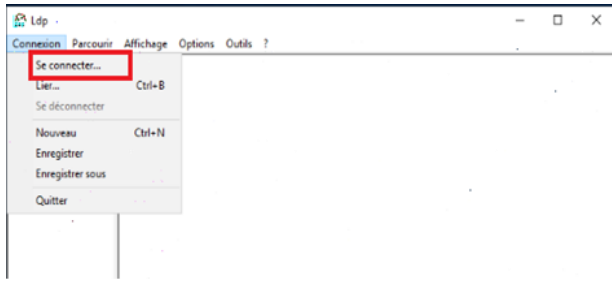
Test de la connectivité LDAP et LDAPS sur le serveur active directory SafetechDC :

Connectivité LDAP :

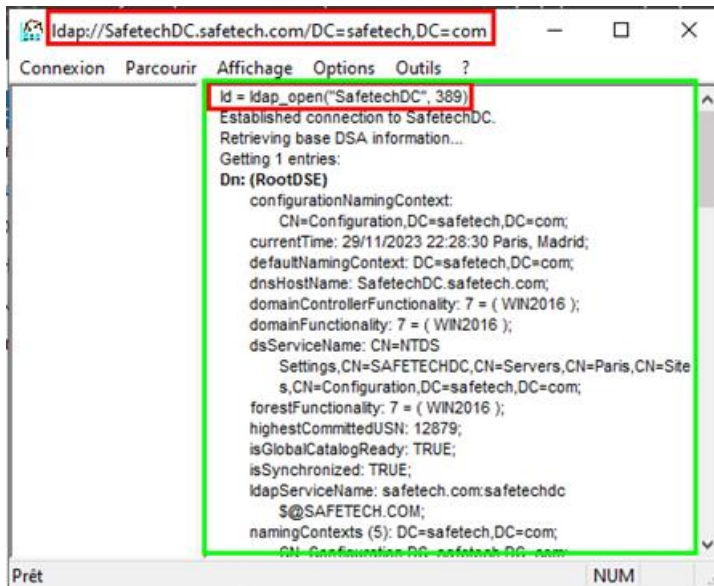
Sur le contrôleur de domaine on teste la connectivité LDAP standard, donc clique droit sur le menu démarrer + exécuter puis on tape **ldp.exe** pour ouvrir l'explorateur LDAP



Une fois l'explorateur LDAP est ouvert l'explorateur on choisit le menu Se connecter et on rentre le nom du serveur **Safetech.com** ainsi que le port de connexion **389**

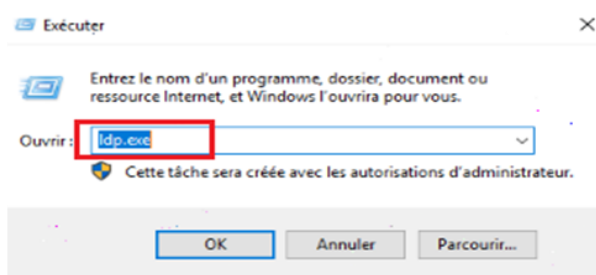
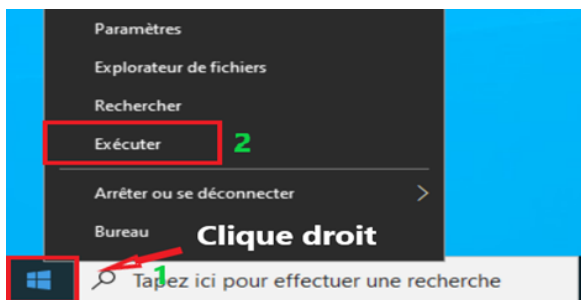


La connexion à la base d'annuaire fonctionne on peut identifier les partitions d'annuaire :

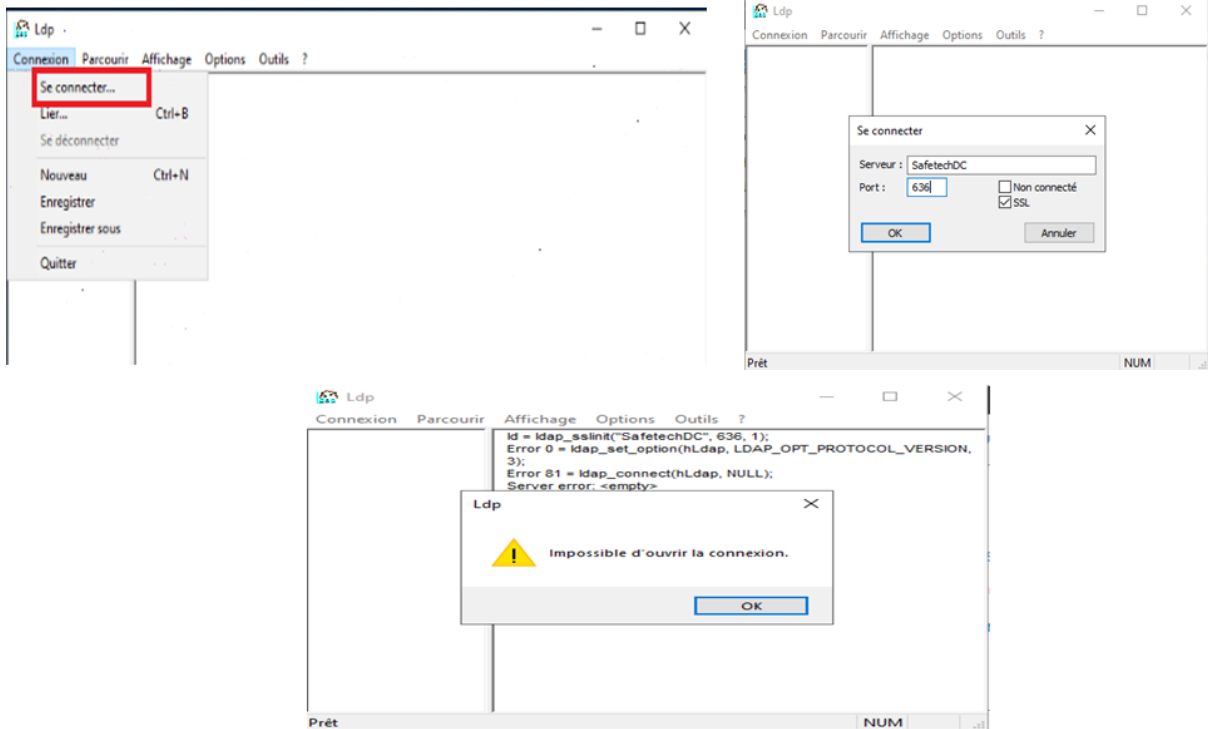


Connectivité LDAPS :

On fait la même chose que la procédure établissant une connexion standard on change juste le numéro de port et on coche SSL



On tombe sur un message d'erreur, le contrôleur de domaine ne supporte pas LDAPS car il n'est pas associé à un certificat.



Il existe deux méthodes pour activer LDAPS (LDAP sur SSL) sur un contrôleur de domaine :

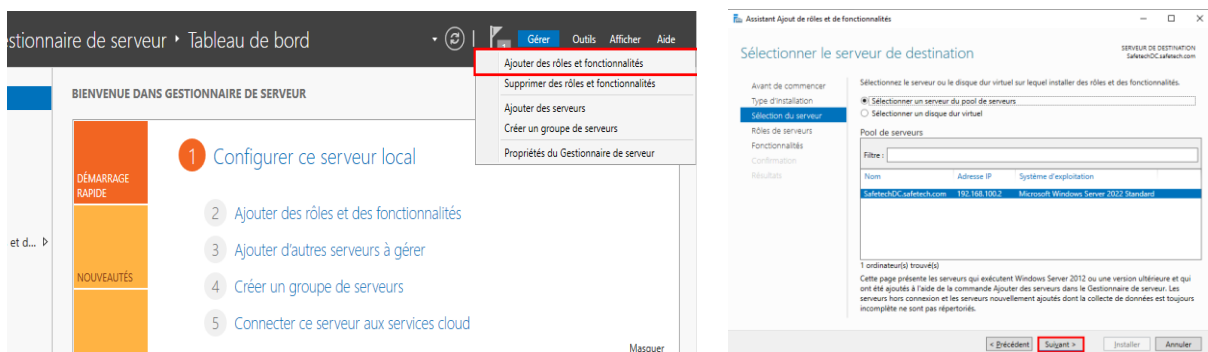
- Mettre un Certificat Racine sur le contrôleur de domaine en installant une autorité de certification racine sur SafetechDC
- Utiliser un certificat tiers sur le contrôleur de domaine. (SafetechDC)

Pour notre procédure on choisira la première méthode afin d'avoir un contrôle total sur la création, la gestion et l'expiration des certificats. Il nous faut donc installer une autorité de certification afin de tirer parti de LDAPS.

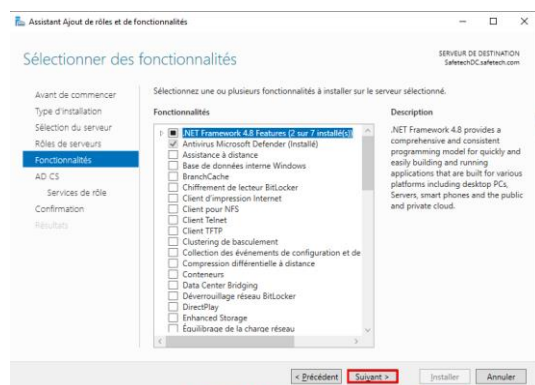
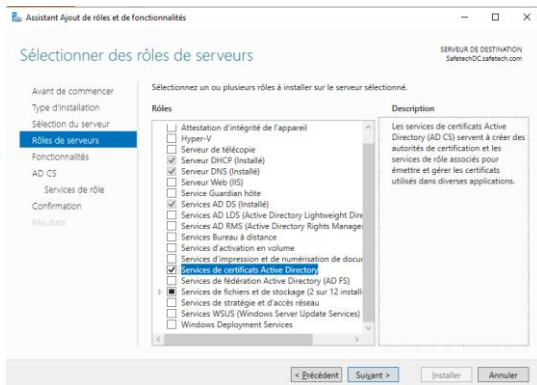
1. Création d'une autorité de certification sur le contrôleur de domaine SafetechDC :

Il est nécessaire d'installer le service autorité de certification. Pour fournir au contrôleur de domaine un certificat qui permettra au service LDAPS d'opérer sur le port 636.

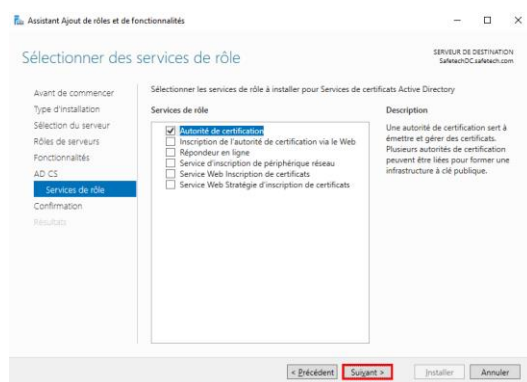
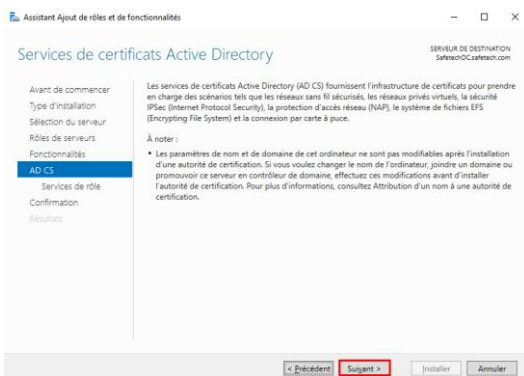
a. Ajouter le rôle certificat sur SafetechDC:



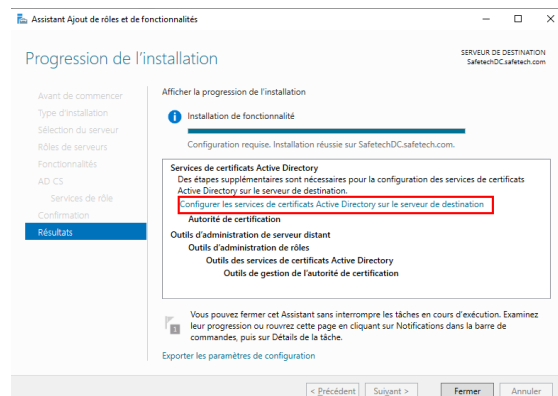
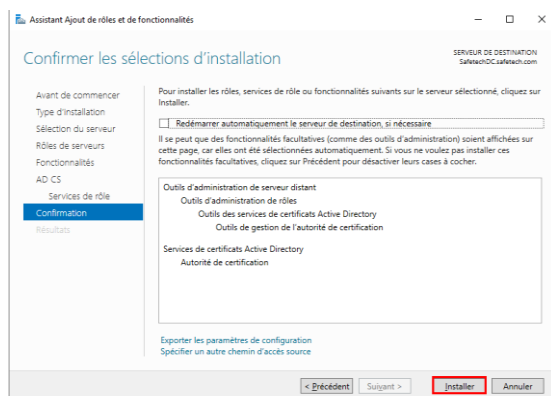
On coche Services de **Certificats Active Directory** et on rejoute les fonctionnalités



On sélectionne uniquement l'option **Autorité de certification**



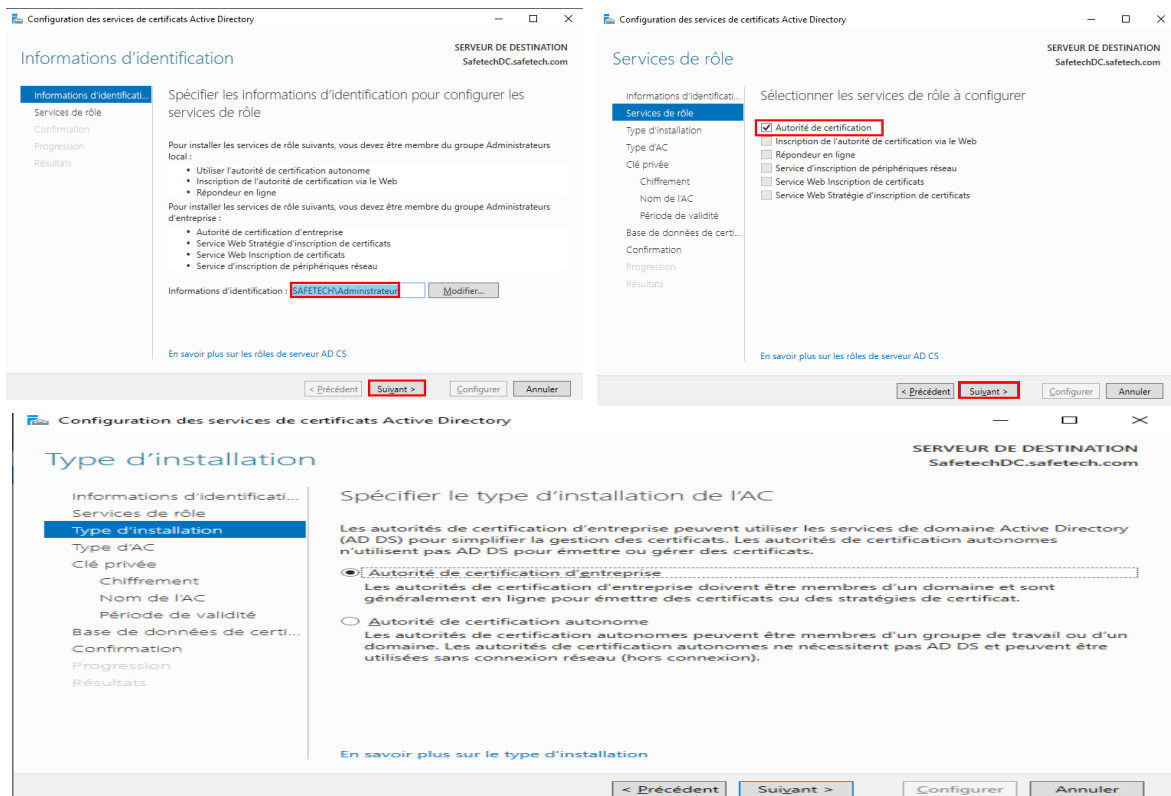
Dernière étape on clique sur le lien **Configurer les services Active Directory sur le serveur de destination**



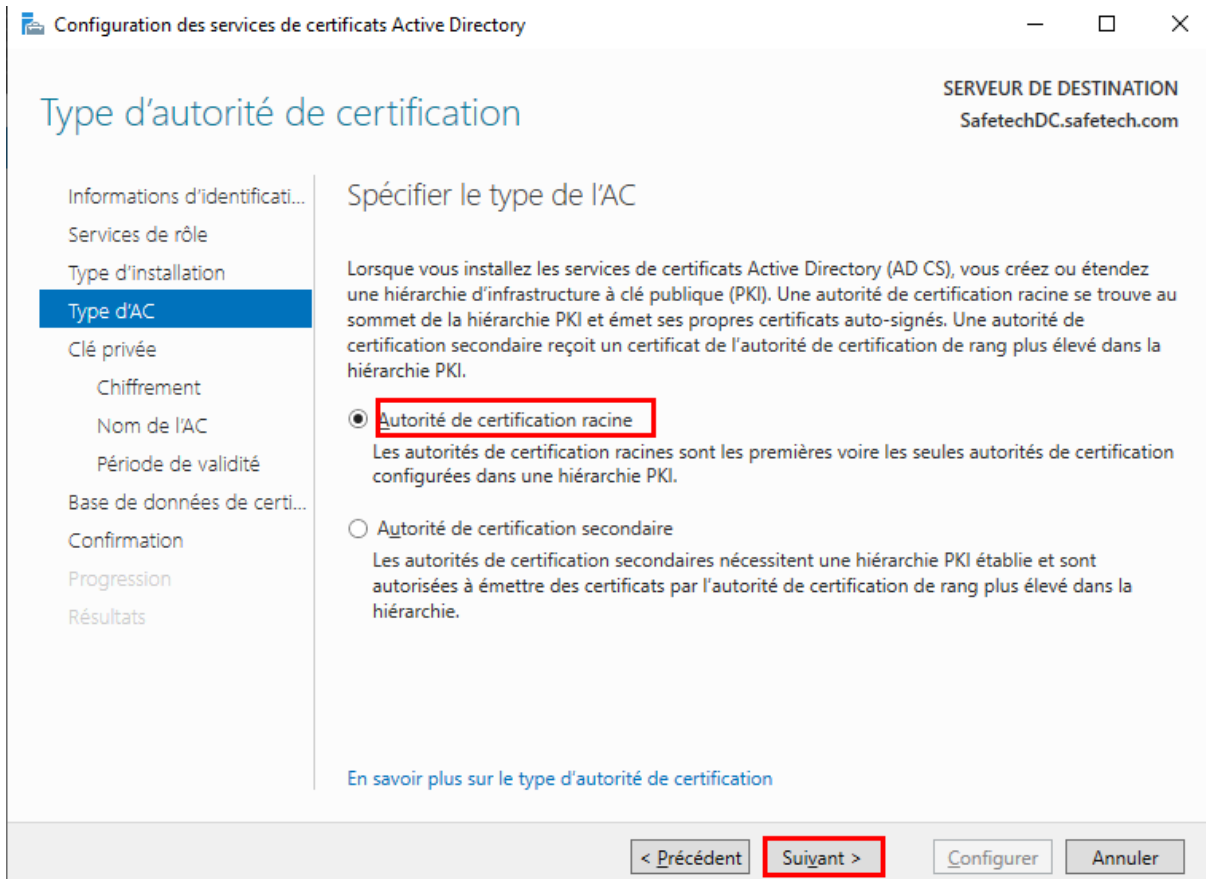
b. Configuration du rôle certificat sur SafetechDC:

Une fois le rôle certificat est installé il faut maintenant le configurer, on vérifie les informations d'identification, il est obligatoire d'être connecté avec le compte de l'administrateur de l'entreprise (domaine\administrateur).

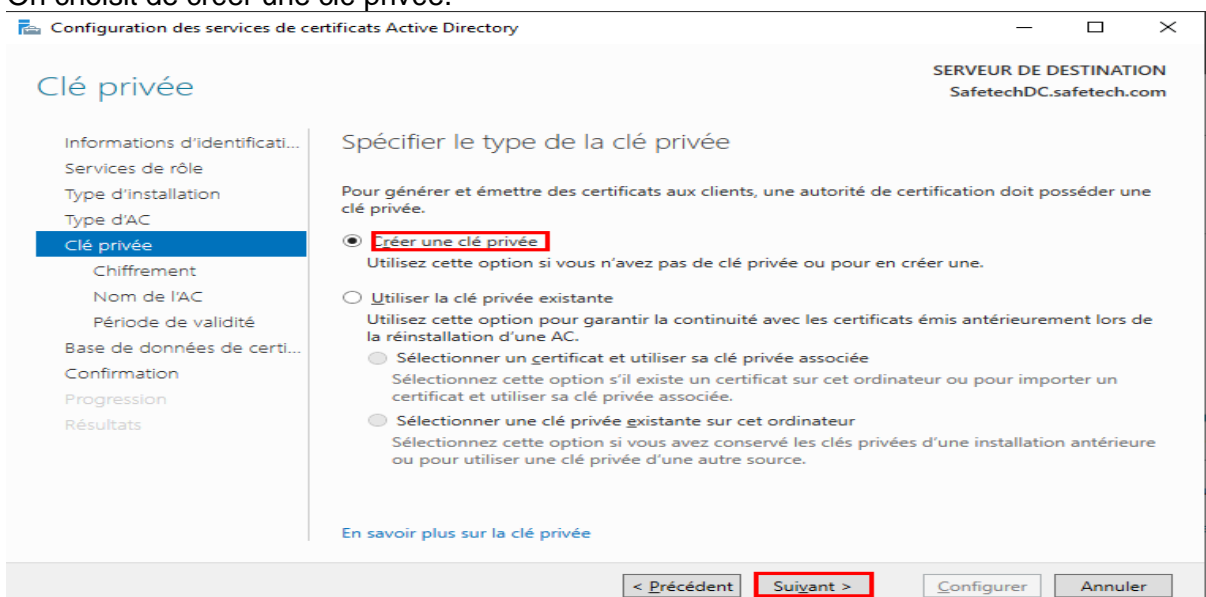
On coche après **Autorité de certification**, toutes les autres options on peut les installer après au besoin



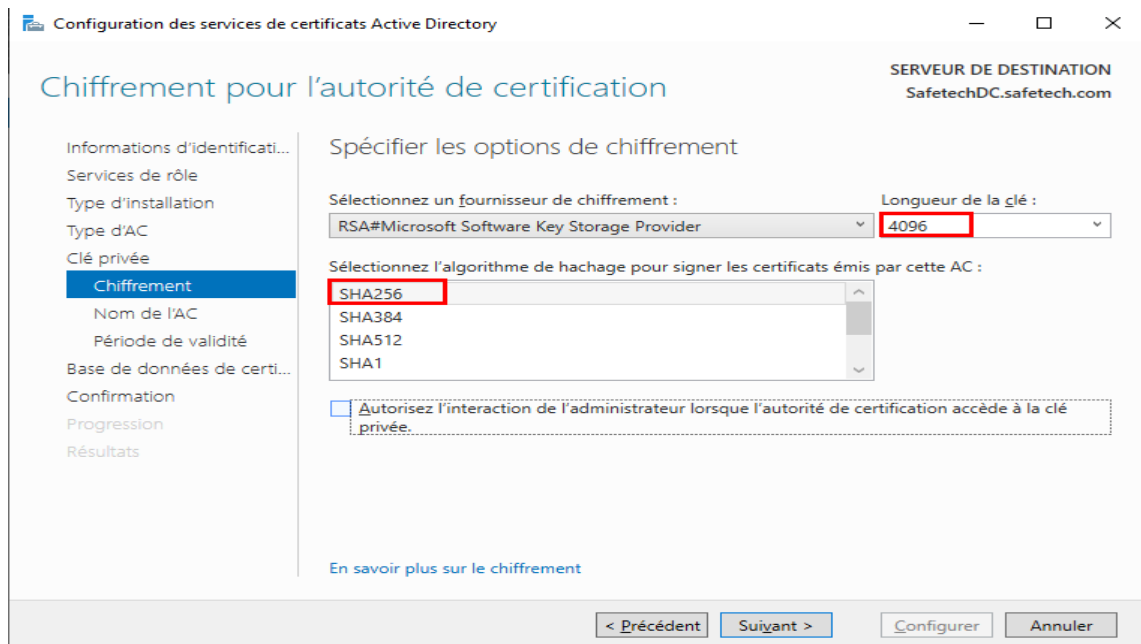
On sélectionne une autorité de certification racine, il est utile pour un intranet mais déconseillé pour un accès public. Puisque notre autorité n'est pas listée parmi les autorités de certification de confiance, les personnes utilisant des certificats émis par notre autorité de certification auront un avertissement mentionnant que nos certificats ne sont pas de confiance.



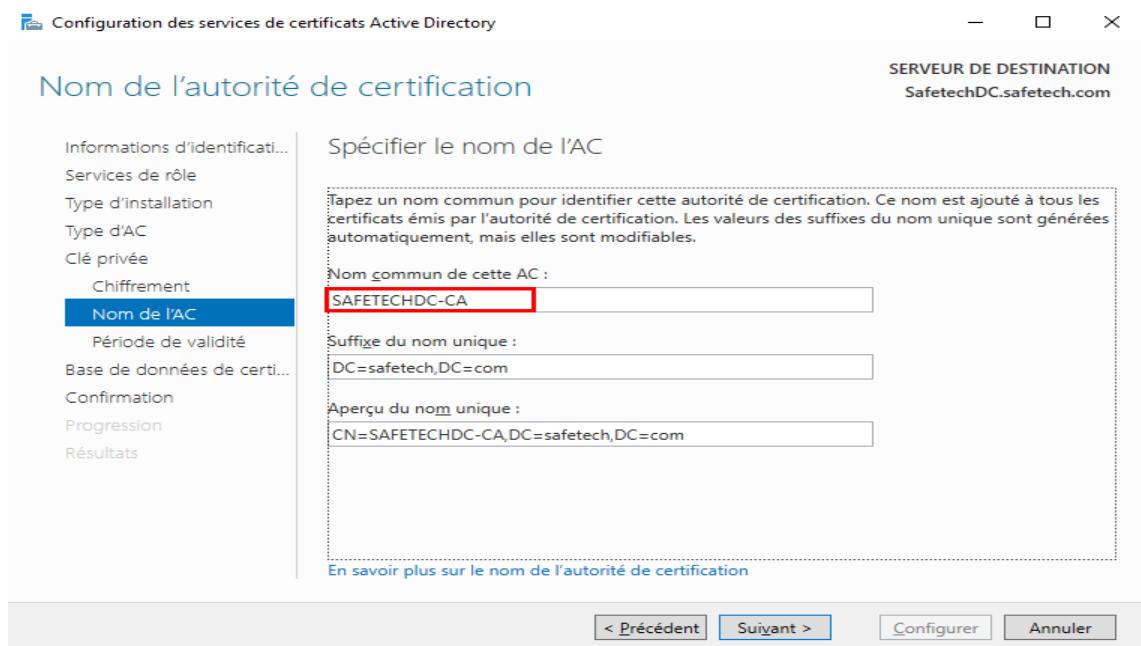
On choisit de créer une clé privée.



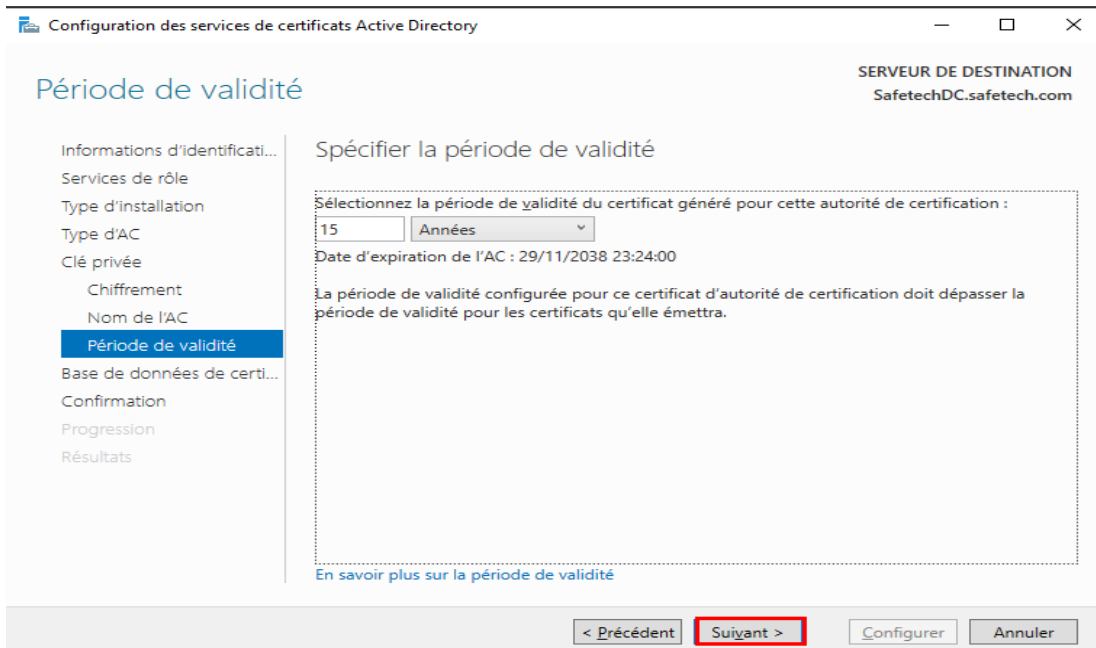
On choisit nos clés de chiffrement, plus les clés sont longues plus la sécurité est renforcée plus les performances seront impactées.



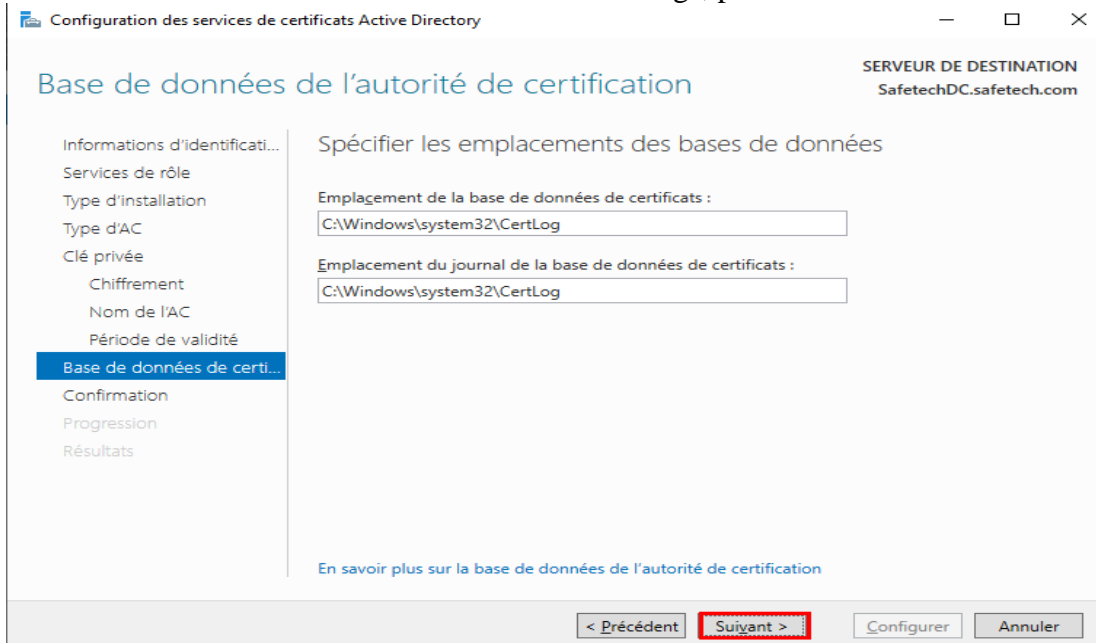
On peut modifier les valeurs par défaut ; je choisis SAFETECHDC-CA comme nom commun de ACR.



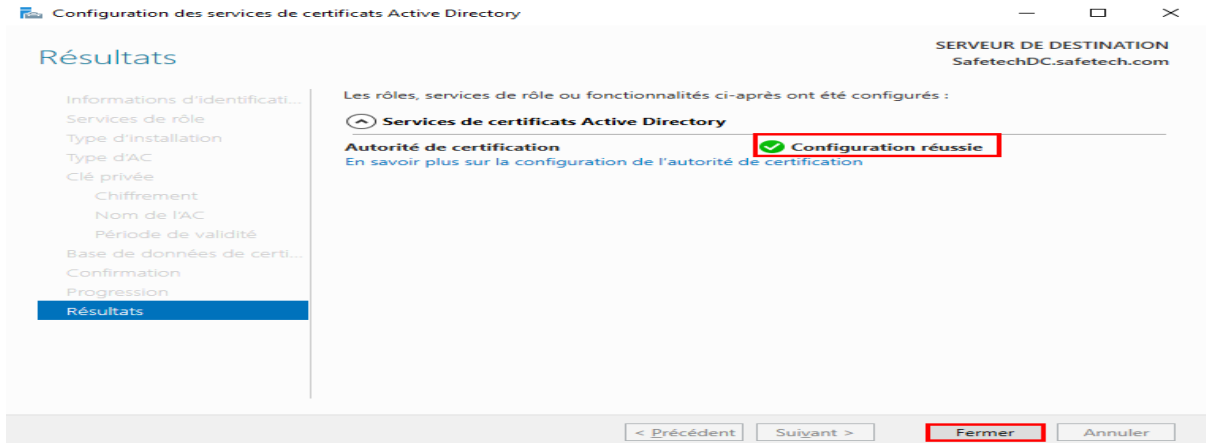
On rentre le période de validité pour le certificat de l'ACR., la période de validité du certificat de l'autorité de certification doit dépasser la période de validité des certificats émis.



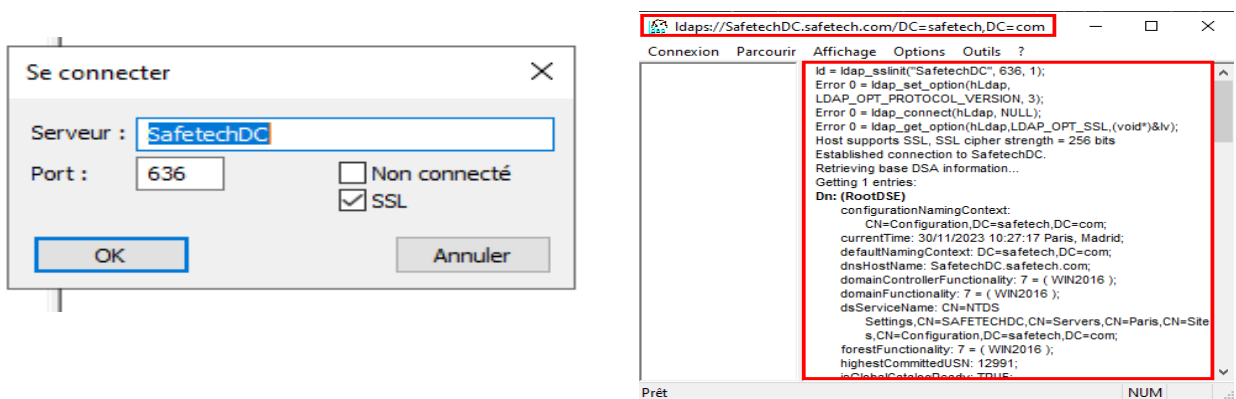
On laisse les dossiers des bases de données et des logs, par défaut.



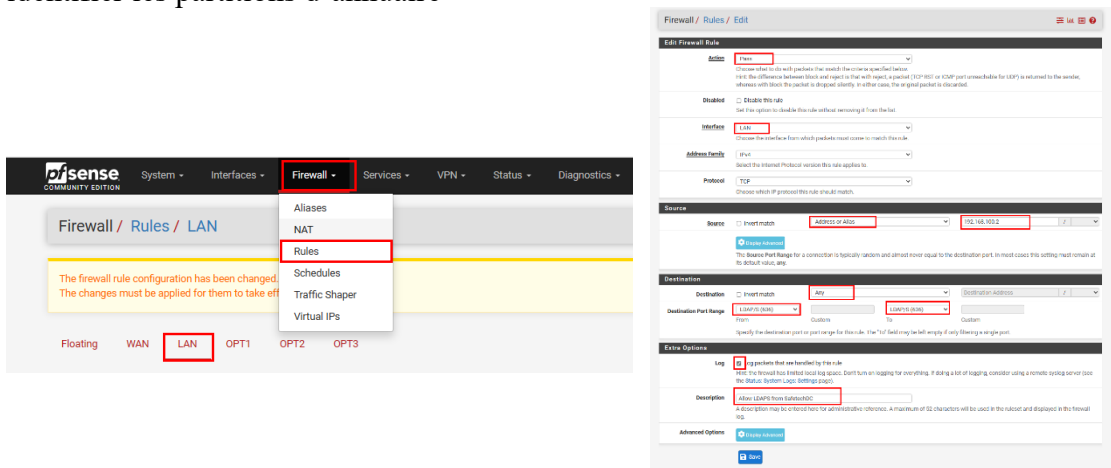
L'assistant nous affiche un résumé de la configuration choisie, on lance ensuite le processus



On reteste maintenant notre connexion LDAPS à partir de l'explorateur LDAP:

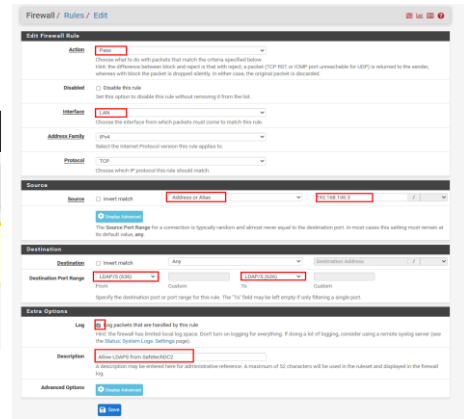
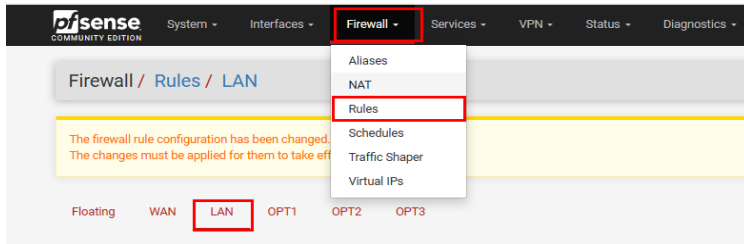


La connexion sécurisée utilisant le ssl sur le port 636 à la base d'annuaire fonctionne on peut identifier les partitions d'annuaire



Sur notre PfSense on crée une règle de sécurité pour autoriser le trafic LDAPS depuis notre contrôleur de domaine principal car il refuse ce trafic par défaut :

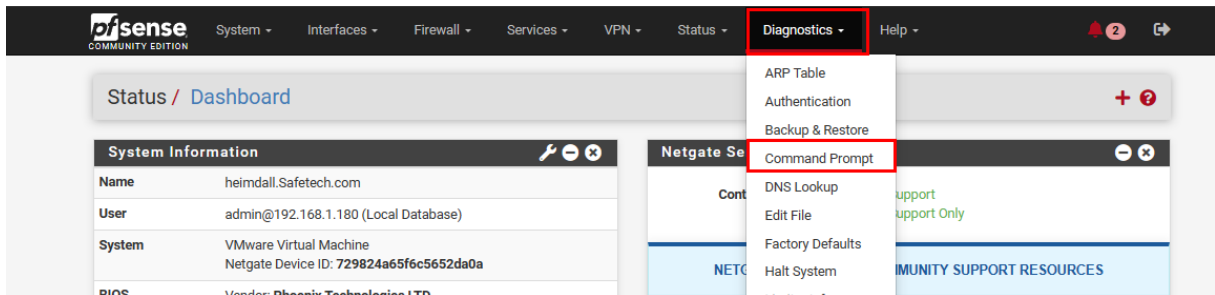
On crée une seconde règle pour autoriser le trafic LDAPS depuis notre contrôleur de domaine secondaire :



On test la connexion de PfSense à la base d'annuaire du contrôleur de domaine en tapant la commande suivante sur PfSense :

```
[2.7.1-RELEASE][admin@heimdall.Safetech.com]/root: openssl s_client -showcerts -connect 192.168.100.2:636 | less
```

On peut faire la meme chose sur l'interface web de pfsense pour tester la connexion de pfsense à la base d'annuaire du controleur de domaine :

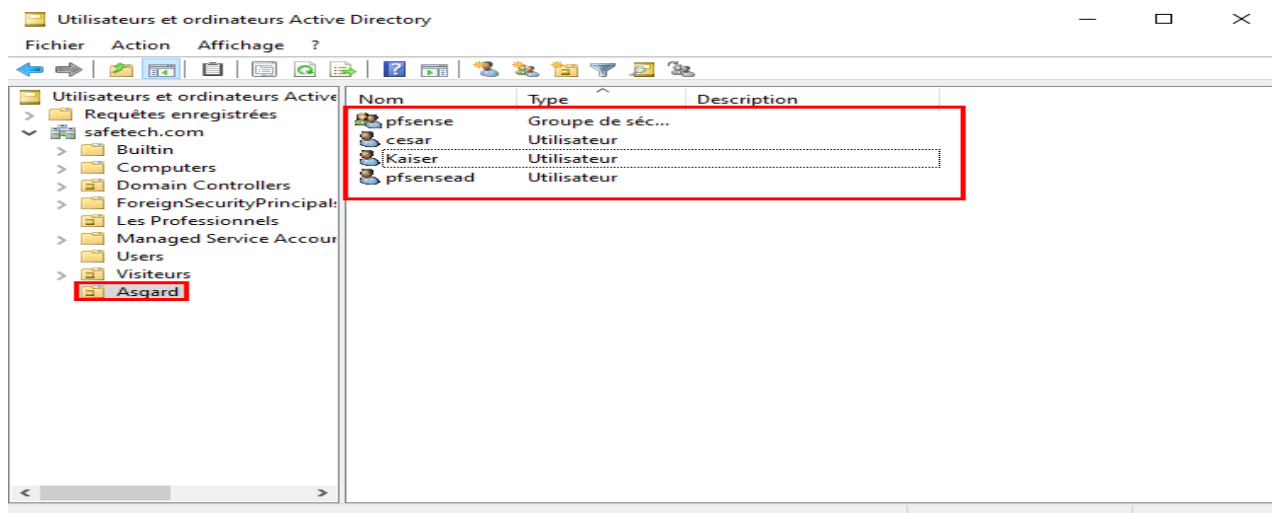
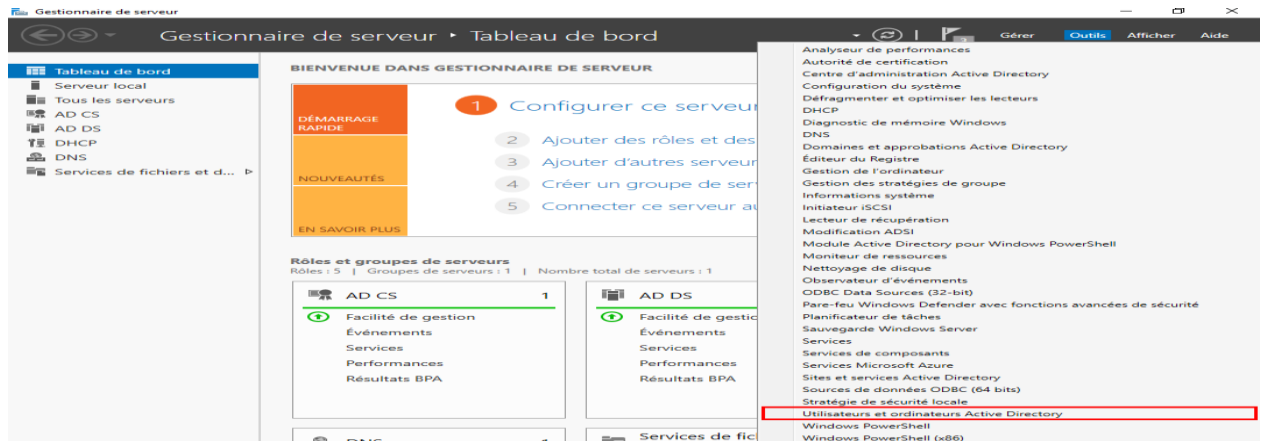


On exécute la commande suivante :

```
openssl s_client -showcerts -connect SafetechDC.safetech.com:636
```



Le contrôleur de domaine nous envoie le certificat qu'il utilise pour appliquer le ssl

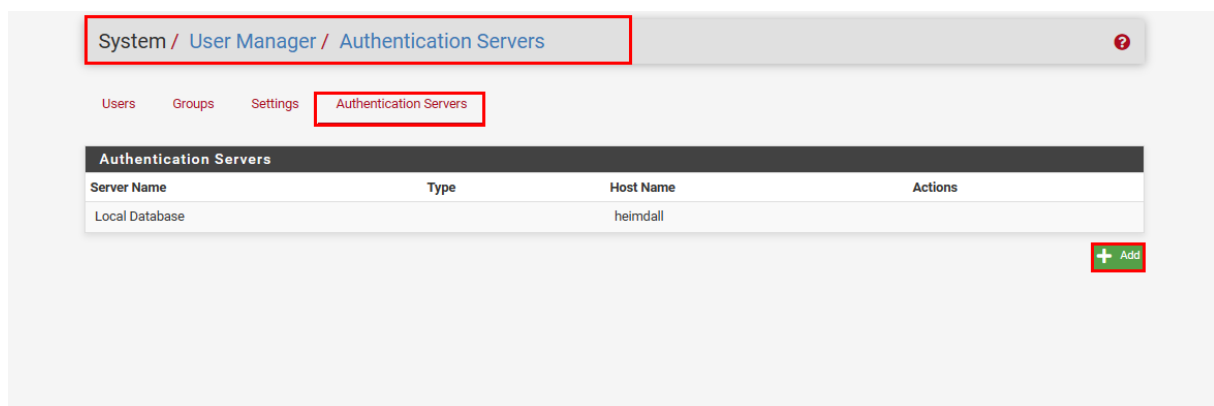


Ajouter le certificat créé par notre contrôleur de domaine :

Création des authentifications LDAPS sur le serveur PfSense :

Sur pfSense, une base locale est déjà disponible pour l'authentification des utilisateurs. Cependant, nous allons opter pour une autre méthode qui utilise l'authentification via LDAPS.

Pour créer cette authentification à partir du WebGUI, on va dans :



Et on remplit les champs avec les paramètres suivants :

Descriptive name	Authentication LDAPS
Type	LDAP
LDAP Server Settings	
Hostname or IP address	safetechdc.safetech.com
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	636
Transport	SSL/TLS Encrypted
Peer Certificate Authority	Global Root CA List
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=Safetech,DC=com
Authentication containers	cn
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	
Extended query	<input type="checkbox"/> Enable extended query
Bind anonymous	<input type="checkbox"/> Use anonymous binds to resolve distinguished names
Bind credentials	CN=pfensead,OU=Asgard,DC=safetech,DC=com
Initial Template	Microsoft AD
User naming attribute	samAccountName
Group naming attribute	cn

Dès que les champs sont remplis appuyez sur "Select a container"

mot de passe de l'utilisateur pfensead

En bas de la page nous avons le message suivant :

Could not connect to the LDAP server. Please check the LDAP configuration.

Le souci vient car PfSense ne reconnaît pas le certificat présenté par SafetechDC. Pour résoudre cela, nous allons importer le certificat de l'autorité de certification racine installé sur SafetechDC vers notre PfSense :

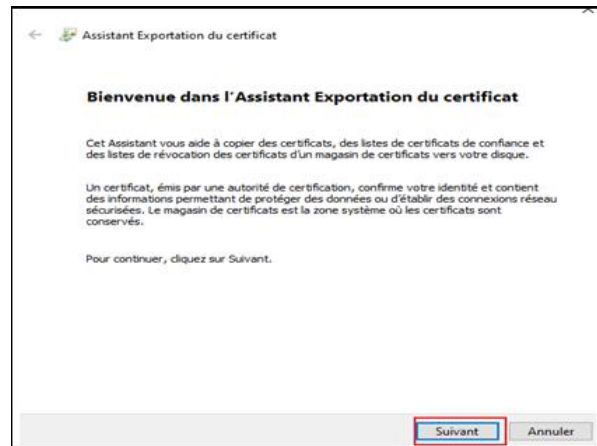
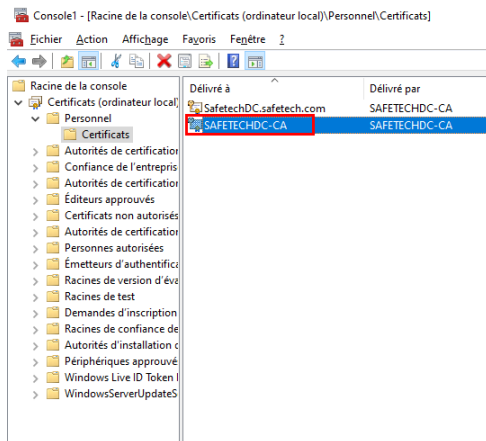
1. Exportation du certificat

Accéder à la console de gestion microsoft avec : WIN+R

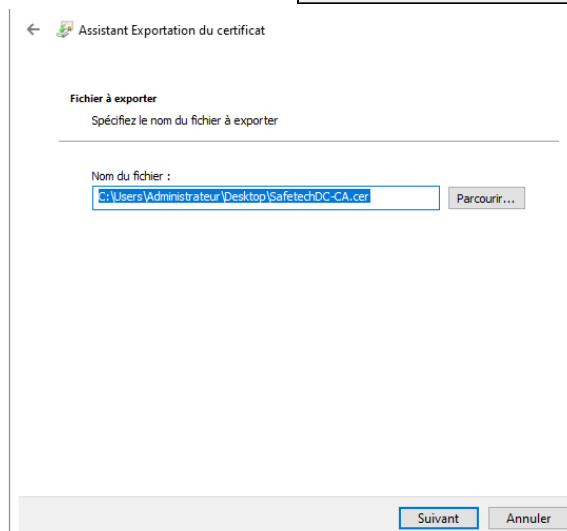
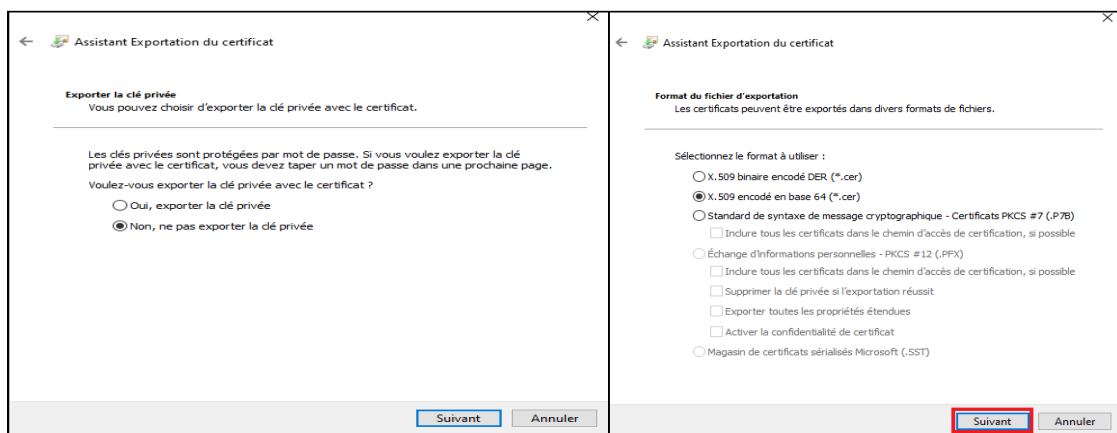
Fichier > Ajouter ou supprimer des composants logiciels enfichables

Ajouter les certificats > un compte d'ordinateur > Terminer

On exporte le certificat de l'autorité de certification racine au format '.cer' avec un nom qu'on choisit : clique droit > toutes les tâches > Exporter





Ne pas exporter la clé privée et on choisit **X.509 encodé DER (*.cer)** et en l'enregistre avec le nom SafetechDC-CA.cer



J'ouvre mon fichier SafetechDC-CA.cer avec le bloc note pour afficher le certificat de l'autorité de certification après on le copie pour l'insérer dans PfSense

Nous avons donc ce résultat :

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
SafetechDC_CA	<input checked="" type="checkbox"/>	self-signed	0	DC=safetech, DC=com, CN=SAFETECHDC-CA Valid From: Wed, 29 Nov 2023 23:17:20 +0100 Valid Until: Mon, 29 Nov 2038 23:27:19 +0100		 

On reteste la connexion LDAPS entre PfSense et SafetechDC dans SystemUser > Manager > Authentication Servers:

Descriptive name: Authentication LDAPS

Type: LDAP

LDAP Server Settings

Hostname or IP address: safetechdc.safetech.com

Port value: 636

Transport: SSL/TLS Encrypted

Peer Certificate Authority: SafetechDC_CA

Protocol version: 3

Server Timeout: 25

Search scope: Level

Base DN: DC=Safetech,DC=com

Authentication containers: cn

Bind credentials: CN=pfsensead,OU=Asgard,DC=safetech,DC=com

Initial Template: Microsoft AD

User naming attribute: samAccountName

Group naming attribute: cn

Group member attribute: memberOf

Select LDAP containers for authentication

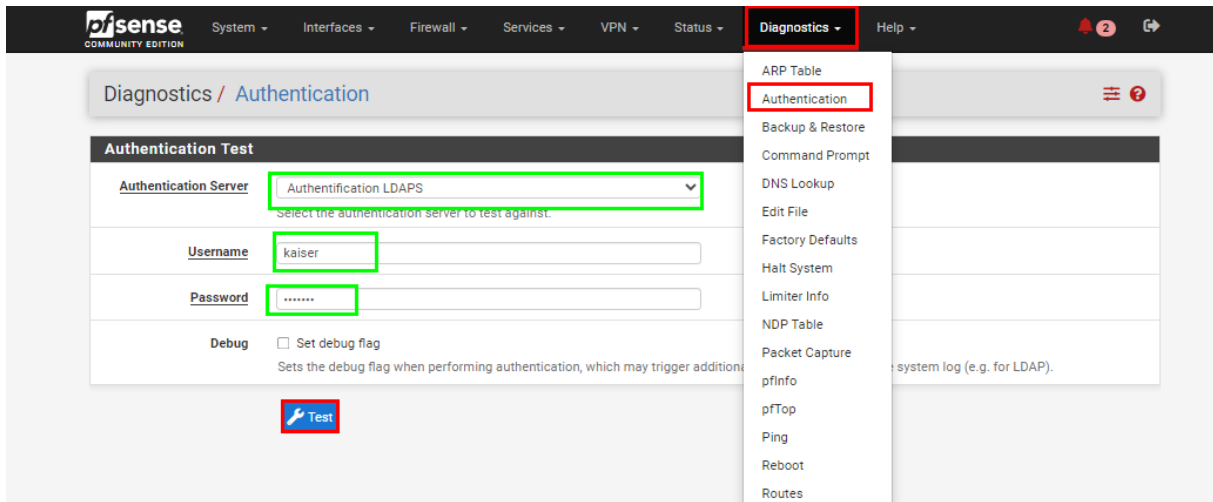
Containers

- OU=Asgard,DC=safetech,DC=com
- OU=Domain Controllers,DC=safetech,DC=com
- OU=Les Professionnels,DC=safetech,DC=com
- OU=Visiteurs,DC=safetech,DC=com
- CN=Users,DC=safetech,DC=com

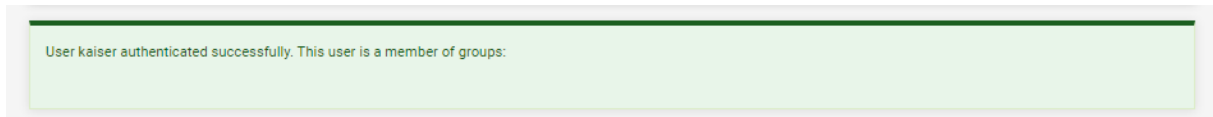
Save

Ensuite sauvegarder les modifications.

Test de l'authentification LDAPS sur PfSense :

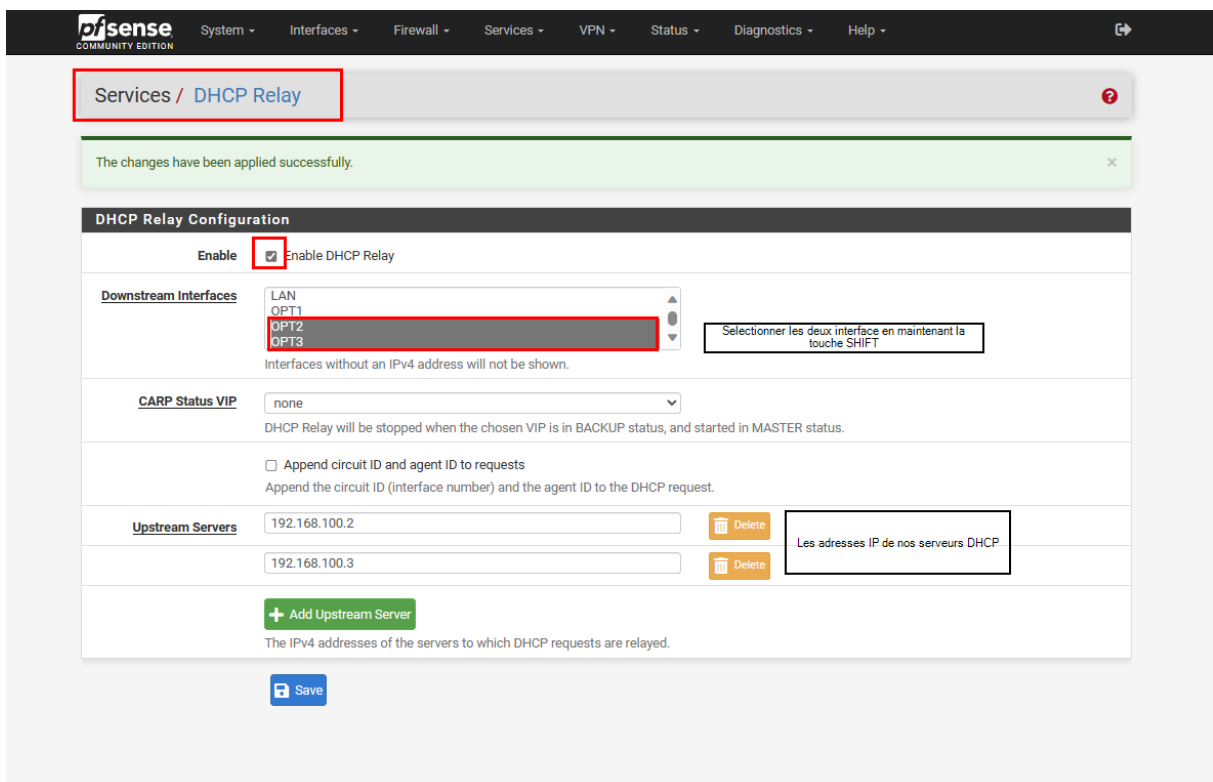


L'authentification avec LDAPs a réussi :



Configuration du relais DHCP sur PfSense :

Configurer notre PfSense comme relais DHCP permettra de relayer les requêtes DHCP des réseaux Professionnels et Visiteurs vers le réseau Serveurs. Ainsi les ordinateurs pourront obtenir leurs configurations réseaux.



Dans un ordinateur du réseau professionnel, mettre les paramètres IP en automatique (DHCP) :

Edit IP settings

Automatic (DHCP) ▼

Save Cancel

IP assignment:	Automatic (DHCP)	Edit
DNS server assignment:	Automatic (DHCP)	Edit
Link speed (Receive/Transmit):	1000/1000 (Mbps)	Copy
Link-local IPv6 address:	fe80::4e25:d6b0:fd81:4731%13	
IPv4 address:	192.168.80.2	
IPv4 DNS servers:	192.168.100.2 (Unencrypted) 192.168.100.3 (Unencrypted)	
Primary DNS suffix:	safetech.com	
Manufacturer:	Intel	
Description:	Intel(R) PRO/1000 MT Network Connection	
Driver version:	8.4.13.0	
Physical address (MAC):	00-0C-29-7F-6E-E2	

Nous remarquons que le PC a été configuré avec une adresse IP et que les informations DNS sont aussi remontées.

Règles autorisant zimbra :

Pas sûr si ça marche

Firewall / Aliases / Edit

Properties

Name Zimbra
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

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

Type Host(s) ▼

Host(s)

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

IP or FQDN 192.168.100.4 Description

Save + Add Host

Properties

Name Zimbra_Ports
The name of the alias may only consist of the characters 'a-z, A-Z, 0-9 and _'.

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

Type Port(s)

Port(s)

Hint Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port	Protocol	Action
25	SMTP	Delete
587	Email message submission (SMTP)	Delete
465	Authenticated SMTP over TLS/SSL (SMTPS)	Delete
110	POP3	Delete
993	IMAP over SSL	Delete
143	IMAP	Delete
995	POP3 over SSL	Delete
443	HTTPS	Delete

Save **+ Add Port**

Edit Redirect Entry

Disabled Disable this rule

No RDR (NOT) Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

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

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source [Display Advanced](#)

Destination Invert match. WAN address / Address/mask

Destination port range Other Zimbra_Ports Other Zimbra_Ports
From port Custom To port Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP Address or Alias Zimbra
Type Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, in must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80*) to local scope (:1)

Redirect target port Other Zimbra_Ports
Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

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

No XMLRPC Sync Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Filter rule association Add associated filter rule
The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

Save

Configuration du NAT pour les réseaux Visiteurs et Professionnels :

Il existe 3 types de NAT :

- Nat Statique
- Nat Dynamique
- PAT (Port Address Translation)

Ici nous allons configurer du PAT