

#### 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 premiere interface en bridge:

Virtu	al Machine Settings	
Hard	ware Options	
De	evice	Summary
	Memory	2.0 GB
÷.	Processors	1
	Hard Disk (SCSI)	20 GB
0	CD/DVD (IDE)	Using file E:\VM ISO\pfSense
5	Network Adapter	Bridged (Automatic)
5	Network Adapter 2	LAN Segment
5	Network Adapter 3	LAN Segment
5	Network Adapter 4	LAN Segment
5	Network Adapter 5	LAN Segment
	USB Controller	Present
	Sound Card	Auto detect
	Display	Auto detect
() 다 다 다 다 만 한 []	<ul> <li>CD/DVD (IDE)</li> <li>Network Adapter</li> <li>Network Adapter 2</li> <li>Network Adapter 3</li> <li>Network Adapter 4</li> <li>Network Adapter 5</li> <li>USB Controller</li> <li>Sound Card</li> <li>Display</li> </ul>	Using file E:\VM ISO\pfSense Bridged (Automatic) LAN Segment LAN Segment LAN Segment LAN Segment Present Auto detect 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 : <u>https://www.pfsense.org/download/</u>

Select Image To Download		
Version:	2.7.1	
Architecture:	AMD64 (64-bit)	< ❷
Installer:	DVD Image (ISO)	)) Installer 🗸
Mirror:	Frankfurt, Germ	nany 🗸
		Supported by
🕹 DOWN	ILOAD	💦 netgate
SHA256 Checksum 2056289d51cf70aae	for compressed (.gz) file: 2d7c56e887a1033926234l	4b79b7bbc817a91e8311cf2651bb

b- Lancement de l'installation

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





On laisse 20 gb par défaut

#### On choisit pfsense comme nom

New Virtual Machine Wizard	×
Name the Virtual Machine What name would you like to use for this virtual machine?	
Virtual machine name: Prisense	
Location:	-
C: (Users (pend) (pocuments (virtual Machines (Prsense	Browse
The default location can be changed at Edit > Preferences.	

## 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)
                    -> ем0
                                     -> v4/DHCP4: 192.168.1.140/24
                                          v6/DHCP6: 2a01:e0a:3cb:31b0:20c:29ff:fe32:6708
∕64
LAN (lan)
                                      -> v4: 192.168.1.1/24
                    -> ем1
                                               9) pfTop
10) Filter Logs
0) Logout (SSH only)
1) Assign Interfaces

    11) Restart webConfigurator
    12) PHP shell + pfSense tools

2) Set interface(s) IP address

    Reset webConfigurator password
    Reset to factory defaults

                                               13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
5) Reboot system
6) Halt system
7) Ping host
8) Shell
                                               16) Restart PHP-FPM
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 querty ; 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 -1 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
(ем0 ем1 ем2 ем3 ем4 ог а): ем0
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode
(ем1 ем2 ем3 ем4 a or nothing if finished): ем1
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
(ем3 ем4 a or nothing if finished): ем3
Enter the Optional 3 interface name or 'a' for auto-detection
(ем4 a or nothing if finished): ем4
The interfaces will be assigned as follows:
WAN
    -> ем0
LAN
     -> ем1
ОРТ1 -> ем2
ОРТ2 -> ем3
ОРТЗ -> ем4
Do you want to proceed [y¦n]? y
```

A la fin on doit avoir un résultat comme ça :

WAN (wan	) -> ем0	-> v4/DHCP4: 192.168.1.140/24 v6/DHCP6: 2a01:e0a:3cb:31b0:20c:29ff:fe32:6708
∕64		
LAN (lan	) -> ем1	-> v4: 192.168.1.1/24
OPT1 (op <sup>.</sup>	:1) -> ем2	->
OPT2 (op	:2) -> емЗ	$-\rangle$
OPT3 (op	t3) -> ем4	->

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 :

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

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



Source (1) (UNY) Exter the number of the interface you wish to configure: [1] Configure IP-4 address HAN interface via DHCP? (y/n) n Exter the num HAN IP-4 address. Press (ENTER) for none: > 122.168.1.259 Submet masks are untered as bit counts (as in CIDR notation) in pfSense. 0-9.955.255.0.8 (a) = 0 255.08.0.8 (b) = 0 Exter the num HAN IP-4 submet bit count (1 to 32): 24 Por a HAN, enter the num HAN IP-4 supercan gatemay address. > 0-2.155.254



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
                  = 8
     255.0.0.0
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 (emΘ - 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 (emθ - 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: &gt; 192.168.90.254</enter>
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense. e.g. 255.255.255.0 = 24 255.255.0.0 = 16 255.0.0.0 = 8
Enter the new OPT3 IPv4 subnet bit count (1 to 32): > 24
For a WAN, enter <u>the new</u> OPT3 IPv4 upstream gateway address. For a LAN, press <mark><enter></enter></mark> for none: >
Configure IPv6 address OPT3 interface via DHCP6? (y/n) n
Enter the new OPT3 IPv6 address. Press <pre><enter></enter></pre> 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 controleur de domaine : SafetechDC :

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

/otre connexion n'est p	pas privée
es utilisateurs malveillants essaient peut- par exemple, les mots de passe, les mess	être de voler vos informations de <b>192.168.100.254</b> ages ou les cartes de crédit).
IET::ERR_CERT_AUTHORITY_INVALID	
Masquer les éléments avancés	Retou
Ce serveur n'a pas pu prouver qu'il s'ag	git de <b>192.168.100.254</b> . Son certificat de sécurité
l'est pas approuvé par le système d'ex ine mauvaise configuration ou à un uti	ploitation de votre ordinateur. Cela peut être dû ilisateur malveillant qui intercepte votre connexio

Nous arrivons ensuite dans la fenêtre de connexion de PfSense :

<b>of</b> sense		Login to pfSense
	SIGN IN	
	SIGN IN	

Connectez-vous avec les identifiants suivants :

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

## Execution du Wizard de la configuration de base :

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.	Netgate® Global Support is available 24/7
Wizard / pfSense Setup /	Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise – on premises to cloud.
alGaza Satua	We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:
Welcome to p/Sense® software! This wized will provide guidance through the initial configuration of p/Sense. The wized mark be stopped at any time by clicking the logo image at the top of the screen.	<ul> <li>Support is available 24 hours a day, seven days a week, including holidays.</li> <li>Support engineers are located around the world, ensuring that no support call is missed.</li> <li>Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.</li> </ul>
pfanne's software is developed and maintained by brigates	Learn more
3) find	35 Next

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
--------------------------	--------------

General Information	
	On this screen the general pfSense parameters will be set.
Hostname	hemdall
	Name of the frewall host, without domain part.
	Examples: phonos, firmual, edgelw
Domain	Safetech.com
	Domáin name for the frewall.
	Examples: home arps, example.com
	Do not end the domain name with 'Jossi' as the Final part (Top Level Domain, TLD). The 'Jossi' TLD is widely used by rdDNG (e.g. Arabh, Borpour, Rendercoux, Aryner, Araphay) and some Windows agatemes and networked donates. These will not network correctly if the router usee Youal as its TLD Arbitransfers such as Norma agat, Coadia (or 'rmylocal' are used.
	The durbat behavior of the DNS Resolver will ignore manually configured DNS servers for cleart queries and query root DNS servers directly. To use the manually configured DNS servers below for cleart queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the votand.
Primary DNS Server	192.166.100.2
Secondary DNS Server	1982.168.100 3
Override DNS	a
	Aliuw DNS servers to be oversidden by DISCP/PPP on WAN
	39 Nort

Time Server Informa	tion
	Please enter the time, date and time zone.
Time server hostname	fr.pool.ntp.org Enter the hostname (FQDN) of the time server.
Timezone	Europe/Paris v
	» Next

## L'interface WAN est déjà configurée

## L'interface LAN est déjà configurée

		Configure LAN Interf	ace
Configure WAN Inter	ase On this screen the Wide Area Network Information will be configured.		On this screen the Local Area Network information will be configured.
General configuratio	state v	LAN IP Address	192.168.100.254
MAC Address	This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: excensescences or leave Mark.		Type dhcp if this interface uses DHCP to obtain its IP address.
мти	- Bet the MTU of the WAN interface. If this field is left blank, an MTU of 1 492 bytes for PPPOR and 1500 bytes for all other connection types will be	Subnet Mask	24 👻
MSS	anumed  v v subar is entend in this full; then MIS clamping to TCP connectors to the value entend above minus 40 (TCP) P hader stop will be in effect. If the field in MIS visuality entends and the VPVAE and TSD bytes final other connection types will be anzened. The should much the above MIS value in event all events.		» Next

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

	Step 6 of 9
Set Admin WebGUI P	assword
	On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.
Admin Password	
Admin Password AGAIN	•••••
	>> Next

Appliquer la configuration en appuyant sur Reload :

Reload configuration	
Click 'Reload' to reload pfSense with new changes.	
» Reload	

On clique sur Finish pour finir la configuration :

Wizard completed.	
	Congratulations! pfSense is now configured.
	We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.
	Check for updates
	Remember, we're here to help.
	Click here to learn about Netgate 24/7/365 support services.
	User survey
	Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)
	Anonymous oser survey
	Useful resources.
	Learn more about Netgate's product line, services, and pfSense software from our website     To learn about Netgate appliances and other offers, while our store
	Become part of the pfSense community. Visit our forum
	Subscribe to our newsletter for ongoing product information, software announcements and special offers.
	Finish

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 :

System /	Advanced Certificates	0	
	General Setup		-
The changes ha	High Availability	iully. ×	
	Package Manager		
System	Register		
	Routing		
Ŀ	Setup Wizard		
	Update	e firewall host, without domain part.	
	User Manager	com	
	Logout (admin)	ne for the firewall.	
	Do not en Rendezvo Alternativ	d the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, us, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. es such as 'home anna'. 'local lan'. or 'mvlocal' are safe.	).

## Ensuite nous allons appliquer les paramètre suivants :

System	
Hostname	heimdall Name of the firewall host, without domain part.
Domain	Safetech.com         Domain name for the firewall.         Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.
DNS Server Settings DNS Servers	192.168.100.2 Safetechdc.safetech.com
	192.168.100.3       safetechdc2.safetech.com       Imit Delete         Address       Hostname       Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query       Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).         Forwarding enabled.       Forwarding enabled.       Enter the DNS Resolver (optional).
Add DNS Server	+ Add DNS Server
DNS Server Override	Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if Pull DNS option is enabled) for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.
DNS Resolution Behavior	Use remote DNS Servers, ignore local DNS By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.

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

	System - Interfe	aces - Firewall - Services - VF		System -	Interfaces - Firewall -	Services + VPN +	Status - Diagnostie	:s → Help →	¢
Status / [	Advanced Cert. Manager		System	/ Package	Manager / Available F	Packages			0
System Info	General Setup High Avail. Sync	۶03	Installed Pa Search	ckages Ava	ilable Packages				Θ
Name	Logout (admin)	m	Search terr	n	shellcmd 2		Both	V Q Search O Clear	
User	Package Manager	IO (Local Database)			Enter a search string or *nix regu	lar expression to search packa	age names and descriptions.		
System	Routing	line	Packages	1					
	Setup Wizard	4d3074036c51f90169	Name	Version	Description				
BIOS	Update	nnologies LTD	Shellomd	1.0.5_3	The shellomd utility is used	to manage commands on sys	stem startup.		+ Install
	User Manager	w 12 2020							
Version	2.5.2-RELEASE (am built on Fri Jul 02 15 FreeBSD 12.2-STABI	d64) :33:00 EDT 2021 LE							
	Version 2.7.0 is avai Version information	lable. 🚯 updated at Wed Nov 29 10:48:15 CET 2023							

Installed Pack	ages .	Available Packages	Energia System - Interfaces - Firewall -	Services • VPN -	Status + Diagnostics +	Help +	G
Search	_		System / Package Manager / Package In	Auto Config Backup Captive Portal DHCP Relay			0
Search term		Inter a search string or vitix regular expression to search package names and descriptions.	pfSense-pkg-Open-VM-Tools installation successfully completed	DHCP Server DHCPv6 Relay			
Packages			Installed Packages Available Packages Package Inst	DHCPv6 Server DNS Forwarder			
Name	Version	Description		DNS Resolver			
Open-VM- Tools	10.1.0_5,1	Valeware Tools is a suite of kellities that enhances the performance of the virtual machine's guest operating system and improves	Package Installation [2/3] Extracting open-vm-tools-moxil-12.3.5,2: [3/3] Installing pfSense-pkg-Open-VM-Tools-10.1.0.5,1, [3/5] Extracting pfSense-pkg-Open-VM-Tools-10.1.0,5,1, [3/5] Extracting pfSense-pkg-Open-VM-Tools-10.1.0,5,1,0,5,	Dynamic DNS IGMP Proxy NTP PPPoE Server			-
		Ø open vm tools 12.3.0,2	Saving updated package information done. Loading package configuration done.	Router Advertisement Shellomd			
			Configuring package components Loading package instructions	SNMP			
			Custom commands Executing custom.jbm_initall_command()done. Servicesdone. iwriting configuration done. >>> Cleming up cachedone. Success	UPnP & NAT-PMP Wake-on-LAN			ļ

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

ackage / Sen	rices: Snellomd Settings										
mand	Shelicmd Type	Desi	cription		Shellcmd	Configuratio	khinntrol J /usr/share/s	sons/keymans/fr isn kt	d		
				+ 100			Enter the command to run.	aconarieritegi negar maoria	~		
					Sh	elicmd Type	shelicmd Choose the shelicmd type. Clic	k Info for details. 🕕	۷		
e						Description	clavier en français				
							Enter a description for this con	mand. (This is for your r	eference only.)		
							🖬 Save				
uris	ation de	la consol	le PfSen	se :							
curis	ation de	la conso	le PfSen	se :							
curis	ation de	la conso	le PfSen	se :		Bamanha	r notantial attackers for u	to detection time a	conside hofore rea	etting their score	
curis ense	ation de	la conso	le PfSen	se :		Remembe	r potential attackers for u	o to detection_time s	econds before res	etting their score.	
uris ense	sation de System • Inter Advanced	la conso	le PfSen Services +	Se:	Pass list	Remembe	r potential attackers for u	o to detection_time s	econds before res	etting their score.	
ense ense ity edition atus /	System • Inter Advanced Certificates	la conso faces - Firewall -	le PfSen	SE : VP	Pass list	Remember Address Addresse	r potential attackers for up s added to the pass list wil	o to detection_time s / 128 v I bypass login protect	econds before res	etting their score.	
curis ense atus /	System - Inter Advanced Certificates General Setup	la conso faces - Firewall -	le PfSen	se : vP	Pass list Add address	Remembe Address Addresse: + Add a	r potential attackers for up s added to the pass list wil cdress	to detection_time s	econds before res	etting their score.	
ense ense atus /	System • Inter Advanced Certificates General Setup High Availability	la conso	le PfSen services -	se : vP	Pass list Add address	Remember Addresser Addresser	r potential attackers for u a added to the pass list wil	to detection_time s / 128 ▼ I bypass login protect	econds before res	etting their score.	
ense ense ity fortion atus / stem Inf	System - Inter Advanced Certificates General Setup High Availability Package Manager	la conso faces - Firewall -	le PfSen Services -	se : ve	Pass list Add address Serial Communicatio	Remember Address Addressee Addressee Addressee	r potential attackers for u s added to the pass list wil ddress	to detection_time s / 128 ▼ I bypass login protect	econds before res	etting their score.	
ense ense ity fortion atus / stem Inf	System - Inter Advanced Certificates General Setup Package Manager Register	faces - Firewall -	le PfSen Services -	se : ve	Pass list Add address Serial Communication Serial Terminal	Remember Addresser Addresser Addresser Addresser Remember Addresser Remembe	r potential attackers for u a added to the pass list wil ddress s the first serial port with	to detection_time s	econds before res tion.	etting their score.	ow.
ense ense atus / atus / atus Inf	System - Inter Advanced Advanced Certificates General Setup General Setup General Setup Package Manager Register Routing	faces - Frewall - m 0 (Local Database) ine	le PfSen Services -	se : v	Pass list Add address Serial Communicatio Serial Terminal	Remember Address Addresser Addresser Remember Addresser Remember Addresser Remember	r potential attackers for up a added to the pass list will didress as the first serial port with will redress the comession	o to detection, time s / 128 ~ I bypass login protect 115200/8/N/1 by de utput and message	econds before res tion.	etting their score. beed selectable bel The console menu serial console.	iow.
ense atus / stem Inf e	Advanced Advanced Certificates General Setup High Availability Package Manager Register Routing Setup Wizard	faces Firewall -	le PfSen services - / C C	se :	Pass list Add address Serial Communicatio Serial Terminal	Remember Address Addresset Addresset Addresset Addresset Construction Note: This construction	r potential attackers for up a ddded to the pass list will ddress as the first serial port with will redirect the console e and .A null modern serial	o to detection_time s / 128 v I bypass login protect 115200/8/N/1 by de utput and message cable or adapter is r	econds before res tion. fault, or another sp fault, or another sp to the serial port. equired to use the	etting their score. Deed selectable bel The console menu serial console.	ow. L can still be accessed from th
ense ense atus / atus /	Advanced Internet Advanced Certificates General Setup High Availability Package Nanager Routing Setup Wizard Update	faces Firewall - m 0 (Local Database) ine 19924a65f6c5652dat mologies LTD	le PfSen Services - Ja	se :	Pass list Add address Serial Communicatio Serial Terminal Serial Speed	Remember Address Addresset Addresset Addresset Addresset Canable Note: This card/Negto	r potential attackers for u a dded to the pass list wil ddress is the first serial port with will redirect the console and A null modern serial	b to detection_time s 1 28 v bypass login protect 1 15200/8/N/1 by de utput and message cable or adapter is r	econds before res tion. fault or another sg to the serial port. equired to use the	etting their score.	low. Li can still be accessed from th
ense atus / stem Inf	Advanced Advanced Advanced Certificates General Setup High Availability Package Manager Register Register Routing Setup Wizard Updr	m o (Local Database) into 19824a55fc5552dat mologies LTD 112 2020	le PfSen Services -	se : vP	Pass list Add address Serial Communication Serial Terminal Serial Speed	Remembe Addresse Addresse Addresse Rodersse Rodersse Note: This card/keyb 115200 Allows se	r potential attackers for u a added to the pass list will address is the first serial port with will redirect the console e and A null modern serial action of different speads	to detection_time is / 128  / 128	econds before res	etting their score.	iow. u can still be accessed from th

Password protect the console menu Cocher la case

On Constate que la console nous demande le login :

ion information updated at Wed Nov 29 12:22:16 CET 2023

12th Gen Intel(R) Core(TM) i5-12400F AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No

Versi

СРИ Туре



Console menu

🖬 Save

## Création de VLAN :

Interfaces / VLA	Ns / Edit	≢ 😧
VLAN Configuration		
Parent Interface	em1 (00:0c:29:32:67:12) - Ian   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).	
VLAN Configuration Parent Interface	em2 (00:0c:29:32:67:1c) - opt1	
VLAN Tag	Only VLAN capable interfaces will be shown.           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	

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).	
	D Saus	
	E Save	

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).	

## 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 :

COMMUNITY EDITION	System - Interfa	aces + Firewall + Services + VF		When this is unchecked, the browser tab shows the host name followed by the current page. Check this box to display the current page followed by the host name.
Status / [	Advanced Certificates General Setup		Secure Shell	
System Info Name User System	High Availability Package Manager Register Routing	M O (Local Database)	Secure Shell Server	Image secure Shell         Password or Public Key         When set to Public Key Cohy, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to Require Both Password and Public Key, the SSH demon requires both authorized keys and valid password as valid authorized key to login.
BIOS	Setup Wizard Update User Manager Logout (admin)	19824a65f6c5652da0a nnologies LTD w 12 2020	Allow Agent Forwarding SSH port	Frables seh-agent forwarding support.      2121      Note: Leave this blank for the default of 22.
* en orient	built on Wed Nov 15 FreeBSD 14.0-CURR The system is on the Version information	Info:66:00 CET 2023 ENT e latest version. updated at Wed Nov 29 12:22:16 CET 2023	Login Protection Threshold	30 Block attackers when their cumulative attack score exceeds threshold. Most attacks have a score of 10.
СРU Туре	12th Gen Intel(R) Co AES-NI CPU Crypto: QAT Crypto: No	re(TM) i5-12400F Yes (inactive)	Blocktime	120 Block attackers for initially blocktime seconds after exceeding threshold. Subsequent blocks increase by a factor of 1.5. Attacks are unblocked at random intervals, so actual block times will be longer.

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** :

		LAN	0P11	Schedules Traffic Sha	per							
ules (I s	Drag to ( States	Change Or Protocol	der) Source	Virtual IPs	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
×	0/6 KiB	*	RFC 1918 net	vorks	*	*	*	*	*		Block private networks	•
×	0/264 B	*	Reserved Not assigned	by IANA	*	*	*	*	*		Block bogon networks	۵

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.

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	<ul> <li>Disable this rule</li> <li>Set this option to disable this rule without removing it from the list.</li> </ul>
Interface	WAN Choose the interface from which packets must come to match this rule.
Address Family	IPv4 v Select the Internet Protocol version this rule applies to.
Protocol	TCP  Choose which IP protocol this rule should match.

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         Extra Options       Image: Description Section	Destination	Invert match	WAN address		~	Destination Address	1
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 Cog 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 serve 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 fine log.         Advanced Options	Destination Port Range	(other) ~	2121 Custom	(other) To	~	2121 Custom	
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 serve 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 find log.         Advanced Options       Image: Display Advanced		Specify the destination p	ort or port range for this rule.	The "To" field may be left	empty if only	filtering a single port.	
Log       Cog 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 serve 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 fire log.         Advanced Options       Image: Display Advanced	Extra Options						
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 fire log.         Advanced Options       Image: Display Advanced	Log	Log packets that are had hint: the firewall has limited the Status: System Logs:	andled by this rule ed local log space. Don't turn Settings page).	on logging for everything	. If doing a lo	t of logging, consider using a rem	note syslog serve
Advanced Options 🗱 Display Advanced							
	Description	autoriser SSH A description may be ente log.	red here for administrative re	eference. A maximum of s	i2 characters	will be used in the ruleset and dis	splayed in the fire

on applique les changements :

Apply Changes

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

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 :

```
sshd
[2.7.1-RELEASE][admin@heimdall.Safetech.com]/etc/ssh: cd /etc/ssh
[2.7.1-RELEASE][admin@heimdall.Safetech.com]/etc/ssh: ls
                              ssh_host_ed25519_key.pub sshd_config
мoduli
ssh_config
                              ssh_host_rsa_key
ssh_host_ed25519_key ssh_host_rsa_key.pub
[2.7.1-RELEASE][admin@heimdall.Safetech.com]/etc/ssh: ssh-keygen -lvf ssh_host_e
d25519
                              ssh host ed25519 key.pub
ssh host ed25519 key
[2.7.1-RELEASE][admin@heimdall.Safetech.com]/etc/ssh: ssh-keygen -lvf ssh_host_e
d25519_key.pub
256 <mark>SHA256:nUIHdeReX3exd1xGE2uMMeKN/FtFN7bLQFh9Vn9OAjQ</mark> root@heimdal1.Safetech.co
м (ED25519)
 --[ED25519 256]--+
          ...+E=.BX:
           .o+=o*=&¦
           · ·+·+00%;
          . o o..==0¦
          S o .. +o¦
                0
                     --[SHA256]--
[2.7.1-RELEASE][admin@heimdall.Safetech.com]/etc/ssh:
```

On va essayer une connexion de notre machine physique :



On remarque qu'il y'a **échec de connexion** ; on essaye de faire un **ping** sur cette interface, même constat :

Ø Windows PowerShell × + ✓
PS C:\> ping 192.168.1.250
Envoi d'une requête 'Ping' 192.168.1.250 avec 32 octets de données : Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination. Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination. Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination. Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination. Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination.
Statistiques Ping pour 192.168.1.250: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), PS C:\>

Cet échec est normal car PfSense bloque toutes les requêtes venant d'une adresse privée dans son interface WAN. On peut vérifier cela en allant dans le menu interface > WAN, en allant tout en bas de la page, nous trouvons ces deux cases cochées.

COMMUNITY EDITION	System +	Interfaces 👻	Firewall <del>-</del>	Services 🗸	VPN <del>-</del>	Status 🗸	Diagnostics 👻	Help 🗕	<b>\$</b> 2 <b>G</b>
Interfaces /	/ WAN (	Assignments	_						幸 ₪ 8
		WAN	_						
General Confi	iguration Enable	OPT1							
Des	cription	0PT2 V 0PT3							
IPv4 Configuration	on Type	Inter a description (na Static IPv4	ime) for the in	terface here.		~			
IPv6 Configuration	on Type	None				~			
MAC A	Address	XXXXXXXXXXXXX							
Reserved Networks									
Reserved Networks Block private networks and loopback addresses	Decks traf RFC 4193 ( private add	fic from IP address (fc00::/7) as well as Iress space, too.	es that are re loopback ad	served for priva dresses (127/8)	te networks p ). This option	er RFC 1918 should gene	: (10/8, 172.16/12 rally be turned on	, 192.168/16) a unless this net	ind unique local addresses per work interface resides in such a
Reserved Networks Block private networks Ind loopback addresses Block bogon networks	Blocks traf RFC 4193 private add Blocks traf routing tab Note: The o	fic from IP address (fc00::/7) as well as Iress space, too. fic from reserved IF le, and so should no update frequency ca	es that are re loopback ad addresses ( ot appear as f n be change	served for priva dresses (127/8) but not RFC 191 the source addr d under System	te networks p ). This option (8) or not yet ess in any pa > Advanced,	er RFC 1918 should gene assigned by ckets receive Firewall & N.	I (10/8, 172.16/12 rally be turned on IANA. Bogons are rd. AT settings.	, 192.168/16) a unless this net prefixes that s	ind unique local addresses per work interface resides in such a hould never appear in the Internet

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

Il faut tout d'abord :

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

Redirection de port		×	
IP Destination :	192.168.1.250	~ @.	IP de l'interface WAN de PfSense
Redirection active :	$\checkmark$		
IP source :	Toutes	~	les adresses IP de qui pourra se connecter sur le serveur
Protocole :	TCP	~ 0	
Port de début :	49555	î 🧕	Les ports sur lesquels on va se connecter
Port de fin :	49555	î 9	
Port de destination :	2121	<u></u>	Le port sur lequel PfSense écoute
Commentaire :			
	X Annuler	Sauvegarder	

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

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



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

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

Connectivité LDAP :

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

Paramètres	Exécuter ×
Explorateur de fichiers	Entrez le nom d'un programme, dossier, document ou
Rechercher	ressource Internet, et Windows l'ouvrira pour vous.
Exécuter 2	Ouvrir: Idp.exe 🗸
Arrêter ou se déconnecter >	Cette tâche sera créée avec les autorisations d'administrateur.
Bureau Clique droit	OK Annuler Parcourir
Tapez ici pour effectuer une recherche	

Un 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

	Paramètres	🖾 Exécuter 🛛 🗙
	Explorateur de fichiers	= Entrez le nom d'un programme, dossier, document ou
	Rechercher	ressource Internet, et Windows l'ouvrira pour vous.
	Exécuter 2	Ouvrir: Idp.exe 🗸
	Arrêter ou se déconnecter >	Cette tâche sera créée avec les autorisations d'administrateur.
	Bureau Clique droit	OK Annuler Parcourir
-	Tapez ici pour effectuer une recherche	

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

	😭 Ldp	– 🗆 X
🔂 Ldp -	- X Connexion	Parcourir Affichage Options Outils ?
Connexion Parcourir Affichage Options Outils	?	
Lier Ctrl+B		
Se déconnecter		Se connecter ×
Nouveau Ctrl+N		Serveur : SafetechDC
Enregistrer		SSL
Enregistrer sous		OK Annuler
Quitter		
	Prét	NUM at
	🔐 Ldp	- • ×
	Connexion Parcourir Affichage Options Outils ?	
	ld = ldap_ssinnt("SafetechDC", 636, 1); Error 0 = ldap_set_option(hLdap, LDAP_OPT_ 3);	PROTOCOL_VERSION,
	Error 81 = Idap_connect(hLdap, NULL); Server error; <empty></empty>	
	Ldp ×	
	Impossible d'ouvrir la connexion.	
	ОК	
	Prêt	NUM

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.

stionna	aire de serv	reur • Tableau de bord • 🕝 l	Gérer Outils Afficher Aide	ቬ Assistant Ajout de rôles et de fonctionnalités	- 🗆 X
		<u> </u>	Ajouter des rôles et fonctionnalités	Sélectionner le serveur de destination	SafetechDC.safetech.com
	RIENVENUE D	ANS GESTIONNAIRE DE SERVEUR	Supprimer des rôles et fonctionnalités	Avant de commencer Sélectionnez le serveur ou le disque dur virtuel sur les	quel installer des rôles et des fonctionnalités.
	DERVENCED	AND GESTIONNAME DE SERVEOR	Ajouter des serveurs	Type d'installation Sélectionner un serveur du pool de serveurs Sélection du serveur O Sélectionner un disque dur virtuel	
			Créer un groupe de serveurs	Rôles de serveurs Pool de serveurs	
		1 Configurer ce serveur local	Propriétés du Gestionnaire de serveur	Fonctionnalités Confirmation Filtre :	
	DÉMARRAGE	5		Résultats Nom Adresse IP Systè	àme d'exploitation
	RAPIDE	2 Ajouter des rôles et des fonctionnalités		SafetechDC.safetech.com 192.168.100.2 Micro	xoft Windows Server 2022 Standard
et d Þ		3 Ajouter d'autres serveurs à gérer			
	NOUVEAUTÉS	4 Créer un groupe de serveurs		1 ordinateur(s) trouve(s) Cette page présente les serveurs qui exécutent Windo ont été ajudés à Taldé de la commande Ajouter des s serveurs hors connecion et les serveurs nouvellement incompléte ne sont pas régerroifs.	sws Server 2012 ou une version ultérieure et qui serveurs dans le Gestionnaire de serveur. Les t ajoutés dont la collecte de données est toujours
		5 Connecter ce serveur aux services cloud	Masquer	< <u>Précédent</u>	Suigant > Installer Annuler

## 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

Assistant Ajout de rôles et de	fonctionnalités	- 🗆 ×	ቬ Assistant Ajout de rôles et de l	onctionnalités	- 0
Services de certi Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs	ificats Active Directory Les services de certificats Active Directory (ADCS) fournissent l'Infae en charge des scientines tells que les reteaux sans fil s'Acurisis, les reis IPSe (Internet Protocol Security), la protection d'accès réseau (NAP) (Encopyting Tégi System) et la connesion par carte à puce. À noter :	SERVIUR DE DESTINATION Safaració Carafracticion tructure de certificats pour prendre exor privés virtuels, la récumé le système de fichiers EFS	Sélectionner des Avant de commencer Type d'installation Sélection du servieur Rôles de servieurs	services de rôle Sélectionner les services de rôle à installer pour Services de ce Services de rôle <u>Outours de centrantice</u> Installer de centrantice Installer de centrantice	servux de destrituirion server de destrituirion ritificats Active Directory Description Une autorité de certification sert à émettre et géner des certification
Pontoonnaides AD CS Services de rôle Confirmation Résultats	dios autorito de certificación. Si van volate comparte es mot de promovoir es envir en certificar de domaine, effectuar com l'autorité de certification. Pour plus d'informations, consultez Attri certification.	an denatur, producter ar discussion ou construction de la construction de la construction de la construction d'un nom à une autorité de	Pontionnallisis AD CS Services de role Confirmation Résultatio	Service d'inscription de périphérique réseu Service Véli Sarotificats Service Web Stretégie d'inscription de certificats	peuvent être liées pour former une infrastructure à clé publique.
	< <u>Précédent</u> Suigant >	Installer Annuler		< Précédent Suiza	nt >InstallerAnnuler

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

Assistant Ajout de rôles et de	fonctionnalités	- 🗆 ×	🛼 Assistant Ajout de rôles et de fonctionnalités	-	
Confirmer les sél	lections d'installation	SERVEUR DE DESTINATION SafetechDC safetech.com	Progression de l'installation	IVEUR DE D afetechDC	DESTINA safetech
Avant de commencer Type d'Installation Sélection du serveurs Fonctionnaîtés AD C5 Services de rôle Confirmation Résultats	Pour installer les rôles, services de trôle ou fonctionnalités suivants aur le se Installer de definierre automatiguement le serveur de destination, si nécessaire. Il se peut que de fonctionnalités facultatives (omme des outils d'administrates automatiguement : Svoan evo fonctionnalités facultatives (oiques sur Précédent pour désactiver leurs cas Outils d'administration de reineur distant Outils d'administration de reineur distant Outils de gestion de l'Austré de certification Outils de gestion de l'Austré de certification Services de certification Services de certification	neur sflectione, cliquez sur trationy soient affichées sur due pas installer ces es à cocher.	Avant die commerzer Type d'installation Selection du serveurs Rondonalité Au Cu Brancos de strike Brancos de strike Bran	s de certi ion écution. I i barre de	ficats Examir e

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.

## 🔁 Configuration des services de certificats Active Directory

# - 🗆 X

SERVEUR DE DESTINATION

SafetechDC.safetech.com

# Type d'autorité de certification

Informations d'identificati	Spécifier le type de l'AC
Services de rôle	
Type d'installation	Lorsque vous installez les services de certificats Active Directory (AD CS), vous créez ou étendez
Type d'AC	une hiérarchie d'infrastructure à clé publique (PKI). Une autorité de certification racine se trouve au sommet de la hiérarchie PKI et émet ses propres certificats auto-signés. Une autorité de
Clé privée	certification secondaire reçoit un certificat de l'autorité de certification de rang plus élevé dans la
Chiffrement	hiérarchie PKI.
Nom de l'AC	Autorité de certification racine
Période de validité	Les autorités de certification racines sont les premières voire les seules autorités de certification
Base de données de certi	configurées dans une hiérarchie PKI.
Confirmation	○ Autorité de certification secondaire
Confirmation	Les autorités de certification secondaires nécessitent une hiérarchie PKI établie et sont
Progression	autorisées à émettre des certificats par l'autorité de certification de rang plus élevé dans la biérarchie
Résultats	metarchie.
	En savoir plus sur le type d'autorité de certification
	< <u>P</u> récédent Sui <u>v</u> ant > <u>C</u> onfigurer Annuler
On choisit de créer une	clé privée.
🔁 Configuration des services de co	rtificats Active Directory – 🗆 🗙
Clé privée	SERVEUR DE DESTINATION SafetechDC.safetech.com
Informations d'identificati	Spécifier le type de la clé privée
Services de rôle	
Type d'installation	Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une clé privée.
Clé privée	Créer une clé privée
Chiffrement	Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.
Période de validité	<ul> <li><u>U</u>tiliser la cle privée existante</li> <li>Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de</li> </ul>
Base de données de certi	la réinstallation d'une AC. Sélectionner un certificat et utiliser sa clé privée associée
Confirmation	Sélectionnez cette option s'il existe un certificat sur cet ordinateur ou pour importer un certificat et utiliser sa clé privée associée.
	Sélectionner une clé privée <u>e</u> xistante sur cet ordinateur
	Sélectionnez cette option si vous avez conservé les clés privées d'une installation antérieure ou pour utiliser une clé privée d'une autre source.
	En savoir plus sur la clé privée
	< <u>Precedent</u> Suivant > Configurer Annuler

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

🚡 Configuration des services de ce	_		$\times$	
Chiffrement pour	SERVEUR D Safetech	E DESTINAT )C.safetech.	'ION com	
Informations d'identificati Services de rôle	Spécifier les options de chiffrement			
Type d'installation	Sélectionnez un <u>f</u> ournisseur de chiffrement :	Longueur de	la <u>c</u> lé :	
Type d'AC	RSA#Microsoft Software Key Storage Provider *	4096		~
Clé privée Chiffrement Nom de l'AC Période de validité Base de données de certi Confirmation Progression Résultats	Sélectionnez l'algorithme de hachage pour signer les certificats émis SHA256 SHA384 SHA512 SHA1	par cette AC :	ède à la clé	
	En savoir plus sur le chiffrement          < Précédent	Configurer	Annul	er

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

🔁 Configuration des services de cer	_		$\times$	
Nom de l'autorité	SERVEUR DE D SafetechDC.s	ESTINATI afetech.c	ON om	
Informations d'identificati Services de rôle	Spécifier le nom de l'AC			
Type d'installation Type d'AC Clé privée Chiffrement <b>Nom de l'AC</b> Période de validité	Tapez un nom commun pour identifier cette autorité de certification. C certificats émis par l'autorité de certification. Les valeurs des suffixes d automatiquement, mais elles sont modifiables. Nom <u>c</u> ommun de cette AC : <u>SAFETECHDC-CA</u> Suffi <u>x</u> e du nom unique :	Ce nom est ajout lu nom unique s	é à tous le ont génére	ées
Base de données de certi Confirmation	DC=safetech,DC=com			
Progression Résultats	Aperçu du no <u>m</u> unique : CN=SAFETECHDC-CA,DC=safetech,DC=com En savoir plus sur le nom de l'autorité de certification			
	< <u>P</u> récédent Sui <u>v</u> ant >	Configurer	Annule	r

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.

峇 Configuration des services de ce	rtificats Active Directory	-		×
Période de validité		SERVEUR DE D SafetechDC.:	ESTINATI	ON
Informations d'identificati Services de rôle Type d'installation Type d'AC Clé privée Chiffrement Nom de l'AC <u>Période de validité</u> Base de données de certi Confirmation Progression Résultats	Spécifier la période de validité Sélectionnez la période de validité du certificat généré pour cette au 15 Années V Date d'expiration de l'AC : 29/11/2038 23:24:00 La période de validité configurée pour ce certificat d'autorité de certi période de validité pour les certificats qu'elle émettra.	torité de certifica	tion :	
	En savoir plus sur la période de validité			
On laisse les dossiers d	<u>Suivant &gt;</u> Les bases de données et des logs, par défaur	<u>C</u> onfigurer	Annule	er 🔹
Base de données	de l'autorité de certification	SERVEUR DE I SafetechDC	DESTINAT	ION
Informations d'identificati Services de rôle	Spécifier les emplacements des bases de donr	nées		
Type d'installation	Empla <u>c</u> ement de la base de données de certificats :			
Type d'AC	C:\Windows\system32\CertLog			
Chiffrement	Emplacement du journal de la base de données de certificats :			
Nom de l'AC	C. (Windows (system 52 (Centrog			
Période de validité				
Confirmation				
Progression				
Résultats				
	En savoir plus sur la base de données de l'autorité de certification			
	< <u>P</u> récédent Suivant >	Configurer	Annul	er

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

🔁 Configuration des services de ce	rtificats Active Directory	_		$\times$
Résultats	SERVEL	R DE DE	ESTINATIO	on
Informations d'identificati	Les rôles, services de rôle ou fonctionnalités ci-après ont été configurés :			
Services de rôle	Services de certificats Active Directory			
Type d'installation				
Type d'AC	En savoir plus sur la configuration de l'autorité de certification	J.		
Clé privée				
Chiffrement				
Période de validité				
Base de données de certi				
Confirmation				
Progression				
Résultats				
	< Précédent Suivant > Ferm	er	Annule	r

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

		Idaps://SafetechDC		$\times$
Se connecter	×	Connexion Parcourir	Affichage         Options         Outils         ?           Id = Idap_sslinit("SafetechDC", 636, 1);	^
Serveur : SafetechDC Port : 636 OK	Non connecté ☑ SSL Annuler		LDAF_UPI_HCIOLOU_VERSION,3); Error 0 = kdap_contect(hLdap,NULL); Error 0 = kdap_contect(hLdap,NULL); Host supports SSL, SSL cipher strength = 256 bits Established connection to SafetechDC. Retrieving base DSA information Getting 1 entries: On: (RootOSE) Dn: (RootOSE) Do: (RootOSE) Configuration/DC=safetech,DC=com; CurrentTime: 30/11/2023 10/27:17 Paris, Madrid; defaultNamingContext: DC=safetech,DC=com; domainControllerFunctionality: 7 = (WIN2016); domainControllerFunctionality: 7 = (WIN2016); domainControllerFunctionality; 7 = (WIN2016); domainControllerFunctionali	Site
		Prêt	NUM	

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

			Edit Firewall Rule Artiss	Yes     Count white take which preserve a periodic binor     Yes     Count when take which preserve a periodic binor     Yes the difference between bine we repeat in the set repeat (PD WE or COMP periodic bine (DD W) in internel to the weeker,     which the setter is the preserve a three periodic binory of the periodic bine (DD W) in internel to the weeker,     where the setter is the preserve a three periodic bine (DD W) in internel to the weeker,     where the setter is the preserve a three periodic bine (DD W) in internel to the weeker,     where we will be the setter is the preserve a three periodic bine (DD W) in internel to the weeker,     where we will be the setter is the preserve a three periodic bine (DD W) in the periodic bine (DD W
			Disabled	Disable this rule     Set this option to disable this rule without removing if from the last.
			Interface	LAN v Chaose the interface from which pedeets must come to match this mile.
			Address Family	[IPv4 v] Benefit the Internet Protocol version this rule applies to
COMMUNITY EDITION System • Interfaces •	Firewall - Services - V	PN • Status • Diagnostics •	Protocol	TCP   Cheose which IP protocol this rule should match.
Firewall / Rules / LAN	Aliases		Source Source	Invertmaten     Address of Allos     V     192.164,100.2     7     V
	Rules			Conserv Annoted The Secure Put Range for a connection is hysically random and almost nover equal to the destination part. In most cases this setting must remain at its dobut visus, any.
The firewall rule configuration has been changed. The changes must be applied for them to take eff	Schedules Traffic Shaper		Destination Destination	□ Invertimatelt Adv
	Virtual IPs		Destination Port Range	LIAMPS (USA)     V     LIAMPS (USA)     LIAMPS (USA)     V
Floating WAN LAN OPT1 (	IPT2 OPT3		Extra Options	Compression that are hardwell by this sub-     Mark the hardwell by this sub-     Mark the hardwell by this sub-     Mark the hardwell back inflate doubling agains. Clinit has an agging for overything, if during a bit of logging consider using a remets systeg server (see the datas, system) cost effecting consol.
			Description	Alter LEAVE from Farlinshoc A decorption may be oritore here for administrative reference. A maximum of 92 characters will be used in the ruleset and displayed in the ferwall IGL
			Advanced Options	Chipter Advanced
				E tore

Sur notre PfSense on crée une régle de securité pour autoriser le traffic LDAPS depuis notre controleur de domaine principal car il refuse ce traffic par défaut :

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

Firewall / Rules   Nat   Rules   Nat   Rules   The firewall rule configuration has been changed.   Schedules   The firewall rule configuration has been changed.   The firewall rule configuration has been changed.   Floating   WAN   LAN   OPT1   OPT2   OPT1   OPT2   OPT1   OPT2   OPT3			Filewait/ Rules/ Euk	
Firewall / Rules     Allases   Nat   Rules   The firewall rule configuration has been changed   The firewall rule rule rule rule rule rule rule ru			Edit Firewall Rule	
System Interfaces     Firewall / Rules / LAN     Aliases   Nat   Rules   The firewall rule configuration has been changed.   The firewall rule configu			Action Pann V Choose what to do with packets that match the others specified below. For the difference between block and negati is that with negat, a packet (CPP) whereas with block the packet is dropped silently in either case, the original pa	IST or ICMP port unreachable for UDP/ is returned to the sender, cket is discarded.
Firewall / Rules     Allases     Nat     Rules     The firewall rule configuration has been changed.   The firewall rule configuration has been changed. <			Disabled  Disable this rule Set this option to disable this rule without removing it from the list.	
Construction       System · Interfaces · VPN · Status · Diagnostics ·         Firewall / Rules / LAN       Aliases · NAT         Rules · NAT       Rules · Traffic Shaper         The firewall rule configuration has been changed.       Schedules · Traffic Shaper         Virtual IPs · Virtual IP			Leve Choose the interface from which packets must come to match this rule.	
Firewall / Rules / LAN     Allass   Nat   Rules   The firewall rule configuration has been changed.   The firewall rule rule rule rule rule rule rule ru	COMMUNITY EDITION	Services • VPN • Status • Diagnostics •	Address Family IPv4 ~ ·	
Firewall / Rules / LAN NAT Rules / LAN NAT Rules / LAN OPT1 OPT2 OPT3	Aliases		Pretocol TOP  Choose which IP protocol this rule should match.	
Rules       Schedules       The firewall rule configuration has been changed.       Schedules       The firewall rule configuration has been changed.       The firewall rule configuration has been changed.       Schedules       The firewall rule configuration has been changed.       The firewall rule configuration ha	Firewall / Rules / LAN NAT		Source Address of Alexan	v 102144.100.8 / v
The firewall rule configuration has been changed.       Schedules         The changes must be applied for them to take of       Traffic Shaper         Virtual IPs       Virtual IPs         Floating       WAN       LAN       OPT1       OPT2       OPT3	Rules		C Tangle Advanced	
The changes must be applied for them to take of The changes must be applied for them to take of Virtual IPs Virtual IPs Vi	Schedules		The Source Part Range for a connection is typically random and almost never its default value, any.	qual to the destination port. In most cases this setting must remain at
Floating     WAN     LAN     OPT1     OPT2     OPT3	The changes must be applied for them to take eff Traffic Share		Destination All	Destination Address
Floating     WAN     LAN     OPT1     OPT2     OPT3	The changes mast be applied for them to take on a manie shap		Destination Port Range LDAP/S (636) V	v
Floating WAN LAN OPT1 OPT2 OPT3	Virtual IPs		From Contom To Specify the destination port or port range for this rule. The "To" field may be left	Custom empty if only filtering a single-port.
the statute spanne Logit stating page.	Floating WAN LAN OPT1 OPT2 OP	Т3	Extra Options Log gadets that are handled by this rule First, the frewall has limited log lagos. Don't turn on logging for everythin the Stature, System Logs. Settings page.	g. If doing a lot of logging, consider using a remote syslog server (see
Non-Uption Table (2014) then indexed (2014) the indexed (2014) the indexed (2014) the indexed (2014) the indexed in the indexe			Allow LDAPS from Safetoch0C2 A description may be entered here for administrative reference. A maximum of log	52 characters will be used in the ruleset and displayed in the firewall
Advanced Options Options			Advanced Options	

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 :

	System - Interfaces - Firewall -	Services - V	/PN +	Status -	Diagnostics -	Help - 🦺 🔁 🕞
Status /	Dashboard				ARP Table Authentication Backup & Restore	+ 0
System Info	rmation	&		Netgate Se	Command Prompt	
Name User	heimdall.Safetech.com admin@192.168.1.180 (Local Database)			Cont	DNS Lookup Edit File	upport upport Only
System	VMware Virtual Machine Netgate Device ID: <b>729824a65f6c5652da0a</b>	3		NETC	Factory Defaults Halt System	MUNITY SUPPORT RESOURCES
BIOS	Vendor: Phoenix Technologies ITD				10 m 11 m	

On exécute la commande suivante :

openssl s\_client -showcerts -connect SafetechDC.safetech.com:636

Execute Shell Command		
openssl s_client -showcerts -connect SafetechDC.safetech.com:636	]	
Clear		

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



## A- Création des comptes utilisateurs sur le contrôleur de domaine

Sur le contrôleur de domaine je crée :

- Un groupe pfsense
- Un utilisateur kaiser faisant partie du groupe pfsense
- Un utilisateur cesar faisant partie du groupe pfsense
- Un utilisateur **pfsensead** faisant partie du groupe **pfsense** et qui va servir de faire la liaison entre pfsense et le contrôleur de domaine.

📾 Gestionnaire de serveur		— — — ×
Gestionna	ire de serveur ► Tableau de l	bord - 🗇   🍢 Gérer Outlis Afficher Aide
🏢 Tableau de bord	BIENVENUE DANS GESTIONNAIRE DE SER	RVEUR Autorité de certification Centre d'administration Active Directory
■ Serveur local ■ Toue les serveurs ■ AD CS ■ AD DS 管理 OHCP 金 DNS ■ Services de fichiers et d ▷	DEMARRAGE 2 Ajouter 3 Ajouter 4 Créer u 5 Connec	Configuration du système Défragmenter et optimiser les lecteurs DHCP Diagnostic de mémoire Windows DHS Ser des rôles et des of d'autres serveur Un groupe de ser lecter ce serveur at Intitiateur ISCSI Lecteur de récupération Modification ADSI
	Rôles et groupes de serveurs Rôles : 5   Groupes de serveurs : 1   Nombre toi	Module Active Directory pour Windows PowerShell Moniteur de ressources total de serveurs : 1 Nettoyage de disque
	AD CS     1       Tracilité de gestion     1       Événements     1       Services     1       Performances     Résultats BPA	Observateur d'événements     Observateur d'événements     Observateur d'événements     Observateur d'événements     Observateur d'événements     Observateur d'événements     Services     Services
Utilisateurs et ordinateur Fichier Action Affichage	s Active Directory e ?   @ 🞰   😰 🗊   🐍 📚 🛅 🦷	> 7 2 %
<ul> <li>Utilisateurs et ordinateurs</li> <li>Requêtes enregistrées</li> <li>safetech.com</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controlle</li> <li>ForeignSecurityPri E Les Professionnels</li> <li>Managed Service a</li> <li>Visiteurs</li> <li>Visiteurs</li> <li>Asgard</li> </ul>	Active Nom Type Pfsense Groupe d cesar Utilisateu Kaiser Utilisateu pfsensead Utilisateu Accour	C Description de séc ur ur ur
•	-	

Ajouter le certificat crée par notre controleur 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.

Users Groups Settings	Authentication Servers			
Authentication Servers				
Server Name	Туре	Host Name	Actions	
Local Database		heimdall		
				_

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

Et on remplit les champs avec les parametres suivants :

Authentification LDAPS
s
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.
636
SSL/TLS Encrypted
Global Root CA List  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.
3
25 Timeout for LDAP operations (seconds)
Level Entire Subtree Dès que les champs sont remplis appuyez sur "Select a container" DC=Safetech,DC=com
Image: 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
Enable extended query     mot de passe de l'utilisateur
Use anonymous binds to resolve distinguished names
CN=pfsensead,0U=Asgard,DC=safetech,DC=com
Microsoft AD
samAccountName

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 reconnait 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

Acceder 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 choisis : 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

- 😺 Assistant Exportation du certificat		← 🛿 & Assistant Exportation du certificat
Exporter la clé privée Vous pouvez choisir d'exporter la dé privé	e avec le certificat.	Format du fichier d'exportation Les certificats peuvent être exportés dans divers formats de fichiers.
Les dés privées sont protégées par mot d privée avec le certificat, vous devez tape Voulez-vous exporter la dé privée avec le Oui, exporter la dé privée	e passe. Si vous voulez exporter la dé r un mot de passe dans une prochaine page. certificat ?	Sélectonnez le format à utiliser : (X.509 binaire encodé DER (*.cer) (*) X.509 encodé en base 64 (*.cer) (*) Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P78) (*) Indure tous les certificats dans le chemin d'accès de certification, si possible (*) Constraints personnelles - PKCS #12 (.PFX) (*) Indure tous les certificats dans le chemin d'accès de certification, si possible (*) Export met out les certificats dans le chemin d'accès de certification, si possible (*) Export ter toutes les propriétés é l'export tation réussit (*) Export en toutes les propriétés étendues (*) Activer la confidentialité de certificat
	Suivant Annuler	Suivant Annuler
	Fichier à exporter Spécifiez le nom du fichier à exporter Nom du fichier : C:\Users\Administrateur\Desktop\Safet	echoC-CA.cer Parcourir

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



On va dans System > Certificates > Authorities on clique sur add pour rajouter une autorité de certification :

System /	Contificantes	horities						0
oyotenin/	Certificates	nontico						
	General Setup							
Authorities	Daakaaa Managar	cation						
Onest	Package Manager	_						
Search	Register							-
Search term	Satup Wittard	-			Both	✓ Q Searce	h 🖒 Clear	
	Update	arch string or *n	nix regular expression to se	earch certificate names an	d distinguished n	ames.		
Certificate /	User Manager							
Name	Logout (admin)	Issuer	Certificates	Distinguished N	lame	In Use	Actio	ns
	Logout (dumin)	_						
Authorities	Certificates	Revocation						
	-							
Create / E	dit CA							
Create / E	dit CA	fetechDC_CA						
Create / E	dit CA iptive name Sa The	fetechDC_CA name of this entry a	as displayed in the GUI for ret	ference.				
Create / Er	dit CA iptive name Sat The This	fetechDC_CA name of this entry a name can contain s	is displayed in the GUI for re spaces but it cannot contain	ference. any of the following charact	ers: ?, >, <, 8, /,  ",			
Create / E	dit CA iptive name Sat The This Method Im	fetechDC_CA name of this entry a name can contain s port an existing Cert	is displayed in the GUI for re spaces but it cannot contain tificate Authority	ference. any of the following charact	ers: ?, >, <, &, /,  *,			
Create / E	dit CA iptive name Sat The This Method Im Trust Store	fetechDC_CA name of this entry a name can contain s port an existing Cert Add this Certificate A	is displayed in the GUI for re- spaces but it cannot contain tificate Authority Authority to the Operating Sy	ference. any of the following charact	ers: ?, >, <, 8, /,  *,			
Create / E	dit CA iptive name Sat This Method Im Trust Store Method Whe	fetechDC_CA name of this entry a name can contain s port an existing Cert Add this Certificate A en enabled, the conte	is displayed in the GUI for re- spaces but it cannot contain tificate Authority Authority to the Operating Sy- ents of the CA will be added	ference. any of the following charact v stem Trust Store to the trust store so that the	ers: ?, >, <, &, /,  ", y will be trusted by	, ,		
Create / Ed	dit CA iptive name Sat This Method Im Trust Store Whe whize Serial U	retechDC_CA name of this entry a name can contain s port an existing Cert Add this Certificate A en enabled, the conte Jse random serial nu	as displayed in the GUI for re spaces but it cannot contain tiffcate Authority Authority to the Operating Sy ents of the CA will be added umbers when signing certific	ference. any of the following charact v stem Trust Store to the trust store so that the ates	ers: ?, >, <, 8, /,  *, y will be trusted by	, the operating system.		
Create / Ed	dit CA iptive name Sat The This Method Im Trust Store Whe mize Serial U Whe	retechDC_CA name of this entry a name can contain s port an existing Cert Add this Certificate A en enabled, the conte Jse random serial nu en enabled, if this CA	is displayed in the GUI for rel papece but it cannot contain tiffcate Authority Authority to the Operating Sy ents of the CA will be added umbers when signing certific is capable of signing certific	ference. any of the following charact stem Trust Store to the trust store so that the ates actes then serial numbers for	era: ?, >, <, &, /,  *, y will be trusted by or certificates sign	, the operating system, ed by this CA will be as		ized and
Create / Ed	dit CA iptive name Sat The This Method Im Trust Store Whe omize Serial U Whe che	letechDC_CA name of this entry a name can contain s port an existing Certificate A en enabled, the conte see random serial nu en enabled, if this CA cked for uniqueness	as displayed in the GUI for ret paces but it cannot contain tiffcate Authority Authority to the Operating Sy ents of the CA will be added umbers when signing certific is capable of signing certific instead of using the sequen	ference. any of the following charact stem Trust Store to the trust store so that the ates cates then serial numbers fo tital value from Next Certifico	era: ?, >, <, &, /,  *, y will be trusted by or certificates sign te Serial.	, the operating system,	.tomatically random	ized and
Create / E	dit CA iptive name Sa The This Method im Trust Store Sa white amize Serial O white chee ertificate Autho	VetechDC_CA name of this entry a name can contain s port an existing Cert Add this Certificate A en enabled, the conte Jse random serial no serial of this CA cked for uniqueness rity	as displayed in the GUI for re- paces but it cannot contain tificate Authority Authority to the Operating Sy ents of the CA will be added umbers when signing certific is capable of signing certific instead of using the sequen	erence. any of the following charact v stem Trust Store to the trust store so that the ates cates then serial numbers fo cates then serial numbers for itai value from Next Certificd	ers: ?, >, <, 8, /,  *, y will be trusted by or certificates sign- te Serial.	I the operating system ed by this CA will be au	.tomatically random	ized and
Create / E	dit CA iptive name Iffe This Method Im Trust Store Whe whe cheir Case Autho ifficate data	letechDC_CA name of this entry a name can contain s port an existing Certi Add this Certificate A se random serial nu ne nabled, if this CA sched for uniqueness rity BEGIN CERTIFIC	as displayed in the GUI for re- paces but it cannot contain tificate Authority Authority to the Operating Sy ents of the CA will be added umbers when signing certific is capable of signing certific instead of using the sequen CATE	Ference. any of the following charact w stem Trust Store to the trust store so that the ates ates date sten serial numbers for tisi vialue from Next Certification tisi vialue from Next Cer	ers: ?, >, <, 8, /,  *, y will be trusted by or certificates sign ate Serial.	I the operating system ed by this CA will be au	.tomatically random	ized and
Create / E Descri Rando Existing C <u>Cer</u>	dit CA jgtive name The The Trust Store Participation Serial ertificate data Free	retechDC_CA name of Tbis entry a name can contain a port an existing Certificate Add this Certificate A en enabled, if this CA cked for uniqueness cked for uniqueness <b>rity</b> 	a displayed in the OLT for re- paces but it cannot contain tiffcate Authority huthority to the Operating Sy enter of the CA will be added umbers when agging certific instead of using the sequence CATE	rence. any of the following charact w stem Trust Store to the trust store so that the ates cases then serial numbers for cases then serial numbers of tail value from Next Certification Tailegich(:towiesQc542bc542bc1) tailey sopervicesQc142bc1	ers: ?, >, <, &, /,  *, y will be trusted by or certificates algo- tate Serial.	, the operating system,	.tomatically random	ized and
Create / E Descri Rando Existing C	dit CA iptive name Sat The The The Trust Store Z whe ertificate Autho fj	VetechDC_CA name of Ubis entry a name can contain a port an existing Cert and this Certificate A certificate A certificate A is enabled, if this CA cited for uniqueness <b>rity</b> 	In displayed in the QUI for re- pares but it cannot contain tiffcate Authority furthority to the Operating Sys- tem of the CA will be added motives when signing certific in capable of signing certific instead of signing certifications ( contains the second contains the second contains contains the second contains the second contains	Itemos any of the following charact with the following charact stem Trust Store to the trust store so that the Attemption of the source of the tial value from Next Centificat Taklegicght Lisoweakogs FADB- Typ (cogent vicit and vicit)	ers: 7, >, <, 8, /,  *, y will be trusted by or certificates sign- ate Serial.	y the operating system ed by this CA will be au On colle ici le oc Safetech	.tomatically random prificat de	ized and
Create / E	dit CA jptive name The This Method Trust Store P mize Serial O Wh che ertificate data F F S C 2 C C C C C C C C C C C C C	tetechDC_CA name of this entry a port an existing Cert and this Certificate A on enabled, the conte see andom serial nu menabled, if this CA cked for uniqueness <b>rity</b> 	a displayed in the OUT for re- places but it cannot contain influse Authority. Uptionly to the Operating Sy- metra of the CA will be added to a space of the operating of the instead of using certification of the space of the operating of the case of the case of the operating of the case of the operating of the	terrice. any of the following charact with any of the following charact with the function of the following characterized stem Trust Store cross their serial numbers for their series of the following characterized the series of the following characterized the series of the s	ers: 7, >, <, 8, /,  ', ' y will be trusted by yr certificates sign ate Serial.	, the operating system, ed by this CA will be au On colle ici le co Safetech	itomatically random	ized and
Create / E Descri Rando Existing C	dit CA iptive name iptive name iptive name istantiation istantiat	tetechDC_CA name of this entry a name can contain a port an existing Certificate A menabled, the conte definition of this CA checked for uniqueness rity 	as displayed in the GUT for re- paces but it cannot contain inflaste Authority. Withority to the Operating Sy- metry of the CA will be added umbers when arigining certific instead of using the sequent is capable of signing certific instead of using the sequent CATE	Arence. any of the following charact any of the following charact stem Trust Store to the trust store so that the area cases then ential numbers for tail value from Next Certifica Truggigght(Sowenget Access) Truggigght(Sowenget Access) area of the store of the store area of the store of the store of the store of the store of the store of the store of the store of the store of the store	ers: $?_r > < s_r / \backslash \uparrow$ y will be trusted by or certificates sign to Serial.	the operating system ed by this CA will be au On celle joi le co Salitech	nonatically random milicat de Dic	ized and
Create / E	dit CA  gipter same Fre Fre Fre Fre Fre Fre Fre Fre Fre Fr	IntechDC_CA manne of tiss entry a manne on contain a set of the context before the contex	In displayed in the QUI for re- places but it cannot contain tiffcate Authority untrointy to the Operating Sys- tem of the CA will be added motions of the CA will be added motions when signing certific in capable of signing certific instead of signing certific instead of signing certific of signing certification contains the signing certification ceritication certification certification certific	Arence. any of the following charact aren Trust Store to the trust store so that the atem Trust Store to the trust store so that the atem Crust Store So trastig charl.coveBago FADB- trastig charlence FADB- Trastig charlence FADB- Trastig charlence FADB- Trastig charlence FADB- Trastig charlence FADB- Trastig charlence FADB- Trastig charlence F	ers: ?, >, <, 8, /,  *, y will be trusted by or certificates sign te Serial.	, y the operating system, ed by this CA will be av dby this CA will be av CA will be av Dr. colls ici la c Safetech	stomatically random wrślicat de	ized and
Create / E	dit CA	HetechDC_CA harine of this entry a harine of this entry a harine can contain a port an existing Cert dist the contraction of the entry of the contraction entry of the cont	as displayed in the OUT for re- places but it cannot contain inflace Authority. Unitority to the Operating Sy- ents of the CA will be added to acabile of signing certific instead of using the sequences (Sy analog asking at signing certific (Sy and Certific (Sy analog asking at signing certific (Sy analog asking at signing certific (Sy and Certific (Sy	Fernice. any of the following characterized any of the following characterized astem Trust Store to the trust store so that the destination of the store of the store destination of the store of the store the store of the store of the store the store of the store of the store destination of the store of the store of the store destination of the store of the store of the store of the store destination of the store of the	ere: ?, >, +, &, /,  *, y will be trusted by or certificates sign ate Serial.	, the operating system ed by this CA will be au On colle ici le co Safetech	itomatically random	ized and
Create / E	dit CA	httenDC_CA name of this entry a name of this entry a mark can contain a mark and a mark can contain a mark the contained and the centre of the contained of the contained and the centre of the contained of the contained and the centre of the contained of the contained and the contained of the contained of the contained the contained of the contained of the contained and the contained of the contained of the contained of the contained of the contained of the contained of the contained of the contained of the contained of the contained and the contained of the	a displayed in the GUT for re- places but it. Cannot contain tifteate Authority. Authority to the Operating Say meters of the GO and the Operating Say meters when signing certifi- instead of using the sequen- tion of the Operating Say (Say (Say (Say (Say (Say (Say (Say	Ference. any of the following characteristic stem Trust Store to the trust store so that the atteristic source of the source of the source of the source train value from Next Certification Traing graph (conversion), joggiery Traing graph (conversion), joggiery phy (oggiery (conversion), joggiery source of the source of the sour	ers: ?, >, <, &, /, \.*, y will be trusted by yr certificates sign ate Serial.	, with e operating system ed by this CA will be au On colle ici le co Safetech		ized and
Create / E	dit CA Garage Caracterization Garage Caracter	etechOL_CA name on cost as entry a name can contain s and this centry as a disting Central and a disting Central and a late random serial nu menablek the cost as a cost of the cost of the cost as a cost of the cost of the cost as a cost of the cost of the cost of the cost as a cost of the cost of the cost of the cost as a cost of the cost of the cost of the cost of the cost as a cost of the	In displayed in the OUT for re- spaces but if cannot contain tiftette Authority uturbority to the Operating S with the added anders when signing certific is capable of signing certific is capable of signing certific instead of using the sequence of the CA will be added and the added and the added and the added added to a strategies and the added added to a strategies and added to a strategies and p FEM format here.	Any of the following characters any of the following characters any of the following characters and the	ere: ?,>, <, &, /, * y will be trusted by or certificates sign- ate Serial.	, with e operating system ed by this CA will be av On colle ini le o Safetech	ntomaticelly random writificat de	ized and
Create / E	dit CA Sample Carrier	etechDC_CA harine of this entry a harine of this entry a harine can contain a port an existing Cert et enabled, the control etechnic and the control etechnic and the control etechnic and the control etechnic and the control etechnic and the control etechnic and the control etechnic and the control etechnic and the control etechnic and the control etechnic and the control etechnic and the contr	as displayed in the OUT for re- places but it cannot contain inflate Authority untroff to the Operating Sy- ents of the CA will be added to the CA will be added to the CA will be added the operating operating operating instead of using the security of source states and operating operating operating (CAR)	Fernor. any of the following characteristic with the function of the following characteristic with the function of the following characteristic actess the excess the excession unrelevent of the following characteristic of the following characteristic of the following characteristic the following characteristic of the following characteristic	ers: $7, s, s, \delta, l, V, s$ y will be trusted by or certificates sign at se Serial.	, the operating system, ed by this CA will be au On colle ici le co Safetech	nomatically random	ized and
Create / E	dit CA	tetechOC_CA name of this entry a name of this entry a marked at orderates port an existing Cert an enabled, the conte of this Certificate A endows with the conte of this Certificate and the content of this Certificate endows with the content of this Certificate endows with the content of th	a displayed in the GUT for re- placed but it cannot contain tiffaate Authority Muthority to the Operating Sy- meters when signing certific instruct of Law (Law Contains) CATE	The grant of the following character of the foll	ers: 7, >, <, 6, /, \.*, y will be trusted by or certificates sign ate Serial.	, ed by this CA will be as On colle ici le co Safetech		ized and
Create / E	dit CA dit CA and the case of	etechOL_CA name on costs are yang name can contain s port an existing Certure did this Certificate and late random serial nu menables the costs <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b> <b>rity</b>	In displayed in the GUI for re- paces but it cannot contain tiffcate Authority. Untrointy to the Operating Sy- tem of the CA will be added and the security of signing certification instead of using the security (galaxiv) and (galaxiv) and (galaxiv) (g	Arence. any of the following character any of the following character to the trust store so that the aster tates then setial numbers for taid value from Next Certifica Tranggloph (soweace, for taid value from Next Certifica Tranggloph (soweace, for taid value from Next Certifica Tranggloph (soweace, for taid value from Next Certifica taid value from Next Certifica t	ers: $7, >, < 8, /, \lor$ ? y will be trusted by or certificates sign to be the second	, , , , , , , , , , , , , ,	ntomatically random writicat de	ized and
Create / E	dit CA Sample Carrier	etechDC_CA harine of tids empry a harine of tids empry a harine can contain a port an existing Cert et analosi, the control eta analosi, the control eta analosi, the control eta analosi, the control eta analosi, the control eta analosi, the contr	as displayed in the OUT for re- places but it cannot contain inflate Authority untroom to the Operating Sy- ents of the CA will be added to the above certificate here. The the above certificate here.	Transport of the following character any of the following character with the transition as on that the distance of the second second second second cases the second secon	ers: $7, s, s, \delta, l, V, s$ y will be trusted by or certificates sign as Serial.	, r the operating system ed by this CA will be au On colle ici le cc Safetech	nomatically random	ized and

Nous avons donc ce résultat :

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
SafetechDC_CA	×	self-signed	0	DC=safetech, DC=com, CN=SAFETECHDC-CA 🚺		e 🖉 🗰 🔟
				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	Authentification LDAPS
Туре	
DAP Server Setting	s
Hostname or IP address	safetechdc.safetech.com NUTE: wrien USINg SSL/TLS UI 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	SafetechDC_CA Choisir l'autorité de certification de SafetechDC This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted or STARTICS 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
uthentication containers	DC=Safetech,DC=com         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	Enable extended query
Bind anonymous	Use anonymous binds to resolve distinguished names
Bind credentials	CN=pfsensead,0U=Asgard,DC=safetech,DC=com
Initial Template	Microsoft AD V
User naming attribute	samAccountName
Group naming attribute	cn
Group member attribute	member0f
Peer Certificate A	elect LDAP containers for authentication
Protocol Server	Containers UU=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
Searc	Save

Ensuite sauvegarder les modifications.

Test de l'authentification LDAPS sur PfSense :

COMMUNITY EDITION	Interfaces      Firewall      Services      VPN      Status	Diagnostics - H	leip + 🐥 😩 🕞
Diagnostics / Aut	thentication	ARP Table Authentication Backup & Restore	≡ø
Authentication Test	Authentification LDAPS 🗸	Command Prompt DNS Lookup Edit File	
Username	kaiser	Factory Defaults Halt System	
Password	[	Limiter Info	
Debug	<ul> <li>Set debug flag</li> <li>Sets the debug flag when performing authentication, which may trigger addition</li> </ul>	Packet Capture	system log (e.g. for LDAP).
	✓ Test	pfTop Ping Reboot	
		Routes	

L'authentification avec LDAPS a réussi :

Us	ser kaiser authenticated successfully. This user is a member of groups:

## 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.

The changes have been ap	plied successfully.	×
DHCP Relay Configu	ration	
Enable	anable DHCP Relay	
Downstream Interfaces	LAN OPT1 OPT2 OPT3 Selectionner les deux interface en maintenant la touche SHIFT	
CARP Status VIP	Interfaces without an IPv4 address will not be shown.	
	Append circuit ID and agent ID to requests     Append the circuit ID (interface number) and the agent ID to the DHCP request.	
Upstream Servers	192.168.100.2	
	192.168.100.3	
	+ Add Upstream Server	

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

		1	IP assignment:	Automatic (DHCP)	Edit
Edit IP settings	Edit IP settings		DNS server assignment:	Automatic (DHCP)	Edit
Automatic (DHCP)	~		Link speed (Receive/Transmit):	1000/1000 (Mbps)	Сору
			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	
Save	Cancel		Description:	Intel(R) PRO/1000 MT Network Connection	
Bare	concer		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 information DNS sont aussi remontées.

## Règles autorisant zimbra :

Pas sur si ca marche

Firewall / Aliases	/ Edit 0
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).
Туре	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

News								
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).							
_								
Туре	Port(s)							
t(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	25	SMTP	m Delete					
	587	Email message submission (SMTP)	面 Delete					
	465	Authenticated SMTP over TLS/SSL (SMTPS)	-					
			Delete					
	110	P0P3	m Delete					
	993	IMAP over SSL	🛅 Delete					
	143	IMAP	📅 Delete					
			L Delete					
	995	POP3 over SSL	🔟 Delete					
		HITPS	The second se					

prospred	Disable this rule						
No RDR (NOT)	<ul> <li>Disable redirection for traffic matching this rule</li> <li>This option is rarely needed. Don't use this without thorough knowledge of the implications.</li> </ul>						
Interface	WAN  V Choose which interface this rule applies to in most cases "WAN" is specified.						
Address Family	Plv4 v  Relet the internet Protocol version this rule aculies to						
Protocol	TCP v Choose which protocol this rule should match. In most cases "TCP" is specified.						
Source	Display Advanced						
Destination	Invert match.	WAN address Type		*	Address/mask	/ ~	
Destination port range	Other 🗸	Zimbra_Ports Custom	Other To port	*	Zimbra_Ports Custom		
Redirect target IP	Enter the internal IP addre In case of IPv6 addresses i.e. it is not possible to rec	Address or Alias Type iss of the server on which to i, in must be from the same "s lirect from link-local address	map the ports. e.g.: 192. scope", es scope (fe80:*) to loca	168.1.12 for	Zimbra Address r IPv4	hung o omgro por c	
Redirect target port	Other         V         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 divertiable to the Yrom port' above.						
Description	A description may be entered here for administrative reference (not passed).						
No XMLRPC Sync	On on 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						

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