

Interconnexion du réseau avec Internet



Table des matières

Contexte StadiumCompany	2
Cahier des charges Stadiumcompany	4
Mission 5	5
Solution :	6
Projet	6
Objectif du projet	6
Mise en place du serveur PfSense	7
Mise en place du service pfSense	12
Configuration basique de pfSense	12
Test d'interconnexion	17
Sécurisation de l'accès à pfSense	18
Sécurisation de la console	18
Sécurisation par accès SSH	19
Sécurisation interface web, HTTPS	21
Protection de la connexion	28
Connexion LDAP	29
Connexion depuis Windows	29
Création de l'authentification LDAP	29
Test connexion LDAP	31
Ajout des propriétés groupes	32
Test de connexion (authentification LDAP)	34
Conclusion	35

Contexte StadiumCompany

StadiumCompany gère un grand stade et avait initialement mis en place un réseau de communication avancé lors de la construction. Cependant, au fil du temps, l'entreprise a ajouté de nouveaux équipements et augmenté les connexions sans tenir compte de ses objectifs commerciaux à long terme ni de la conception de son infrastructure réseau. Cela a conduit à des problèmes de bande passante et de gestion du trafic, limitant la capacité de la société à offrir des services de qualité.

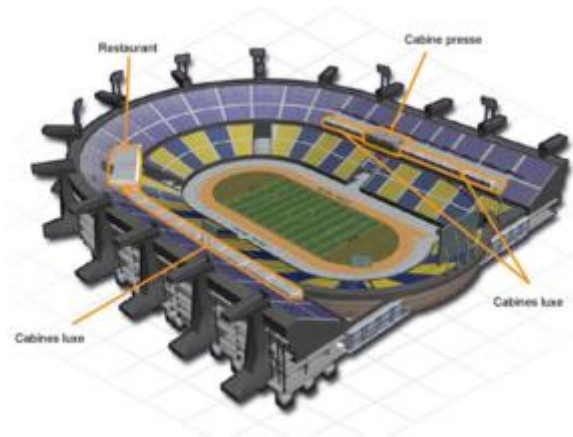


Maintenant, la direction de StadiumCompany souhaite améliorer la satisfaction de ses clients en introduisant de nouvelles technologies et en permettant l'organisation de concerts, mais le réseau actuel ne le permet pas. Sachant qu'elle ne possède pas l'expertise nécessaire en matière de réseau, la direction a décidé de faire appel à des consultants réseau pour concevoir, gérer et mettre en œuvre ce projet en trois phases.

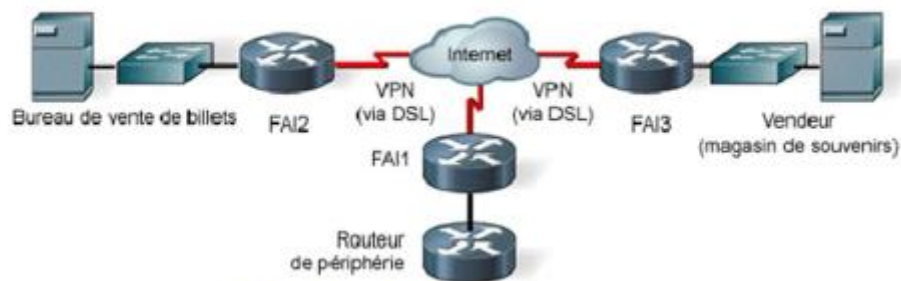
La première phase consiste à planifier le projet et à préparer une conception réseau de haut niveau. Pour cela, StadiumCompany a engagé NetworkingCompany, une société spécialisée en conception de réseaux, qui a interrogé le personnel du stade pour comprendre l'organisation et les installations.



StadiumCompany emploie 170 personnes à temps plein, dont 35 dirigeants et responsables, ainsi que 135 employés. Ils ont également recours à environ 80 intérimaires pour des événements spéciaux. Tous les employés, à l'exception des préposés au terrain et des gardiens, utilisent des PC et des téléphones connectés à un PABX vocal numérique.



Le stade propose des installations pour deux équipes sportives, une équipe visiteuse, un restaurant de luxe et un fournisseur de concessions. Il dispose également de deux sites distants, une billetterie en centre-ville et une boutique de souvenirs, connectés via DSL à un FAI local.



Le stade est construit sur deux niveaux, avec des locaux techniques reliés par des câbles à fibre optique en raison de sa grande taille. Les équipes sportives ont leurs bureaux et installations, tandis que le restaurant de luxe loue également des bureaux auprès de StadiumCompany

En résumé, StadiumCompany souhaite moderniser son réseau pour répondre aux besoins actuels et futurs, et a fait appel à des experts pour le guider à travers ce processus de mise à niveau.

Cahier des charges Stadiumcompany

Le Cahier des Charges de StadiumCompany révèle votre intégration au sein de la division Systèmes d'Information (SI) de l'entreprise pour cette année. Votre mission centrale consistera à assumer la responsabilité de l'administration des systèmes et des réseaux informatiques.

StadiumCompany se compose de plusieurs sites distincts, chacun ayant un rôle spécifique :

1. Site 1 : Stade - Ce site est le cœur de l'entreprise, abritant l'hébergement informatique, le siège social et le centre administratif. Il est le pivot autour duquel s'articulent toutes les opérations et activités de l'entreprise.

2. Site 2 : Billetterie - Ce site est dédié à la gestion des ventes de billets, un élément essentiel pour les événements sportifs et les spectacles organisés au stade.

3. Site 3 : Magasin - Ce site est spécialement conçu pour la vente d'articles souvenirs, offrant aux fans et aux visiteurs la possibilité d'acheter des produits liés à l'équipe ou aux événements.

Le Cahier des Charges insiste sur la nécessité de documenter les différentes solutions retenues pour le projet en fonction de leur niveau de complexité. Cette approche méthodique garantira que chaque aspect de l'infrastructure informatique soit clairement spécifié et que les procédures soient consignées de manière exhaustive. Cela s'inscrit dans la vision globale adoptée par StadiumCompany pour assurer une gestion efficace et cohérente de ses ressources informatiques.

Votre rôle au sein de cette mission sera d'une importance cruciale, car vous devrez contribuer à façonner et à maintenir l'infrastructure technologique qui soutient les opérations de l'entreprise et qui permet de répondre aux défis uniques posés par chaque site.

Mission 5 : Sécurisation de l'Interconnexion du Réseau de Stadiumcompany avec Internet

Contexte : Après avoir mis en place l'architecture réseau interne du site du stade, le Directeur des Systèmes d'Information (DSI) de StadiumCompany souhaite désormais interconnecter le réseau de l'entreprise avec Internet. Cette expansion vers Internet offre de nombreux avantages, mais elle expose également l'entreprise à de nouvelles menaces en matière de sécurité. Il est donc essentiel d'intégrer la sécurité au sein de l'architecture réseau pour réduire ces risques.

Définition du besoin : Le DSI de StadiumCompany souhaite réaliser une étude complète des risques liés à l'accès à Internet, en prenant en compte les éléments de sécurité suivants :

1. **Mise en place d'une DMZ :** Création d'une zone démilitarisée (DMZ) contenant un ensemble de serveurs accessibles depuis l'extérieur, en particulier le serveur web.
2. **Restriction de l'accès au réseau interne :** L'environnement du réseau interne du stade doit être accessible uniquement aux acteurs de l'entreprise.
3. **Hébergement en interne des serveurs :** Les serveurs exécutant les applications et les besoins de StadiumCompany sont hébergés en interne.
4. **Accès Internet pour les collaborateurs :** Les employés de l'entreprise sont autorisés à accéder à Internet à partir du réseau interne.
5. **Accès Internet restreint pour les utilisateurs du réseau Wi-Fi Visiteurs :** Les utilisateurs du réseau Wi-Fi Visiteurs ont un accès limité, uniquement à Internet.

Travail à réaliser : Pour répondre à ces besoins, les tâches suivantes doivent être accomplies :

1. **Identification des Risques :** Il est essentiel d'identifier les risques potentiels associés à l'interconnexion avec Internet. Cela comprend la menace de cyberattaques, d'intrusions, de fuites de données, etc.
2. **Détermination de la Démarche de Sécurité :** Élaboration d'une démarche visant à réduire ces risques. Cela inclut la mise en place de pare-feux, de systèmes de détection d'intrusions, de systèmes de prévention des intrusions, et d'autres mesures de sécurité.
3. **Définition de la Problématique de l'Accès à Internet :** Élaboration d'une stratégie de sécurité pour gérer l'accès au réseau Internet à partir d'un réseau privé, en garantissant la confidentialité, l'intégrité et la disponibilité des données.
4. **Conception de la Politique de Filtrage :** Définition d'une politique de filtrage des flux de données conformément aux exigences du cahier des charges. Cette politique devrait déterminer quels types de trafic sont autorisés ou bloqués.
5. **Adaptation de la Maquette :** Mise à jour de l'architecture réseau actuelle en fonction de la solution proposée, en intégrant les éléments de sécurité nécessaires pour garantir la protection du réseau et des données.

La réalisation de cette mission est cruciale pour assurer la sécurité de l'entreprise dans un environnement connecté à Internet, en réduisant les risques potentiels et en mettant en place les contrôles de sécurité adéquats.

Solution :

pfSense est un système d'exploitation open source ayant pour but la mise en place de routeur ou de firewall basé sur le système d'exploitation FreeBSD. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnelles propriétaires. Après l'installation manuelle nécessaire pour assigner les interfaces réseaux, l'administration se fait à distance par interface web. pfSense peut fonctionner sur du matériel de serveur ou domestique, sur des solution embarquées sans toutefois demander beaucoup de ressource.

Quelques fonctionnalités de pfSense

pfSense permet :

1. Filtrage par IP source et destination, port du protocole, IP source et destination pour le trafic TCP et UDP
2. Portail Captif
3. Dynamic DNS
4. VPN
5. NAT

Projet

Objectif du projet

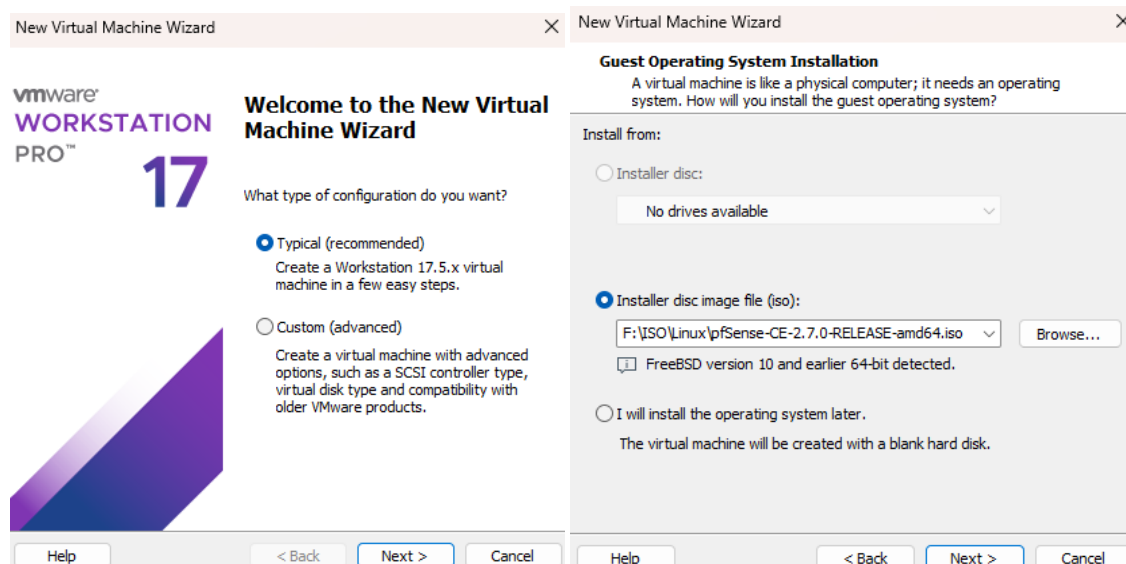
L'objectif du projet est de mettre en place un service d'interconnexion avec Internet donnant ainsi une possibilité aux utilisateurs de se connecter à l'extérieur du réseau tout en bénéficiant d'une sécurité contre les risques.

Mise en place du serveur PfSense

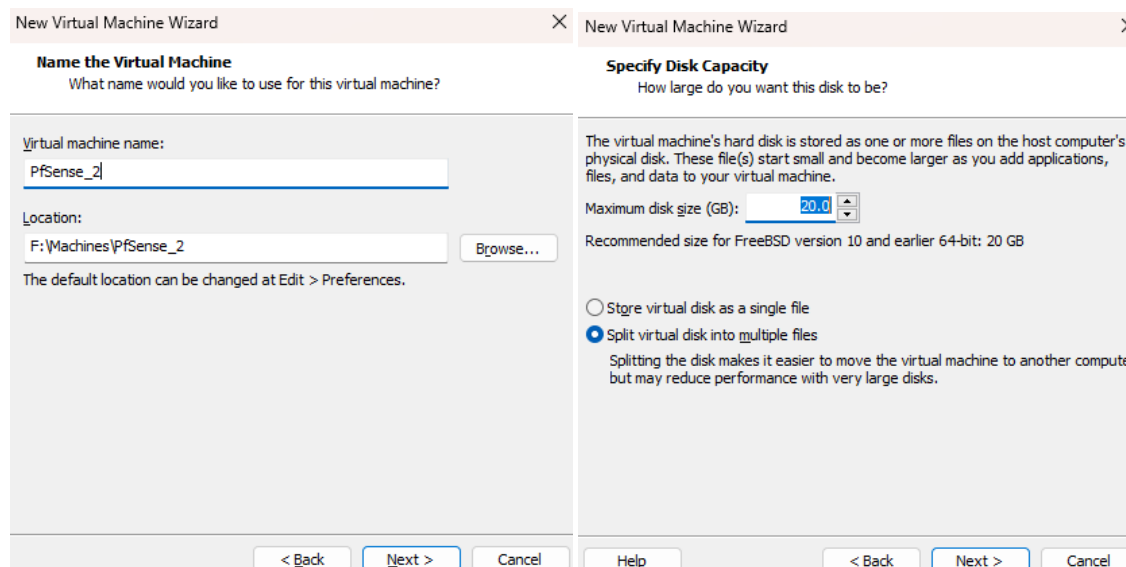
On télécharge le fichier depuis le site officiel (<https://www.pfsense.org/download/>)

On décompresse notre fichier **pfSense-CE-2.7.0-RELEASE-p1-amd64.iso.gz** puis on procède à l'installation sur notre outil de virtualisation (VMWare Workstation Pro)

On crée une nouvelle machine et on sélectionne le fichier décompressé (ISO)

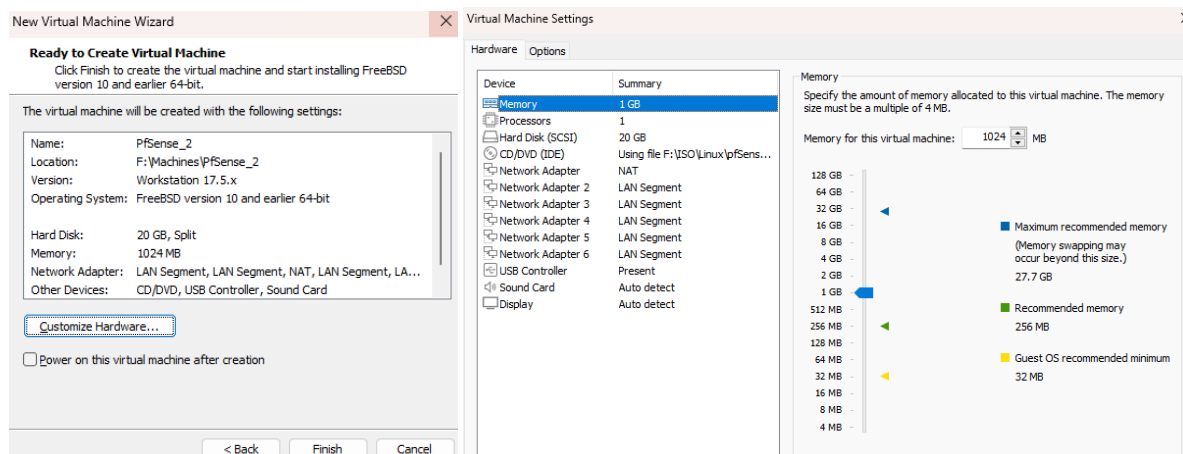


On le renomme (PfSense_2) et on lui attribue un espace de stockage (20Go)

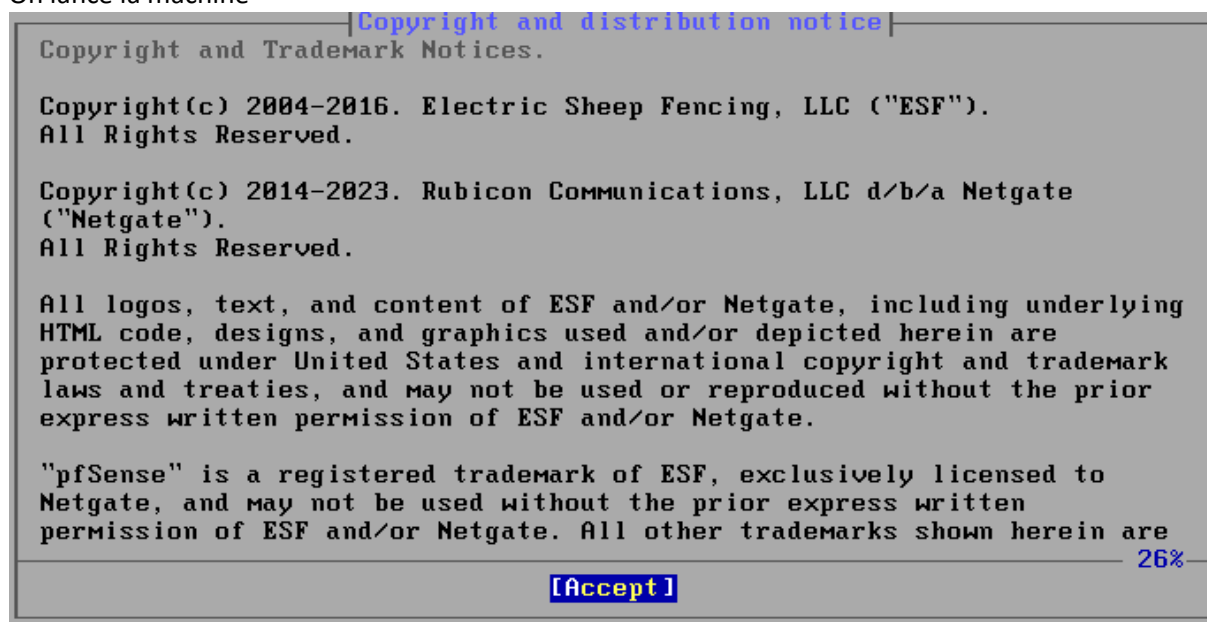


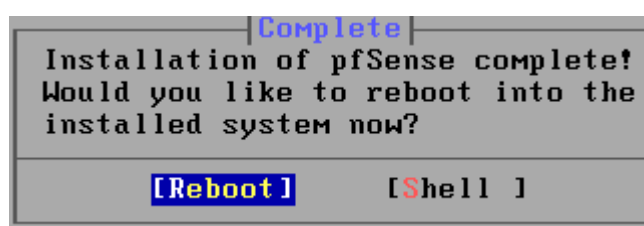
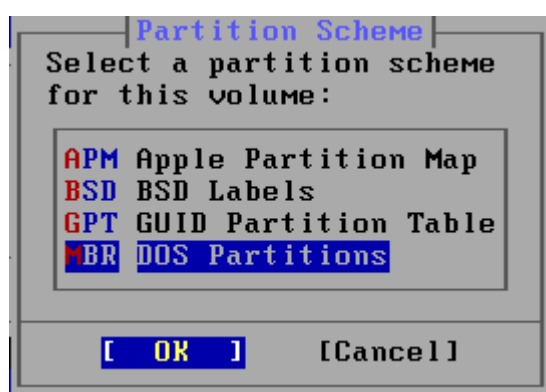
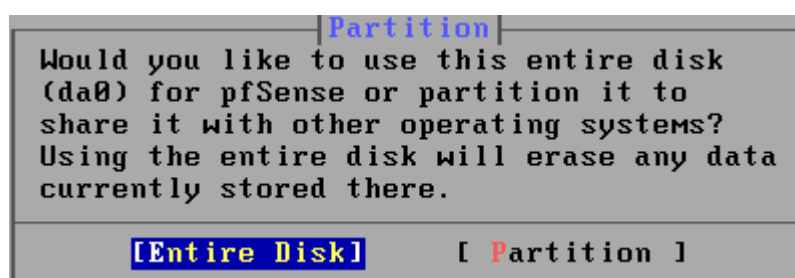
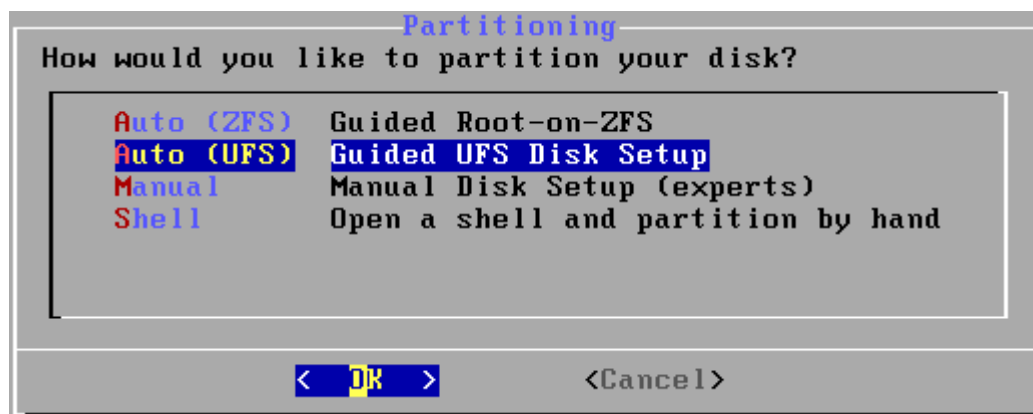
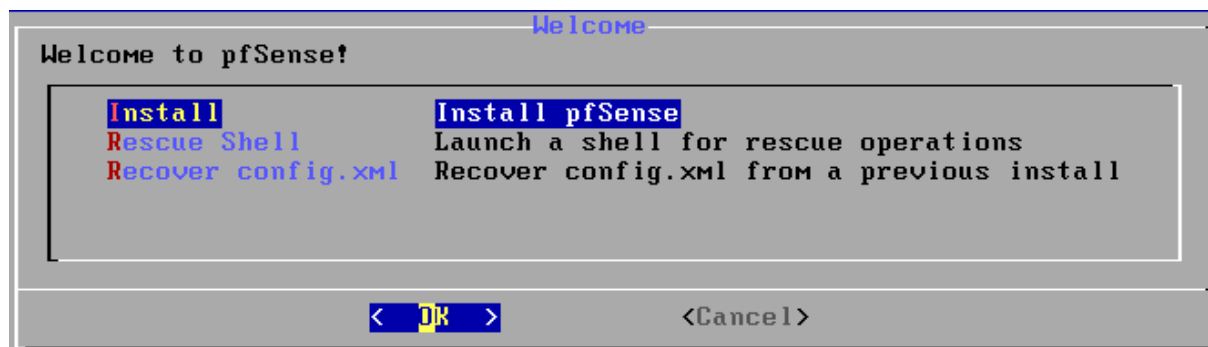
On change des paramètres machines pour ajouter des cartes réseaux correspondant aux réseaux que nous avons :

1. Network Adapter → WAN (Accès à Internet)
2. Network Adapter 2 → LAN_Serveur
3. Network Adapter 3 → LAN_Equipe
4. Network Adapter 4 → LAN_WiFi
5. Network Adapter 5 → LAN_DMZ
6. Network Adapter 6 → LAN_Service
7. Memory → 1GB



On lance la machine





Panneau de configuration basique

```

em5      00:0c:29:31:74:b9 (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

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

Should VLANs be set up now [y:n]? ^CUMware Virtual Machine - Netgate Device ID:
dc2b08fbbce6b09be40c

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.62.148/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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

Enter an option: █

```

Mettre manuellement la langue en français pour une meilleure configuration : 8 puis #kbdcontrol -l fr

Il manque nos 4 autres interfaces que l'on va ajouter, choisir l'option 1 :

- Should VLANs be set up now ? n
- Enter the WAN interface name : **em0**
- Enter the LAN interface name : **em1**
- Enter the Optional (numéro de l'interface) name : **em2/em3/em4/em5**

```

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.62.148/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2      ->
OPT2 (opt2)    -> em3      ->
OPT3 (opt3)    -> em4      ->
OPT4 (opt4)    -> em5      ->

```

On configure ensuite nos interfaces (en fonction des VLANs), choisir l'option 2 :

Interface WAN en DHCP

```

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) y
Configure IPv6 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

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

Please wait while the changes are saved to WAN... █

```

Interface LAN en manuel

```

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:
> 172.20.0.1

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

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

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) n

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

```

Les interfaces sont configurées en fonction de leur VLAN

```

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.62.148/24
LAN (lan)      -> em1      -> v4: 172.20.0.1/24
OPT1 (opt1)    -> em2      -> v4: 172.20.1.1/24
OPT2 (opt2)    -> em3      -> v4: 172.20.2.1/24
OPT3 (opt3)    -> em4      -> v4: 172.20.3.1/24
OPT4 (opt4)    -> em5      -> v4: 172.20.4.1/24

```

On peut tester de ping nos serveurs et les DNS de Google

```

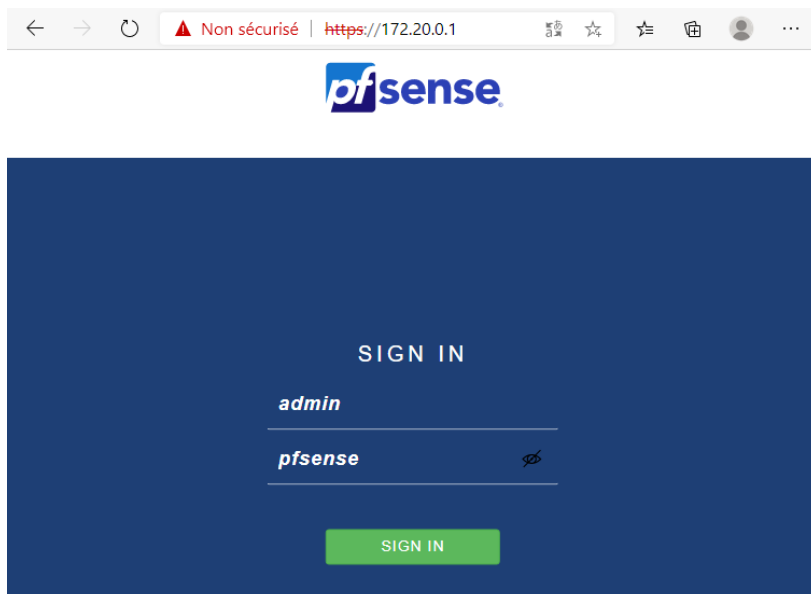
--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 7.596/7.596/7.596/0.000 ms
[2.7.0-RELEASE][root@pfSense.home.arpal/root]: ping 172.20.0.10
PING 172.20.0.10 (172.20.0.10): 56 data bytes
64 bytes from 172.20.0.10: icmp_seq=0 ttl=128 time=0.393 ms
^C
--- 172.20.0.10 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.393/0.393/0.393/0.000 ms
[2.7.0-RELEASE][root@pfSense.home.arpal/root]: ping 172.20.0.20
PING 172.20.0.20 (172.20.0.20): 56 data bytes
64 bytes from 172.20.0.20: icmp_seq=0 ttl=64 time=1.017 ms
^[[A^C
--- 172.20.0.20 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.017/1.017/1.017/0.000 ms
[2.7.0-RELEASE][root@pfSense.home.arpal/root]: ping 172.20.0.30
PING 172.20.0.30 (172.20.0.30): 56 data bytes
64 bytes from 172.20.0.30: icmp_seq=0 ttl=64 time=0.975 ms
^C
--- 172.20.0.30 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.975/0.975/0.975/0.000 ms
[2.7.0-RELEASE][root@pfSense.home.arpal/root]: 

```

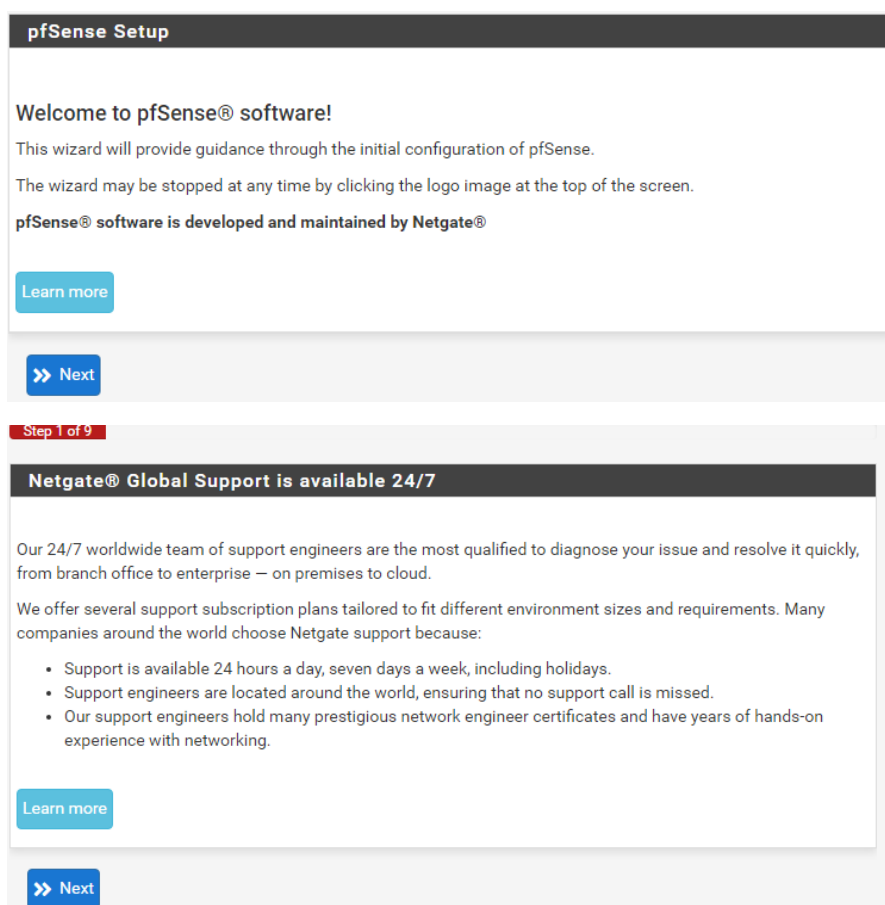
Mise en place du service pfSense

Configuration basique de pfSense

Se connecter sur l'interface web (172.20.0.1) avec les identifiants : admin et pfsense



On se retrouve sur la configuration basique à faire, on configure comme suit :



General Information

On this screen the general pfSense parameters will be set.

Hostname

Name of the firewall host, without domain part.

Examples: pfsense, firewall, edgefw

Domain

Domain name for the firewall.

Examples: home.arpa, example.com

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.

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

Primary DNS Server

Secondary DNS Server

Override DNS



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

Time Server Information

Please enter the time, date and time zone.

Time server hostname

Enter the hostname (FQDN) of the time server.

Timezone

[» Next](#)

Step 4 of 9

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType

General configuration

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: xx:xx:xx:xx:xx:xx or leave blank.

MTU

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask

>> Next

Set Admin WebGUI Password

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

Reload configuration

Click 'Reload' to reload pfSense with new changes.

>> Reload

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)

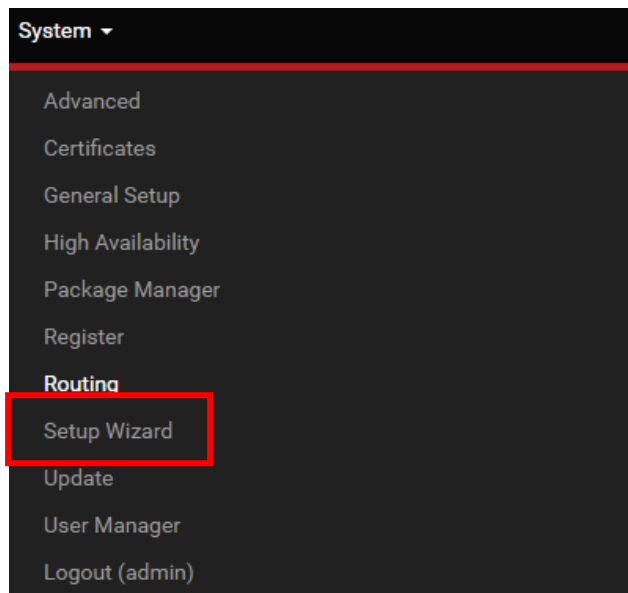
[Anonymous User Survey](#)

Useful resources.

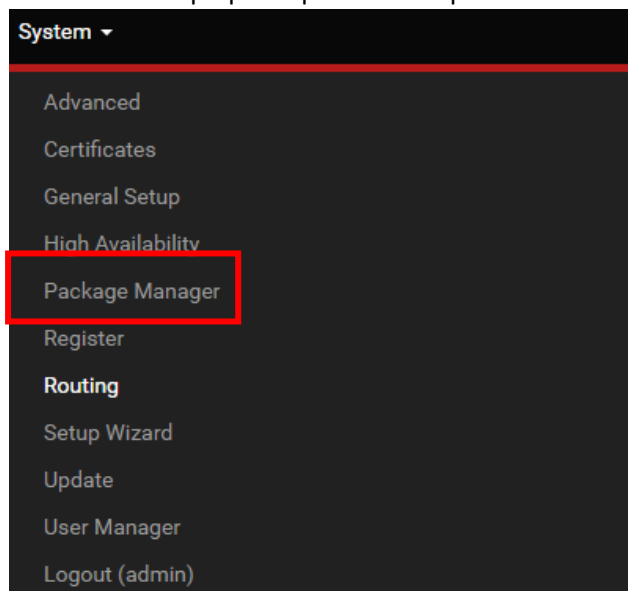
- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

Finish

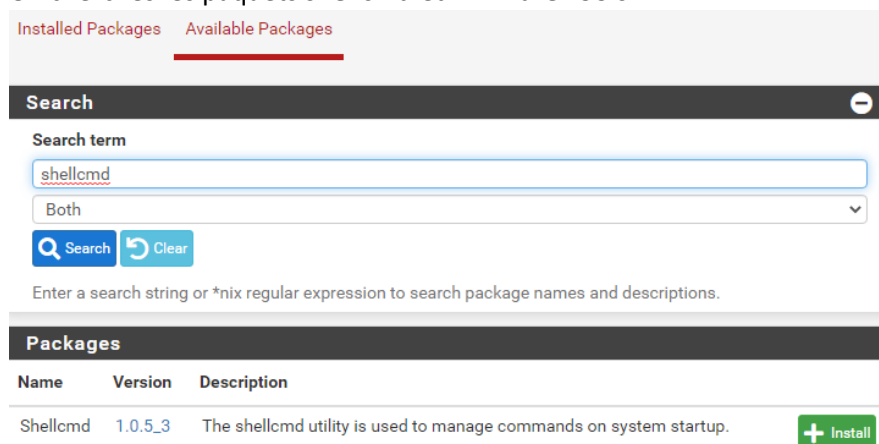
On peut relancer cette procédure via **Setup Wizard**

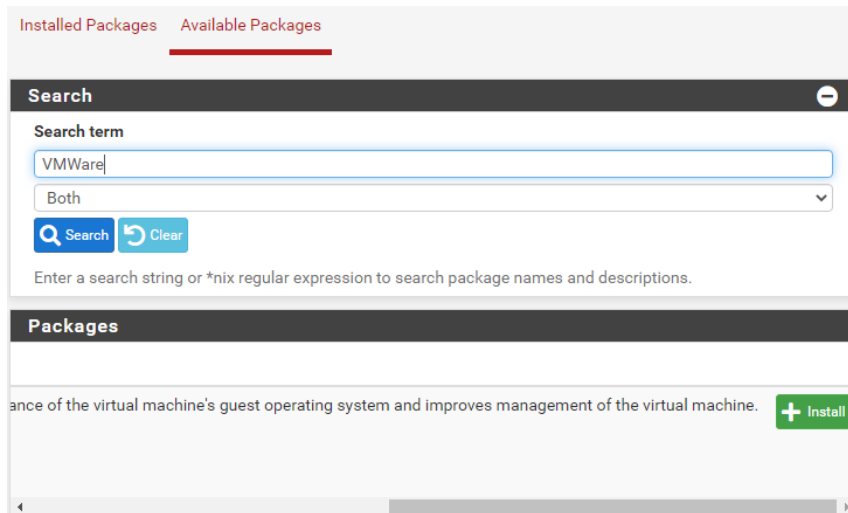


On installe des paquets qui serviront pour une meilleure utilisation du pare-feu

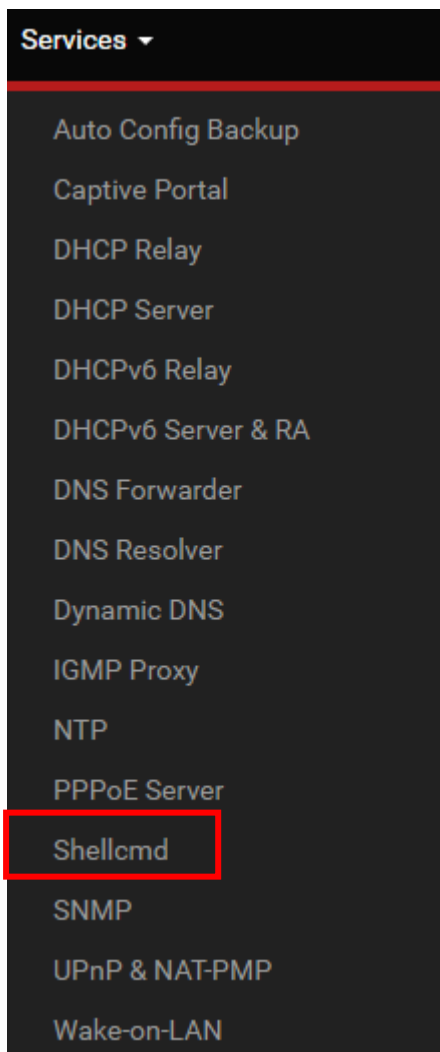


On cherche les paquets **shellcmd** et **VMWare Tools**





On configure le shellcmd qui lancera à chaque démarrage le clavier français



Services: Shellcmd Settings

Command	Shellcmd Type	Description
+ Add		

Save

Shellcmd Configuration

Command

Enter the command to run.

Shellcmd Type

Choose the shellcmd type. Click Info for details.

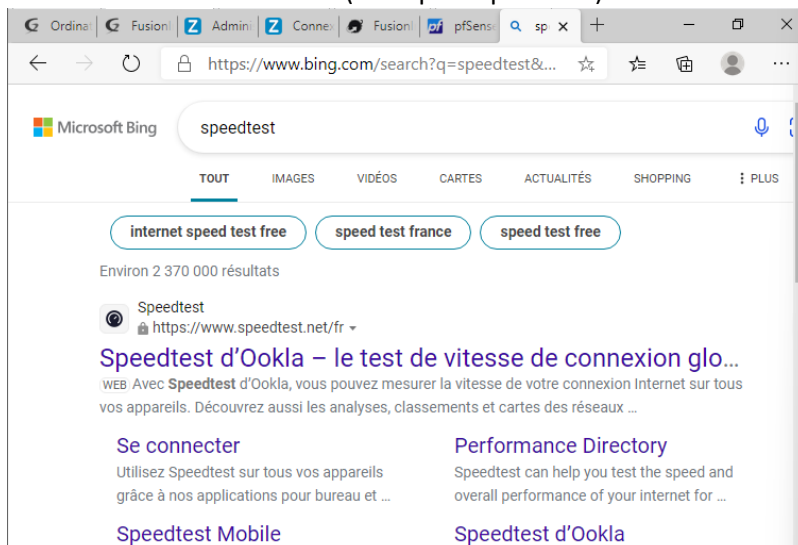
Description

Enter a description for this command. (This is for your reference only.)

Save

Test d'interconnexion

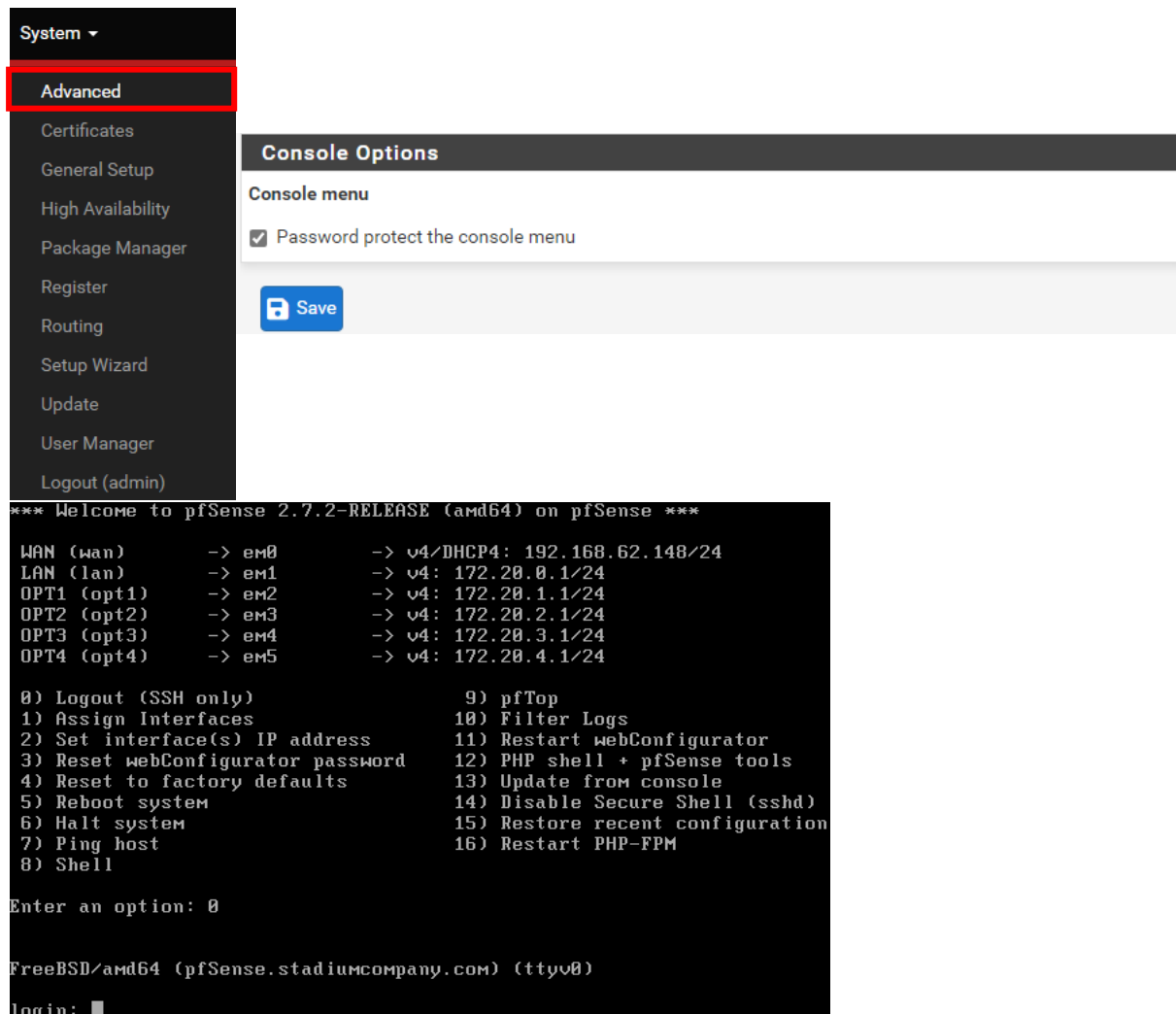
On fait un test de recherche (exemple : Speedtest) et on a bien accès à Internet



Sécurisation de l'accès à pfSense

Sécurisation de la console

On sécurise notre console en cochant la case indiquant qu'à chaque connexion, le mot de passe sera demandé



The screenshot shows the pfSense web interface. On the left, the 'System' menu is expanded, and the 'Advanced' tab is selected. The 'Console Options' section is visible, showing a checkbox for 'Password protect the console menu' which is checked. Below this is a 'Save' button. Below the web interface is a terminal window showing the pfSense console menu. The terminal output is as follows:

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.62.148/24
LAN (lan)      -> em1      -> v4: 172.20.0.1/24
OPT1 (opt1)    -> em2      -> v4: 172.20.1.1/24
OPT2 (opt2)    -> em3      -> v4: 172.20.2.1/24
OPT3 (opt3)    -> em4      -> v4: 172.20.3.1/24
OPT4 (opt4)    -> em5      -> v4: 172.20.4.1/24

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

Enter an option: 0

FreeBSD/amd64 (pfSense.stadiumcompany.com) (ttyv0)
login: 
```

Sécurisation par accès SSH

On repart dans **System > Advanced**

Secure Shell

Secure Shell Server

☒ Enable Secure Shell

SSHD Key Only

Password or Public Key

When set to *Public Key Only*, 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 daemon requires both authorized keys **and** valid passwords to gain access. The default *Password or Public Key* setting allows either a valid password or a valid authorized key to login.

Allow Agent Forwarding

☒ Enables ssh-agent forwarding support.

SSH port

2121

Note: Leave this blank for the default of 22.

On ajoute une règle qui autorise **SSH** sur l’interface **WAN (Firewall > Rules)**

Edit Firewall Rule

Action

Pass

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

Disabled

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

Interface

WAN

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

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Any

Source Address

Destination

Destination

☐ Invert match

WAN address

Destination Address

Destination Port Range

(other)

From

2121

Custom

(other)

To

2121

Custom

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

Extra Options

Log

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

Description

authoriser ssh

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

Advanced Options

Display Advanced

Rules (Drag to Change Order)										
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	
<input checked="" type="checkbox"/>	0/0 B	*	RFC 1918 networks	*	*	*	*	*		
<input checked="" type="checkbox"/>	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		
<input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	0/0 B	IPv4 TCP	*	WAN address	2121	*	none		
<div><div>↑ Add</div><div>↓ Add</div><div>🗑 Delete</div><div>🔄 Toggle</div><div>📄 Copy</div><div>💾 Save</div><div>➕ Separator</div></div>										

Charlie Li, Mehdy Lacroix, Claudys BIKINDOU
BTS SIO SISR

École IRIS

Appliquer les changements

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

✓ Apply Changes

On tente une connexion SSH via **Hermes (ssh admin@172.20.0.1)**, on peut se connecter

```
OpenSSH SSH client
PS C:\Users\Administrateur> ssh admin@172.20.0.1 -p 2121
The authenticity of host '[172.20.0.1]:2121 ([172.20.0.1]:2121)' can't be established.
ED25519 key fingerprint is SHA256:heTg4AnsX6ZB3GQDMtKUbni0dBbK9FktI2k8k9934Dw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.20.0.1]:2121' (ED25519) to the list of known hosts.
Password for admin@pfSense.stadiumcompany.com:
/Mware Virtual Machine - Netgate Device ID: dc2b08fbbce6b09be40c

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.62.148/24
LAN (lan)      -> em1      -> v4: 172.20.0.1/24
OPT1 (opt1)    -> em2      -> v4: 172.20.1.1/24
OPT2 (opt2)    -> em3      -> v4: 172.20.2.1/24
OPT3 (opt3)    -> em4      -> v4: 172.20.3.1/24
OPT4 (opt4)    -> em5      -> v4: 172.20.4.1/24

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

Enter an option: _
```

On tente une connexion depuis une machine physique, impossible de connecter car des règles **bloquent les connexions privées** dehors des réseaux **WAN, lan1, opt (1/2/3/4)**

```
Administrateur : Windows PowerShell
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> ssh admin@192.168.62.148
ssh: connect to host 192.168.62.148 port 22: Connection timed out
PS C:\WINDOWS\system32> ping 192.168.62.148

Envoi d'une requête 'Ping' 192.168.62.148 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.62.148:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
PS C:\WINDOWS\system32>
```

On peut retrouver ces règles sur l'**interface WAN** ou dans les règles du pare-feu

Reserved Networks

Block private networks and loopback addresses

☒

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

Block bogon networks

☒

Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.

This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.

Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Save

✗	0/760 B	*	RFC 1918 networks	*	*	*	*	*
✗	0/0 B	*	Reserved	*	*	*	*	*
Not assigned by IANA								

Sécurisation interface web, HTTPS

On procède à la création d'une autorité de certification interne

System ▾

Advanced

Certificates

General Setup
High Availability
Package Manager
Register
Routing
Setup Wizard
Update
User Manager
Logout (admin)

Authorities
Certificates
Revocation

Search

Search term

Both

Search
Clear

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

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
<div>+ Add</div>						

Remplir les champs

Create / Edit CA

Descriptive name

Autorité de certification StadiumCompany

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

Method

Create an internal Certificate Authority

Trust Store

☒ Add this Certificate Authority to the Operating System Trust Store

When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial

☒ Use random serial numbers when signing certificates

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

Internal Certificate Authority

Key type

RSA

2048

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

Digest Algorithm

sha256

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

Lifetime (days)

3650

Common Name

internal-ca-stadiumcompany

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

Country Code

FR

State or Province

IDF

City

Paris

Organization

stadiumcompany

Organizational Unit

SC

Save

On affiche notre certificat ainsi que sa clé dans les modifications

Certificate Authorities

Distinguished Name	In Use	Actions
O=stadiumcompany, L=Paris, CN=internal-ca-stadiumcompany, C=FR		

Valid From: Sun, 05 May 2024 15:25:49 +0200
Valid Until: Wed, 03 May 2023 15:25:49 +0200

Certificate data

```
-----BEGIN CERTIFICATE-----
MIIEVjCCAz6gAwIBAgIIAYDTxYTwc04wDQYJKoZIhvcNAQELBQAwZjEjMCEGA1UE
AxMaal50ZXJ1YWwtY2EtY2Etc3RhZG11bWVubXBhbnkxZzAJBgNVBAYTAkZSMQwwCgYD
VQQIEwNJREYxZjAMBgNVBACTBVBhcnlzMRCwFQYDVQQKEw5zdGFkaXVtY29tcGFu
eTELMakGA1UECzMCMU0MwHhcNMjQwNTA1MTMyNTQ5WhcNMzQwNTAzMTMyNTQ5WjB2
-----
```

Paste a certificate in X.509 PEM format here.

Certificate Private Key (optional)

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBywggSiAgEAAoIBAQC0PjymU1/LhE+A
kXNzk6dHCiP7zetxDHho5KHxXS+tdqCn+fQw1QWYa4+hhndCTxuZpABdv0CNI2Iy
mgVHgS1/f5CWGI/eqx1PZi9/Td4C0Aqp04N+7Y6eGCK6T0hi4p2c7WI1w0R/pP6Q
0DbXSUN26zoQ0osyvpC1AZt/7rSVKE0HuWM3b+UwE+fsFUINpKiLQTbiI5tWbDnN
-----
```

Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

On crée le certificat web

Authorities **Certificates** Certificate Revocation

Search

Search term

Both

Search Clear

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

Certificates

Name	Issuer	Distinguished Name
webConfigurator default (66376e862b4f5) Server Certificate	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense webConfigurator
CA: No		Valid From: Sun, 05 May 2024 13:33:26 +0200
Server: Yes		Valid Until: Sat, 07 Jun 2025 13:33:26 +0200

Add/Sign

On remplit les champs comme suit avec les réseaux

Add/Sign a New Certificate
Method <div> Create an internal Certificate </div>
Descriptive name <div> Certificat SSL pour Stadiumcompany </div> <p>The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", ' </p>
Internal Certificate
Certificate authority <div> Autorité de certification StadiumCompany </div>
Key type <div> RSA </div>
<div> 2048 </div> <p>The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid. </p>
Digest Algorithm <div> sha256 </div> <p>The digest method used when the certificate is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid. </p>

Digest Algorithm

The digest method used when the certificate is signed.

The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days)

The length of time the signed certificate will be valid, in days.

Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name

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

Country Code**State or Province****City****Organization****Organizational Unit**

Certificate Attributes

Attribute Notes

The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type

Server Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names

FQDN or Hostname

pfsense.stadiumcompany.com

Delete

IP address

172.20.0.1

Delete

IP address

172.20.1.1

Delete

IP address

172.20.2.1

Delete

IP address

172.20.3.1

Delete

IP address

172.20.4.1

Delete

TypeValue

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add SAN Row

+ Add SAN Row

Save

Le certificat est ajouté

Certificat SSL pour Stadiumcompany
Server Certificate
CA: No
Server: Yes

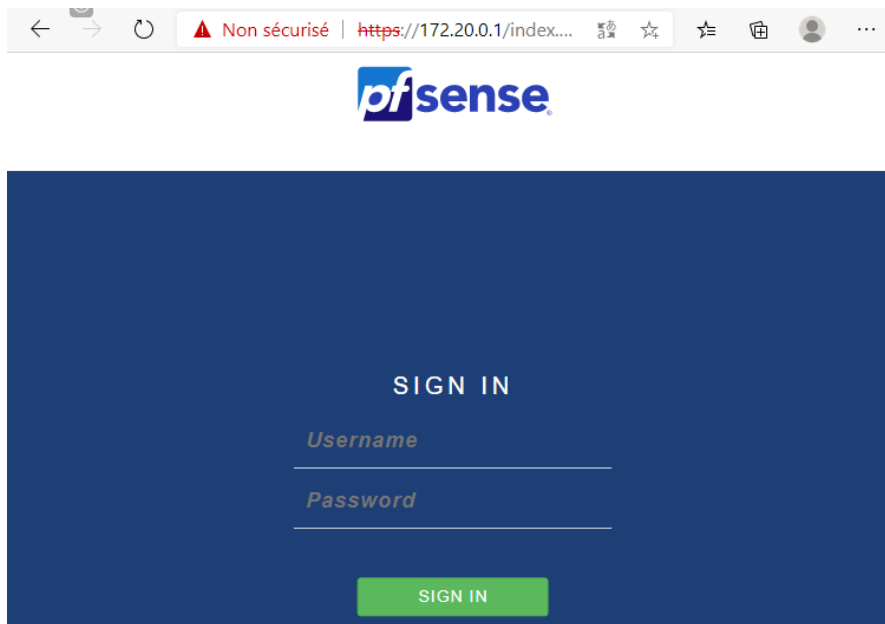
Autorité de certification StadiumCompany

ST=IDF, OU=SC, O=stad
Valid From: Sun, 05 May 20
Valid Until: Wed, 03 May 20

On injecte notre certificat dans le serveur PfSense, **System > Advanced**, avec les paramètres suivants et on enregistre

webConfigurator
Protocol <input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS (SSL/TLS)
SSL/TLS Certificate <div>Certificat SSL pour Stadiumcompany</div> <p>Certificates known to be incompatible with use for HTTPS are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.</p>
TCP port <div></div> <p>Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.</p>
Max Processes <div>2</div> <p>Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.</p>
WebGUI redirect <input checked="" type="checkbox"/> Disable webConfigurator redirect rule <p>When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.</p>
HSTS <input type="checkbox"/> Disable HTTP Strict Transport Security <p>When this is unchecked, Strict-Transport-Security HTTPS response header is sent by the webConfigurator to the browser. This will force the browser to use only HTTPS for future requests to the firewall FQDN. Check this box to disable HSTS. (NOTE: Browser-specific steps are required for disabling to take effect when the browser already visited the FQDN while HSTS was enabled.)</p>
WebGUI Login Autocomplete <input checked="" type="checkbox"/> Enable webConfigurator login autocomplete <p>When this is checked, login credentials for the webConfigurator may be saved by the browser. While convenient, some security standards require this to be disabled. Check this box to enable autocomplete on the login form so that browsers will prompt to save credentials (NOTE: Some browsers do not respect this option).</p>

Le serveur est passé en **https**



Protection de la connexion

On protège la connexion en mettant des **tentatives** ainsi **qu'un temps de blocage**

Login Protection

Threshold

8

Block attackers when their cumulative attack score exceeds threshold. Most attacks have a score of 10.

Blocktime

180

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.

Detection time

259200

Remember potential attackers for up to detection_time seconds before resetting their score.

Pass list

Address / 128

Addresses added to the pass list will bypass login protection.

Add address

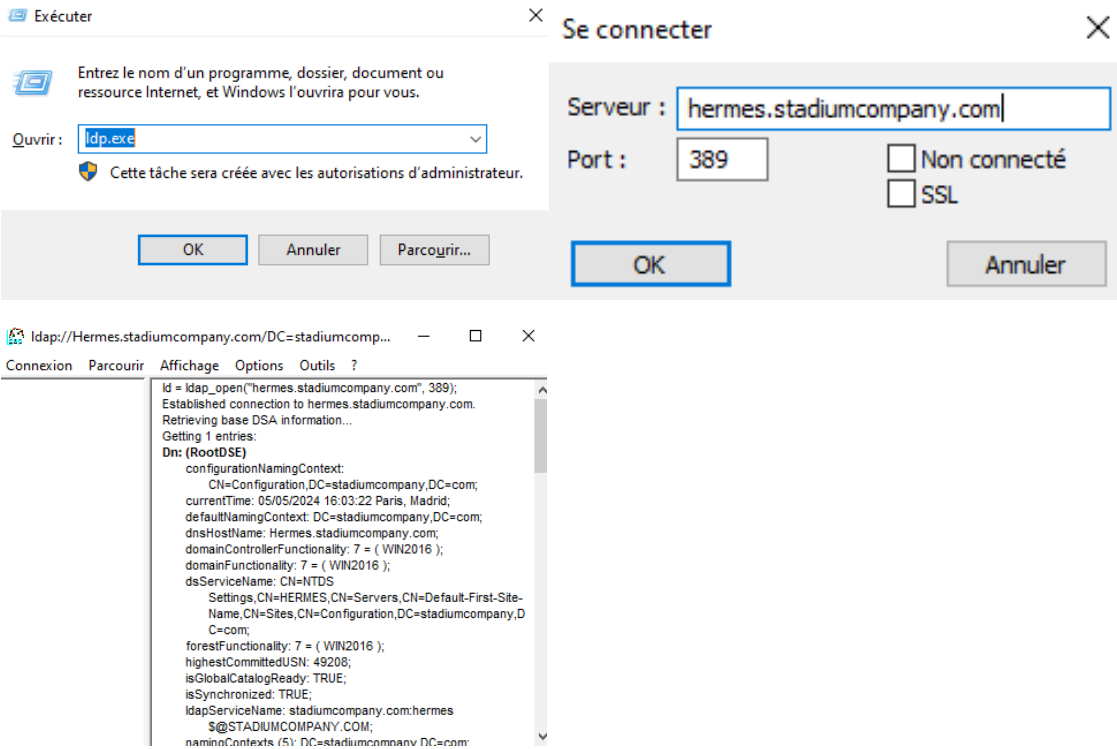
+ Add address

Connexion LDAP

Connexion depuis Windows

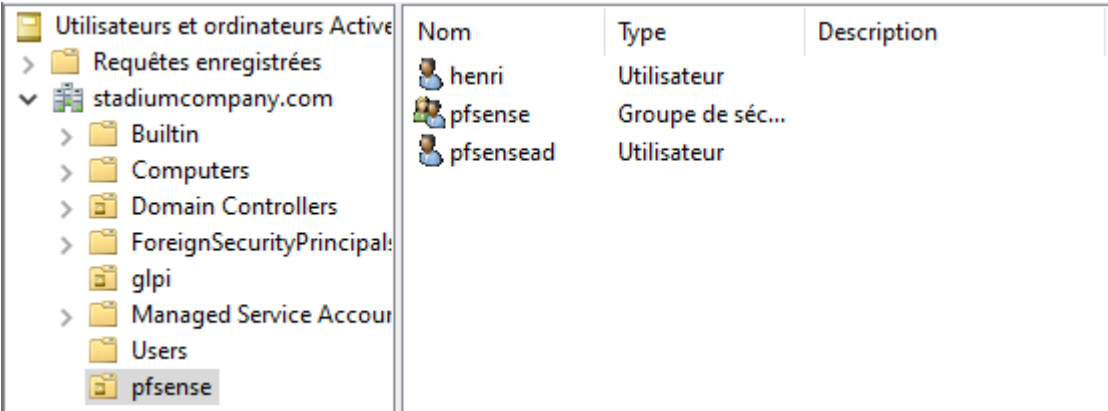
On teste la connexion d'authentification LDAP

LDAP



Création de l'authentification LDAP

On crée une OU avec des utilisateurs et un groupe



On va dans **System > User Manager > Authentication Servers** et on crée notre liaison LDAP

Users	Groups	Settings	Authentication Servers
-----------------------	------------------------	--------------------------	--

Authentication Servers			
Server Name	Type	Host Name	Actions
Local Database		pfSense	

+ Add

On remplit les champs comme suit et on clique sur **Select a container**

Server Settings
Descriptive name <input type="text" value="authentification LDAP"/>
Type <input type="text" value="LDAP"/>
LDAP Server Settings
Hostname or IP address <input type="text" value="hermes.stadiumcompany.com"/> <small>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.</small>
Port value <input type="text" value="389"/>
Transport <input type="text" value="Standard TCP"/>
Peer Certificate Authority <input type="text" value="Global Root CA List"/> <small>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.</small>
Protocol version <input type="text" value="3"/>
Server Timeout <input type="text" value="25"/> <small>Timeout for LDAP operations (seconds)</small>

Search scope

Level
Entire Subtree

Base DN
DC=stadiumcompany,DC=com

Authentication containers

cn

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

Select a container

Extended query

☐ Enable extended query

Bind anonymous

☐ Use anonymous binds to resolve distinguished names

Bind credentials

CN=pfsensead,OU=pfsense,DC=stadiumcompany,DC=com

Initial Template

OpenLDAP

On sélectionne notre OU qui contient nos utilisateurs et on enregistre

Select LDAP containers for authentication

Containers

☐ OU=Domain Controllers,DC=stadiumcompany,DC=com

☐ OU=glpi,DC=stadiumcompany,DC=com

☒ OU=pfsense,DC=stadiumcompany,DC=com

☐ CN=Users,DC=stadiumcompany,DC=com

Save

Test connexion LDAP

On va tester l'authentification LDAP, on va dans **Diagnostics > Authentication**

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

Authentication Test

Authentication Server

authentication LDAP

Select the authentication server to test against.

Username

henri

Password

Debug

☐ Set debug flag

Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).

Test

Ajout des propriétés groupes

On va **System > User Manager > Groups > Add**

Group Properties

Group name

pfsense

Scope

Remote

Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description

compte Active Directory

Group description, for administrative information only

Group membership

admin

Not members

Members

>> Move to "Members"

On revient sur le groupe que l'on a créé et on va dans **Assigned Privileges** et on ajoute le privilège **WebCfg – All pages** (accès admin)

Group Privileges

Group


pfsense


Assigned privileges

- System - HA node sync
- User - Config: Deny Config Write
- User - Notices: View
- User - Notices: View and Clear
- User - Services: Captive Portal login
- User - System: Copy files (scp)
- User - System: Copy files to home directory (chrooted scp)
- User - System: Shell account access
- User - System: SSH tunneling
- User - VPN: IPsec xauth Dialin
- User - VPN: L2TP Dialin
- User - VPN: PPPoE Dialin
- WebCfg - AJAX: Get Queue Stats
- WebCfg - AJAX: Get Service Providers
- WebCfg - AJAX: Get Stats
- WebCfg - All pages**
- WebCfg - Crash reporter
- WebCfg - Dashboard (all)
- WebCfg - Dashboard widgets (direct access).
- WebCfg - Diagnostics: ARP Table

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Assigned Privileges

Name	Description	Action
WebCfg - All pages	Allow access to all pages (admin privilege)	
Security notice: Users in this group effectively have administrator-level access		

 Add

On change le temps de connexion pour les utilisateurs LDAP et on sauvegarde et teste, une fenêtre s'affiche indiquant que les connexions se sont faites

Settings

Session timeout

30

Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire sessions. NOTE: This is a security risk!

Authentication Server

authentification LDAP

Password Hash Algorithm

bcrypt -- Blowfish-based crypt

Selects which algorithm the firewall will use when creating hashes for local user passwords. The most secure option is currently bcrypt. Some users may prefer SHA-512-based crypt hashes for compatibility or compliance purposes.

Shell Authentication

☐ Use Authentication Server for Shell Authentication



If RADIUS or LDAP server is selected it is used for console and SSH authentication. Otherwise, the Local Database is used.

To allow logins with RADIUS credentials, equivalent local users with the expected privileges must be created first.

To allow logins with LDAP credentials, Shell Authentication Group DN must be specified on the LDAP server configuration page.

Auth Refresh Time

Time in seconds to cache authentication results. The default is 30 seconds, maximum 3600 (one hour). Shorter times result in more frequent queries to authentication servers.

 Save  Save & Test

LDAP settings

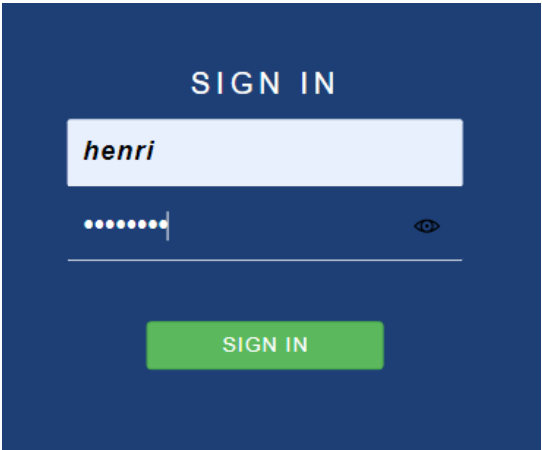
x

Test results

Attempting connection to	hermes.stadiumcompany.com	OK
Attempting bind to	hermes.stadiumcompany.com	OK
Attempting to fetch Organizational Units from	hermes.stadiumcompany.com	OK
Organization units found		
OU=Domain Controllers,DC=stadiumcompany,DC=com		
OU=glpi,DC=stadiumcompany,DC=com		
OU=pfSense,DC=stadiumcompany,DC=com		
CN=Users,DC=stadiumcompany,DC=com		

Test de connexion (authentification LDAP)

On tente de se connecter avec le compte **henri** et on a bien l'accès avec indication de provenance LDAP



Dashboard		+ ?
System Information		🔧 - ✕
Name	pfSense.stadiumcompany.com	
User	henri@172.20.0.10 (LDAP/authentification LDAP)	
System	VMware Virtual Machine Netgate Device ID: dc2b08fbbce6b09be40c	
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020	
Version	2.7.2-RELEASE (amd64) built on Mon Mar 4 20:53:00 CET 2024 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Sun May 5 18:59:35 CEST 2024 ↻	
CPU Type	12th Gen Intel(R) Core(TM) i7-12700H AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No	

Conclusion

Nous avons mis en place un service de pare-feu open source sur son propre système d'exploitation, ce service répond au cahier des charges grâce à sa facilité d'utilisation de gestion et de son interface intuitive. Il permet ainsi au service informatique de mieux gérer les problèmes d'interconnexion du réseau.