

STADIUMCOMPANY

Mission 5

Sécurisation de l'accès à Internet
et mise en place d'une DMZ

Projet	StadiumCompany - Infrastructure Réseau
Formation	BTS SIO option SISR - IRIS Paris
Année scolaire	2025 - 2026
Épreuve	E5 - Support et mise à disposition des services informatiques
Réalisation	Laurent HUSTIN, Ibrahim HAIDARA et Marcel OUTOU LASM

Sommaire

1. Introduction et contexte
2. Infrastructure du laboratoire
3. Installation de pfSense
 - 3.1 Téléchargement et vérification d'intégrité
 - 3.2 Déroulement de l'installation
 - 3.3 Configuration post-installation des interfaces
4. Configuration de base de pfSense
 - 4.1 Tests de connectivité initiale
 - 4.2 Assistant de configuration (Wizard)
 - 4.3 Configuration permanente du clavier
5. Sécurisation du pare-feu pfSense
 - 5.1 Protection de la console par mot de passe
 - 5.2 Sécurisation de l'accès SSH
 - 5.2.1 Configuration SSH et règles de pare-feu
 - 5.2.2 Test de connexion interne
 - 5.2.3 Test de connexion externe (WAN)
 - 5.2.4 Accès distant via adresse publique
 - 5.3 Sécurisation de l'interface Web par HTTPS
 - 5.3.1 Création d'une autorité de certification interne
 - 5.3.2 Génération du certificat Web
 - 5.3.3 Injection du certificat dans pfSense
6. Tableau des règles de filtrage
7. Compétences E5 validées
8. Conclusion

1. Introduction et contexte

Dans le cadre du projet StadiumCompany, après la mise en place du réseau interne (VLAN, Active Directory, services DNS/DHCP) et des mécanismes de redondance, l'entreprise souhaite désormais ouvrir son système d'information vers Internet. Cette ouverture est indispensable pour permettre aux collaborateurs d'accéder au Web, rendre le site vitrine accessible depuis l'extérieur, et offrir un accès Internet aux visiteurs du stade.

Cependant, cette exposition au réseau public entraîne des risques majeurs : tentatives d'intrusion, attaques par déni de service, fuites de données sensibles, accès non autorisés aux serveurs internes. Il est donc impératif de déployer une architecture sécurisée reposant sur un pare-feu professionnel, une zone démilitarisée (DMZ) pour isoler les services publics, et des politiques de filtrage strictes.

Objectif de la mission : Déployer et configurer pfSense comme pare-feu central de StadiumCompany, mettre en place une architecture sécurisée avec DMZ, configurer les règles de filtrage, sécuriser l'administration du pare-feu (console, SSH, HTTPS avec certificat), et garantir la séparation entre le réseau interne, la DMZ et Internet.

pfSense est une solution de pare-feu open source basée sur FreeBSD. Elle intègre un pare-feu à états (Packet Filter), des fonctions de routage, de NAT, de VPN, et un ensemble de services équivalents à ceux des solutions propriétaires. Sa fiabilité et sa richesse fonctionnelle en font un choix adapté à la sécurisation du réseau d'entreprise de StadiumCompany.

2. Infrastructure du laboratoire

L'environnement de test a été mis en place sous VMware avec trois machines virtuelles interconnectées via trois réseaux distincts, simulant l'architecture réelle de StadiumCompany.

Machine	Rôle	Réseau	Adresse IP
heimdall (pfSense)	Pare-feu / Routeur	WAN (bridge)	192.168.1.250/24
heimdall (pfSense)	Pare-feu / Routeur	LAN_Server	172.20.1.250/24
heimdall (pfSense)	Pare-feu / Routeur	OPT (lan_dmz)	172.20.4.250/24
hermes (Windows Server)	AD / DNS	LAN_Server	172.20.1.14/24
Machine Debian/Ubuntu	Poste client	OPT (lan_dmz)	DHCP

Le serveur pfSense (heimdall) dispose de trois interfaces réseau correspondant aux trois zones de sécurité : l'interface WAN connectée au réseau physique (accès Internet via la box), l'interface LAN reliée au réseau interne de l'entreprise (domaine stadiumcompany.local), et l'interface OPT destinée à la zone DMZ.

Plan d'adressage des réseaux internes

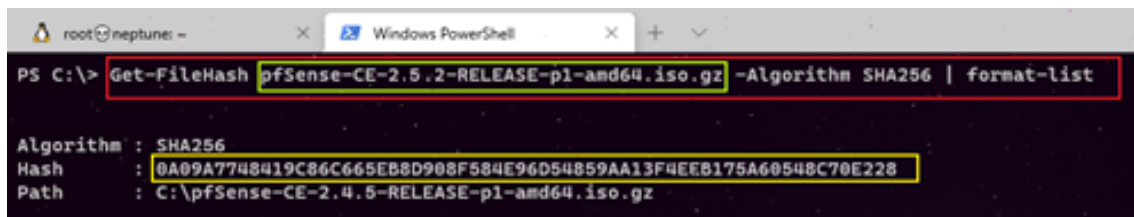
Réseau	Plage IP	Masque	Rôle
LAN_Server	172.20.1.0/24	255.255.255.0	Serveurs (AD, DNS, DHCP)
LAN_Equipe	172.20.2.0/24	255.255.255.0	Postes des équipes / employés
LAN_WiFi	172.20.3.0/24	255.255.255.0	Réseau Wi-Fi (employés et visiteurs)
LAN_DMZ	172.20.4.0/24	255.255.255.0	Zone démilitarisée (services publics)

Composant	Configuration minimale	Configuration recommandée
Processeur	600 MHz	1 GHz
Mémoire vive	512 Mo	1 Go
Stockage	> 6 Go	20 Go

3. Installation de pfSense

3.1 Téléchargement et vérification d'intégrité

L'image ISO de pfSense Community Edition a été téléchargée depuis le site officiel (pfsense.org). Avant toute installation, il est essentiel de vérifier l'intégrité du fichier téléchargé en comparant son empreinte SHA-256 avec celle publiée par l'éditeur. Cette étape garantit que le fichier n'a pas été altéré durant le téléchargement.

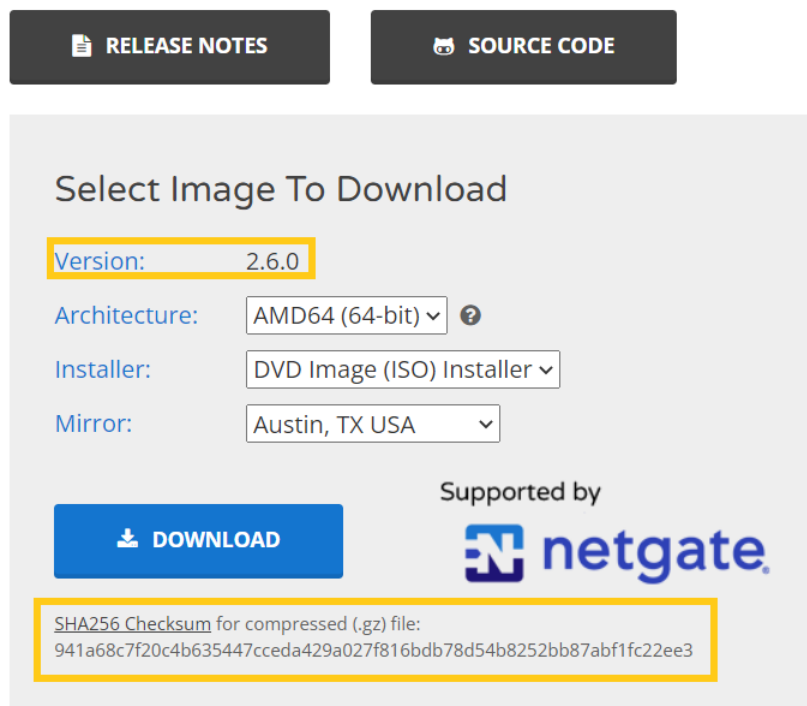


```
PS C:\> Get-FileHash pfSense-CE-2.5.2-RELEASE-p1-amd64.iso.gz -Algorithm SHA256 | format-list

Algorithm : SHA256
Hash       : 0A09A7748419C86C665EB8D908F584E96D54859AA13F4EEB175A60548C70E228
Path       : C:\pfSense-CE-2.4.5-RELEASE-p1-amd64.iso.gz
```

Figure 1 - Page de téléchargement officielle de pfSense CE

La vérification de l'empreinte s'effectue sous PowerShell avec la commande **Get-FileHash**. Si les deux empreintes (celle calculée localement et celle affichée sur le site officiel) sont identiques, le fichier est intègre et peut être utilisé en toute confiance.



RELEASE NOTES SOURCE CODE

Select Image To Download

Version: 2.6.0

Architecture: AMD64 (64-bit) ?

Installer: DVD Image (ISO) Installer

Mirror: Austin, TX USA

Supported by netgate

SHA256 Checksum for compressed (.gz) file:
941a68c7f20c4b635447cceda429a027f816bdb78d54b8252bb87abf1fc22ee3

Figure 2 - Vérification de l'intégrité SHA-256 du fichier ISO téléchargé

3.2 Déroulement de l'installation

Une fois l'image ISO vérifiée, la machine virtuelle est créée dans VMware avec les paramètres suivants : 1 Go de RAM, 20 Go de disque, et trois cartes réseau (bridge pour le WAN, deux réseaux personnalisés pour le LAN et l'OPT). L'installation suit un processus guidé.

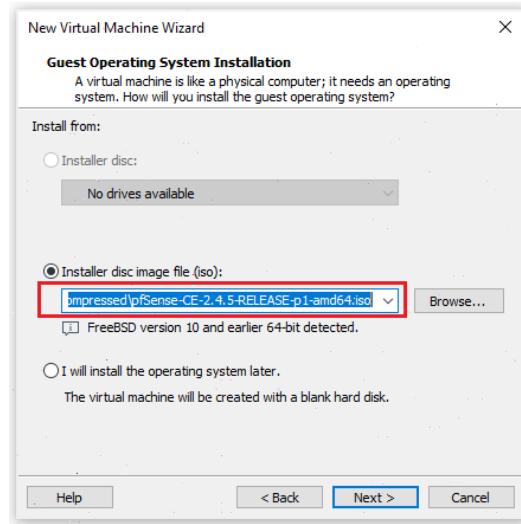


Figure 3 - Sélection de l'image ISO et nommage de la VM pfSense

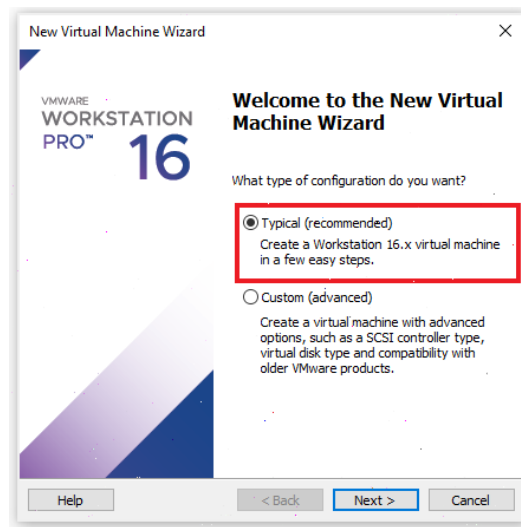


Figure 4 - Allocation de l'espace disque (20 Go)

New Virtual Machine Wizard

Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name:
Pfsense

Location:
C:\Users\bendi\Documents\Virtual Machines\Pfsense Browse...

The default location can be changed at Edit > Preferences.

< Back Next > Cancel

Figure 5 - Configuration matérielle : 3 cartes réseau, 1 Go RAM

New Virtual Machine Wizard

Specify Disk Capacity
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB) 20.0

Recommended size for FreeBSD version 10 and earlier 64-bit: 20 GB

☐ Store virtual disk as a single file
☒ Split virtual disk into multiple files
 Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Help < Back Next > Cancel

Figure 6 - Ajout des adaptateurs réseau supplémentaires

Au démarrage de l'installation, pfSense propose d'accepter la licence d'utilisation, puis de choisir le mode d'installation. Le système de fichiers UFS est sélectionné pour la création des partitions.

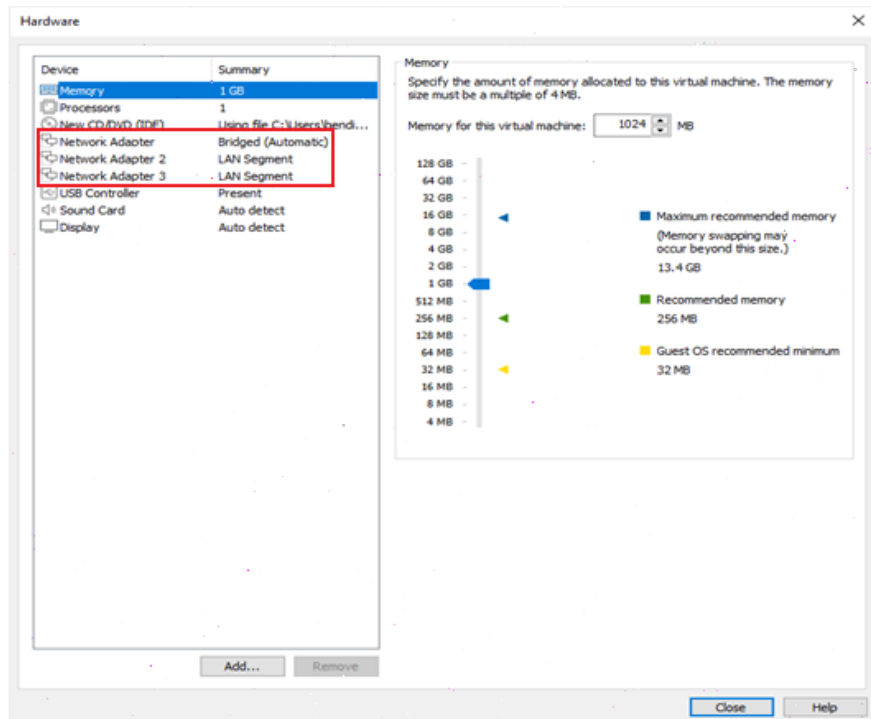


Figure 7 - Acceptation du contrat de licence pfSense

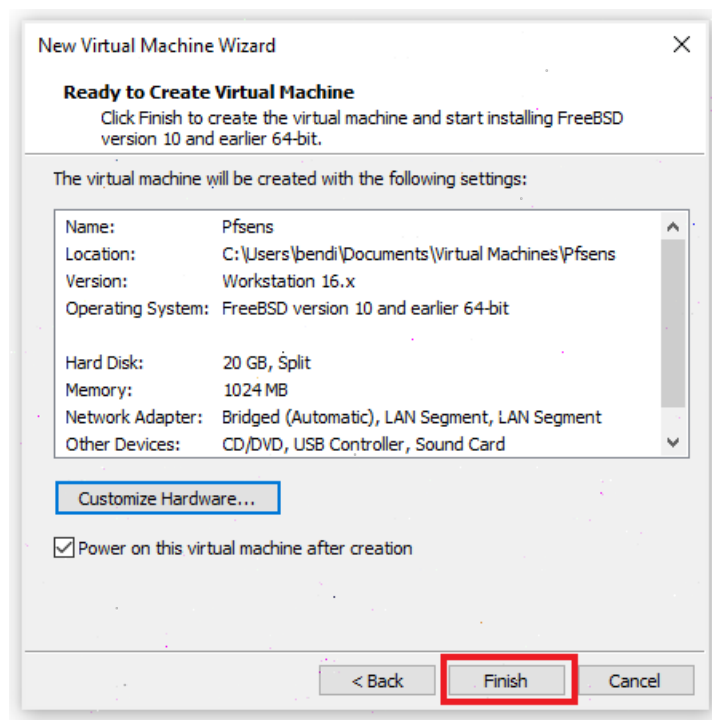


Figure 8 - Sélection du mode Install pour l'installation sur disque

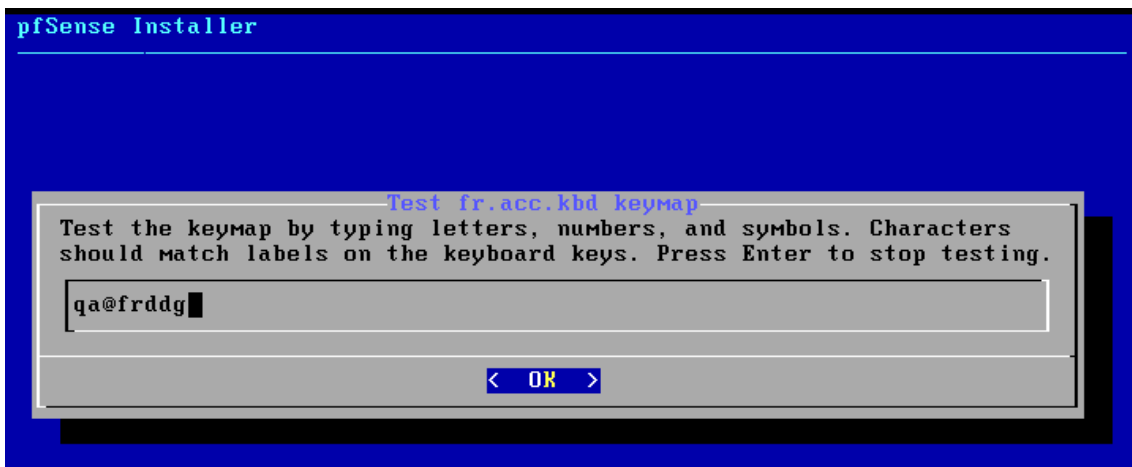


Figure 9 - Sélection du système de fichiers UFS pour le partitionnement

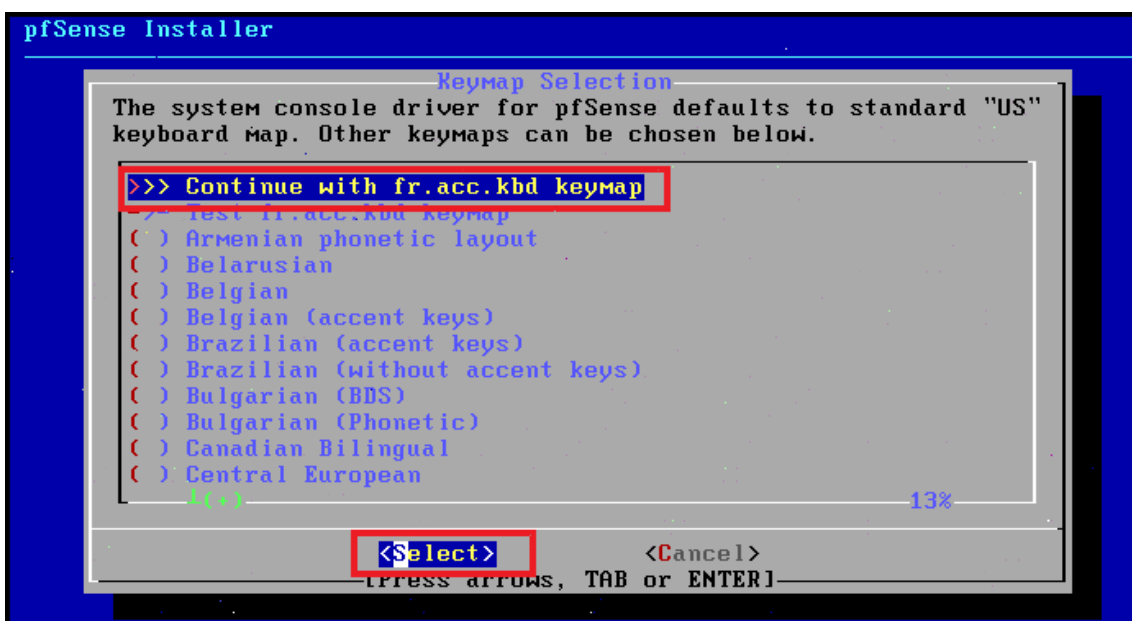


Figure 10 - Fin de l'installation - redémarrage du système

Après le redémarrage, pfSense démarre sur son interface console. A ce stade, seules deux interfaces réseau sont détectées automatiquement (em0 et em1). L'interface em2 sera déclarée manuellement lors de la configuration post-installation.

```
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y!n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

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

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

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

The interfaces will be assigned as follows:

WAN -> em0
LAN -> em1
OPT1 -> em2

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

Figure 11 - Interface console pfSense après le premier démarrage

3.3 Configuration post-installation des interfaces

La configuration post-installation consiste à déclarer les trois interfaces réseau (WAN, LAN, OPT1) et à leur attribuer les adresses IP correspondantes. L'option 1 du menu console permet de déclarer et associer les interfaces physiques aux interfaces logiques de pfSense.

```
Carte Ethernet Ethernet :
  Suffixe DNS propre à la connexion. . . . :
  Description. . . . . : Killer E2200 Gigabit Ethernet Controller
  Adresse physique . . . . . : FC-AA-14-24-82-7B
  DHCP activé. . . . . : Oui
  Configuration automatique activée. . . . : Oui
  Adresse IPv6 de liaison locale. . . . . : fe80::b523:e2a4:2139:24c5%16(préfééré)
  Adresse IPv4. . . . . : 192.168.1.142(préfééré)
  Masque de sous-réseau. . . . . : 255.255.255.0
  Passerelle par défaut. . . . . : 192.168.1.1
  Serveur DHCP . . . . . : 192.168.1.1
  IAID DHCPv6 . . . . . : 268216852
  DUID de client DHCPv6. . . . . : 00-01-00-01-27-51-18-51-FC-AA-14-24-82-7B
  Serveurs DNS. . . . . : 192.168.1.1
  NetBIOS sur Tcpip. . . . . : Activé
```

Figure 12 - Déclaration des interfaces réseau (WAN, LAN, OPT1)

Attribution des adresses IP

Interface WAN : L'adresse IP 192.168.1.250/24 est attribuée manuellement, avec 192.168.1.1 comme passerelle (box Internet). Le serveur DHCP n'est pas activé sur cette interface et le configurateur Web n'est pas exposé sur le WAN pour des raisons de sécurité.

```
Configure IPv6 address WAN interface via DHCP6? (y/n) N
Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) N
Please wait while the changes are saved to WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 WAN address has been set to 192.168.1.250/24
Press <ENTER> to continue.
```

Figure 13 - Configuration de l'interface WAN (192.168.1.250/24)

Interface LAN : L'adresse IP 172.20.1.250/24 est attribuée. Un serveur DHCP est activé avec la plage 172.20.1.20 à 172.20.1.30. Le configurateur Web est accessible depuis cette interface.

```
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)

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

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

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.1.250

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

Enter the new WAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.1
```

Figure 14 - Configuration de l'interface LAN (172.20.1.250/24) avec DHCP

Interface OPT : L'adresse IP 172.20.4.250/24 est attribuée. Cette interface sera utilisée pour la zone DMZ ou le réseau visiteurs. Aucun DHCP n'est configuré sur cette interface à ce stade.

```
Enter an option: 2

Available interfaces:
1 - WAN (em0 - static)
2 - LAN (em1 - static)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 3

Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 192.168.2.250

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

Enter the new OPT1 IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

Figure 15 - Configuration de l'interface OPT (172.20.4.250/24)

A l'issue de cette configuration, le menu console de pfSense affiche les trois interfaces avec leurs adresses respectives. Le pare-feu est désormais opérationnel et prêt pour la configuration avancée via l'interface Web.

```
Enter an option: 2
Available interfaces:
1 - WAN (em0 - static)
2 - LAN (em1 - static)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.20.0.250

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

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

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

Figure 16 - Menu console avec les trois interfaces configurées

4. Configuration de base de pfSense

4.1 Tests de connectivité initiale

Avant de procéder à la configuration avancée, il est indispensable de valider la connectivité réseau depuis une machine du LAN. Les tests suivants sont réalisés depuis le serveur Active Directory (hermes, 172.20.1.14) :

Commande	Cible	Objectif
ping 172.20.1.250	pfSense LAN	Connectivité avec le pare-feu
ping 192.168.1.250	pfSense WAN	Accès à l'interface WAN
ping 172.20.4.250	pfSense OPT	Accès à l'interface DMZ
ping 192.168.1.1	Box Internet	Routage vers la passerelle FAI
ping 8.8.4.4	Google DNS	Accès Internet
ping www.google.fr	Google	Résolution DNS

L'accès à l'interface d'administration Web s'effectue depuis un navigateur en saisissant l'adresse `http://172.20.1.250` avec les identifiants par défaut (admin / pfsense).

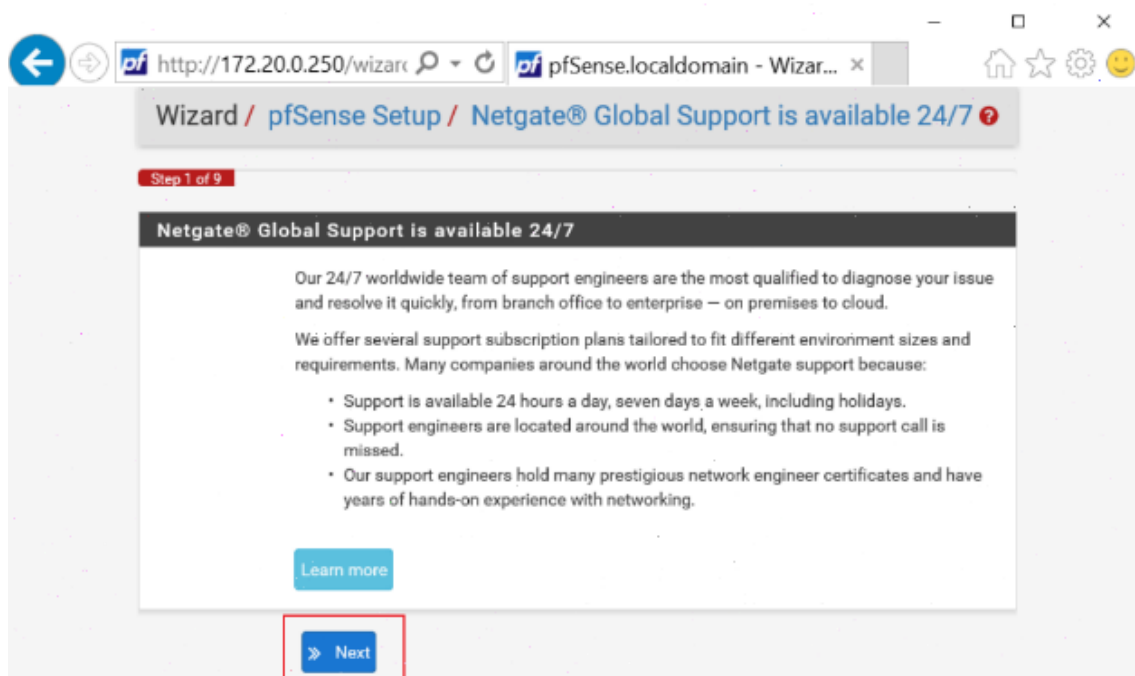


Figure 17 - Interface de connexion Web de pfSense

4.2 Assistant de configuration (Wizard)

Au premier accès à l'interface Web, pfSense lance un assistant de configuration en 9 étapes permettant de paramétrer les informations générales du système : nom d'hôte (heimdall), nom de domaine (stadiumcompany.local), serveur NTP (fr.pool.org), fuseau horaire (Europe/Paris), et modification du mot de passe administrateur.

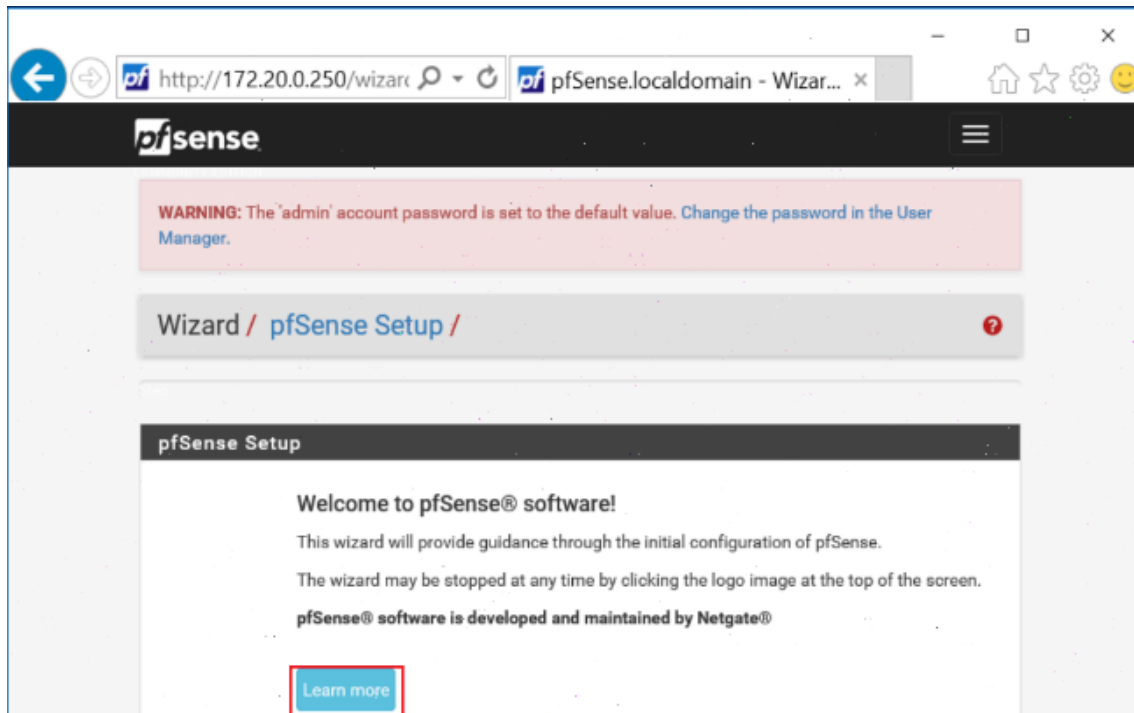


Figure 18 - Wizard étape 1 - Informations générales Netgate

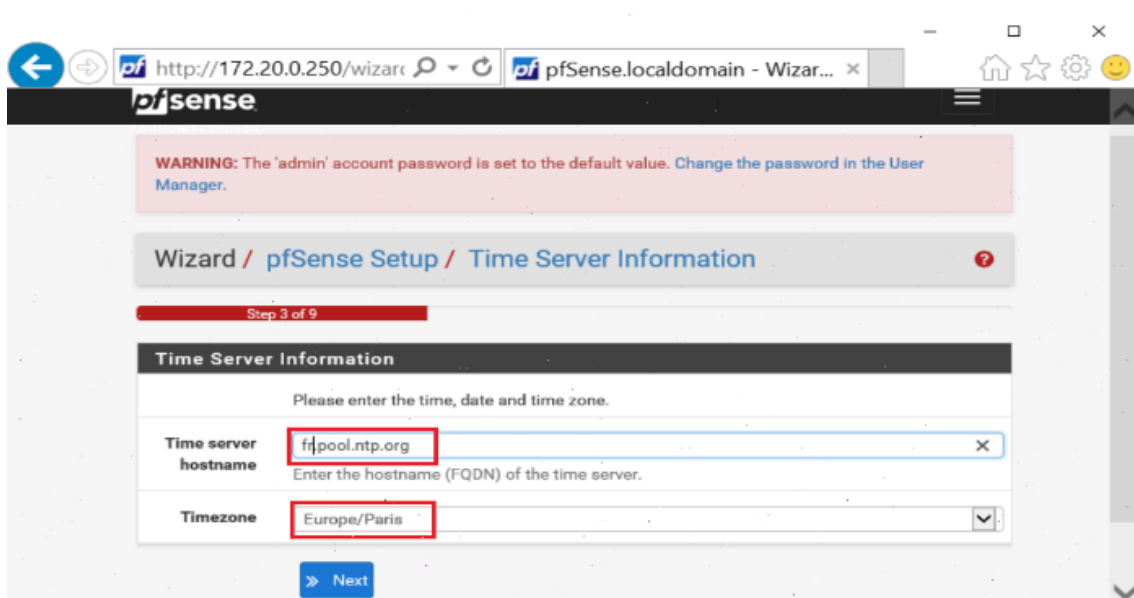


Figure 19 - Wizard étape 2 - Configuration du nom d'hôte et domaine

pfSense System Interfaces Firewall Services VPN Status Diagnostics Help

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname: ×
EXAMPLE: myserver

Domain:
EXAMPLE: mydomain.com

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

[Next](#)

Figure 20 - Configuration du serveur NTP et du fuseau horaire

← → pf http://172.20.0.250/wizard pf pfSense.localdomain - Wizar... x

pfSense

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

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](#)

Figure 21 - Vérification de la configuration de l'interface WAN

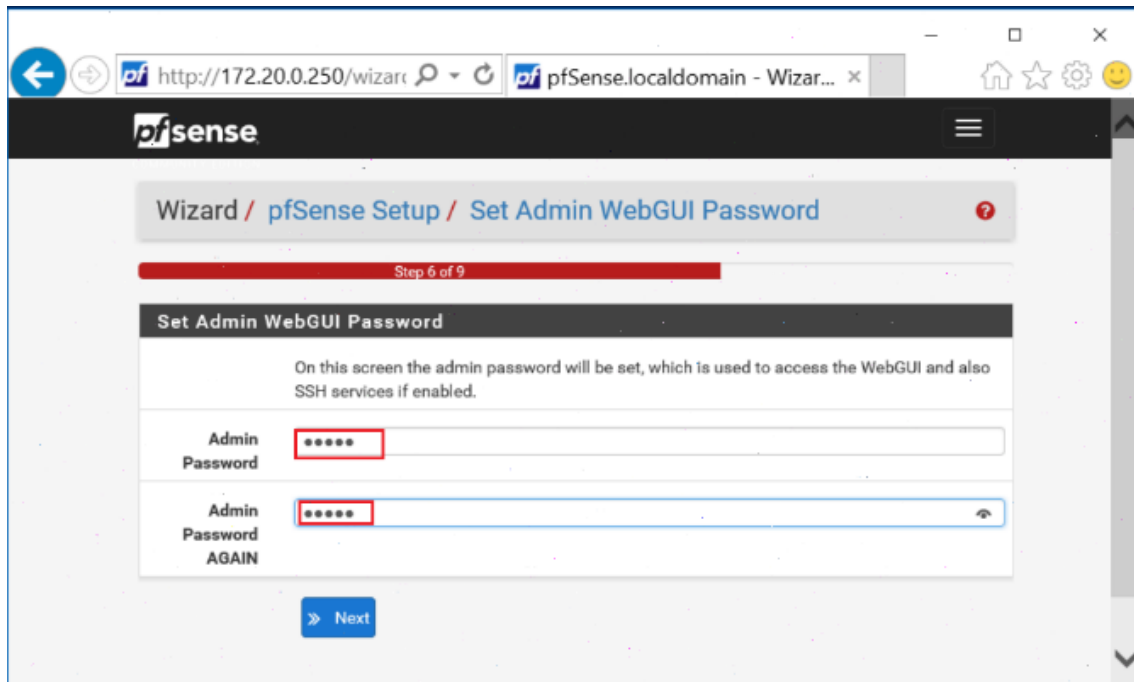


Figure 22 - Modification du mot de passe administrateur

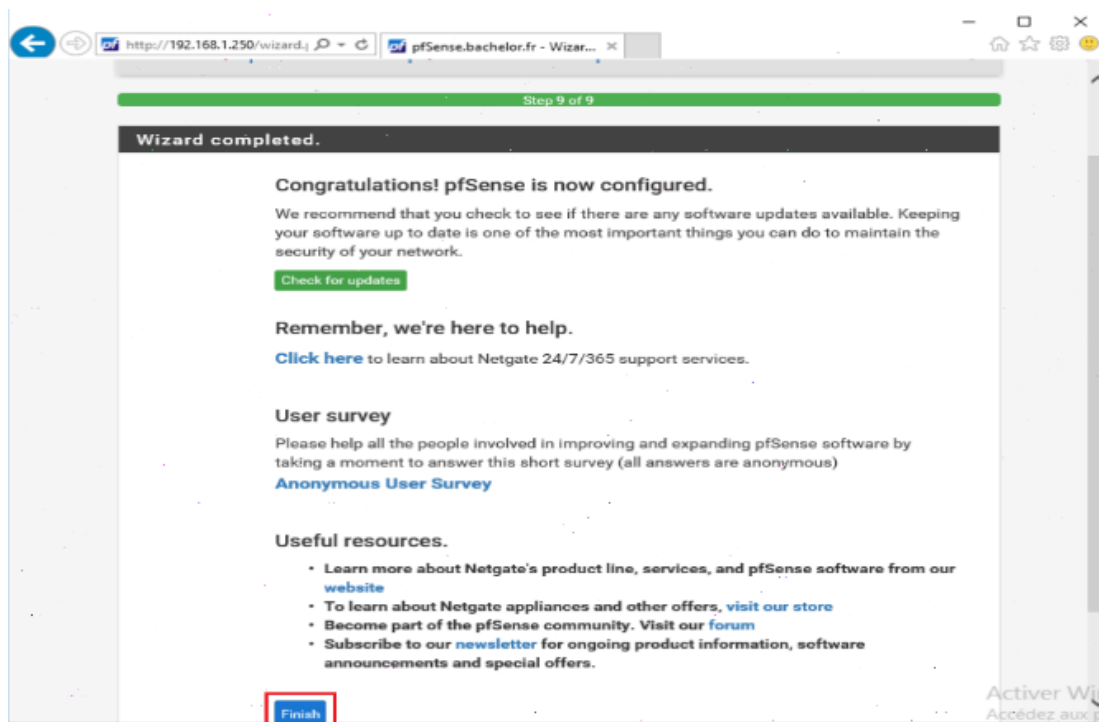


Figure 23 - Application de la configuration (Reload)

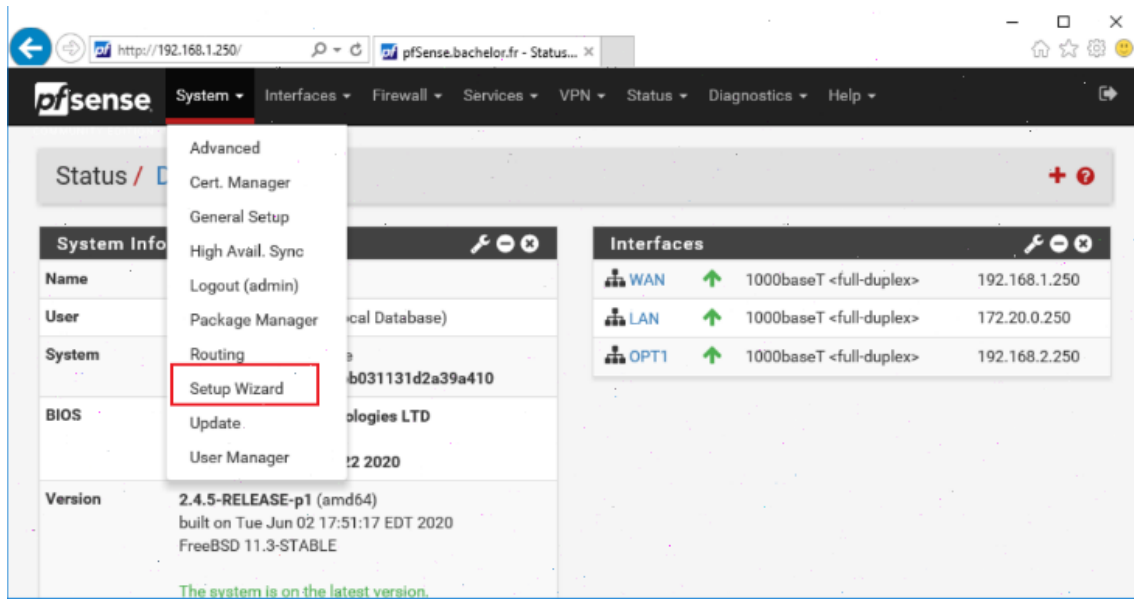


Figure 24 - Finalisation du Wizard - écran de confirmation

En cas d'erreur lors de la configuration initiale, l'assistant peut être relancé à tout moment depuis le menu Système > Setup Wizard.

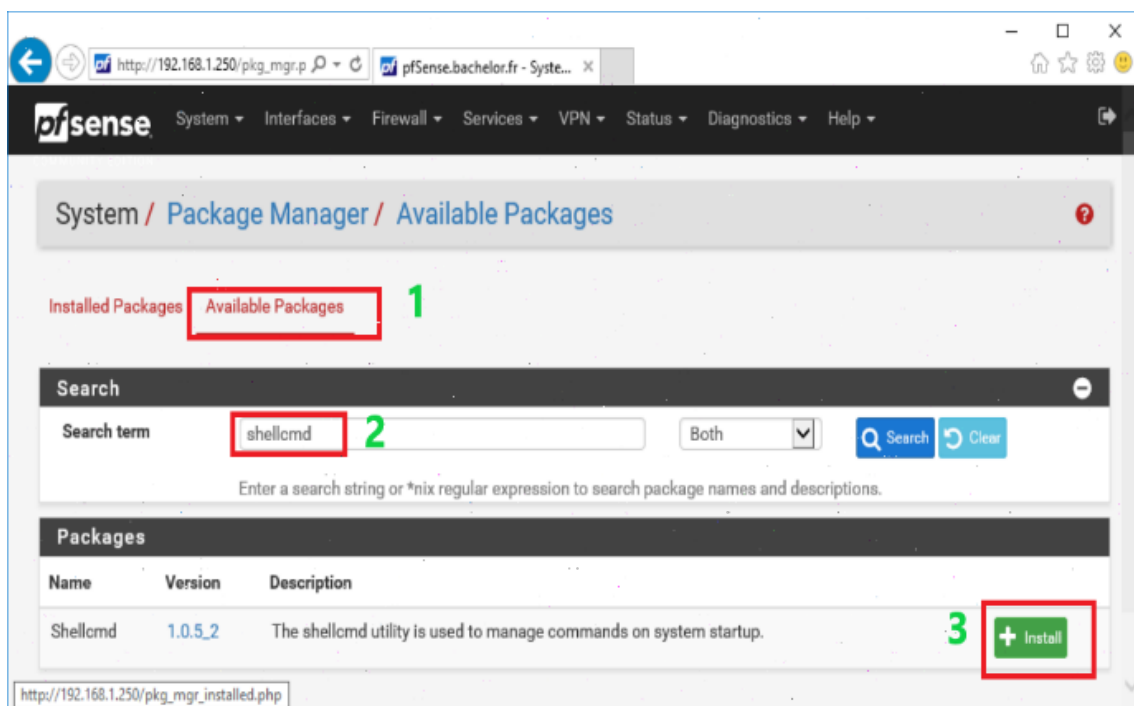


Figure 25 - Tableau de bord pfSense après la configuration initiale

4.3 Configuration permanente du clavier en français

Par défaut, le clavier de la console pfSense est en QWERTY. La commande **kbdcontrol -l /usr/share/syscons/keymaps/fr.iso.kbd** permet de le passer en AZERTY, mais cette modification est temporaire. Pour rendre le changement permanent, il est nécessaire d'installer le paquet **shellcmd** qui permet d'exécuter des commandes au démarrage du système. Le paquet **VMware Tools** est également installé pour améliorer l'intégration avec l'hyperviseur.

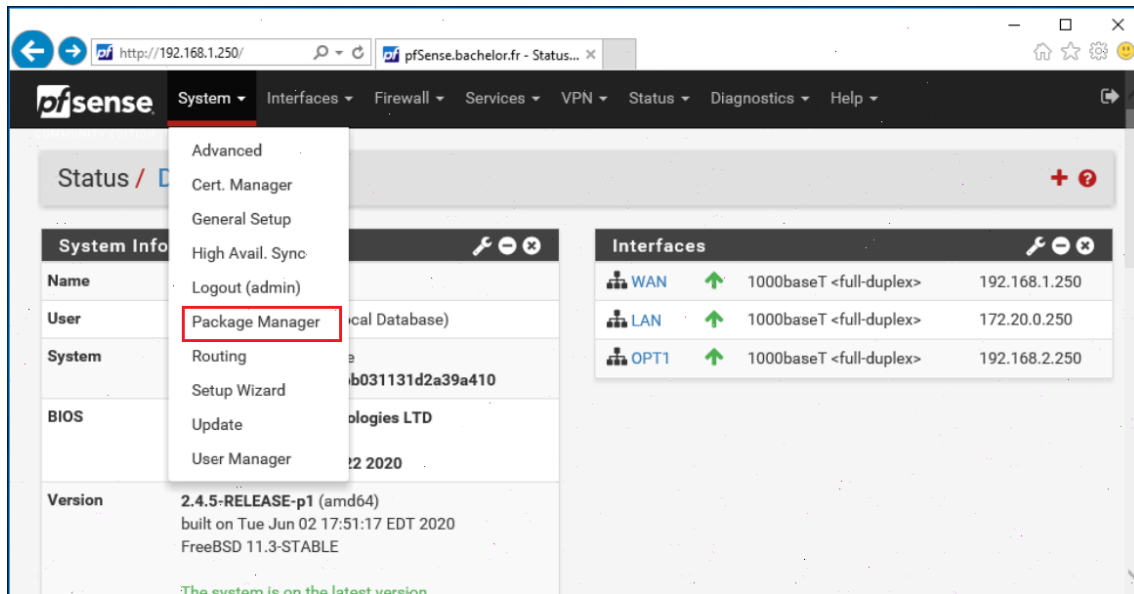


Figure 26 - Installation du paquet Shellcmd via le gestionnaire de paquets

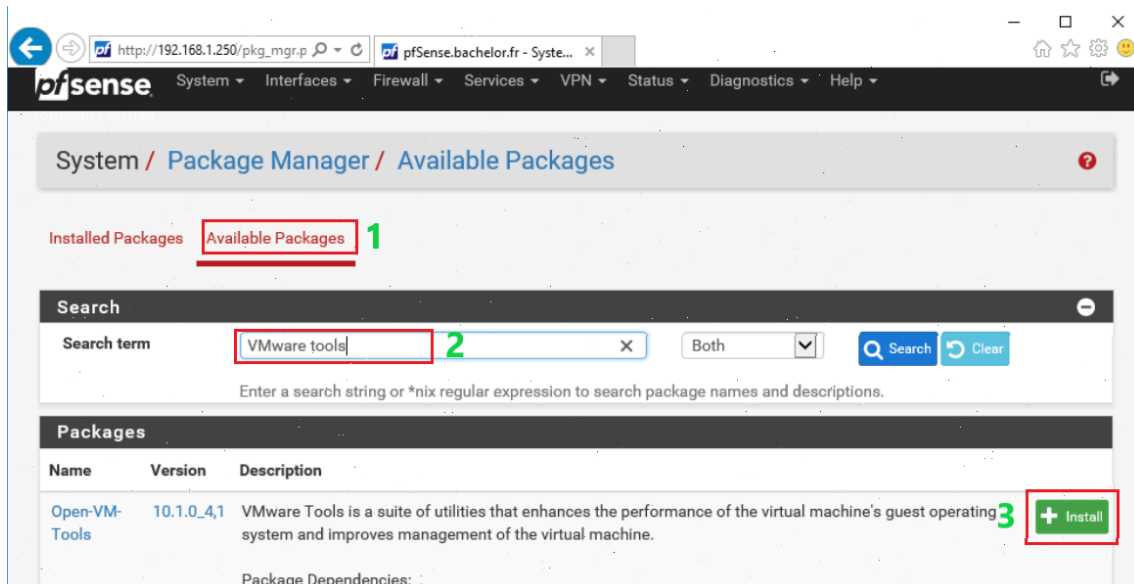


Figure 27 - Installation de VMware Tools (Open VM Tools)

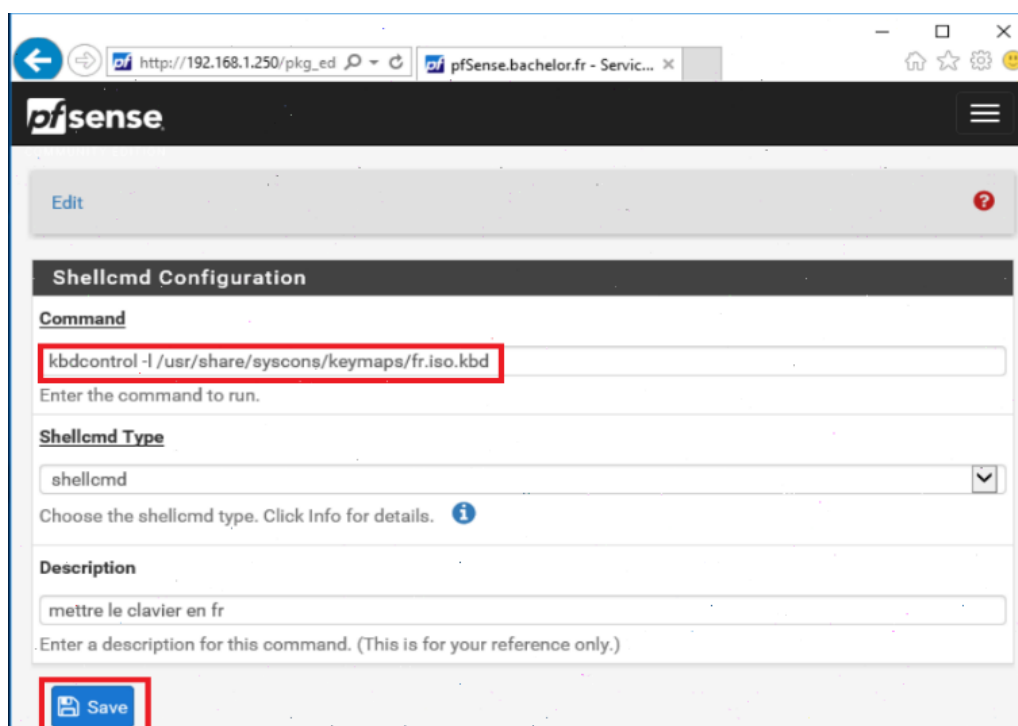


Figure 28 - Configuration de la commande shellcmd pour le clavier AZERTY

5. Sécurisation du pare-feu pfSense

La sécurisation de pfSense est une étape cruciale. Un pare-feu mal protégé peut devenir lui-même un vecteur d'attaque. Cette section couvre la protection de la console physique, la mise en place d'un accès SSH sécurisé, et le passage de l'interface Web en HTTPS avec un certificat émis par une autorité de certification interne.

5.1 Protection de la console par mot de passe

Par défaut, toute personne ayant un accès physique au serveur pfSense peut accéder au menu console sans authentification. Pour remédier à cette vulnérabilité, la protection par mot de passe de la console est activée dans les paramètres avancés du système. Cette option force une authentification avant l'accès au menu de gestion.

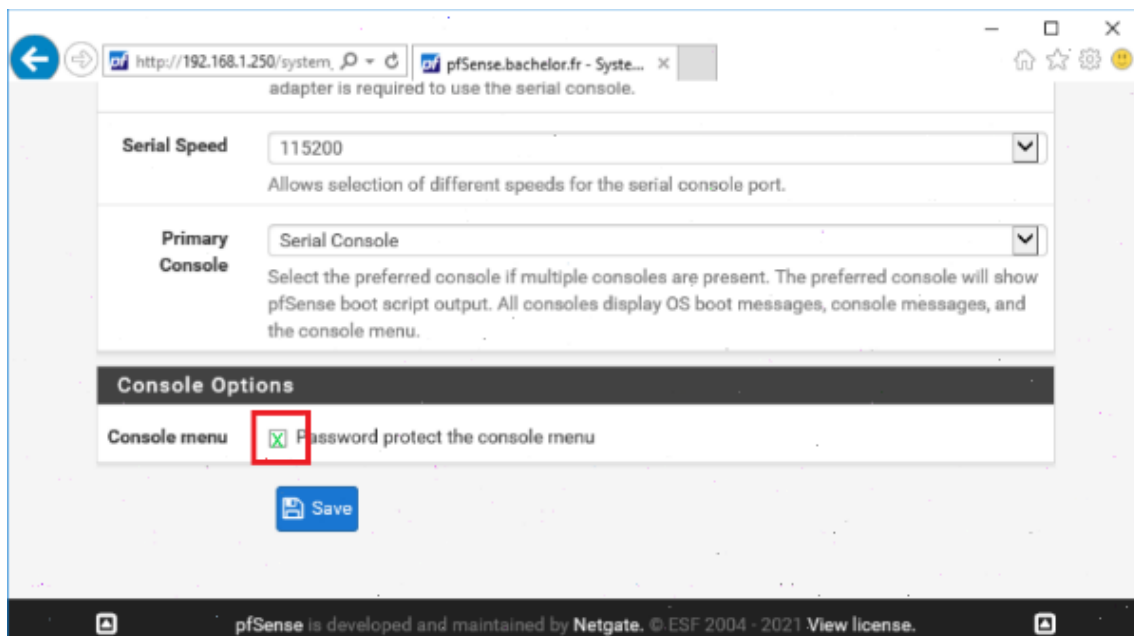


Figure 29 - Activation de la protection par mot de passe de la console

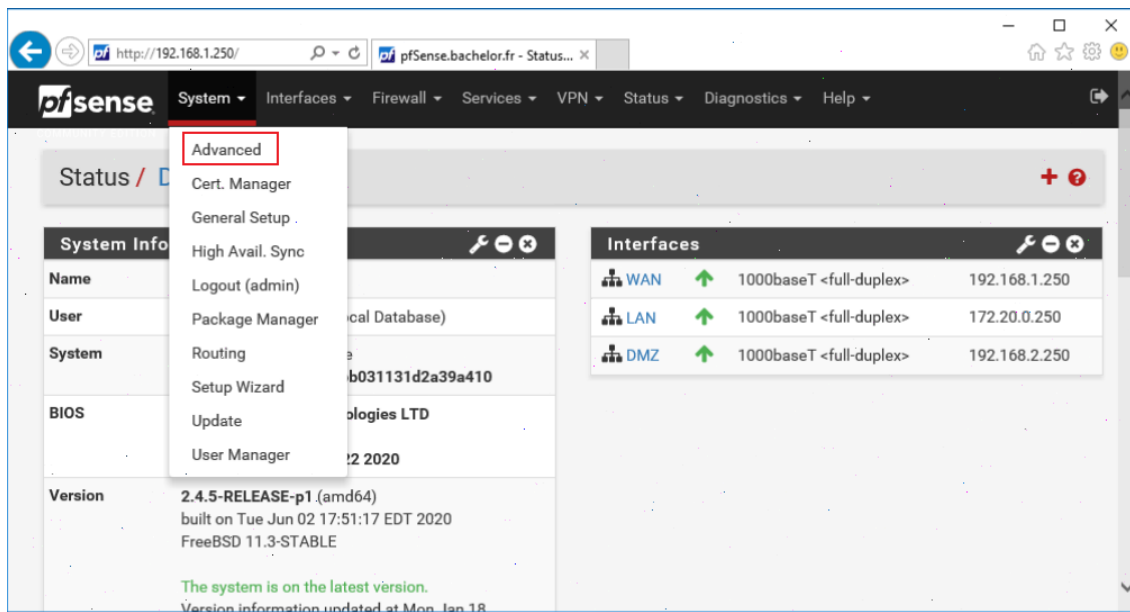


Figure 30 - Console pfSense avec invite de connexion (login requis)

5.2 Sécurisation de l'accès SSH

5.2.1 Configuration SSH et règles de pare-feu

Le protocole SSH est activé sur pfSense pour permettre l'administration à distance sécurisée. En matière de bonnes pratiques de sécurité, le port par défaut (22) est modifié en **port 2121** afin de réduire la surface d'attaque face aux scans automatisés. L'authentification par clé publique/privée peut également être mise en place en complément du mot de passe.

```
WAN (wan)      -> em0      -> v4: 192.168.1.250/24
LAN (lan)      -> em1      -> v4: 172.20.0.250/24
OPT1 (opt1)    -> em2      -> v4: 192.168.2.250/24

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:

FreeBSD/amd64 (Heimdall.sitka.local) (ttyv0)
login: █
```

Figure 31 - Activation SSH avec port personnalisé 2121

Une règle de pare-feu doit être créée sur l'interface WAN pour autoriser les connexions SSH entrantes sur le port 2121. Sans cette règle, pfSense bloquera toute tentative de connexion SSH depuis l'extérieur du réseau LAN.

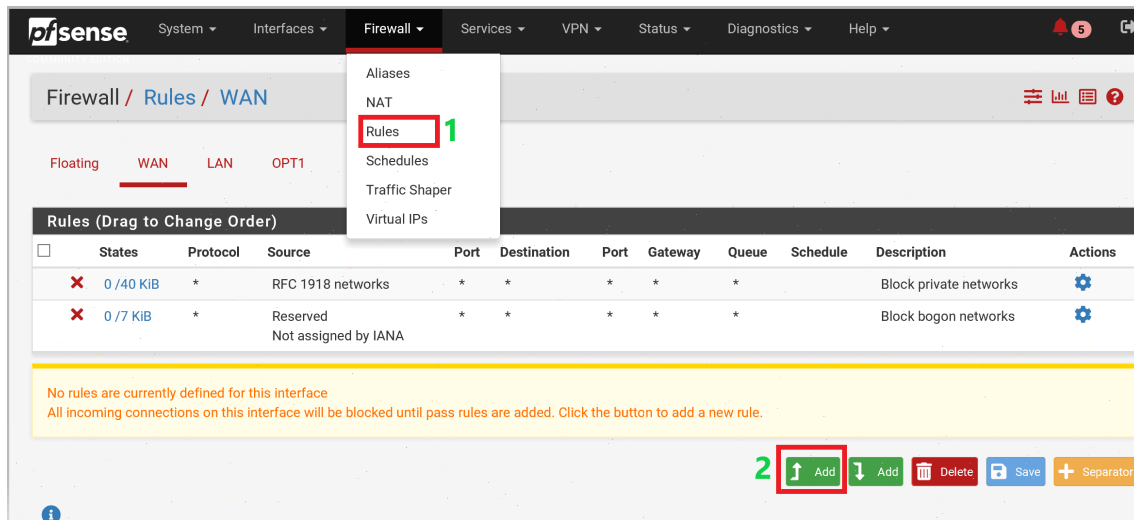


Figure 32 - Création de la règle de pare-feu autorisant SSH sur le WAN

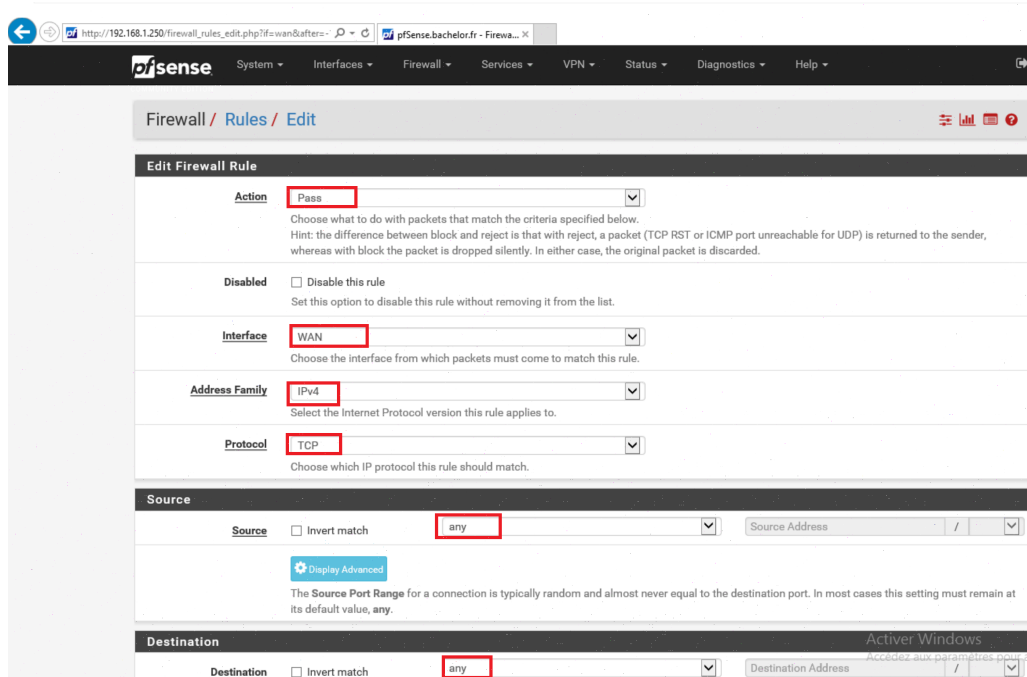


Figure 33 - Détail de la règle SSH : protocole TCP, port 2121, source any

Destination

Destination ☐ Invert match Destination Address

Destination Port Range (other) (other)

From Custom To Custom

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

Extra Options

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

Description
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

Rule Information

Tracking ID	1640165746
Created	12/22/21 10:35:46 by admin@172.20.0.14 (Local Database)
Updated	12/22/21 10:39:53 by admin@172.20.0.14 (Local Database)

Figure 34 - Enregistrement de la règle de pare-feu

Après l'enregistrement de la règle, il est impératif d'appliquer les changements en cliquant sur le bouton **Apply Changes** pour que la modification soit prise en compte par le moteur de filtrage de pfSense.

5.2.2 Test de connexion SSH interne

Le premier test consiste à vérifier la connexion SSH depuis une machine du réseau LAN. Depuis le serveur Active Directory (hermes), la connexion est établie via PowerShell. Le serveur pfSense envoie l'empreinte numérique de sa clé publique que l'administrateur doit valider avant de poursuivre.

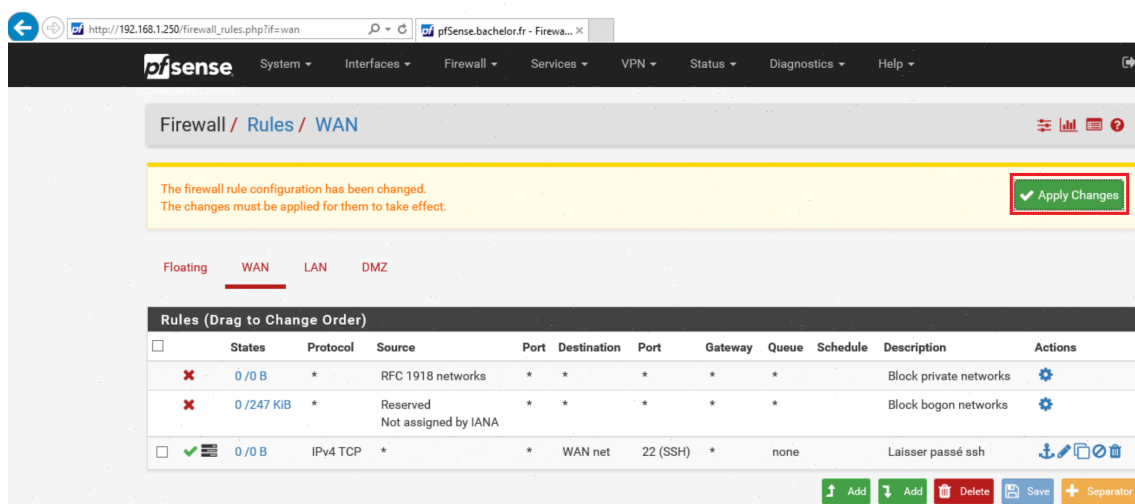


Figure 35 - Connexion SSH réussie depuis le réseau LAN vers pfSense

Pour vérifier l'authenticité du serveur, l'empreinte reçue est comparée avec celle calculée directement sur le serveur. La correspondance des deux empreintes confirme qu'il n'y a pas d'attaque de type man-in-the-middle.

```

PS C:\Users\Administrateur> ssh admin@172.20.0.250 -p 2121
The authenticity of host '[172.20.0.250]:2121 ([172.20.0.250]:2121)' can't be established.
ED25519 key fingerprint is SHA256:riqHfD03Z9fhNsyAM1TC2shBu9F6+qSnpokCTL/0dTo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.20.0.250]:2121' (ED25519) to the list of known hosts.
Password for admin@heimdall.sitka.local:
VMware Virtual Machine - Netgate Device ID: 7c7777e1ee8ed9111e66

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on heimdall ***

WAN (wan)      -> em0      -> v4: 192.168.1.250/24
LAN (lan)      -> em1      -> v4: 172.20.0.250/24
OPT1 (opt1)    -> em2      -> v4: 192.168.2.250/24

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:

```

Figure 36 - Vérification de l'empreinte de la clé publique SSH sur le serveur

5.2.3 Test de connexion SSH externe (WAN)

Le test suivant vérifie le comportement de pfSense face à une connexion SSH provenant de l'extérieur de son périmètre. Depuis la machine physique (hôte VMware), la tentative de connexion SSH échoue, de même que le ping.

Figure 37 - Tentative de connexion SSH depuis l'extérieur - échec

Explication du blocage : pfSense bloque par défaut toutes les requêtes provenant d'adresses IP privées sur l'interface WAN. Ce comportement de sécurité est contrôlé par deux options dans la configuration de l'interface WAN : le blocage des réseaux privés (RFC 1918) et le blocage des réseaux bogons.

Figure 38 - Options de blocage des réseaux privés et bogons sur l'interface WAN

5.2.4 Accès distant via adresse publique

Pour accéder à pfSense depuis Internet (en dehors du réseau local), il est nécessaire de configurer une redirection de port sur la box Internet (port forwarding du port SSH vers l'adresse WAN de pfSense) et d'utiliser l'adresse IP publique pour la connexion.

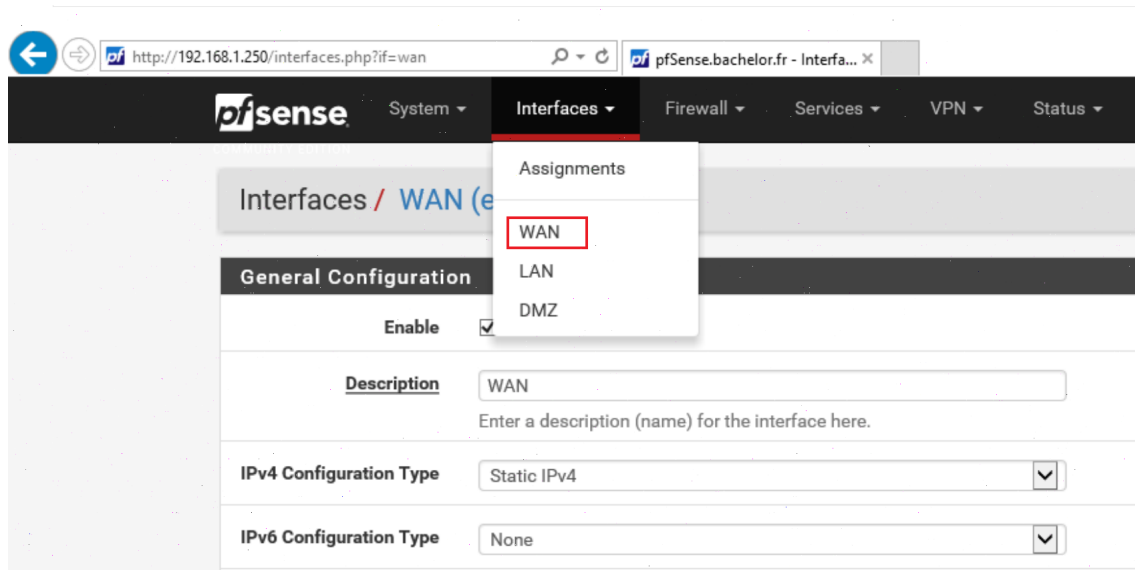


Figure 39 - Configuration de la redirection de port sur la box Internet

Le test a été réalisé depuis un smartphone en connexion 4G (hors réseau Wi-Fi local) à l'aide de l'application JuiceSSH. La connexion est établie avec succès vers l'adresse publique, et l'empreinte de la clé correspond bien à celle vérifiée précédemment.

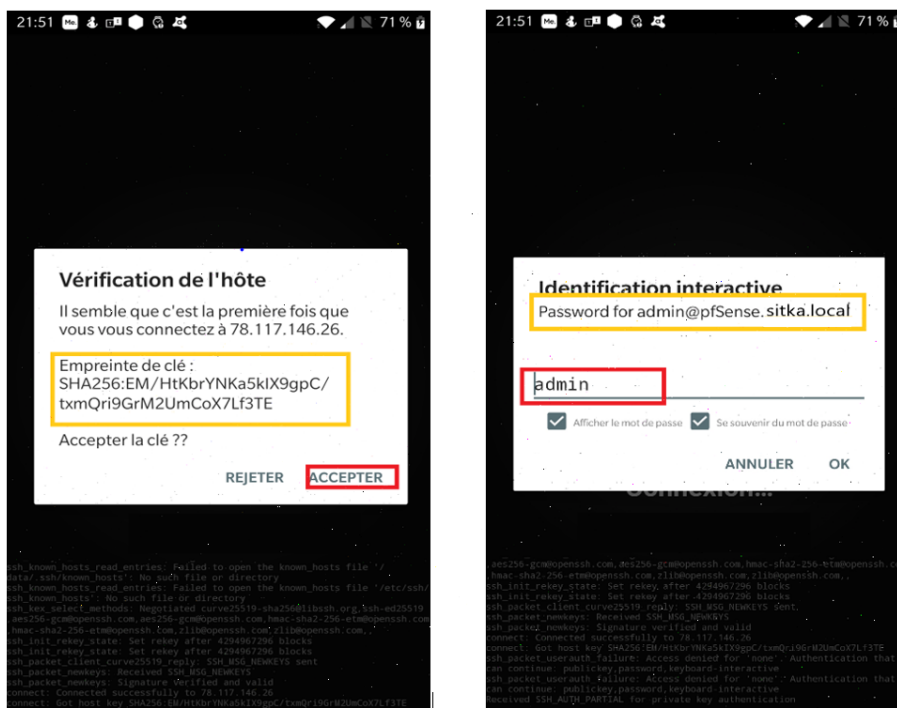


Figure 40 - Connexion SSH distante réussie via smartphone en 4G (JuiceSSH)

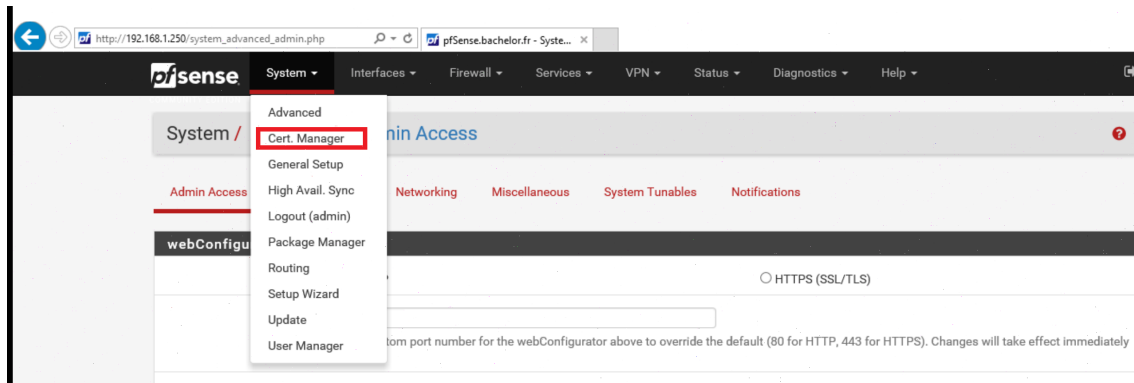


Figure 41 - Vérification de l'empreinte et saisie du mot de passe

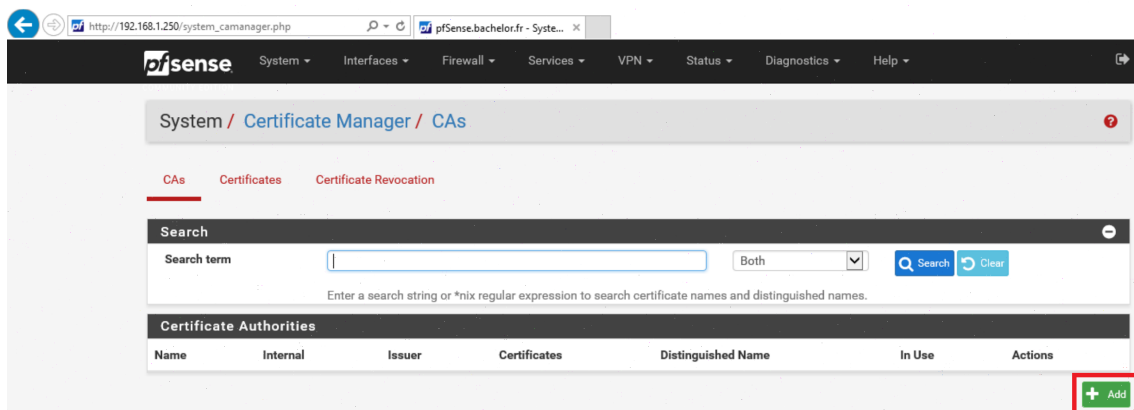


Figure 42 - Accès à la console pfSense depuis le smartphone en 4G

5.3 Sécurisation de l'interface Web par HTTPS

Par défaut, l'interface d'administration de pfSense est accessible en HTTP (non chiffré). Les identifiants transitent en clair sur le réseau, ce qui représente un risque de sécurité. La mise en place d'HTTPS nécessite la création d'une autorité de certification interne, la génération d'un certificat Web signé, puis son intégration dans le serveur Web de pfSense.

5.3.1 Création d'une autorité de certification interne

La première étape consiste à créer une autorité de certification (CA) interne depuis le menu Système > Cert Manager. Cette CA sera utilisée pour émettre le certificat Web du serveur pfSense. Les champs suivants sont renseignés : nom descriptif, longueur de clé, algorithme de hachage, durée de validité, et informations d'identification (organisation, pays, etc.).

The screenshot shows the pfSense web interface for creating an internal Certificate Authority (CA). The breadcrumb trail is 'System / Certificate Manager / CAs / Edit'. The 'Create / Edit CA' section contains the following fields and options:

- Descriptive name:** Autorité de certification Sitka
- 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.

The 'Internal Certificate Authority' section contains the following fields:

- Key type:** RSA
- Key length:** 2048 (Note: 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 (Note: The digest method used when the CA is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.)
- Lifetime (days):** 3650
- Common Name:** internal-ca-sitka (Note: The following certificate authority subject components are optional and may be left blank.)
- Country Code:** FR
- State or Province:** IDF
- City:** Paris
- Organization:** sitka
- Organizational Unit:** SK

A 'Save' button is located at the bottom of the form.

Figure 43 - Création de l'autorité de certification interne (CA)

System / Certificate Manager / CAs / Edit

CA's Certificates Certificate Revocation

Create / Edit CA

Descriptive name: Autorité de certification Sitka

Method: Import an existing 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.

Existing Certificate Authority

Certificate data: -----BEGIN CERTIFICATE-----
MIIEIDCCAwIlgAwIBAgIIPmg7c9/Sa8swDQYJKoZIhvcNAQELBQAwZD
EaBggGA1UE
AxkRah50ZXJ1Y2Vtc210a2ExCzA3BgglVBAQYAKZSNQumCgYDVQ
QIEwNjREYx
Paste a certificate in X.509 PEM format here.

Certificate Private Key (optional): -----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQFAASCBKcwgg5jAgEAAoIBAQC70e
KVlxgQcd/7
FjH4jAa0qA1145sW5P9Ts6INa772Qd88szCh2CUBvgg9V9VX2T8r
h1ebXA+BmH
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).

Next Certificate Serial: 0
Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA.

Save

Figure 44 - Autorité de certification créée - affichage du certificat

System / Certificate Manager / Certificates

CA's Certificates Certificate Revocation

Search

Search term: Both

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

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (6001f6f281597) Server Certificate CA: No Server: Yes	self- signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-6001f6f281597 Valid From: Fri, 15 Jan 2021 21:11:30 +0100 Valid Until: Thu, 17 Feb 2022 21:11:30 +0100		

+ Add/Sign

Figure 45 - Détail du certificat CA et de sa clé publique associée

5.3.2 Génération du certificat Web

Un certificat de type serveur Web est ensuite créé et signé par l'autorité de certification interne. Ce certificat sera associé au serveur Web intégré de pfSense pour chiffrer les communications HTTPS avec les navigateurs des administrateurs.

The screenshot shows the pfSense web interface for the 'Certificate Manager' section. The breadcrumb trail is 'System / Certificate Manager / Certificates / Edit'. The 'Certificates' tab is active. The form is titled 'Add/Sign a New Certificate'. It has two main sections: 'Internal Certificate' and 'Certificate Attributes'. In the 'Internal Certificate' section, the 'Method' is 'Create an internal Certificate', the 'Descriptive name' is 'Certificat SSL pour le serveur web Heimdal', the 'Certificate authority' is 'Autorité de certification Sitka', the 'Key type' is 'RSA' with a length of '2048', the 'Digest Algorithm' is 'sha256', and the 'Lifetime (days)' is '3650'. The 'Common Name' is 'heimdall.sitka.local'. Below this, there are optional fields for 'Country Code' (FR), 'State or Province' (IDF), 'City' (Paris), 'Organization' (sitka), and 'Organizational Unit' (SK). The 'Certificate Attributes' section is shown in a separate figure.

Figure 46 - Création du certificat Web signé par la CA interne

The screenshot shows the 'Certificate Attributes' form. It has a title bar 'Certificate Attributes'. The 'Attribute Notes' section explains that attributes are added to certificates and requests. The 'Certificate Type' is 'Server Certificate'. The 'Alternative Names' section lists several attributes: 'FQDN or Hostname' (heimdall.sitka.local), 'FQDN or Hostname' (pfsense.sitka.local), 'IP address' (172.20.0.250), 'IP address' (192.168.1.250), 'IP address' (192.168.2.250), and 'URI' (www.heimdall.local). Each attribute has a 'Delete' button. At the bottom, there is an 'Add' button and a 'Save' button, which is highlighted with a red box.

Figure 47 - Paramètres du certificat Web (type serveur, CN, durée)

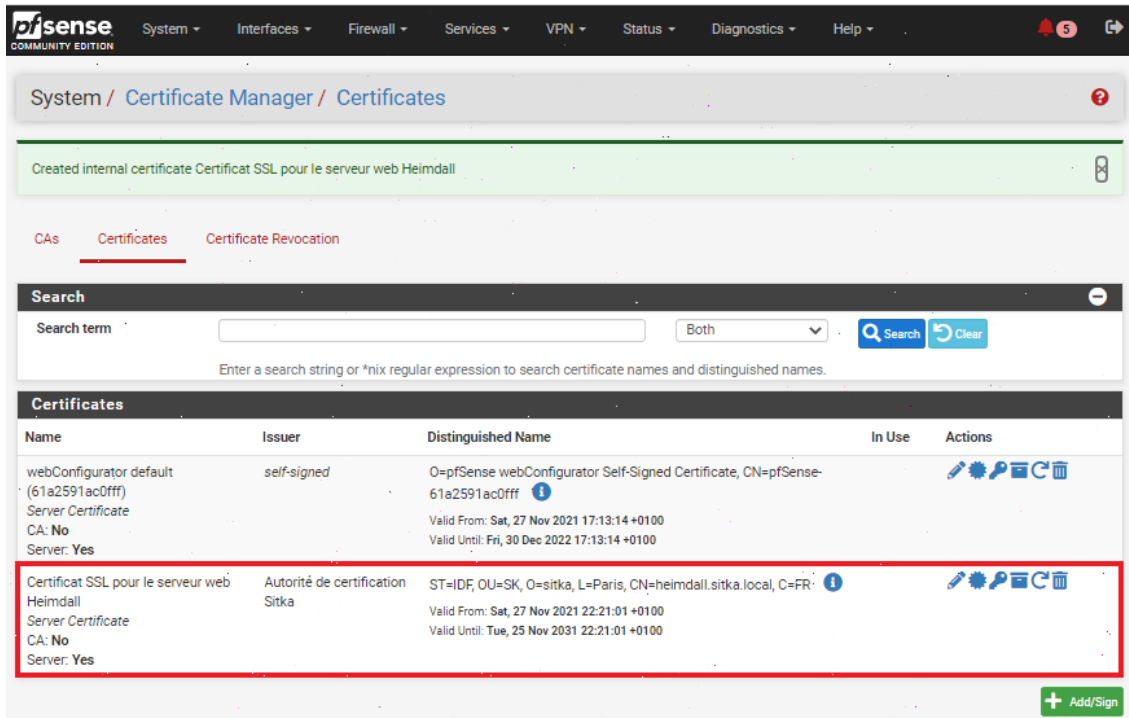


Figure 48 - Informations complémentaires du certificat Web

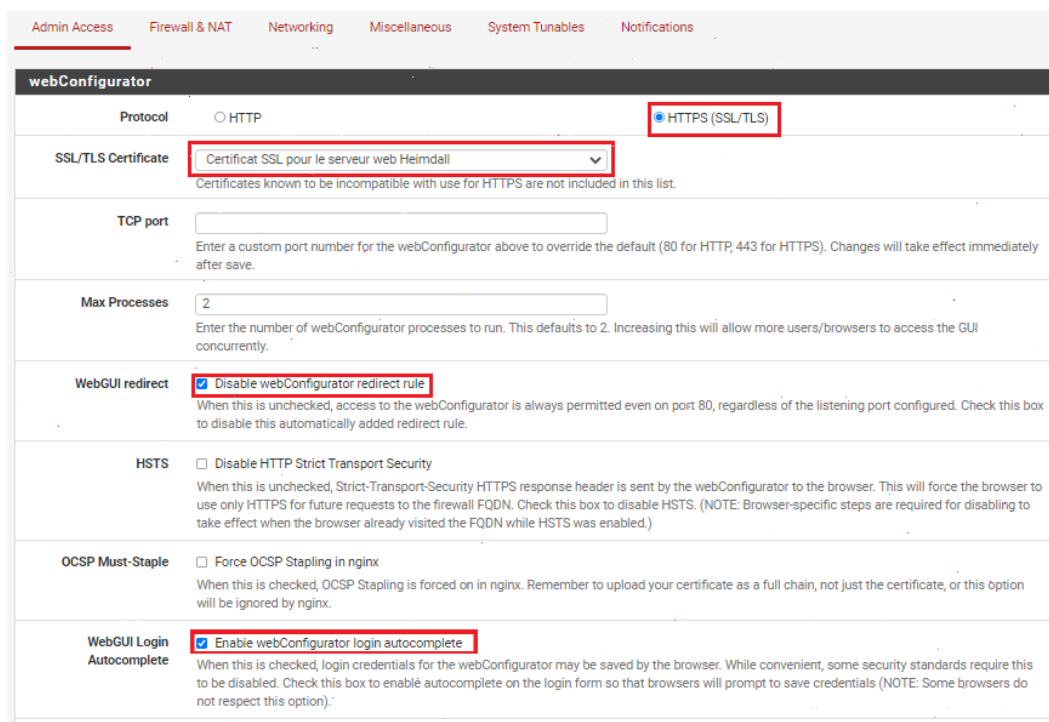


Figure 49 - Certificat Web généré et visible dans le gestionnaire

5.3.3 Injection du certificat dans pfSense

Le certificat est ensuite intégré dans la configuration du serveur Web de pfSense depuis le menu Système > Advanced. Les paramètres suivants sont appliqués : sélection du certificat créé, conservation du port HTTPS par défaut (443), limitation à 2 connexions simultanées sur l'interface Web, refus des connexions HTTP non chiffrées, et interdiction d'enregistrement des identifiants par le navigateur.

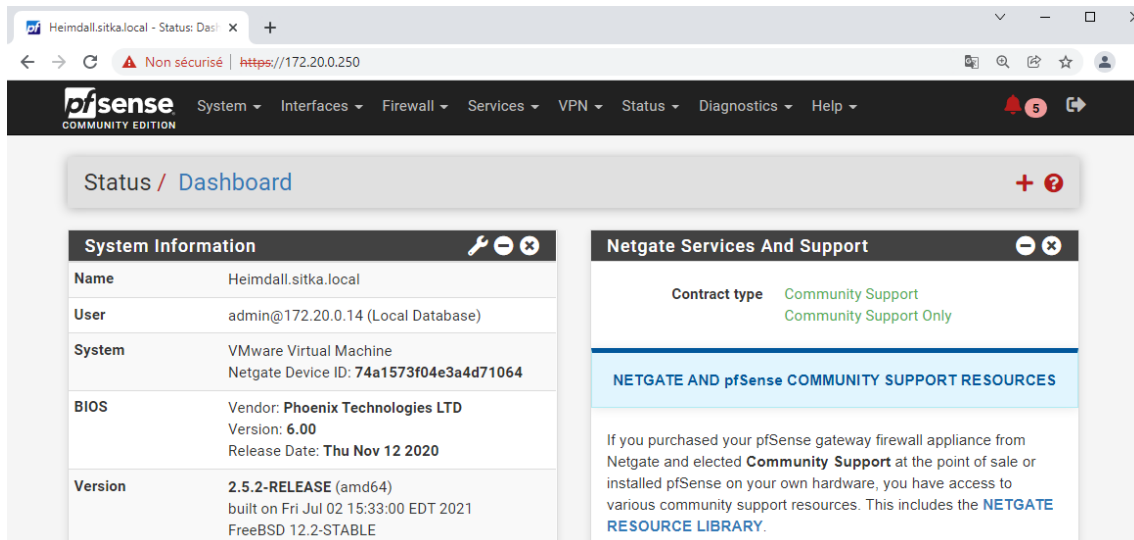


Figure 50 - Configuration HTTPS : sélection du certificat et paramètres de sécurité

Après sauvegarde, le navigateur est automatiquement redirigé vers l'adresse sécurisée <https://172.20.1.250/>. Le navigateur affiche un avertissement car l'autorité de certification interne n'est pas reconnue comme autorité de confiance. Pour supprimer cet avertissement, le certificat de la CA racine doit être installé dans le magasin des autorités de certification de confiance du navigateur ou du système d'exploitation.

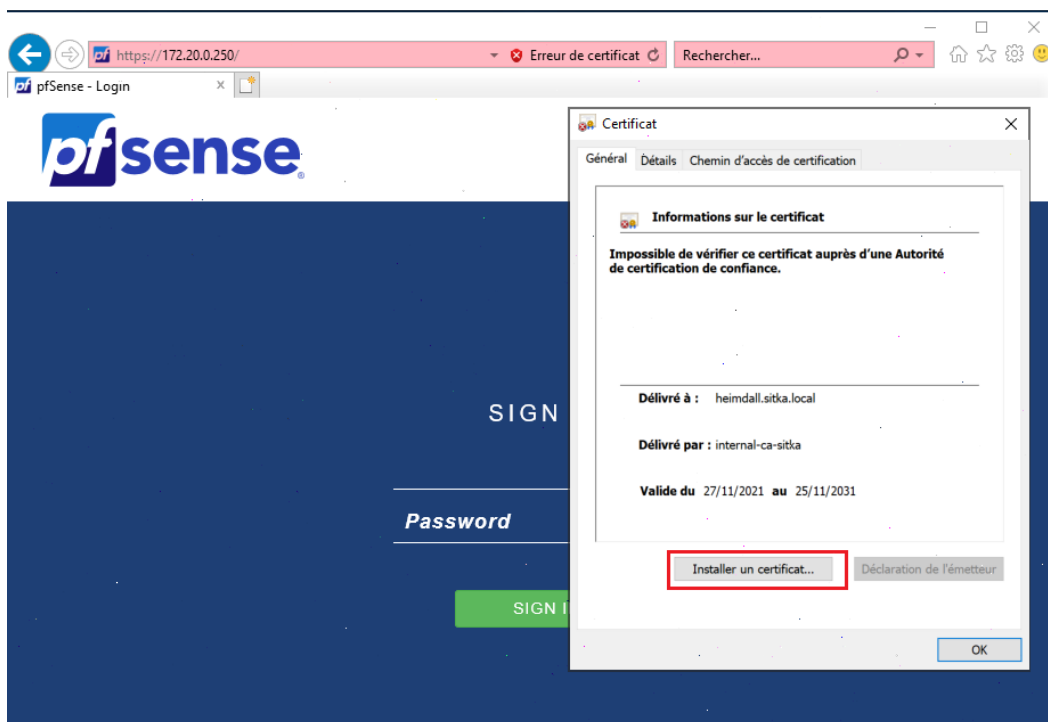


Figure 51 - Accès HTTPS à pfSense - avertissement de certificat

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.

Whitelist

Address / 128

Addresses added to the whitelist will bypass login protection.

Add address

+ Add address

Figure 52 - Connexion sécurisée HTTPS établie avec succès

6. Tableau des règles de filtrage

Le tableau ci-dessous synthétise les principales règles de filtrage mises en place sur le pare-feu pfSense pour les trois interfaces (WAN, LAN, OPT). Ces règles définissent la politique de sécurité de StadiumCompany en contrôlant les flux autorisés entre les différentes zones du réseau.

Interface	Action	Source	Destination	Port/Proto	Description
WAN	Bloquer	RFC 1918	Toute	*	Bloquer les IP privées
WAN	Bloquer	Bogons	Toute	*	Bloquer les IP bogons
WAN	Autoriser	Toute	WAN addr	TCP/2121	SSH administration
LAN	Autoriser	LAN net	Toute	*	Accès complet LAN
LAN	Autoriser	LAN net	LAN addr	TCP/443	Interface Web pfSense
OPT	Autoriser	OPT net	Toute	TCP/80,443	Accès Web Internet
OPT	Bloquer	OPT net	LAN net	*	Isoler DMZ du LAN

Principe de sécurité appliqué : Le pare-feu suit une politique de filtrage stricte. Sur l'interface WAN, tout est bloqué par défaut sauf les flux explicitement autorisés. Le réseau LAN dispose d'un accès complet (réseau de confiance), tandis que la zone OPT/DMZ est isolée du réseau interne et ne dispose que d'un accès HTTP/HTTPS vers Internet.

7. Compétences E5 validées

Compétence E5	Mise en oeuvre dans cette mission
Vérifier le respect des règles d'utilisation des ressources numériques	Mise en place de règles de filtrage, blocage des accès non autorisés, politique de sécurité WAN/LAN/DMZ.
Mettre à disposition un service informatique	Déploiement de pfSense, configuration des interfaces, mise en service du pare-feu et des accès sécurisés.
Traiter des demandes réseau et système	Configuration des interfaces réseau, règles de NAT, résolution des problèmes de connectivité.
Gérer le patrimoine informatique	Documentation de l'architecture sécurisée, inventaire des règles de filtrage, procédures d'administration.

8. Conclusion

La mission 5 a permis de déployer une solution de pare-feu complète pour sécuriser l'accès à Internet de StadiumCompany. Le choix de pfSense, solution open source éprouvée, répond aux exigences de l'entreprise en matière de sécurité, de flexibilité et de coût.

L'installation et la configuration de base ont été réalisées avec succès, incluant la mise en place de trois zones réseau distinctes (WAN, LAN, OPT/DMZ) avec des politiques de filtrage adaptées à chaque zone. La séparation entre le réseau interne et la zone exposée à Internet garantit la protection des données sensibles de l'entreprise.

La sécurisation du pare-feu lui-même constitue un point fort de cette mission : protection de la console physique par mot de passe, accès SSH sur un port non standard avec vérification des empreintes de clés, et passage de l'interface d'administration en HTTPS grâce à un certificat émis par une autorité de certification interne. Ces mesures garantissent que l'outil de sécurité ne devient pas lui-même une faille.

L'infrastructure est désormais prête pour accueillir les services publics de StadiumCompany (site Web, billetterie en ligne) dans la zone DMZ, tout en protégeant le réseau interne des menaces extérieures. Les employés disposent d'un accès Internet filtré et les visiteurs peuvent être orientés vers un réseau isolé, conformément aux exigences de la direction.

StadiumCompany - Mission 5 : Sécurisation de l'accès à Internet et mise en place d'une DMZ

BTS SIO SISR - IRIS Paris - Année scolaire 2025-2026