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

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.

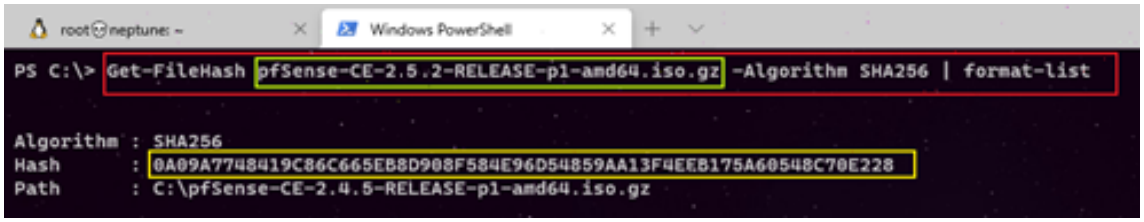

Figure 1 - Page de téléchargement officielle de pfSense CE

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.

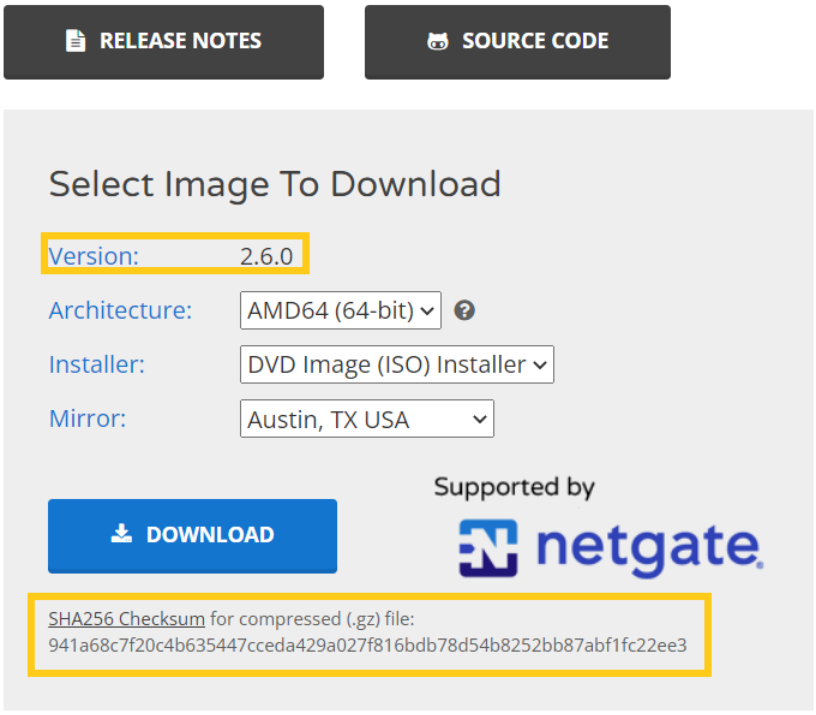

Figure 2 - Vérification de l'intégrité SHA-256 du fichier ISO téléchargé

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.

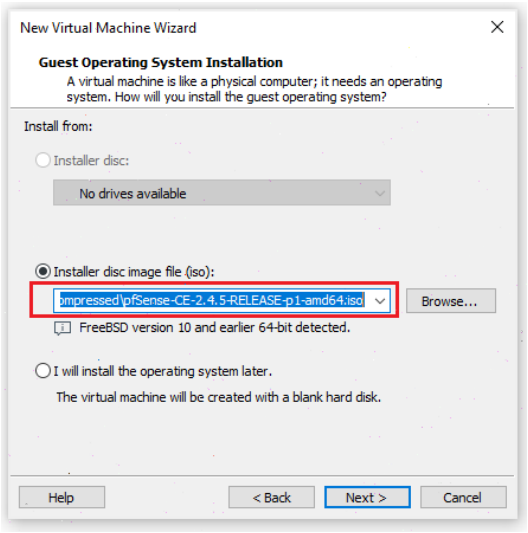

Figure 3 - Sélection de l'image ISO et nommage de la VM pfSense

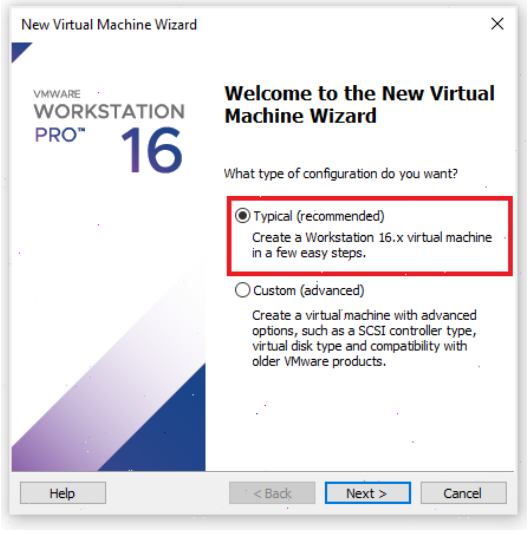

Figure 4 - Allocation de l'espace disque (20 Go)

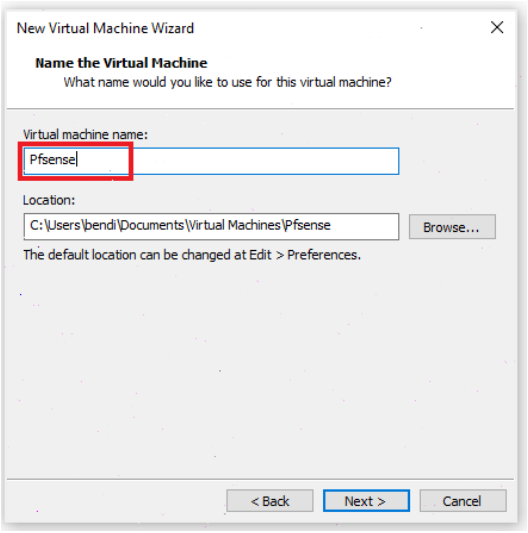

Figure 5 - Configuration matérielle : 3 cartes réseau, 1 Go RAM

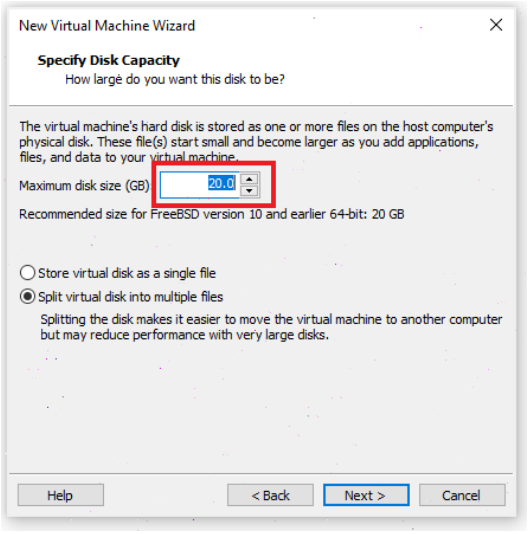

Figure 6 - Ajout des adaptateurs réseau supplémentaires

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.

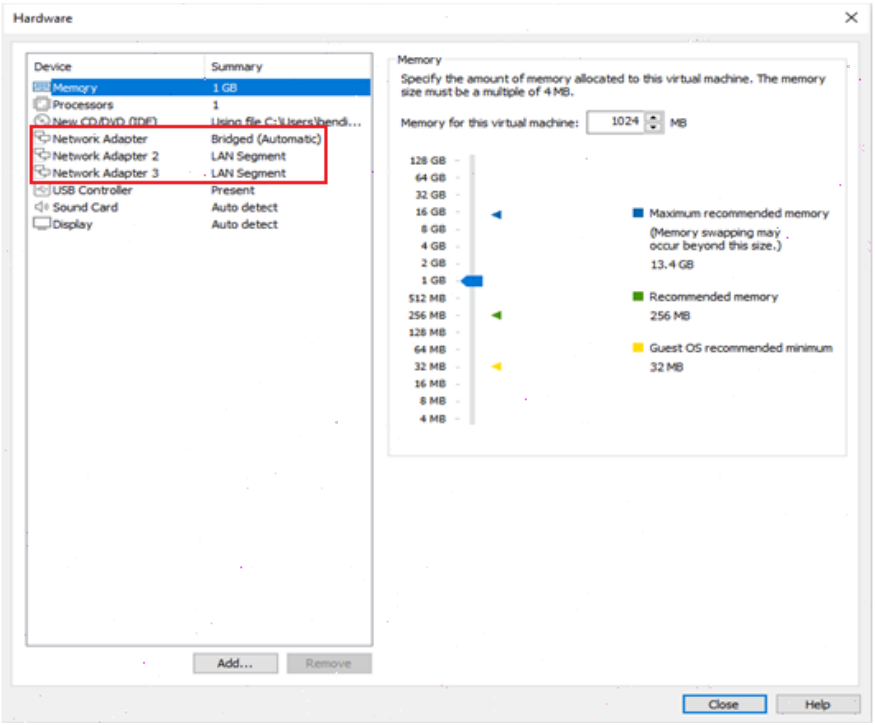

Figure 7 - Acceptation du contrat de licence pfSense

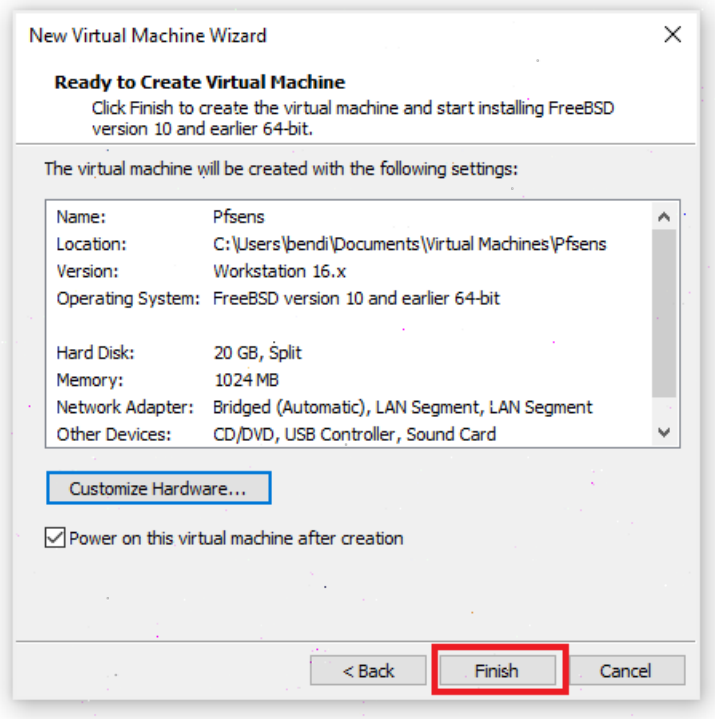

Figure 8 - Sélection du mode Install pour l'installation sur disque

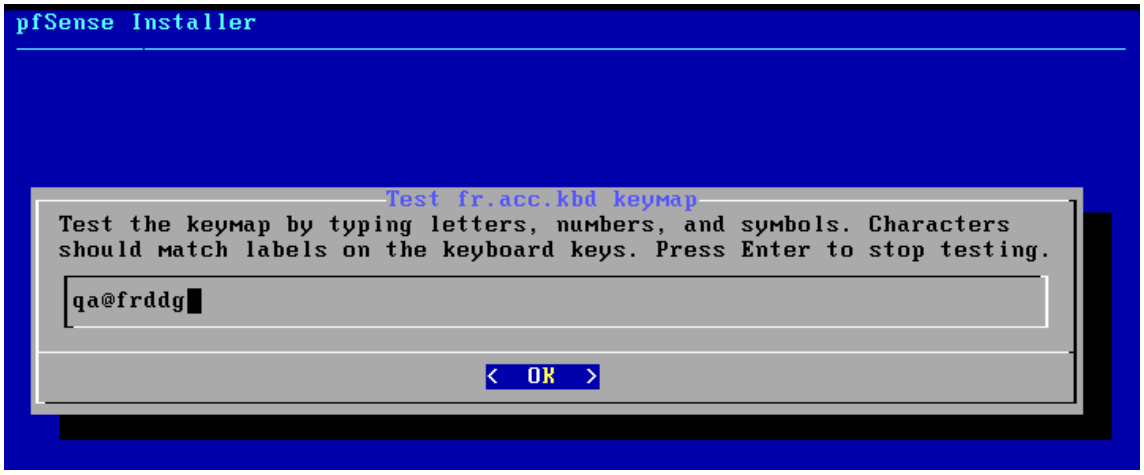

Figure 9 - Sélection du système de fichiers UFS pour le partitionnement

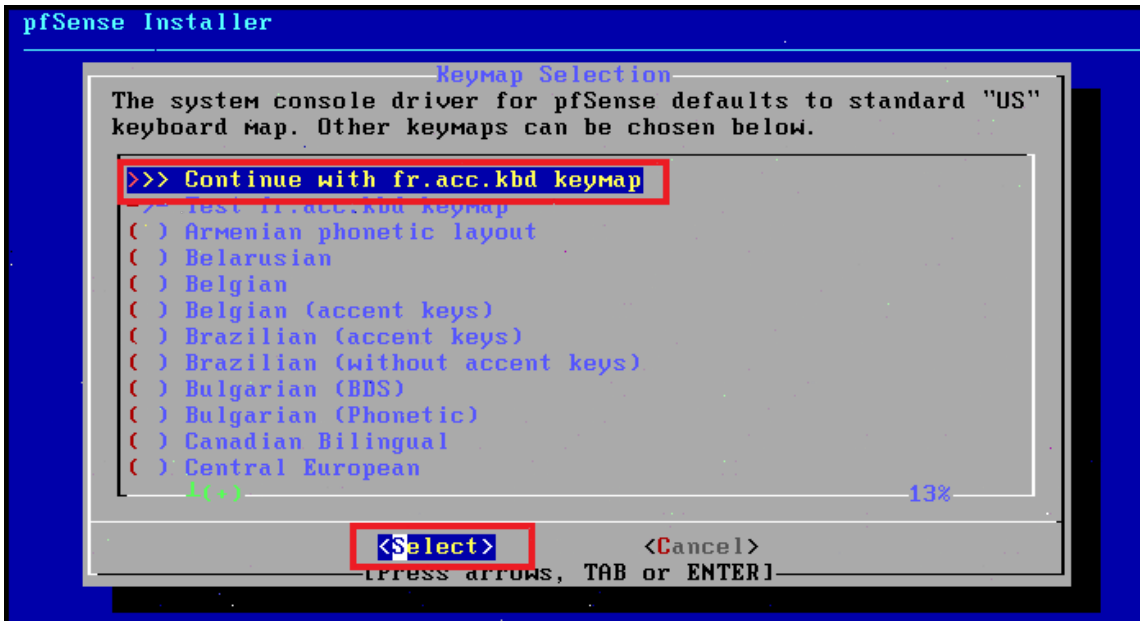

Figure 10 - Fin de l'installation - redémarrage du système

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.

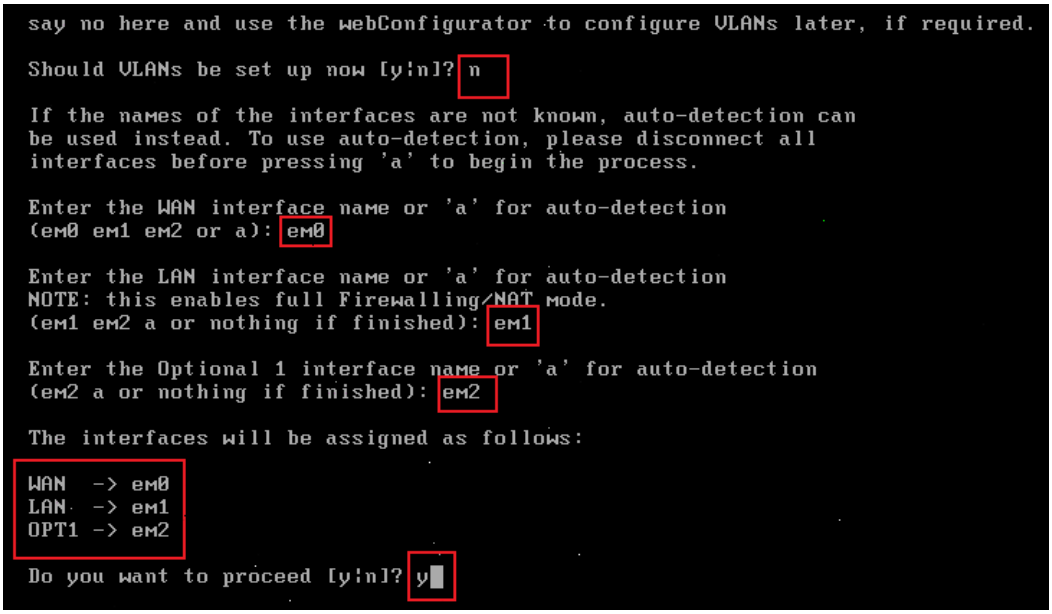

Figure 11 - Interface console pfSense après le premier démarrage

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.

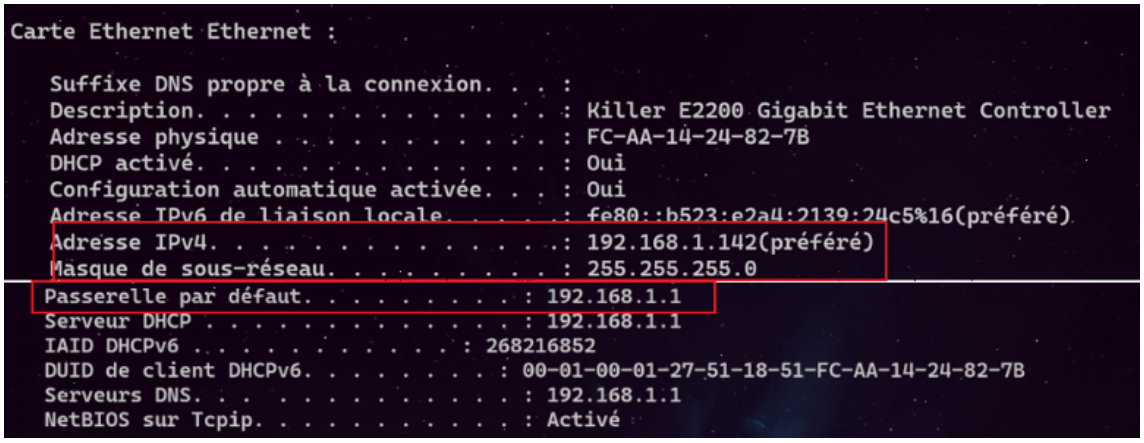

Figure 12 - Déclaration des interfaces réseau (WAN, LAN, OPT1)

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.

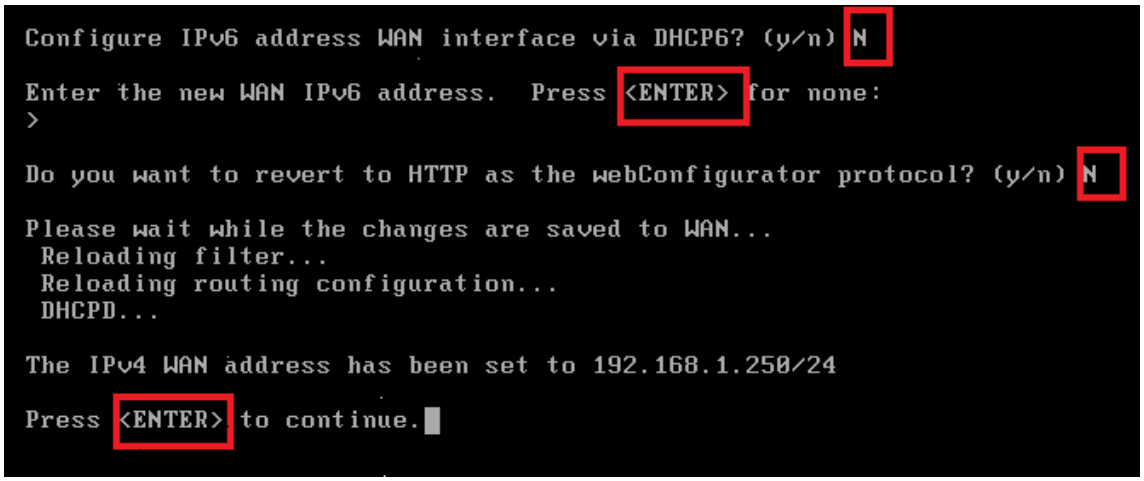

Figure 13 - Configuration de l'interface WAN (192.168.1.250/24)

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.

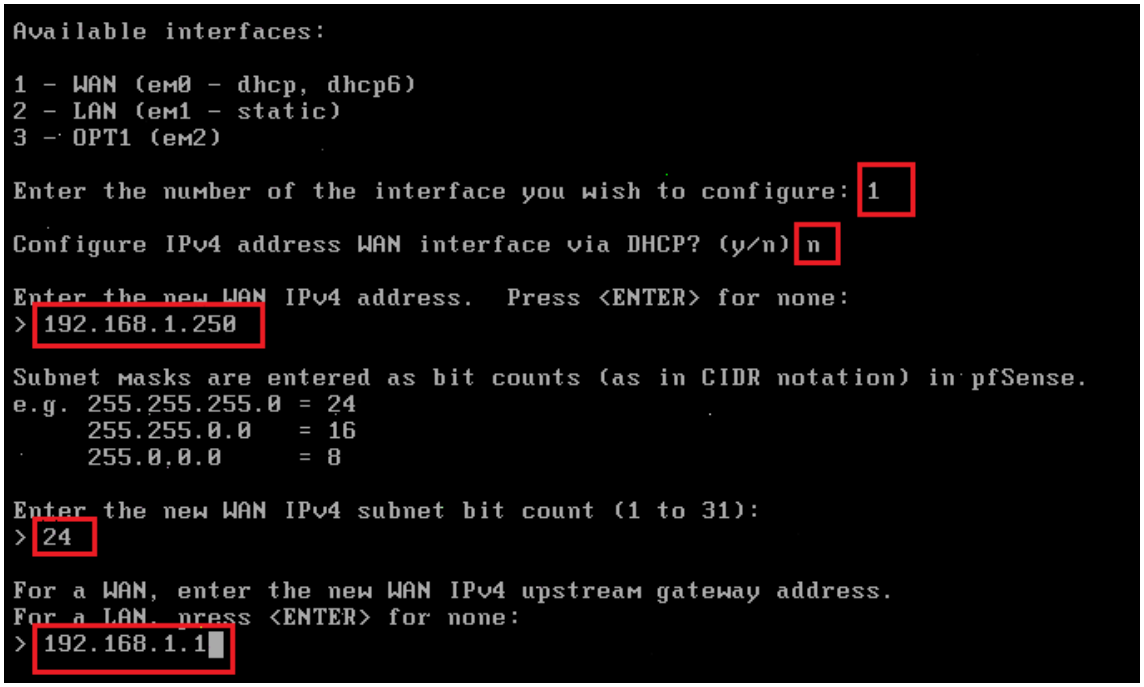

Figure 14 - Configuration de l'interface LAN (172.20.1.250/24) avec DHCP

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.

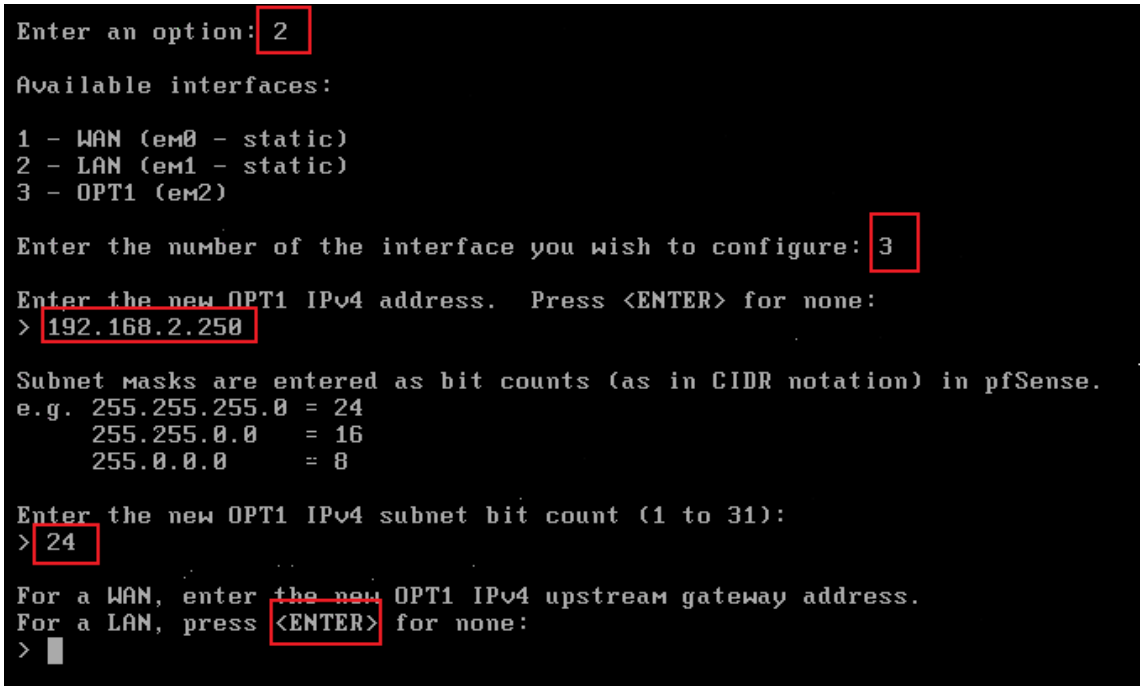

Figure 15 - Configuration de l'interface OPT (172.20.4.250/24)

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.

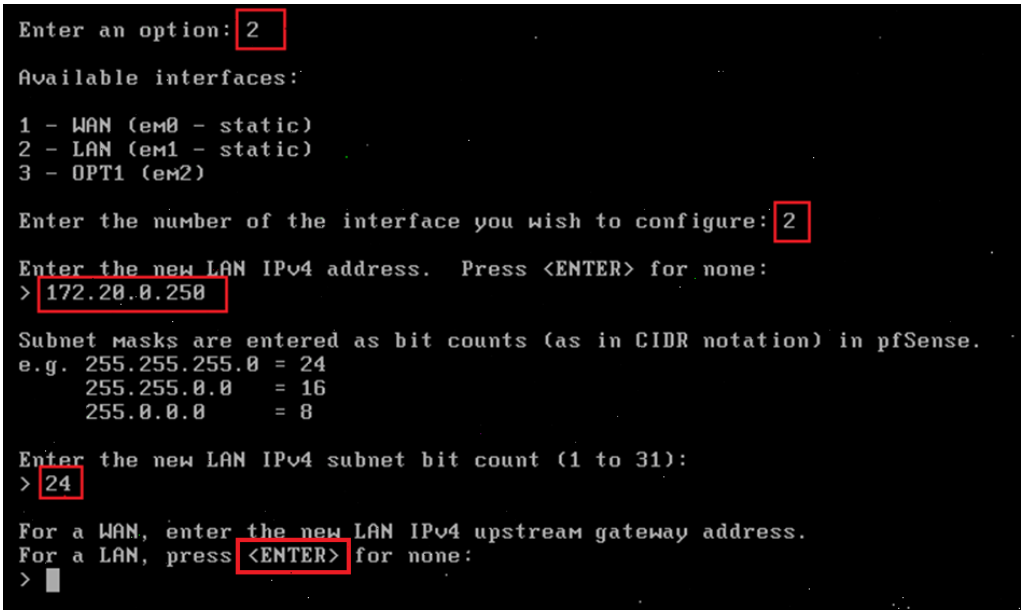

Figure 16 - Menu console avec les trois interfaces configurées

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).

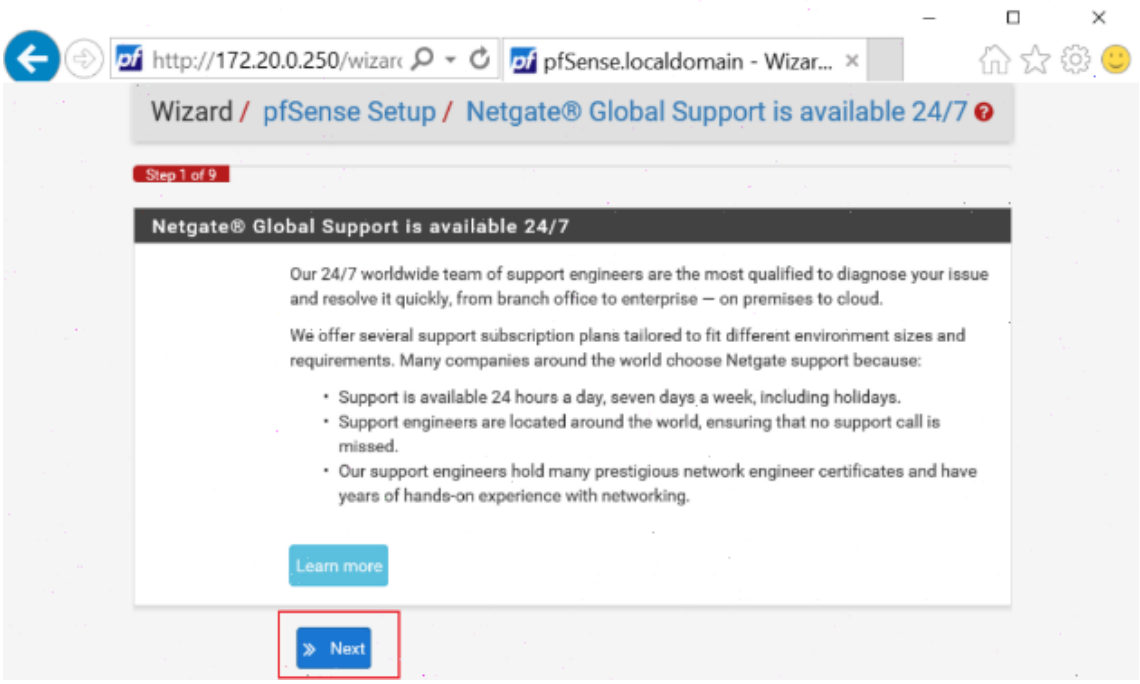

Figure 17 - Interface de connexion Web de pfSense

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.

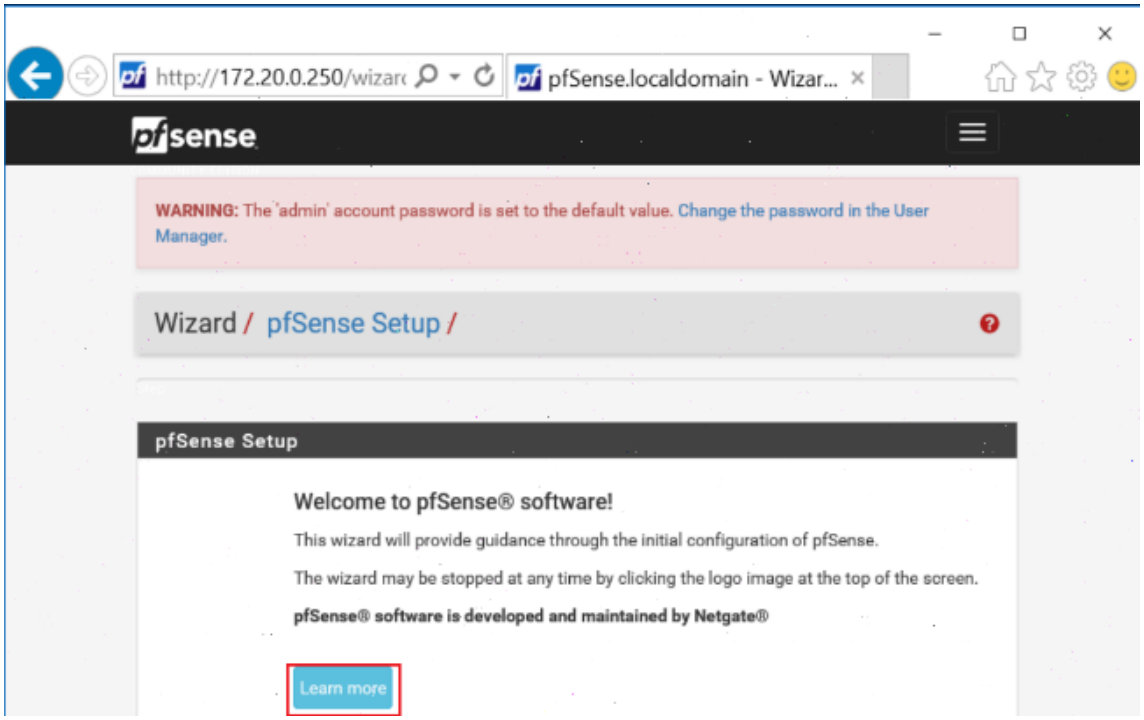

Figure 18 - Wizard étape 1 - Informations générales Netgate

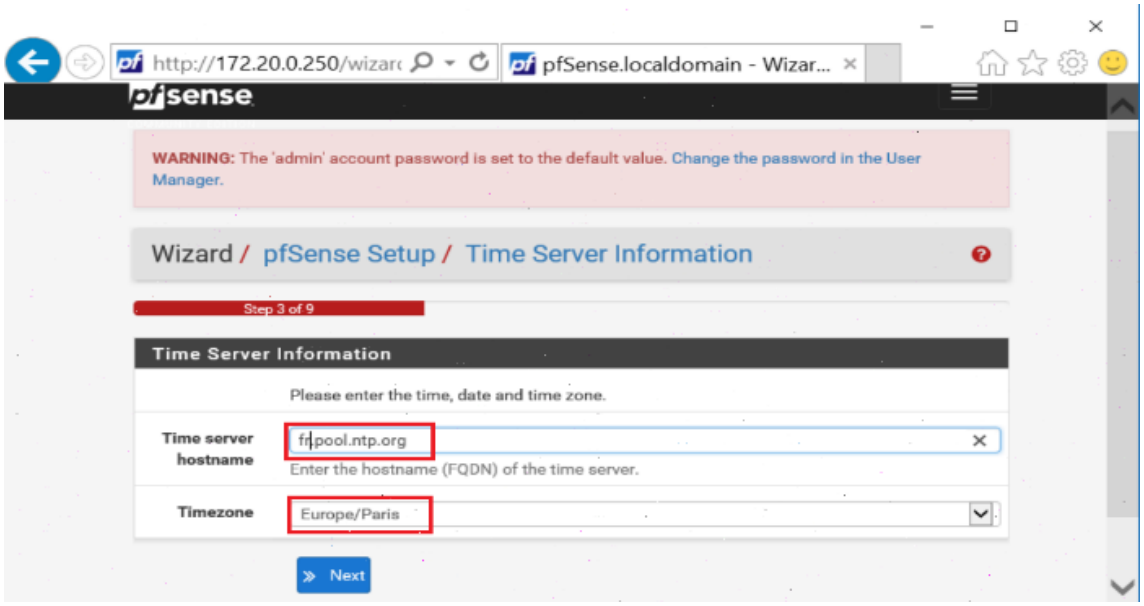

Figure 19 - Wizard étape 2 - Configuration du nom d'hôte et domaine

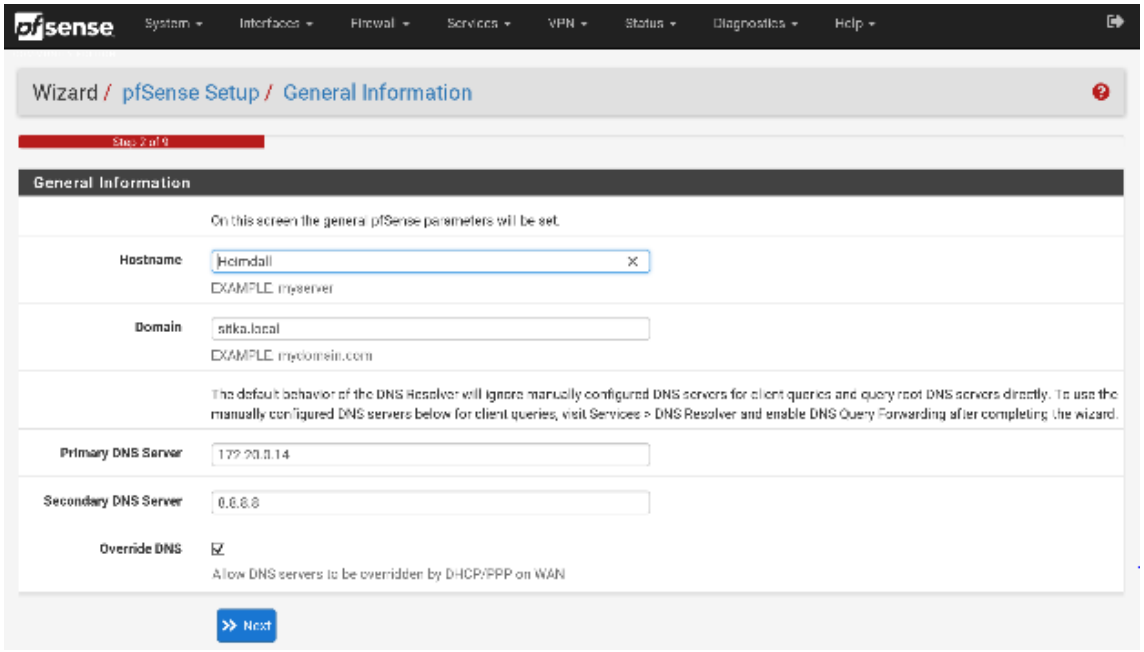

Figure 20 - Configuration du serveur NTP et du fuseau horaire

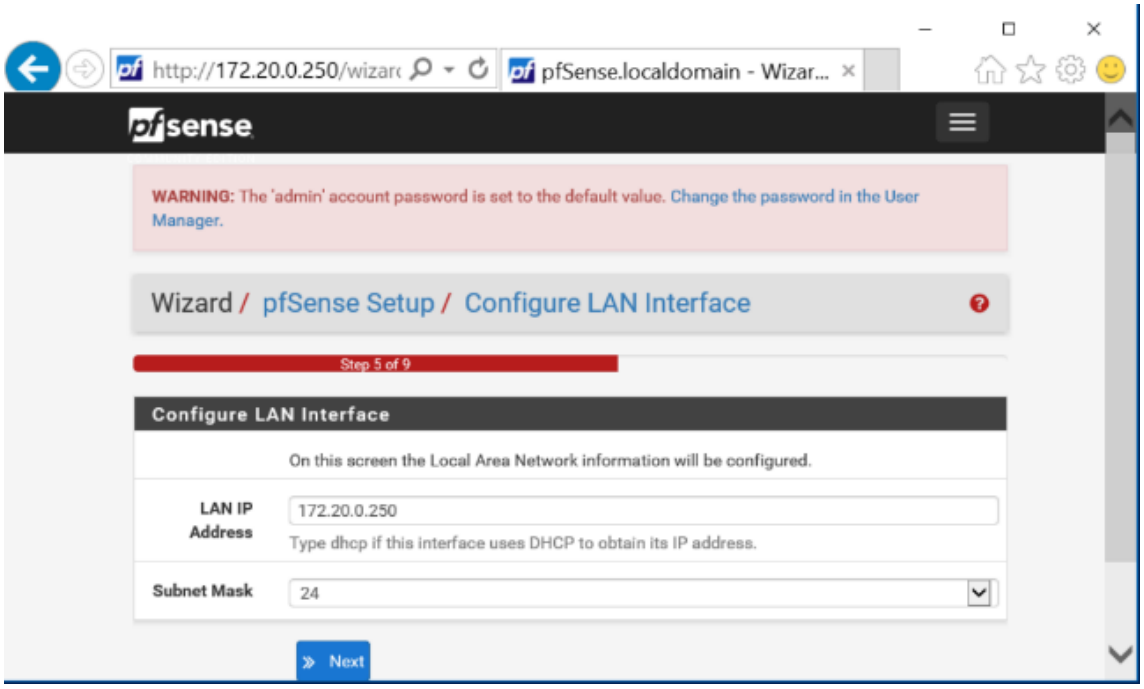

Figure 21 - Vérification de la configuration de l'interface WAN

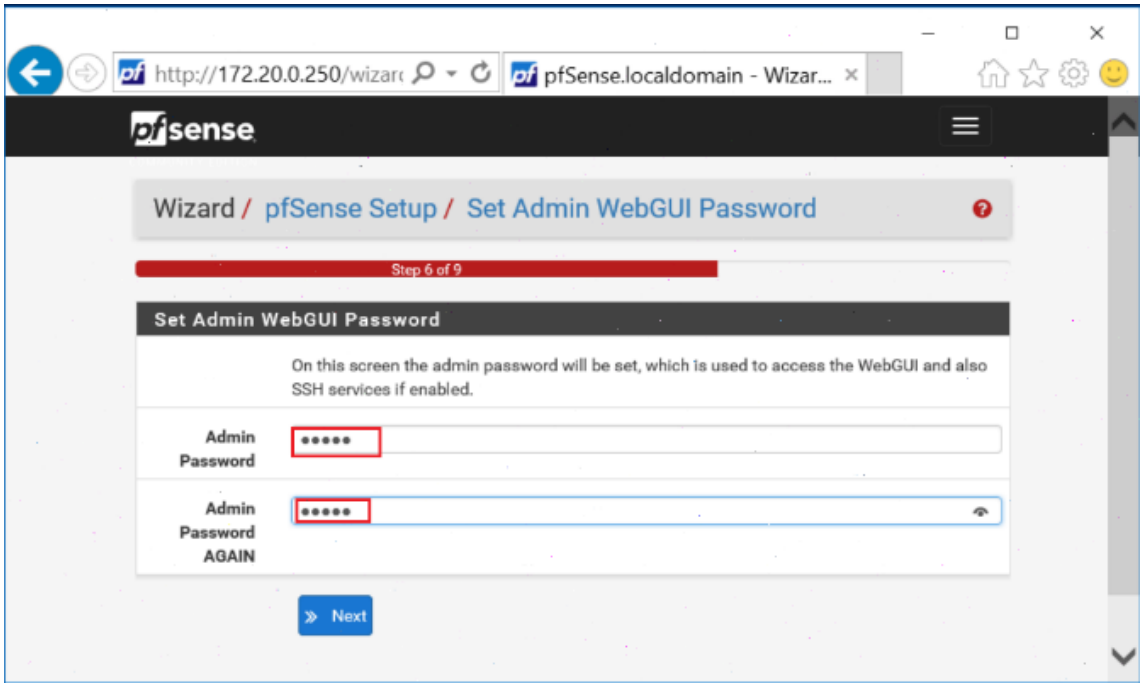

Figure 22 - Modification du mot de passe administrateur

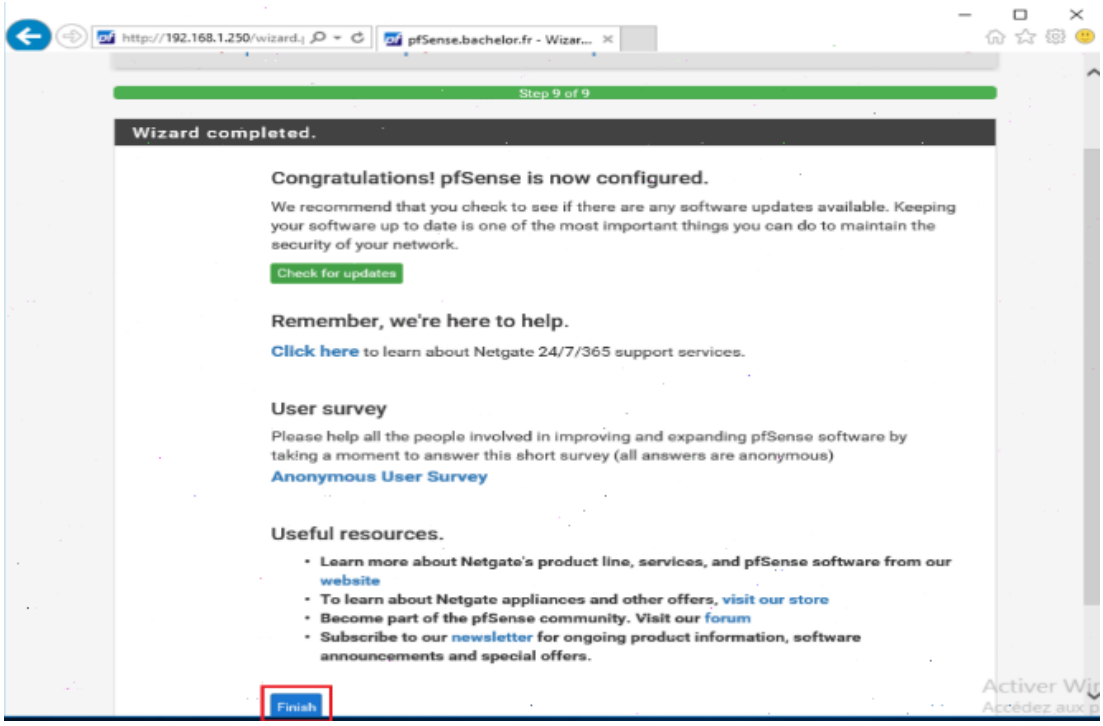

Figure 23 - Application de la configuration (Reload)

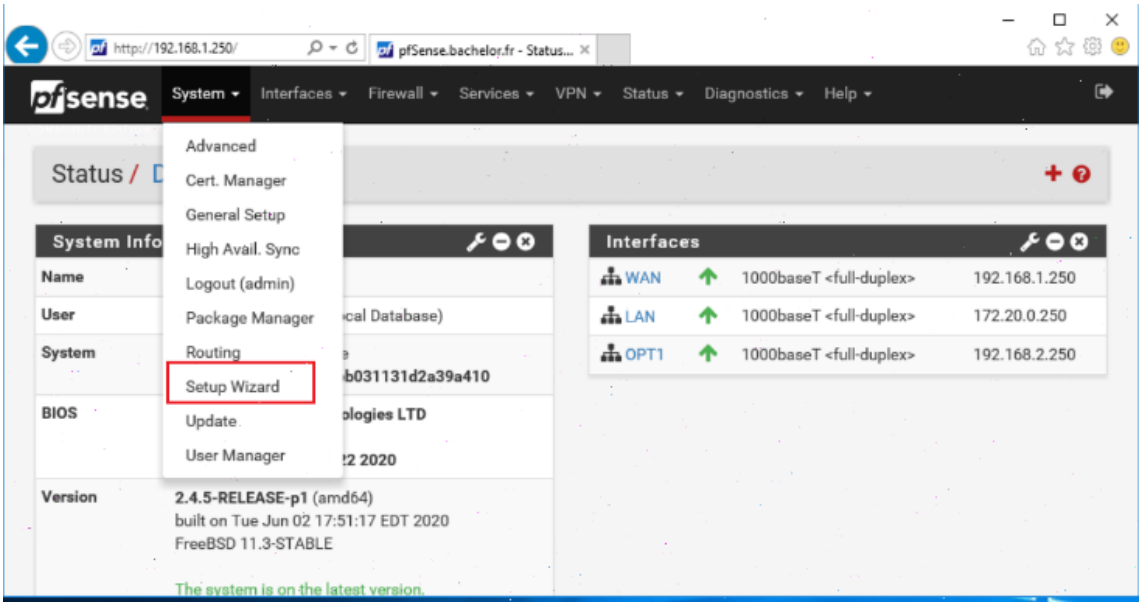

Figure 24 - Finalisation du Wizard - écran de confirmation

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

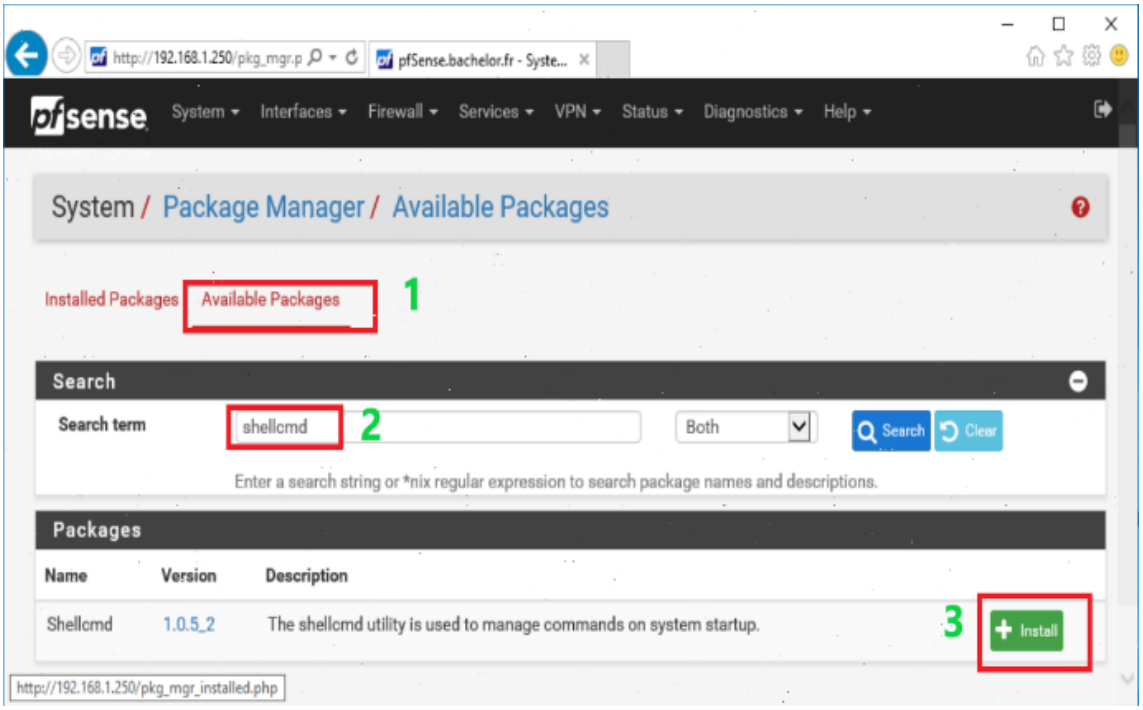

Figure 25 - Tableau de bord pfSense après la configuration initiale

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.

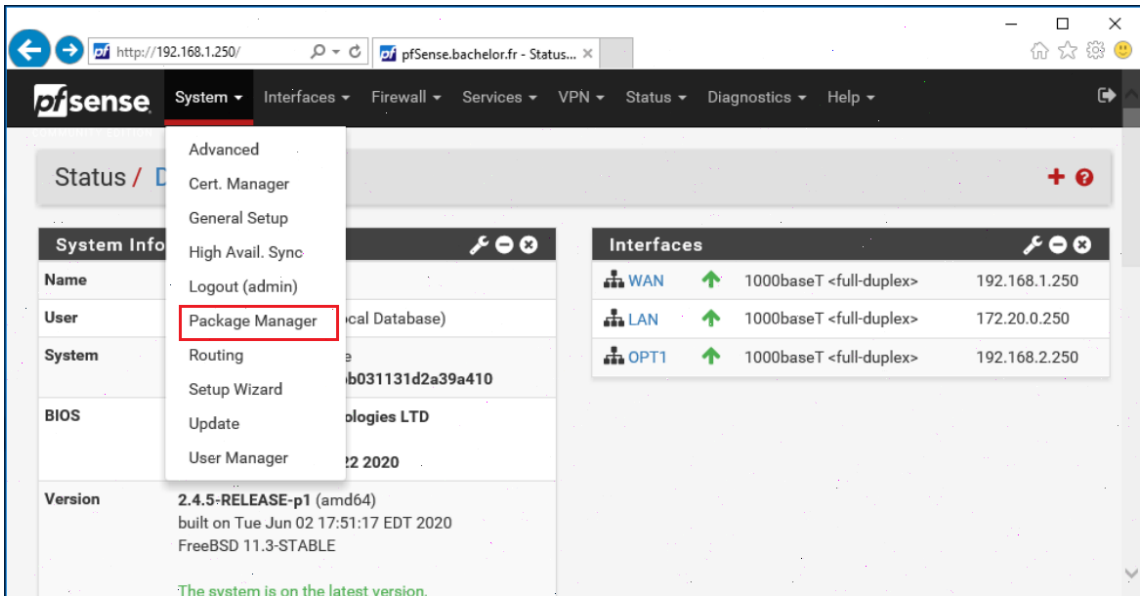

Figure 26 - Installation du paquet Shellcmd via le gestionnaire de paquets

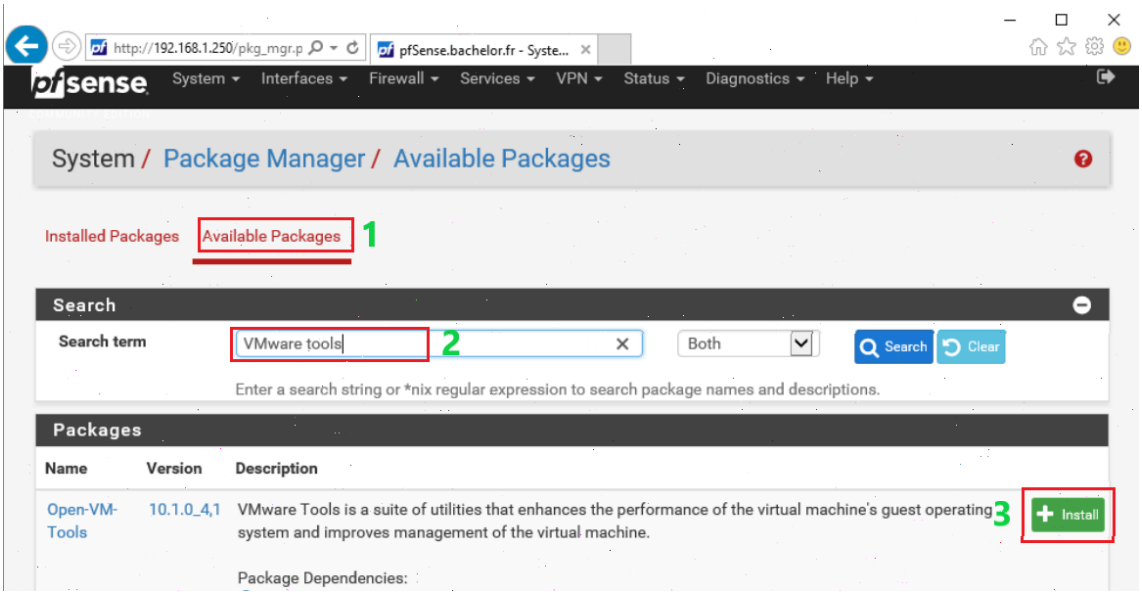

Figure 27 - Installation de VMware Tools (Open VM Tools)

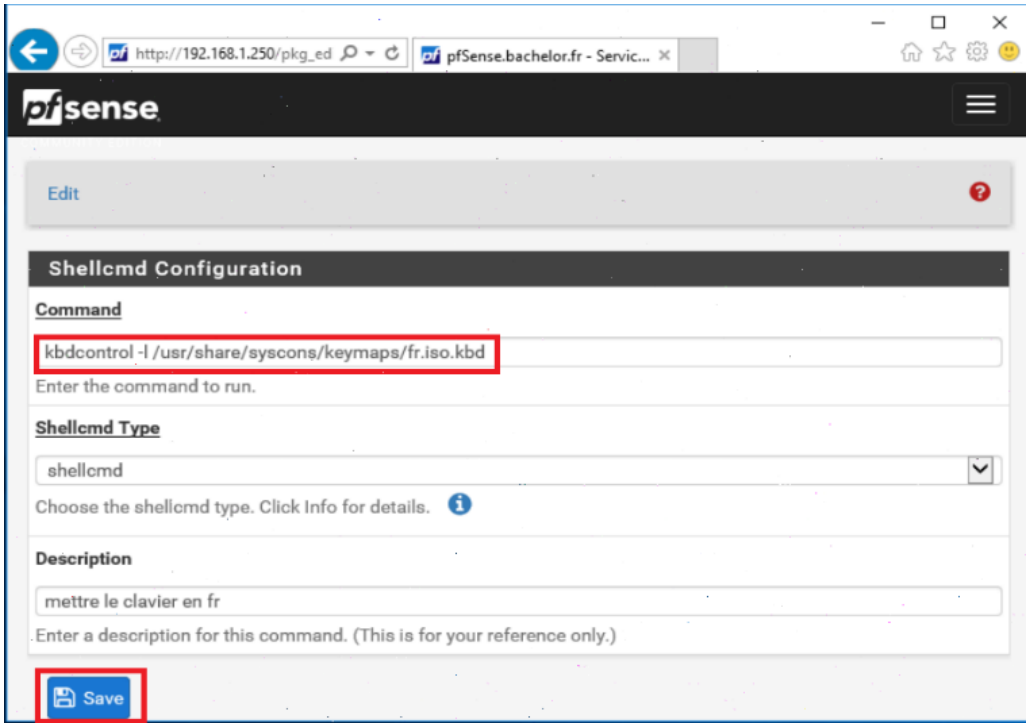

Figure 28 - Configuration de la commande shellcmd pour le clavier AZERTY

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.

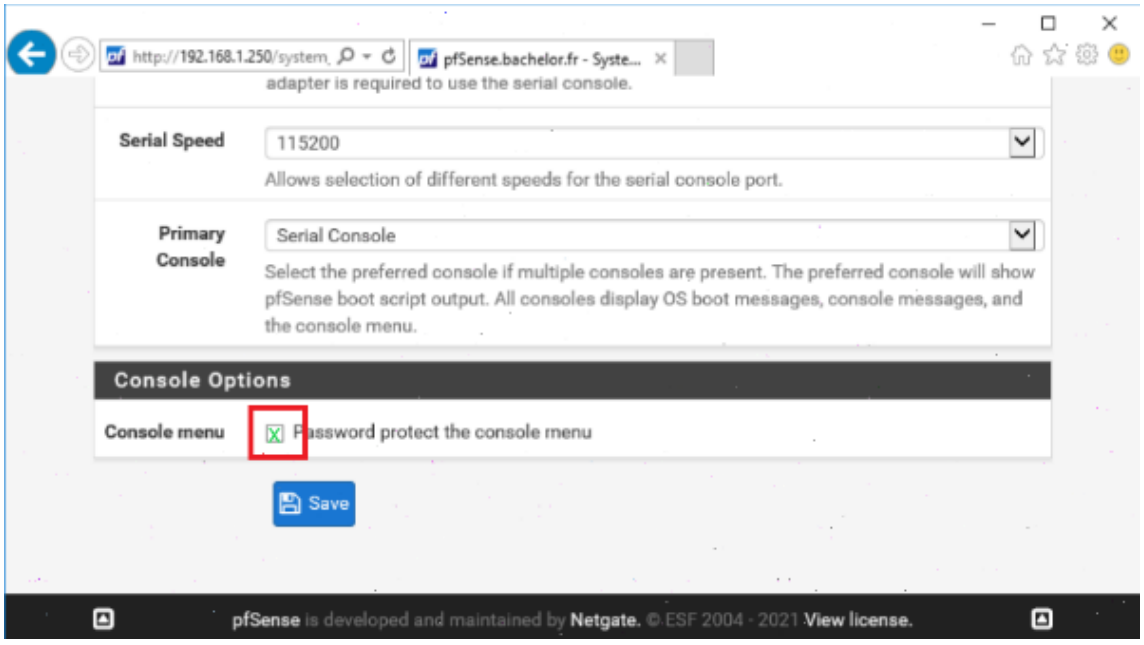

Figure 29 - Activation de la protection par mot de passe de la console

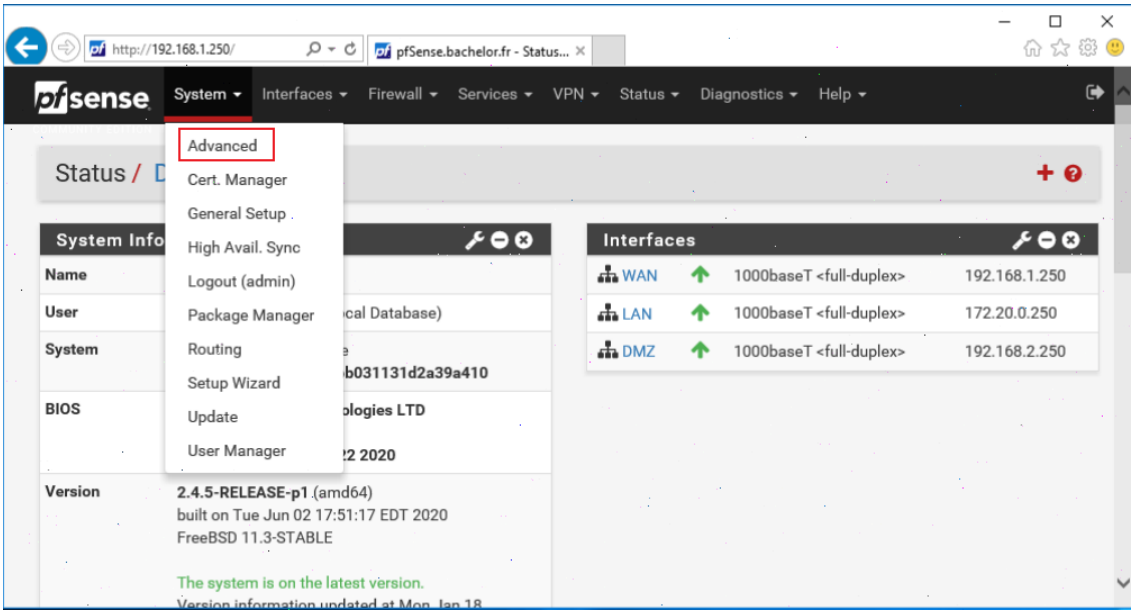

Figure 30 - Console pfSense avec invite de connexion (login requis)

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.

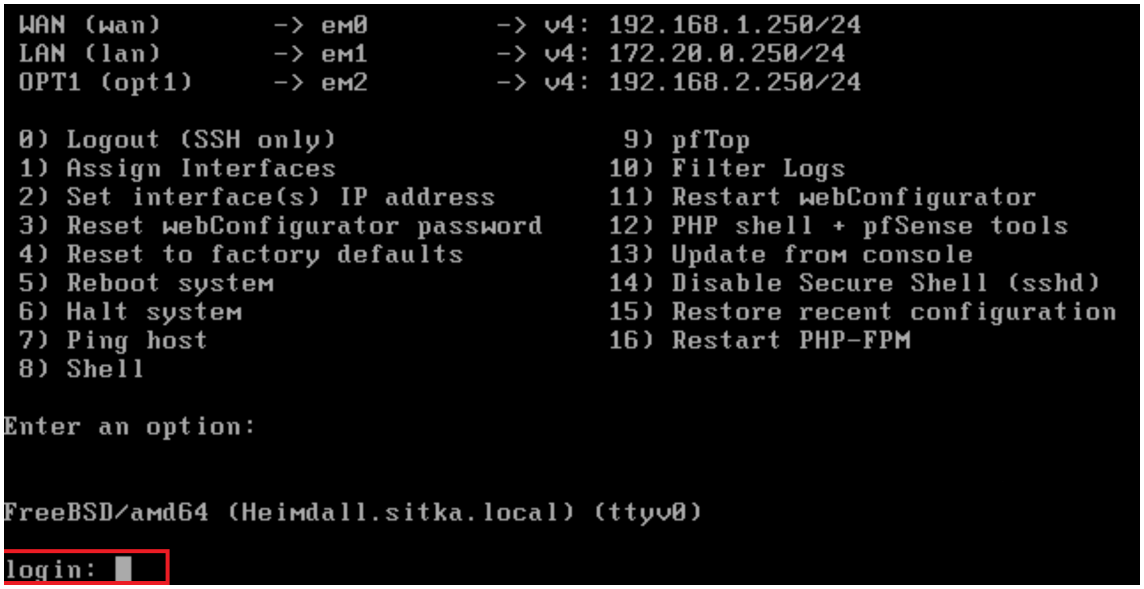

Figure 31 - Activation SSH avec port personnalisé 2121

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.

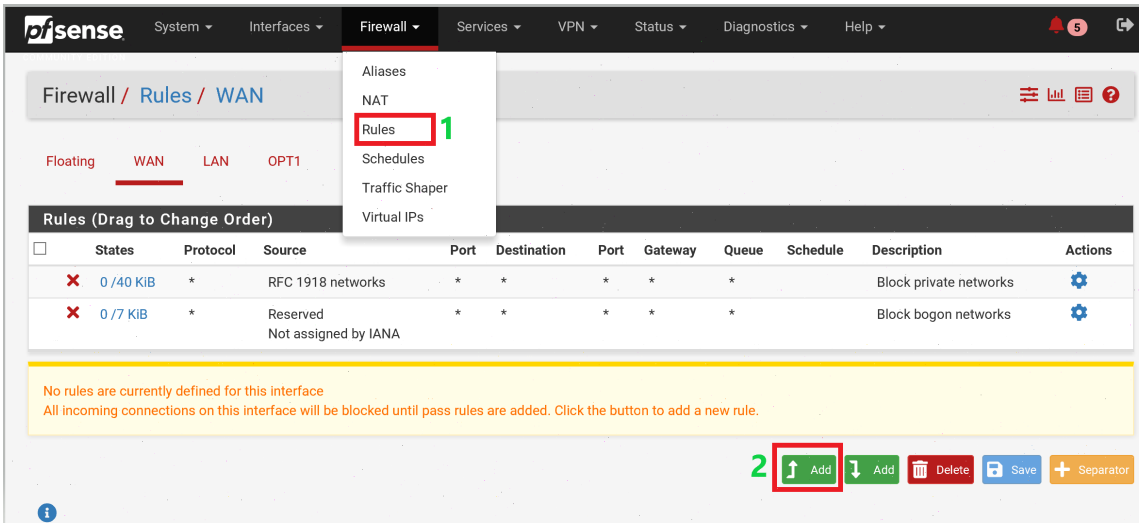

Figure 32 - Création de la règle de pare-feu autorisant SSH sur le WAN

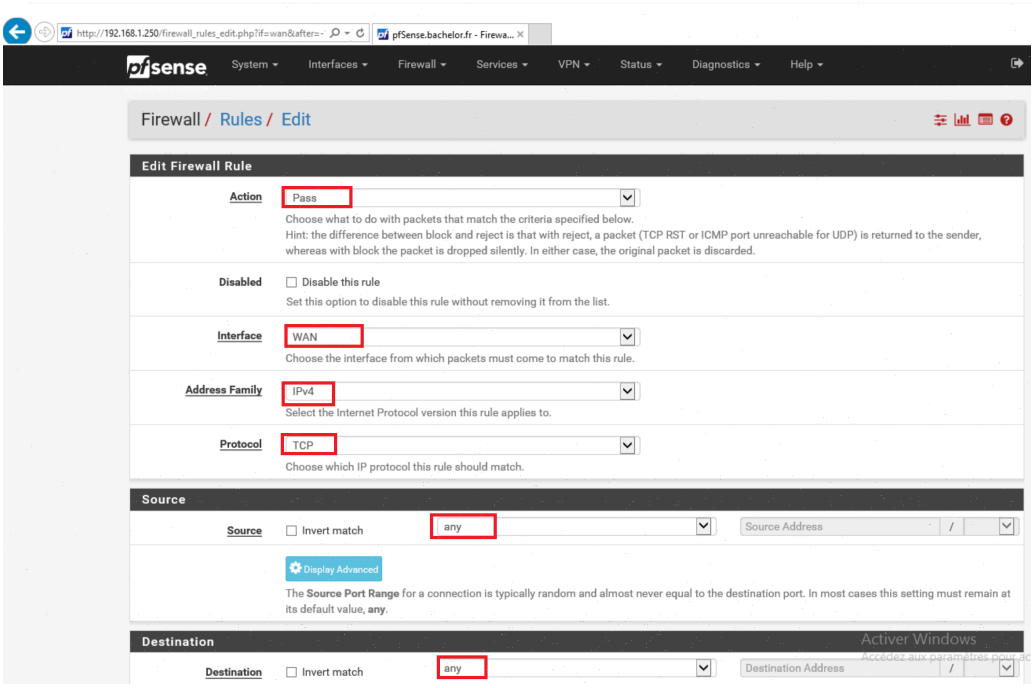

Figure 33 - Détail de la règle SSH : protocole TCP, port 2121, source any

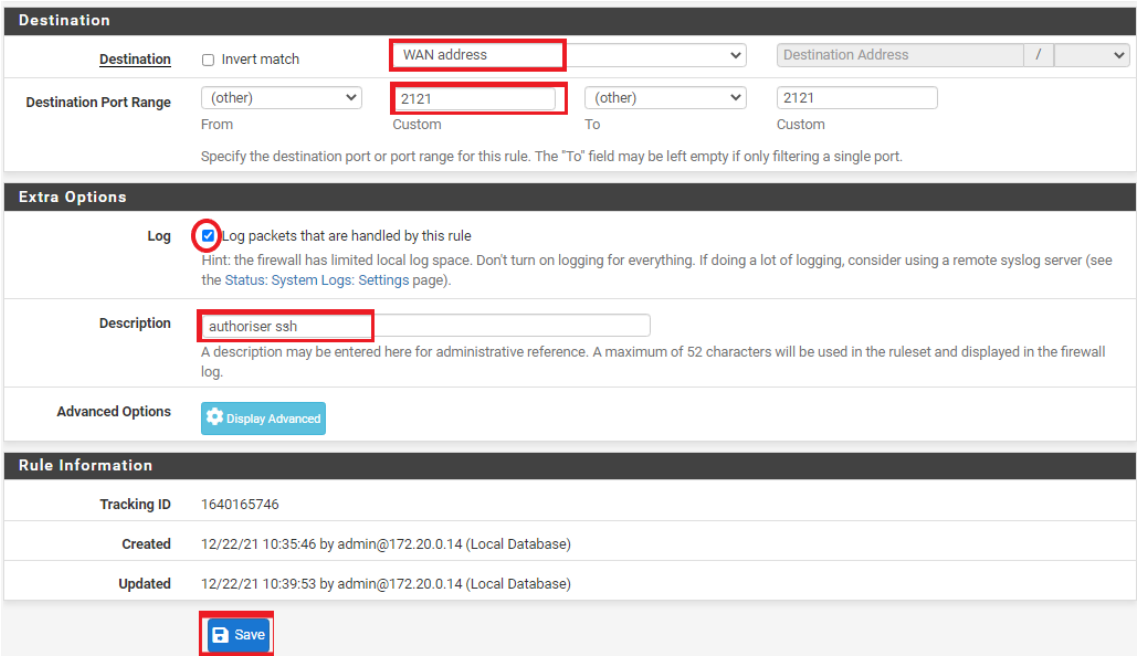

Figure 34 - Enregistrement de la règle de pare-feu

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.

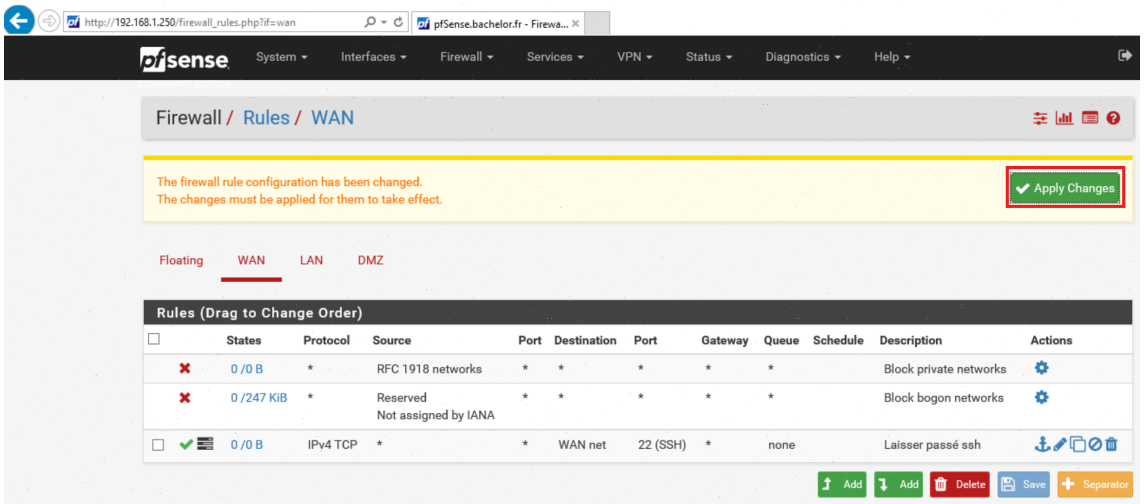

Figure 35 - Connexion SSH réussie depuis le réseau LAN vers pfSense

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.

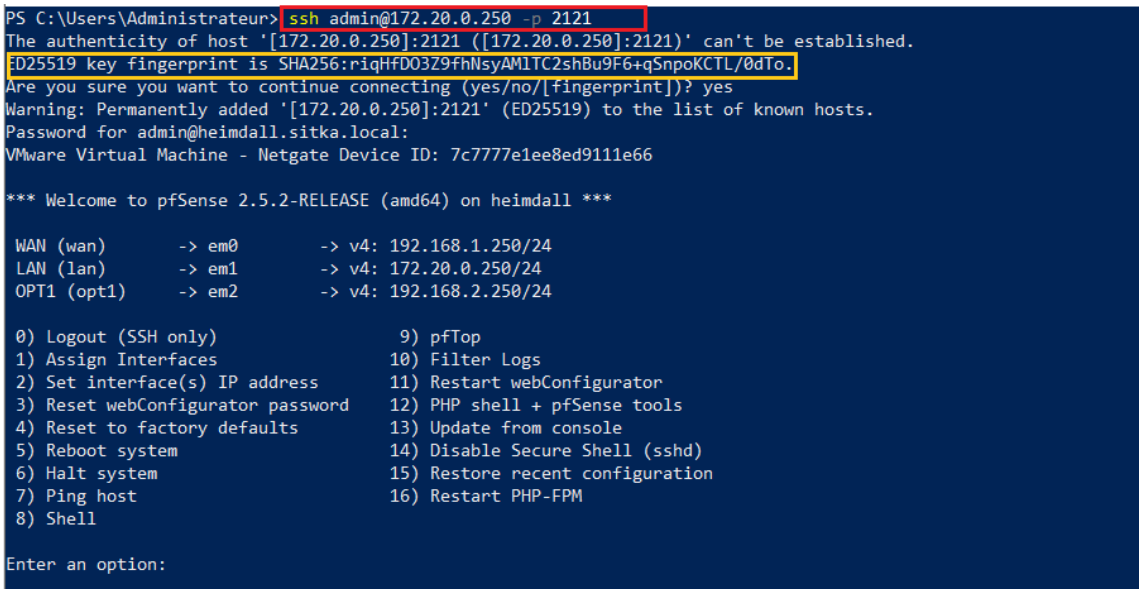

Figure 36 - Vérification de l'empreinte de la clé publique SSH sur le serveur

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.

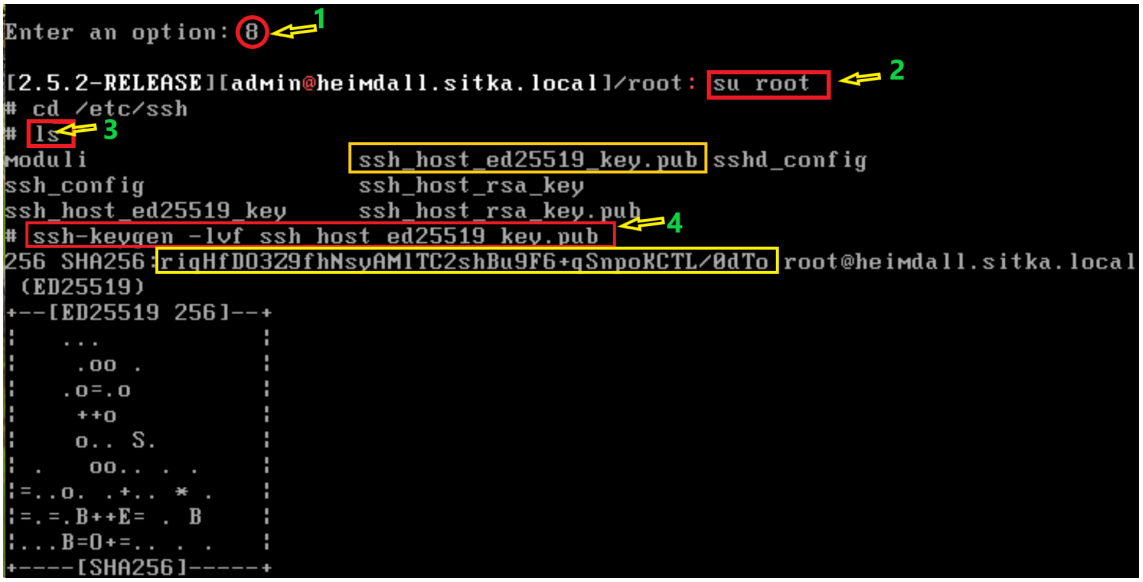

Figure 37 - Tentative de connexion SSH depuis l'extérieur - échec

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.

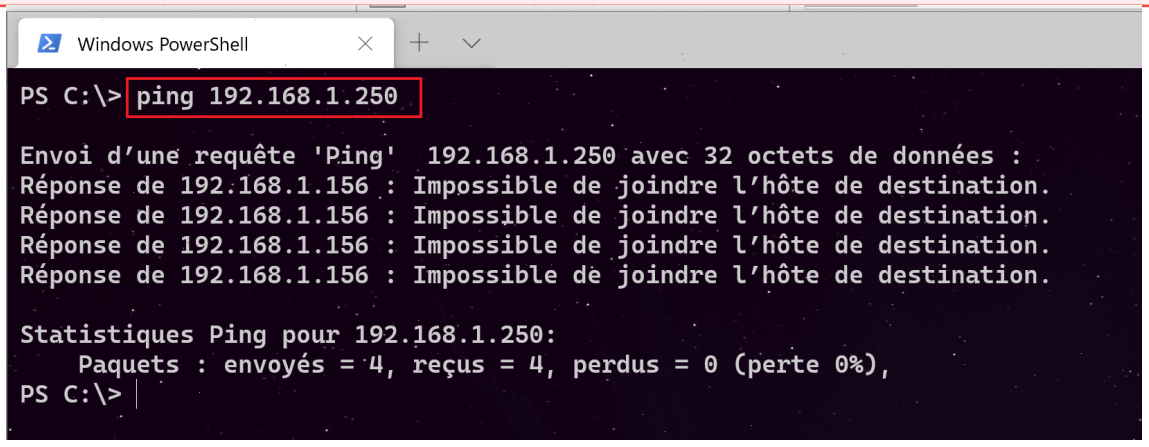

Figure 38 - Options de blocage des réseaux privés et bogons sur l'interface WAN

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.

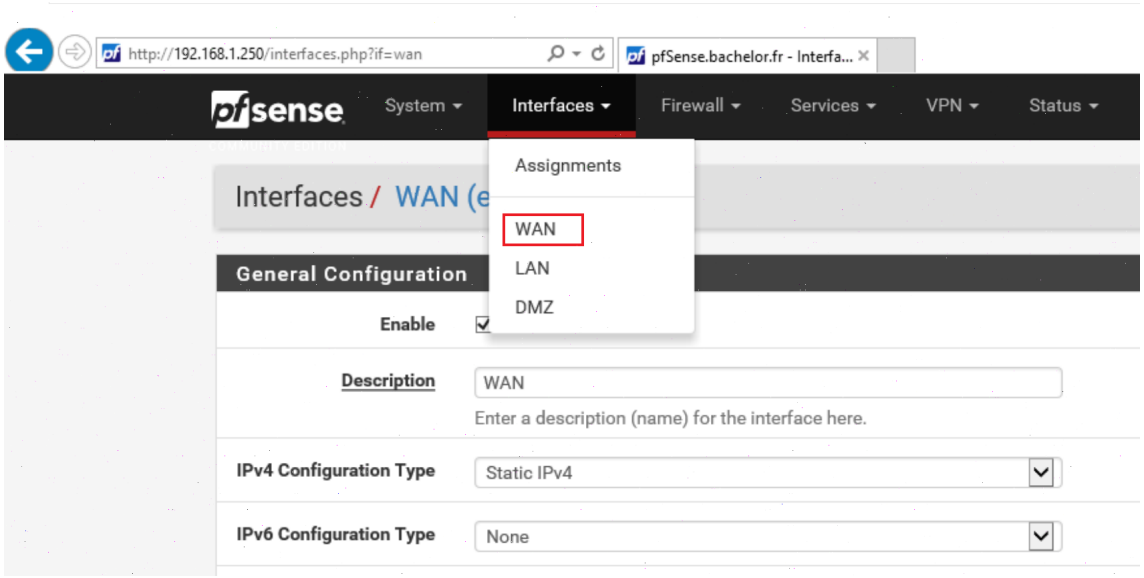

Figure 39 - Configuration de la redirection de port sur la box Internet

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.

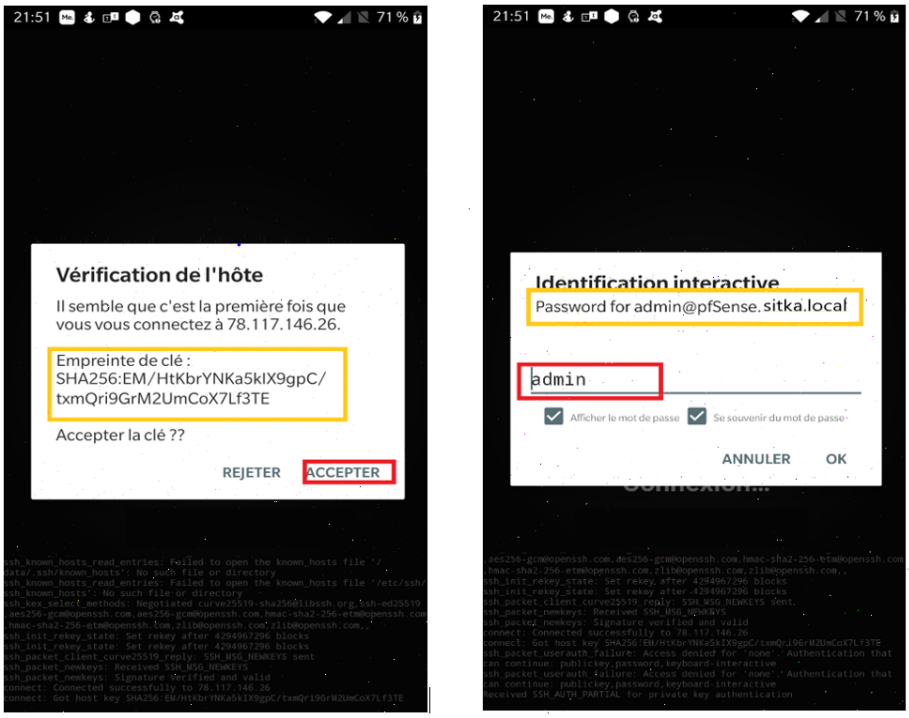

Figure 40 - Connexion SSH distante réussie via smartphone en 4G (JuiceSSH)

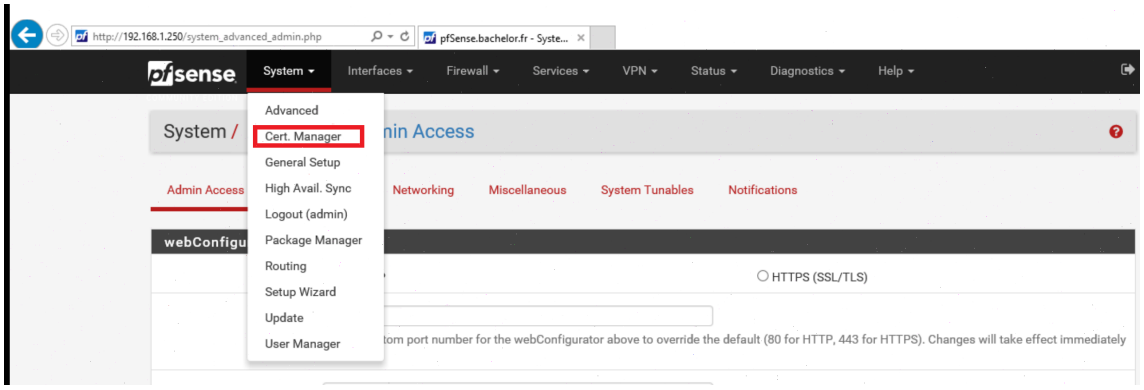

Figure 41 - Vérification de l'empreinte et saisie du mot de passe

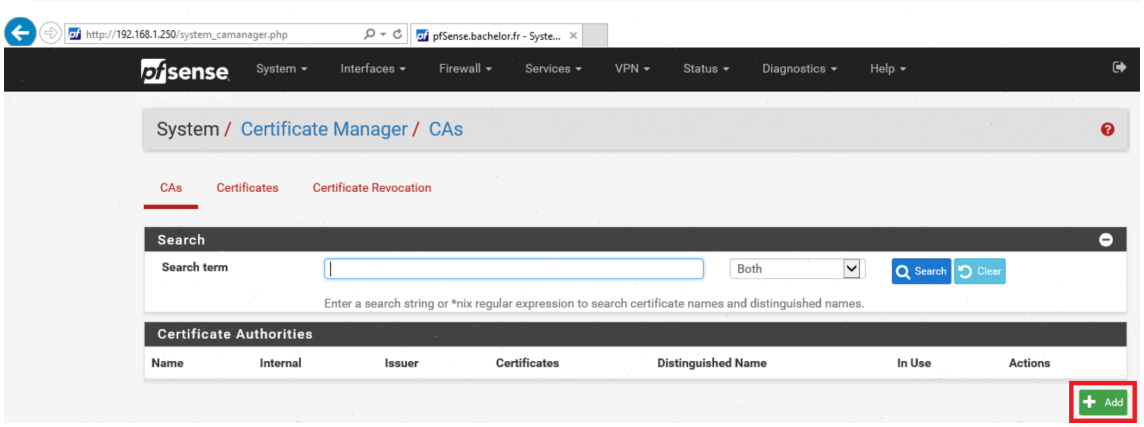

Figure 42 - Accès à la console pfSense depuis le smartphone en 4G

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.).

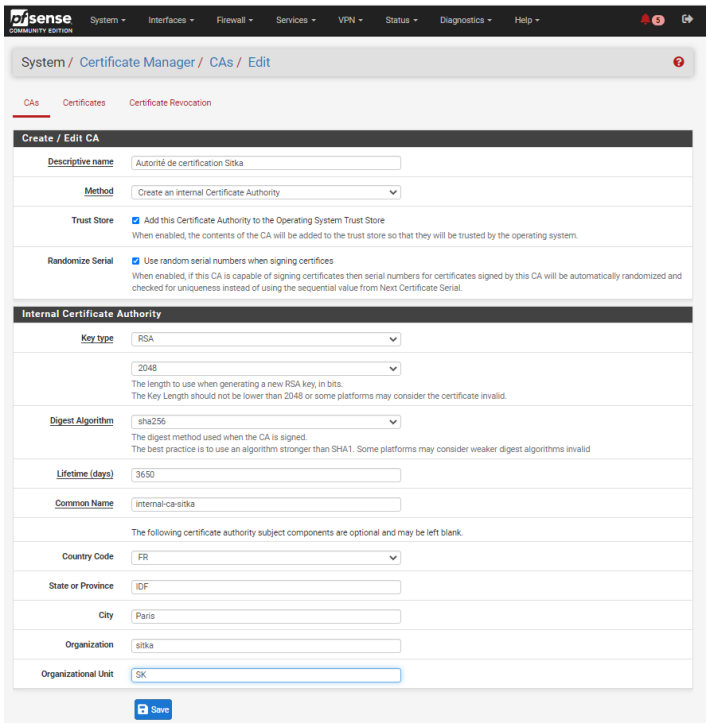

Figure 43 - Création de l'autorité de certification interne (CA)

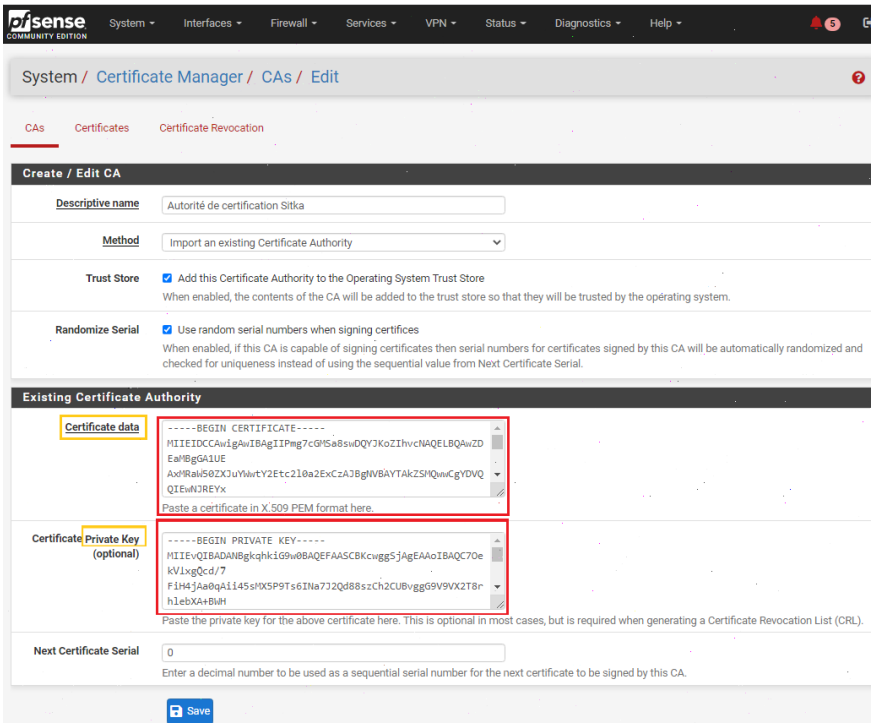

Figure 44 - Autorité de certification créée - affichage du certificat

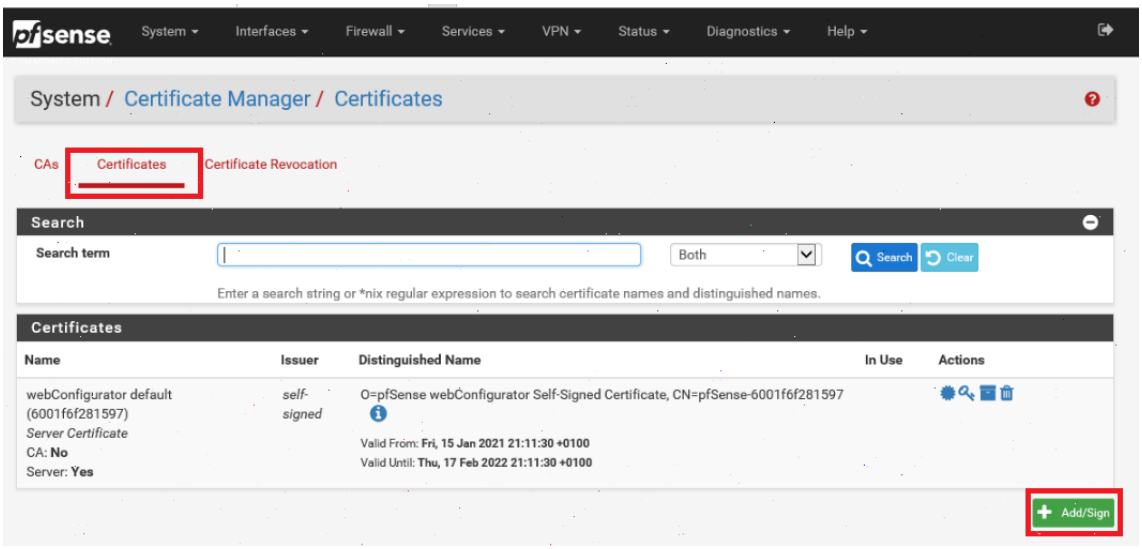

Figure 45 - Détail du certificat CA et de sa clé publique associée

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.

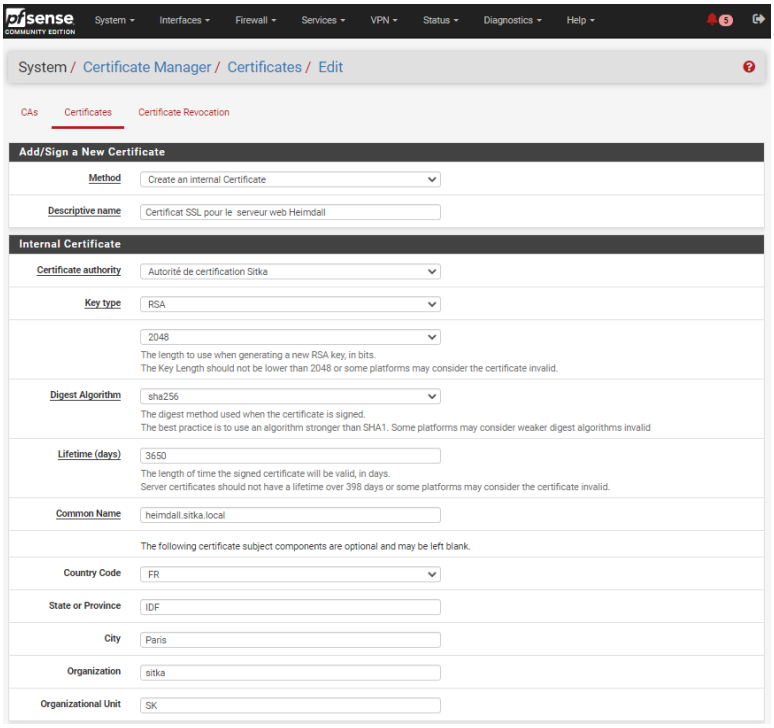

Figure 46 - Création du certificat Web signé par la CA interne

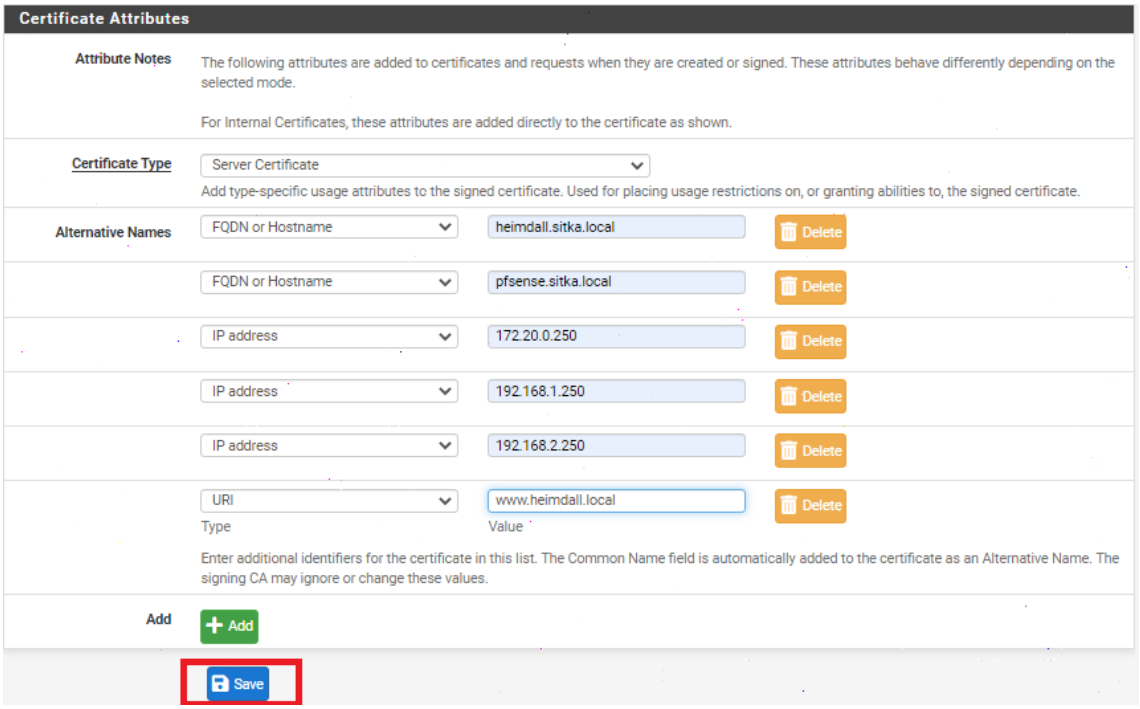

Figure 47 - Paramètres du certificat Web (type serveur, CN, durée)

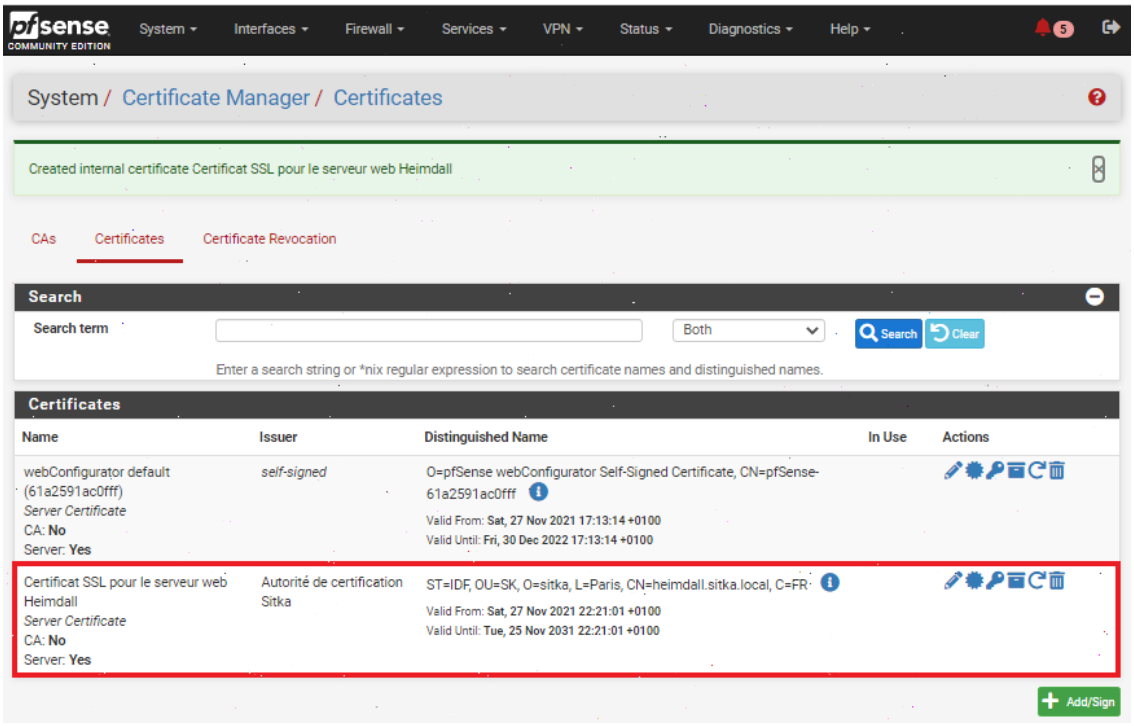

Figure 48 - Informations complémentaires du certificat Web

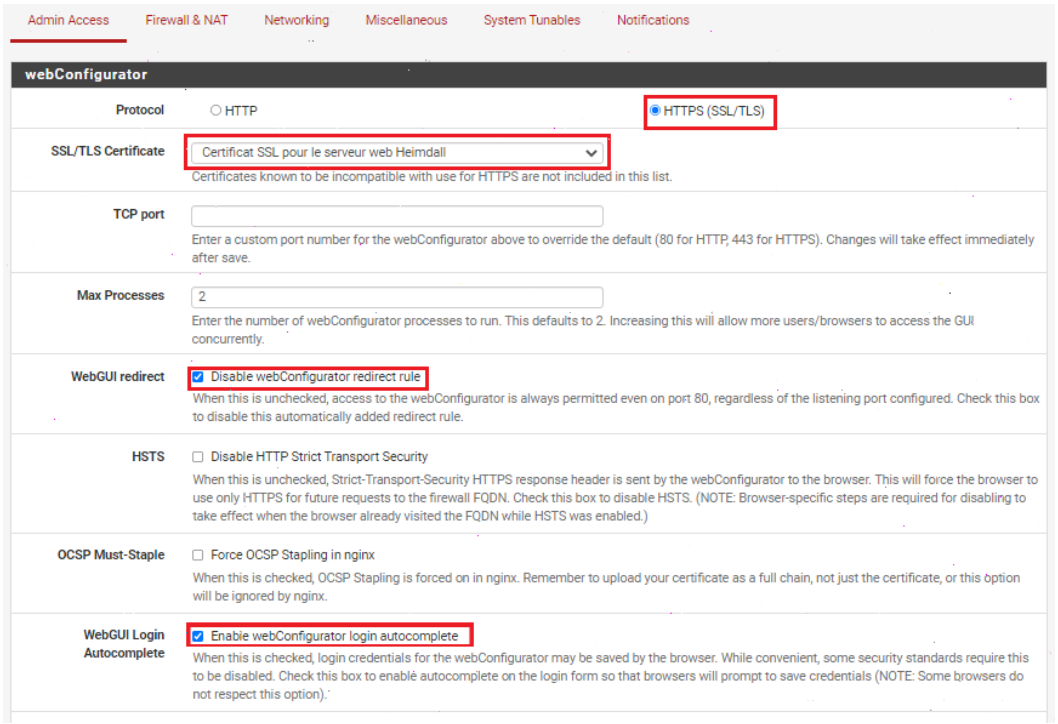

Figure 49 - Certificat Web généré et visible dans le gestionnaire

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.

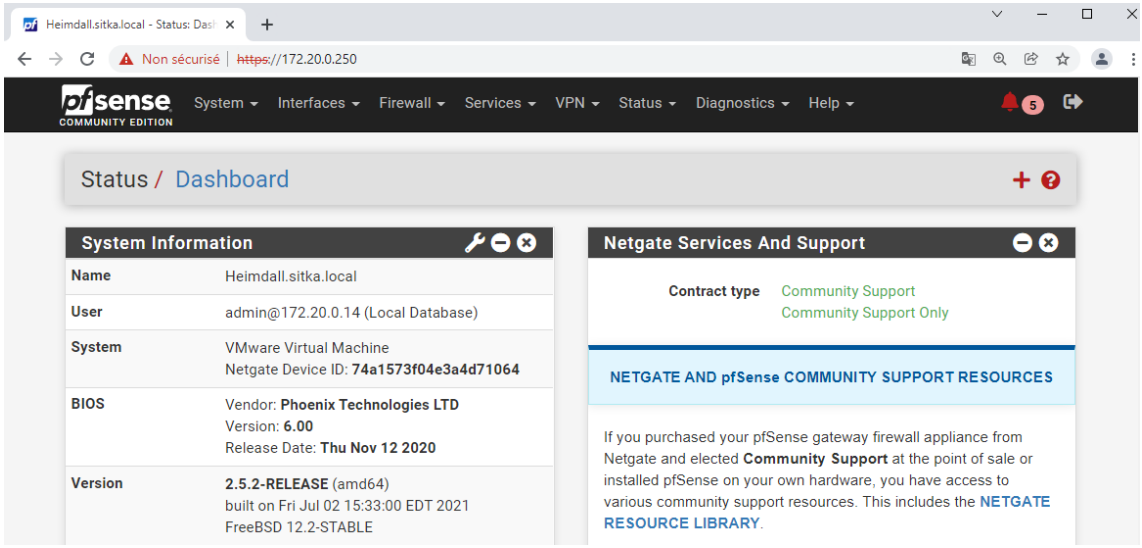

Figure 50 - Configuration HTTPS : sélection du certificat et paramètres de sécurité

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.

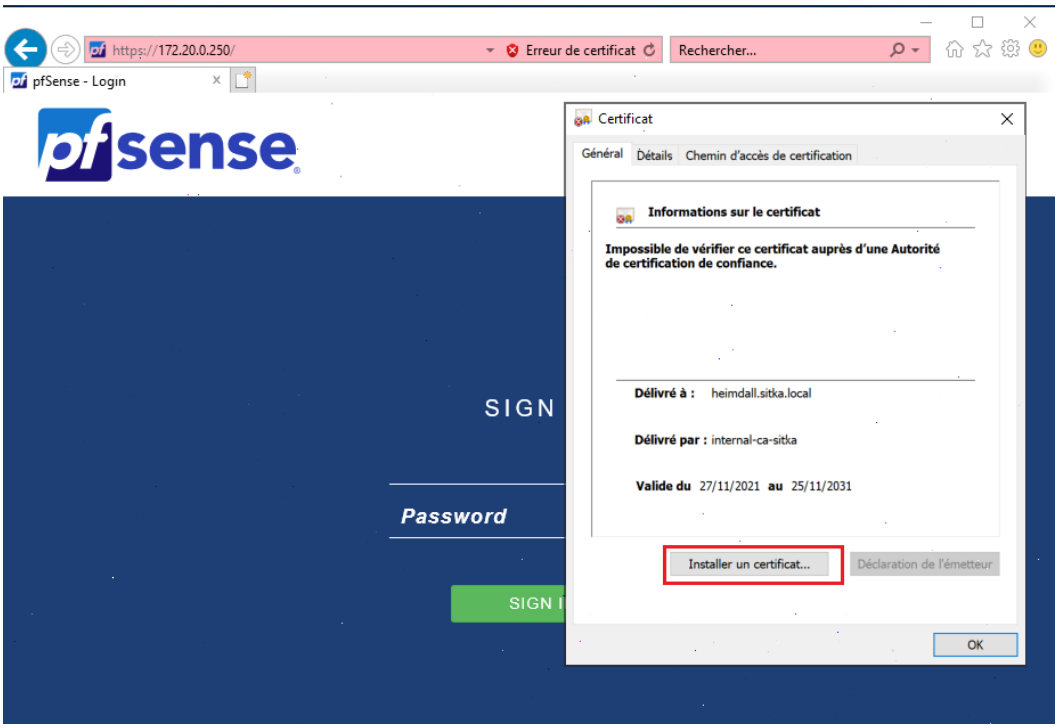

Figure 51 - Accès HTTPS à pfSense - avertissement de certificat

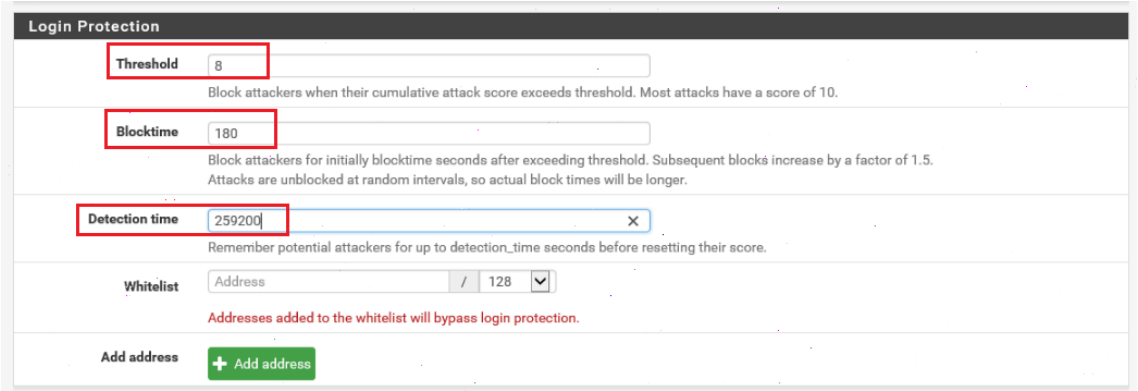

Figure 52 - Connexion sécurisée HTTPS établie avec succès

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.