BTS SIO – Session 2026

Candidat libre

PROJET PERSONNEL ENCADRÉ N°2

Mise en place d'une infrastructure de sécurité réseau avec pfSense, Squid et liaison LDAP

Dossier Technique

SAAD Brandon

BTS Services Informatiques aux Organisations

Option SISR – Solutions d'Infrastructure, Systèmes et Réseaux

Session 2026

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS — SESSION 2026

Épreuve E5 — Administration des systèmes et des réseaux (option SISR)

ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE
Nom, prénom du candidat : SAAD Brandon
Organisation support : MindLab (entreprise fictive) — basée à Senlis (Oise)
Intitulé de la réalisation : Mise en place d'une infrastructure de sécurité réseau avec pfSense, Squid et liaison LDAP
Période de réalisation : Janvier — Avril 2026
Lieu : Domicile / Plateau technique
Modalité : Seul ☒ En équipe ☐

Compétences travaillées
☒ Concevoir une solution d'infrastructure réseau
☒ Installer, tester et déployer une solution d'infrastructure réseau
☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation (cahier des charges)
• Installation et configuration d'une infrastructure pfSense avec zones LAN et DMZ
• Mise en place du proxy Squid (HTTP et HTTPS) avec filtrage de contenu
• Hébergement d'un serveur Web GLPI dans la DMZ
• Définition de règles de pare-feu sur les interfaces WAN, LAN et DMZ
• Mise en place d'un VPN OpenVPN pour l'accès distant au LAN
• Liaison LDAP entre pfSense et l'Active Directory

Ressources matérielles et logicielles utilisées
• VMware Workstation Pro (hyperviseur)
• pfSense 2.7.2 (pare-feu/routeur)
• Windows Server 2022 (Active Directory, DNS)
• Debian 12 (serveur web GLPI)
• Windows 11 (postes clients)
• Squid (paquet pfSense — proxy HTTP/HTTPS)

Table des matières

I. Présentation de la mission

1.1. Introduction

Dans le cadre de l'épreuve E5 du BTS SIO option SISR, ce projet vise à déployer une infrastructure de sécurité réseau complète pour l'entreprise fictive MindLab, basée à Senlis (Oise). L'objectif est de mettre en place une solution de pare-feu open-source robuste, capable de protéger le réseau interne et de filtrer les flux Web, tout en permettant aux utilisateurs distants d'accéder aux ressources internes via un VPN.

L'infrastructure repose sur trois briques techniques complémentaires : pfSense comme pare-feu et routeur, Squid comme serveur proxy avec filtrage HTTP/HTTPS, et une liaison LDAP avec l'Active Directory pour centraliser l'authentification des administrateurs sur l'interface pfSense.

L'architecture est segmentée en deux zones distinctes : une zone LAN hébergeant les postes clients et le contrôleur de domaine, et une zone DMZ hébergeant le serveur Web GLPI. Cette segmentation permet d'appliquer des règles de filtrage adaptées à chaque type de flux et de limiter la surface d'attaque en cas de compromission d'un serveur exposé.

II. Contexte

2.1. Scénario

MindLab est une PME en pleine croissance qui souhaite renforcer la sécurité de son système d'information. L'entreprise dispose actuellement d'un réseau plat sans segmentation ni filtrage applicatif, ce qui expose ses données à de nombreux risques : navigation Web non maîtrisée, absence de contrôle d'accès aux ressources internes depuis l'extérieur, et impossibilité de tracer les activités des utilisateurs sur Internet.

À l'issue du projet, MindLab disposera d'une infrastructure de sécurité périmétrique complète. Le pare-feu pfSense filtrera tous les flux entrants et sortants, le proxy Squid contrôlera et journalisera la navigation Web (y compris HTTPS via interception SSL), et la liaison LDAP permettra une administration centralisée du pare-feu avec les comptes du domaine Active Directory.

2.2. Cahier des charges

- Installation et configuration d'une infrastructure pfSense avec trois interfaces réseau (WAN, LAN, DMZ)
- Mise en place d'un proxy transparent Squid pour filtrer le trafic HTTP et HTTPS
- Hébergement d'un serveur web GLPI sur la DMZ accessible depuis l'extérieur via redirection NAT
- Définition de règles de pare-feu strictes entre les zones LAN, DMZ et WAN
- Mise en place du protocole HTTPS pour les services exposés
- Configuration d'un accès VPN OpenVPN pour la connexion distante au LAN
- Liaison LDAP entre pfSense et l'Active Directory pour l'authentification administrateur

2.3. Besoins matériels et logiciels

- 1 machine virtuelle pfSense 2.7.2 (3 cartes réseau virtuelles)
- 1 serveur Windows Server 2022 (rôles Active Directory et DNS)
- 2 postes clients Windows 11
- 1 serveur Debian 12 (hébergement de GLPI sur Apache/MySQL)
- Hyperviseur VMware Workstation Pro pour virtualiser l'ensemble de la maquette

2.4. Architecture réseau

L'architecture de la maquette s'articule autour du pare-feu pfSense, qui interconnecte trois réseaux distincts. Le réseau WAN (192.168.70.0/24) simule le réseau public et constitue le point d'entrée externe, notamment pour les connexions VPN. Le réseau LAN (192.168.80.0/24) regroupe les postes utilisateurs et le contrôleur de domaine. Enfin, la DMZ (192.168.90.0/24) isole le serveur Web GLPI exposé.

Plan d'adressage retenu :

- pfSense WAN : 192.168.70.1/24
- pfSense LAN : 192.168.80.1/24
- pfSense DMZ : 192.168.90.1/24
- DC-01 (AD/DNS) : 192.168.80.4/24
- PC-01 et PC-02 : 192.168.80.2 et 192.168.80.3
- DEB-01 (serveur GLPI) : 192.168.90.2/24

2.5. Présentation des solutions utilisées

2.5.1. pfSense

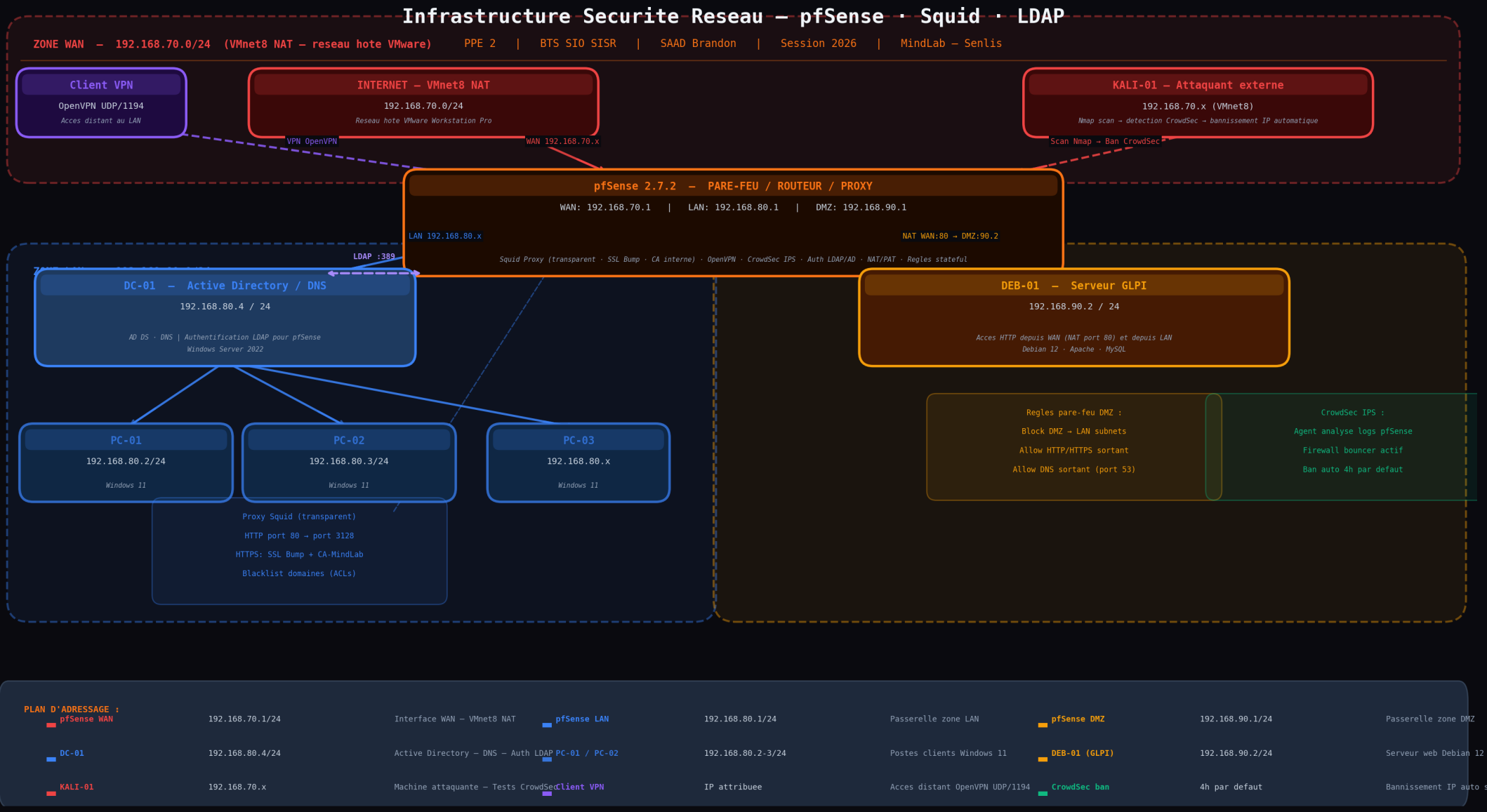
pfSense est un système d'exploitation open-source basé sur FreeBSD, spécifiquement conçu pour agir en tant que pare-feu et routeur. Il offre une large gamme de fonctionnalités : filtrage stateful, NAT, VPN (OpenVPN, IPsec, WireGuard), proxy via paquets additionnels, supervision, haute disponibilité. Sa popularité dans les PME tient à sa robustesse, à son interface Web complète et à la richesse de son écosystème de paquets.

2.5.2. Squid

Squid est un serveur proxy open-source qui agit comme un intermédiaire entre les utilisateurs internes et Internet. Il permet de mettre en cache les contenus pour accélérer la navigation, mais surtout de contrôler et journaliser le trafic Web. Couplé à une autorité de certification interne, Squid peut intercepter le trafic HTTPS (mode SSL Bump) pour appliquer des politiques de filtrage sur les domaines visités.

2.5.3. Active Directory et LDAP

L'Active Directory de Microsoft est un service d'annuaire qui centralise la gestion des comptes utilisateurs et des ressources d'un domaine Windows. Le protocole LDAP (Lightweight Directory Access Protocol) permet à pfSense d'interroger cet annuaire pour authentifier les administrateurs.



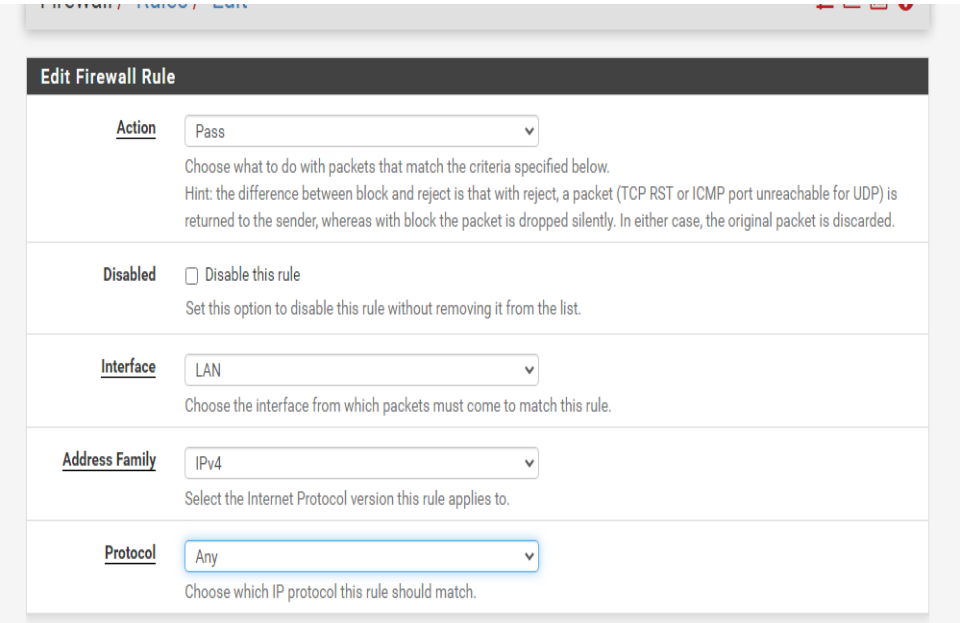
PLAN D'ADRESSAGE :

pfSense WAN	192.168.70.1/24	Interface WAN — VMnet8 NAT	pfSense LAN	192.168.80.1/24	Passerelle zone LAN	pfSense DMZ	192.168.90.1/24	Passerelle zone DMZ
DC-01	192.168.80.4/24	Active Directory — DNS — Auth LDAP	PC-01 / PC-02	192.168.80.2-3/24	Postes clients Windows 11	DEB-01 (GLPI)	192.168.90.2/24	Serveur web Debian 12 en DMZ
KALI-01	192.168.70.x	Machine attaquante — Tests CrowdSec	Client VPN	IP attribuee	Acces distant OpenVPN UDP/1194	CrowdSec ban	4h par defaut	Bannissement IP auto sur scan

Cette intégration évite la duplication des comptes et applique automatiquement les politiques de sécurité du domaine (complexité du mot de passe, désactivation, etc.).

III. Configuration initiale de pfSense

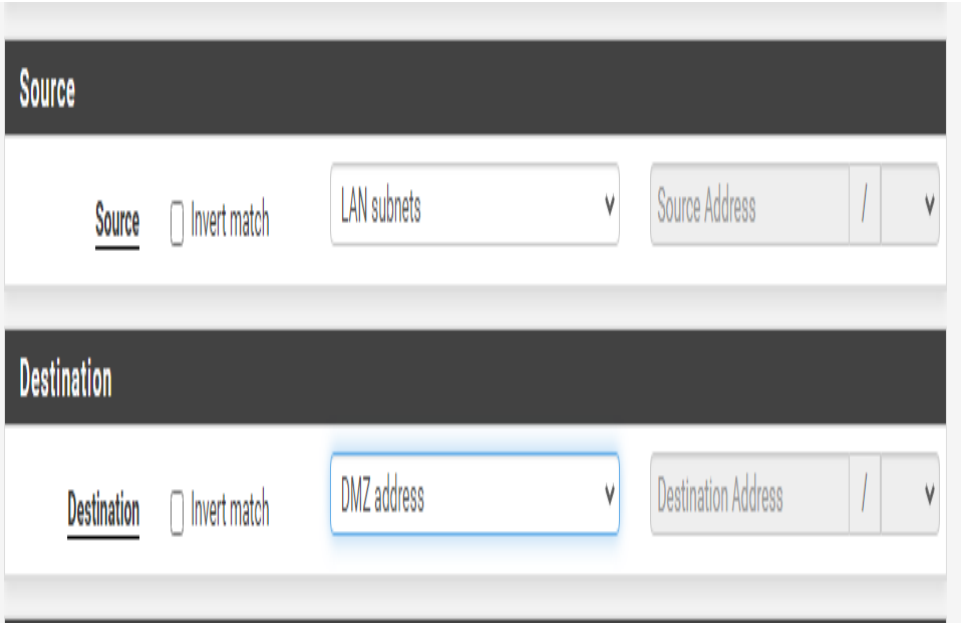
Lors du premier démarrage de la machine virtuelle pfSense, le système détecte automatiquement les interfaces réseau qui lui sont attachées. L'interface WAN est rattachée à em0 (première carte réseau, configurée en DHCP par défaut) et l'interface LAN à em1.



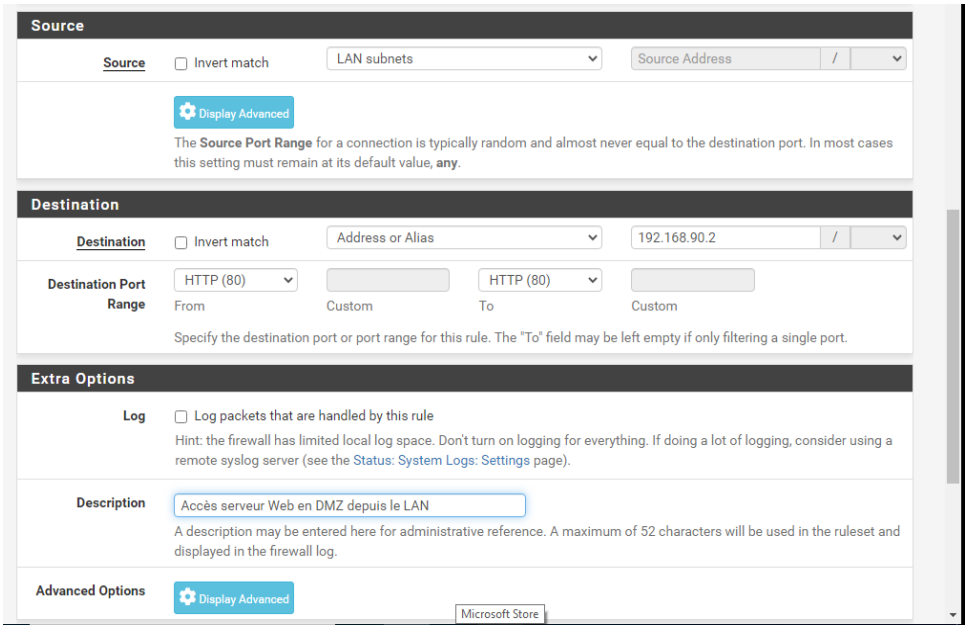
Console pfSense après démarrage : interfaces WAN et LAN détectées

L'interface WAN reçoit son adresse IP automatiquement depuis le DHCP du réseau hôte (192.168.14.128/24 dans cet exemple, qui sera ensuite remplacé par 192.168.70.1 dans la maquette finale). L'interface LAN doit en revanche être configurée manuellement avec une IP statique.

Pour modifier la configuration IP du LAN, on choisit l'option 2 (Set interface(s) IP address) dans le menu console, puis on sélectionne l'interface LAN. Le serveur DHCP n'est pas activé sur cette interface puisque l'attribution des IP sera gérée par le contrôleur de domaine.



Sélection de l'interface LAN à configurer



Saisie de l'adresse IP statique 192.168.80.1/24 pour le LAN

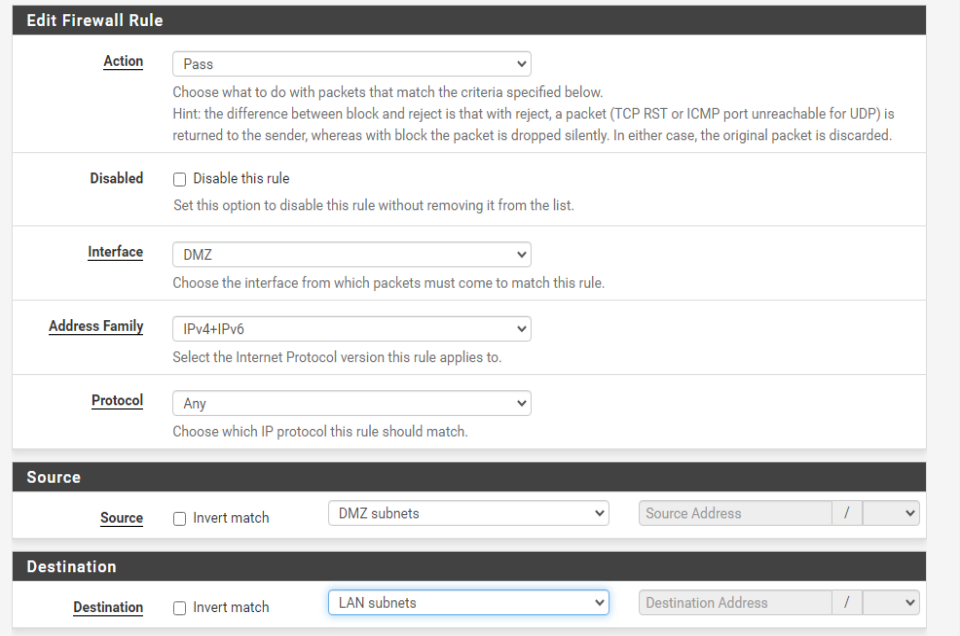
La configuration retenue pour l'interface LAN est la suivante : adresse IP 192.168.80.1, masque /24, pas de passerelle (puisque pfSense est lui-même la passerelle du LAN), pas de configuration IPv6 et pas de serveur DHCP IPv4 (le DHCP est délégué au contrôleur de domaine).

IV. Première connexion à l'interface d'administration

Une fois l'interface LAN configurée, l'interface Web d'administration de pfSense devient accessible à l'URL https://192.168.80.1/ depuis n'importe quel poste du LAN. Les identifiants par défaut sont admin / pfsense, qui devront impérativement être changés lors de l'assistant initial.

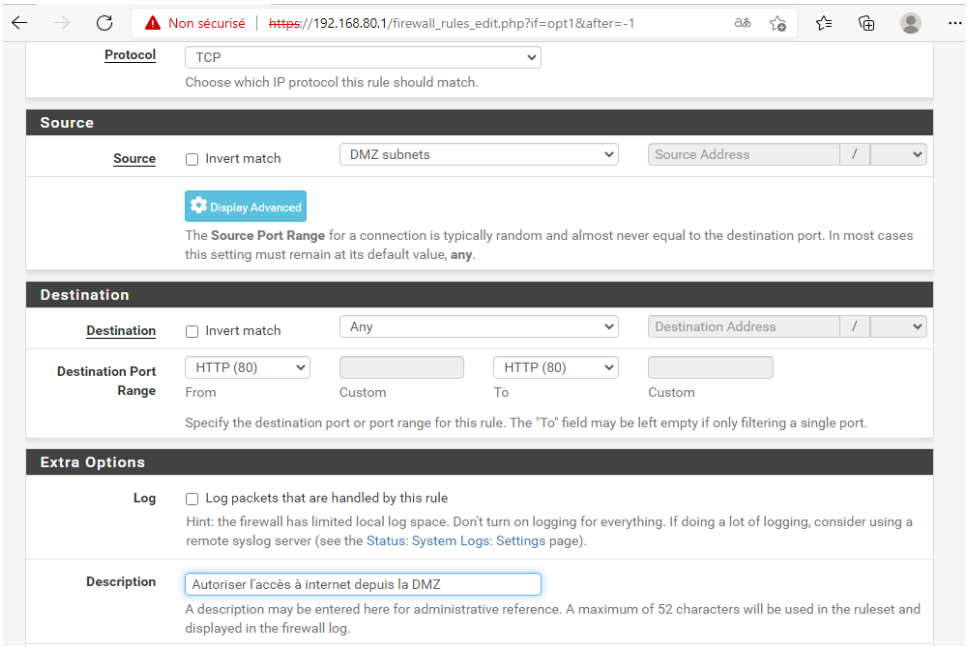
4.1. Assistant de configuration Web

L'assistant de configuration s'ouvre automatiquement à la première connexion. Il guide l'administrateur à travers plusieurs étapes : nom d'hôte, domaine, serveurs DNS, fuseau horaire, configuration de l'interface WAN puis du LAN, et enfin redéfinition du mot de passe administrateur.



Étape 1 : nom d'hôte, domaine et serveurs DNS

On configure pfSense comme nom d'hôte, home.arpa comme domaine (alternative recommandée à .local pour éviter les conflits avec mDNS), et on renseigne deux serveurs DNS : 192.168.80.4 (le contrôleur de domaine, qui hébergera le DNS interne) et 8.8.8.8 (DNS public Google en secours).



Configuration des serveurs DNS primaire et secondaire

Le fuseau horaire Europe/Paris est sélectionné pour que les logs et alertes affichent l'heure locale. Cette étape est cruciale pour la cohérence des journaux lors d'investigations ultérieures.

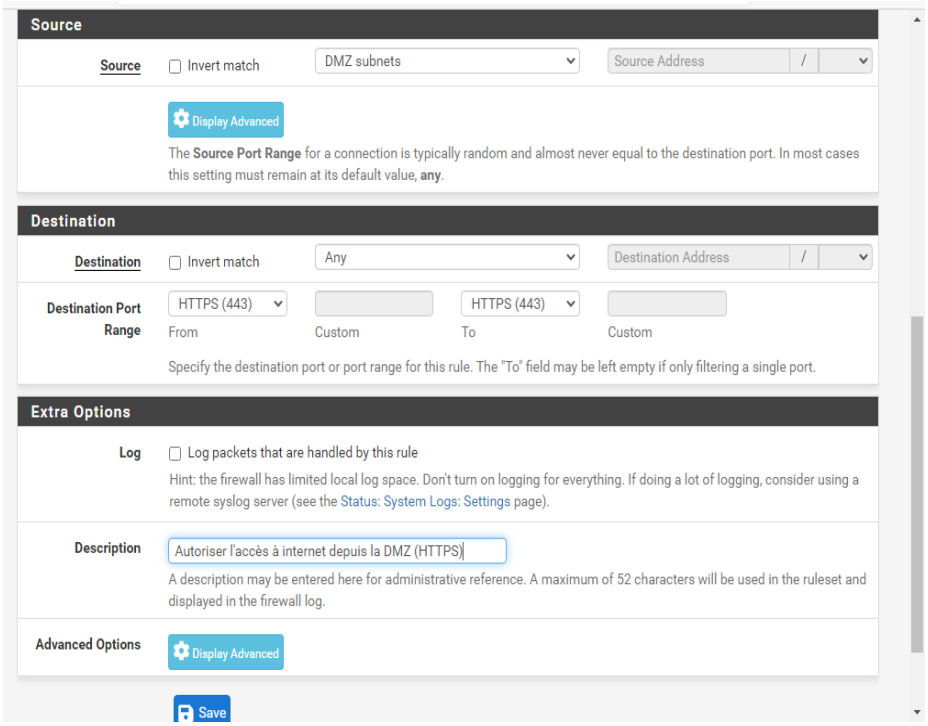
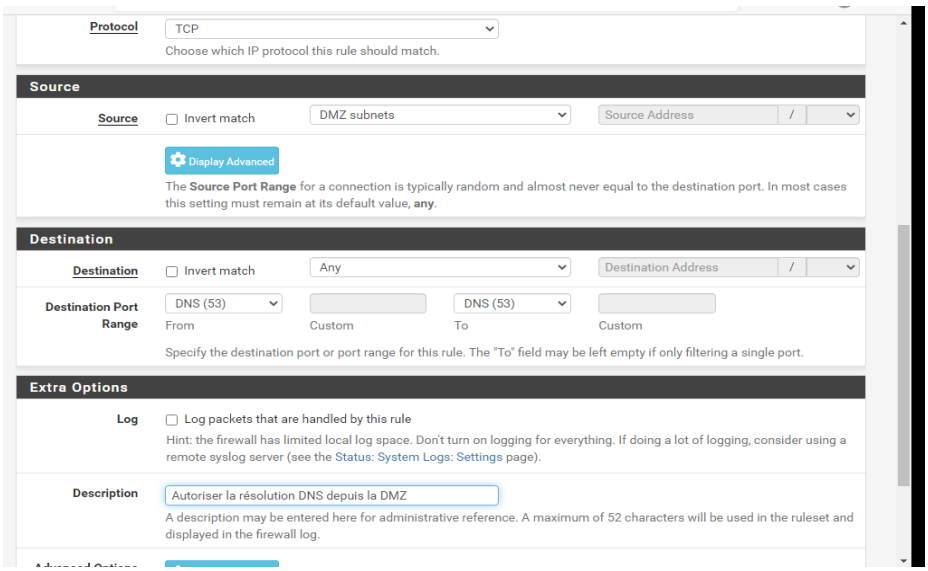


Tableau de bord pfSense après l'assistant de configuration

Le tableau de bord confirme que pfSense est opérationnel : les interfaces WAN et LAN sont actives, la version 2.7.2-RELEASE est installée et les services systèmes fonctionnent.

4.2. Ajout de l'interface DMZ

Pour héberger le serveur GLPI dans une zone isolée, il faut ajouter une troisième interface réseau à pfSense. On accède au menu Interfaces > Assignments, on associe l'interface em2 (carte réseau ajoutée au préalable dans VMware) et on l'active sous le nom DMZ.

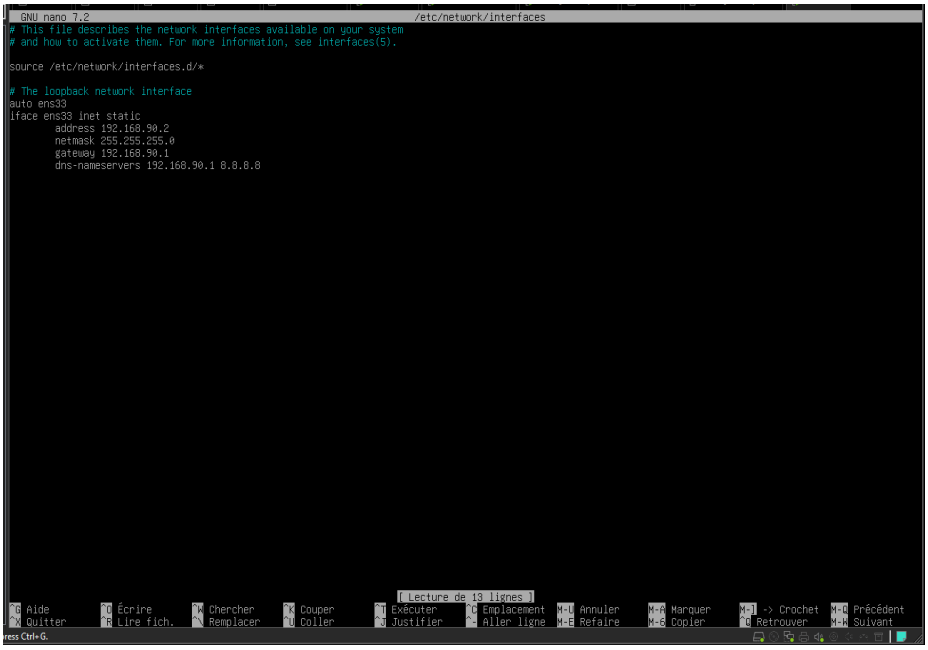


Configuration statique de l'interface DMZ en 192.168.90.1/24

Une fois la nouvelle interface activée et configurée, pfSense dispose de ses trois interfaces opérationnelles. Les règles NAT sortantes sont créées automatiquement par pfSense pour permettre aux machines du LAN et de la DMZ d'accéder à Internet via l'interface WAN.

V. Configuration des règles de pare-feu

Le pare-feu pfSense fonctionne sur un principe de filtrage stateful : il analyse l'état de chaque connexion et applique les règles définies sur chaque interface. Par défaut, tout le trafic entrant est bloqué (deny by default) et seules les règles explicitement autorisées laissent passer les paquets. Les règles sont évaluées de haut en bas dans l'ordre où elles apparaissent.



Liste des règles par défaut sur l'interface LAN

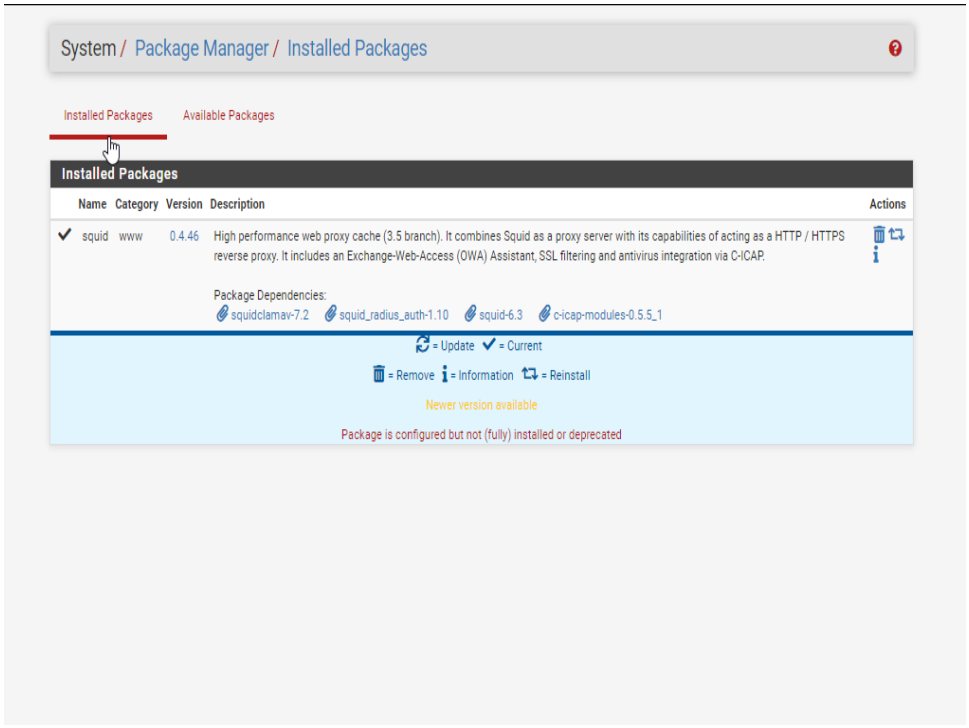
La création d'une nouvelle règle se fait via le menu Firewall > Rules, en sélectionnant l'interface concernée puis en cliquant sur Add. Pour chaque règle, on définit l'action (Pass / Block / Reject), l'interface, la famille d'adresses (IPv4/IPv6), le protocole, la source, la destination et éventuellement les ports.

5.1. Règles de l'interface WAN

Sur l'interface WAN, on autorise uniquement les flux entrants strictement nécessaires depuis l'extérieur. Une première règle autorise le protocole OpenVPN (UDP/1194) pour permettre aux utilisateurs distants de se connecter au VPN.

Règle WAN autorisant le port OpenVPN

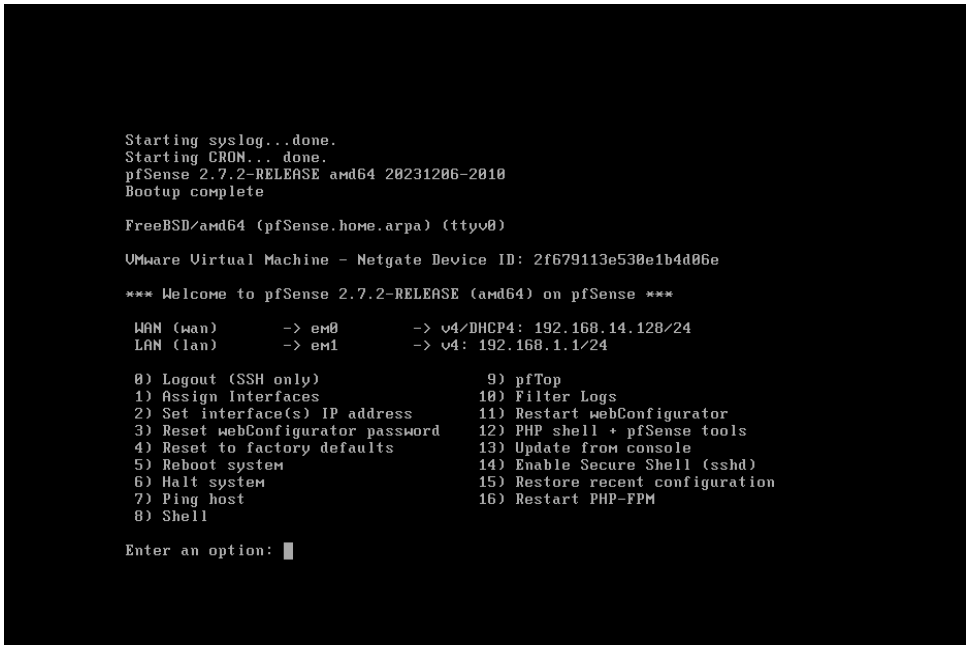
Une seconde règle redirige le trafic HTTP entrant (port 80) vers le serveur Web GLPI hébergé dans la DMZ à l'adresse 192.168.90.2. Cette règle est associée à une règle NAT (port forwarding) qui effectue la translation d'adresse de destination.



Règle NAT redirigeant le port 80 WAN vers 192.168.90.2 (GLPI)

5.2. Règles de l'interface LAN

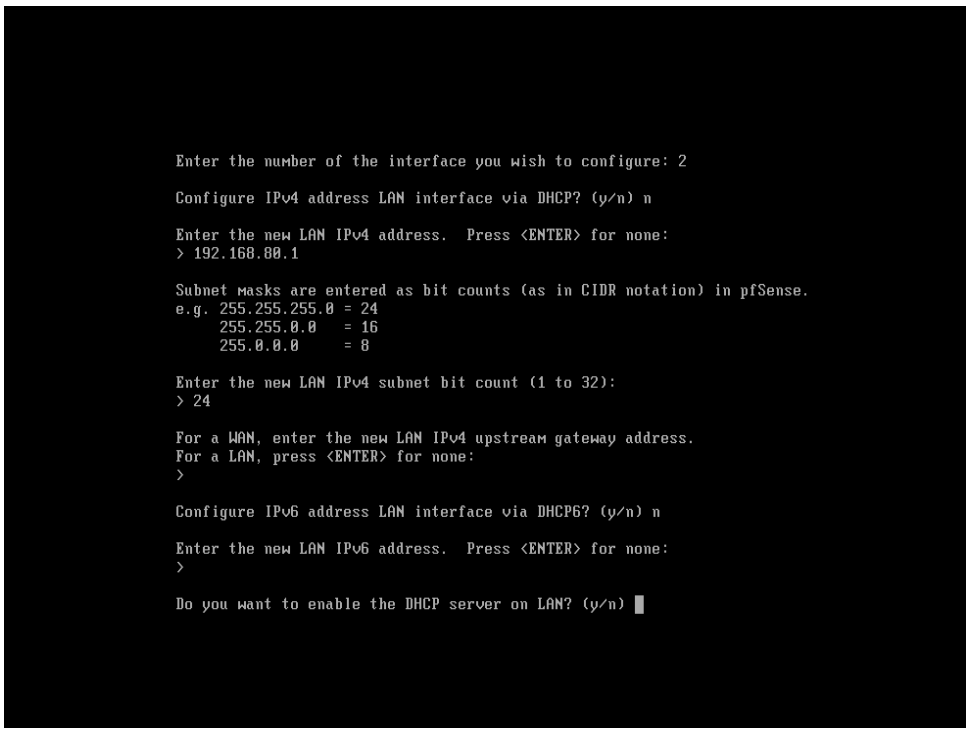
Depuis le LAN, le principe est inverse : il faut bloquer explicitement les flux indésirables tout en conservant l'autorisation par défaut vers Internet. Une première règle bloque tous les flux du LAN vers la DMZ pour empêcher un poste compromis d'attaquer directement le serveur GLPI.



Règle Block bloquant les flux LAN vers la DMZ

Source LAN subnets / Destination DMZ address

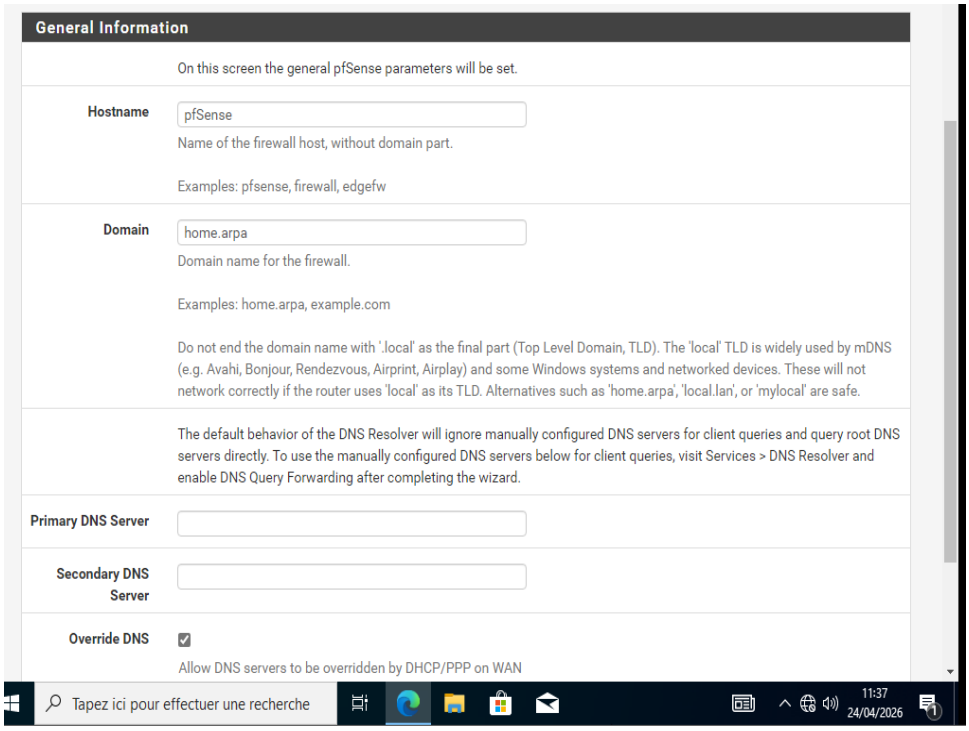
Une seconde règle, placée au-dessus de la précédente, autorise spécifiquement l'accès au serveur GLPI sur le port HTTP (80). Cette approche "liste d'autorisations" garantit que seul le service web est joignable depuis le LAN, et qu'aucun autre flux ne peut transiter du LAN vers la DMZ.



Règle autorisant uniquement le port 80 vers 192.168.90.2

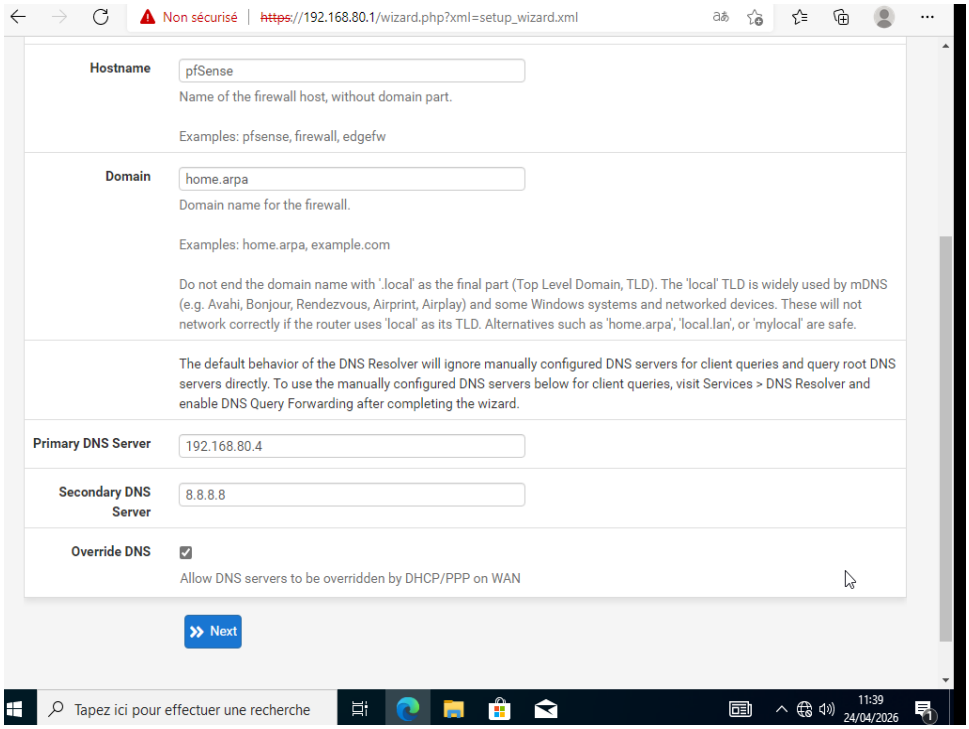
5.3. Règles de l'interface DMZ

La DMZ étant la zone la plus exposée, ses règles de sortie doivent être les plus restrictives. Une première règle bloque tout flux de la DMZ vers le LAN, afin qu'un éventuel attaquant ayant compromis le serveur GLPI ne puisse pas pivoter vers le réseau interne.

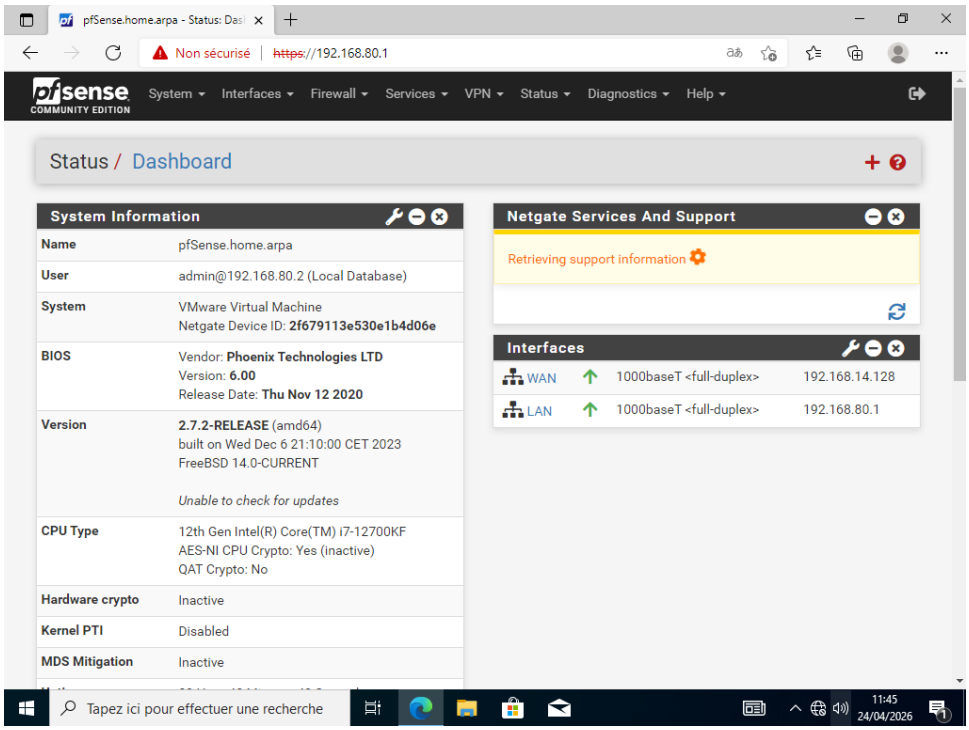


Règle Block des flux DMZ vers LAN subnets

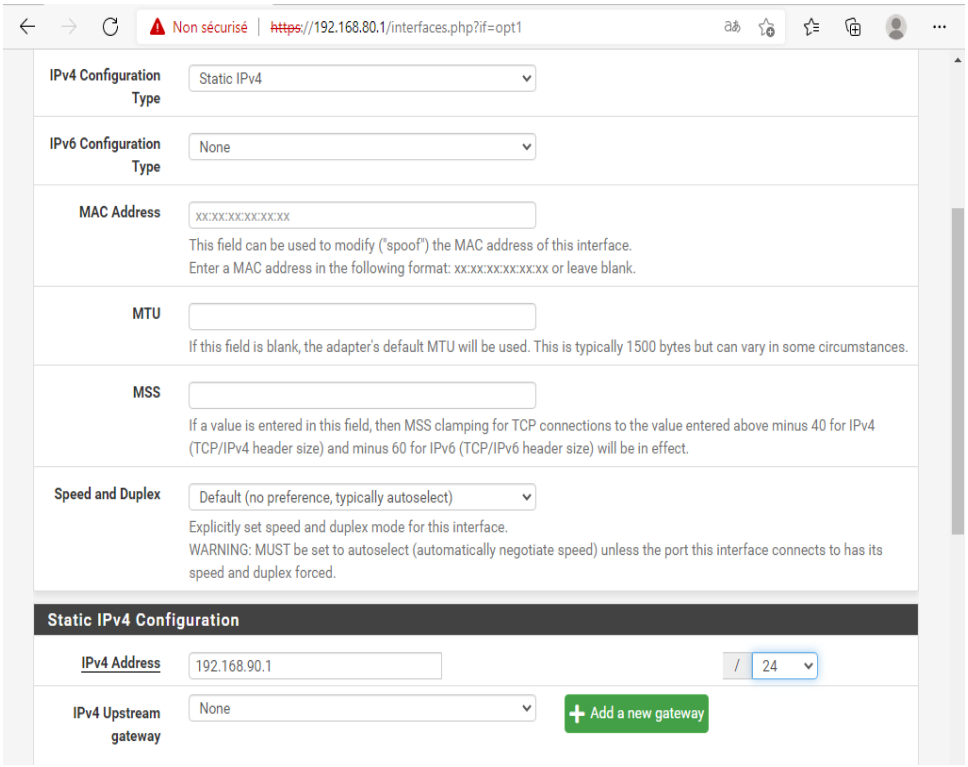
Trois règles complémentaires autorisent les flux indispensables au fonctionnement du serveur GLPI : HTTP sortant pour les mises à jour Debian, HTTPS pour la majorité des dépôts modernes, et DNS pour la résolution de noms.



Autorisation HTTP sortant depuis la DMZ



Autorisation HTTPS sortant depuis la DMZ

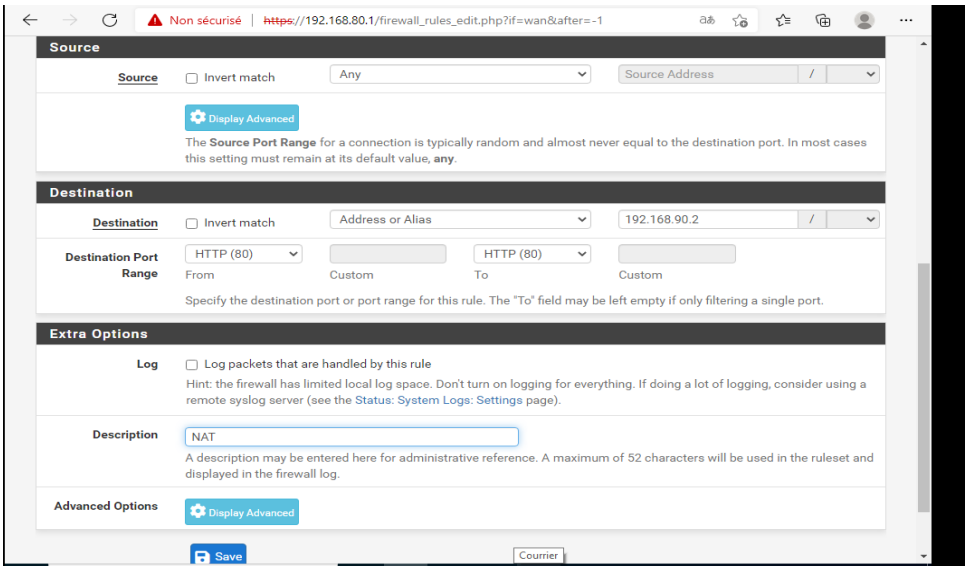


Autorisation de la résolution DNS depuis la DMZ

VI. Installation et configuration du proxy Squid

6.1. Installation du paquet

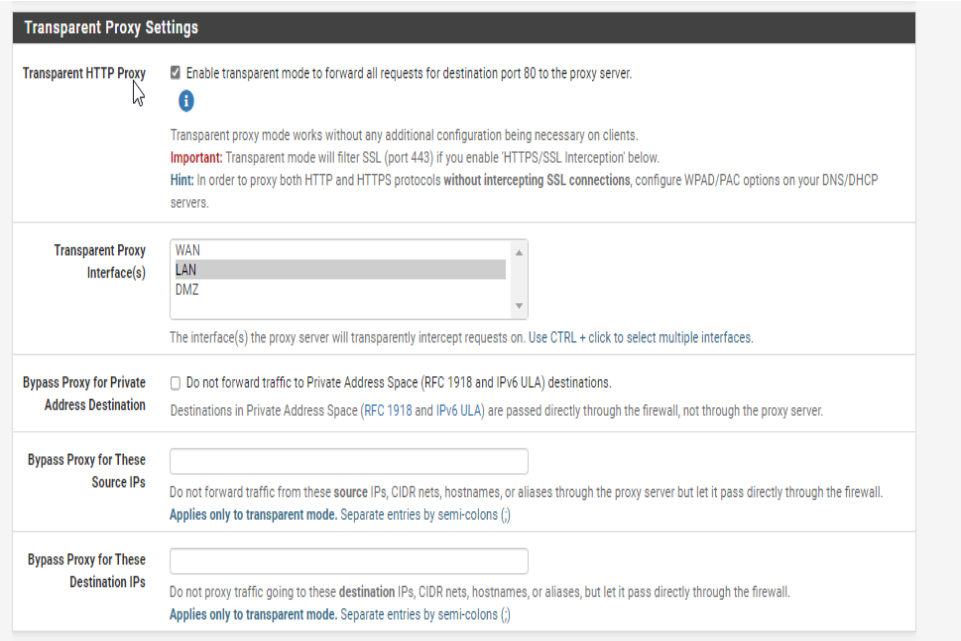
Squid s'installe comme paquet additionnel via le gestionnaire de paquets de pfSense (System > Package Manager > Available Packages). On recherche "squid" puis on clique sur Install. L'installation déploie également les dépendances : squid_radius_auth, c-icap-modules et squidclamav.



Paquet Squid installé dans pfSense

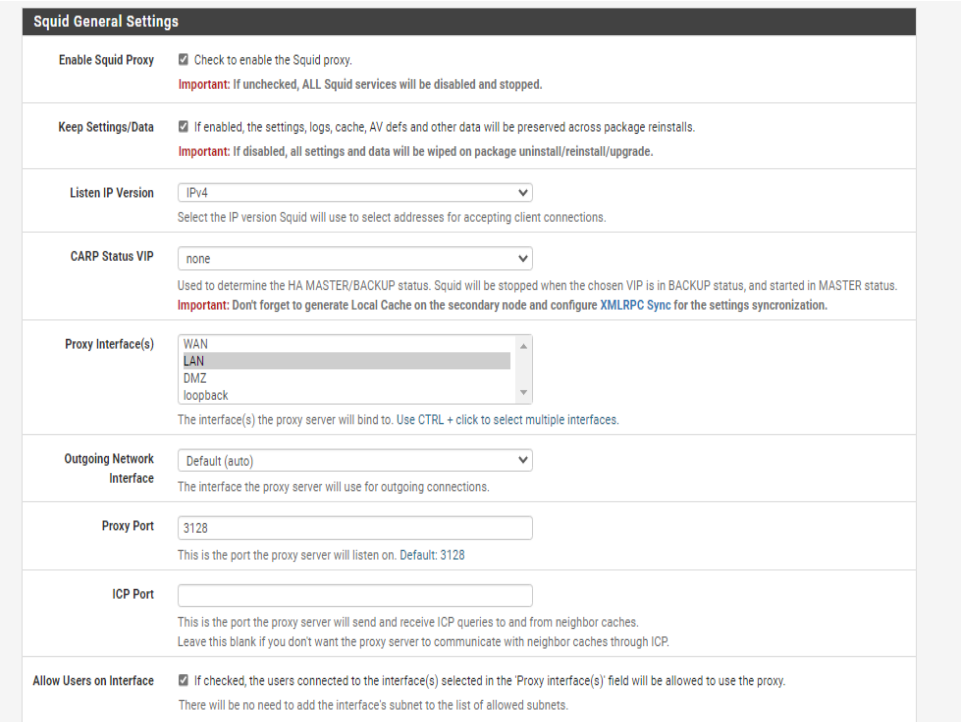
6.2. Configuration générale

La configuration de Squid s'effectue via le menu Services > Squid Proxy Server. Avant d'activer le proxy, il faut d'abord visiter l'onglet Local Cache et cliquer sur Save : sans cette étape, le démon Squid refuse de démarrer car le répertoire de cache n'est pas initialisé.



Activation du proxy Squid sur les interfaces LAN

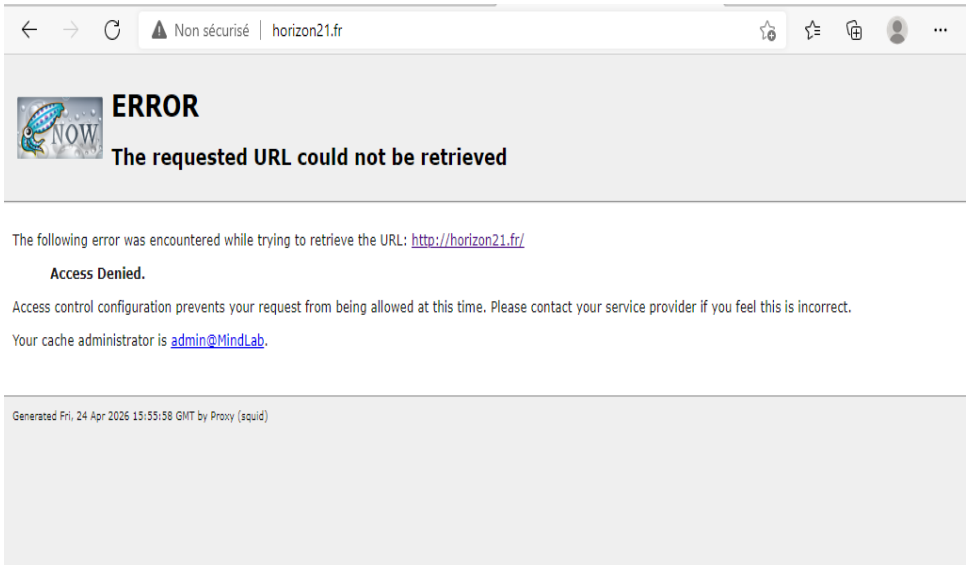
Dans l'onglet General, on coche Enable Squid Proxy, on sélectionne l'interface LAN dans Proxy Interface(s), on conserve le port par défaut 3128, et on coche Allow Users on Interface pour autoriser tous les postes du LAN à utiliser le proxy sans déclaration manuelle.



Paramètres généraux Squid : interface LAN, port 3128

6.3. Mode proxy transparent

Le mode transparent permet d'intercepter automatiquement tout le trafic HTTP des clients sans nécessiter de configuration manuelle du navigateur ou du système. On active l'option Transparent HTTP Proxy et on sélectionne l'interface LAN comme interface de capture.



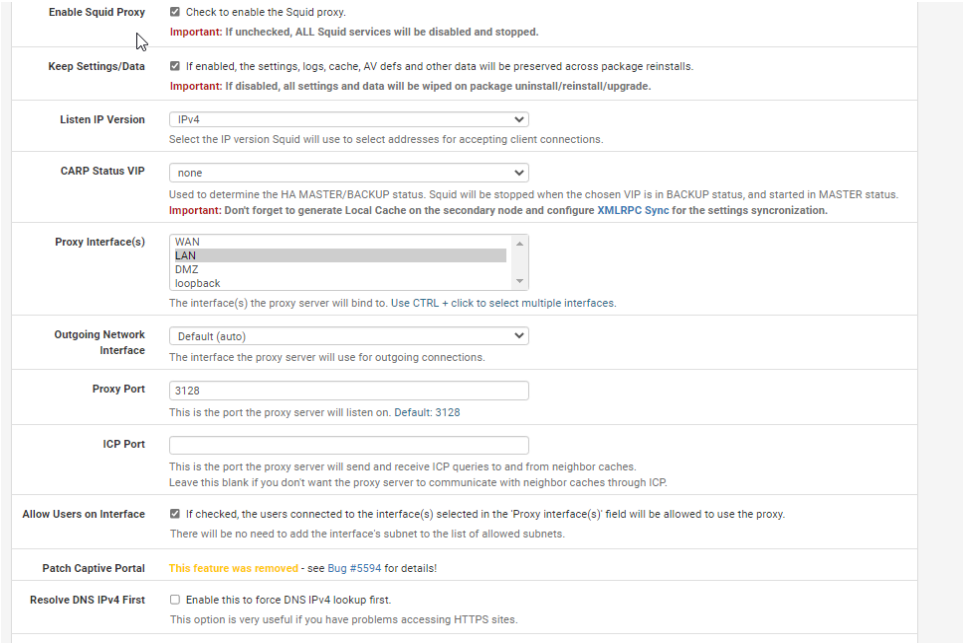
Activation du mode proxy transparent sur l'interface LAN

Concrètement, pfSense crée automatiquement une règle NAT en arrière-plan qui redirige tous les paquets à destination du port 80 issus du LAN vers le port 3128 de Squid. Le navigateur du client n'a aucune connaissance de l'existence du proxy.

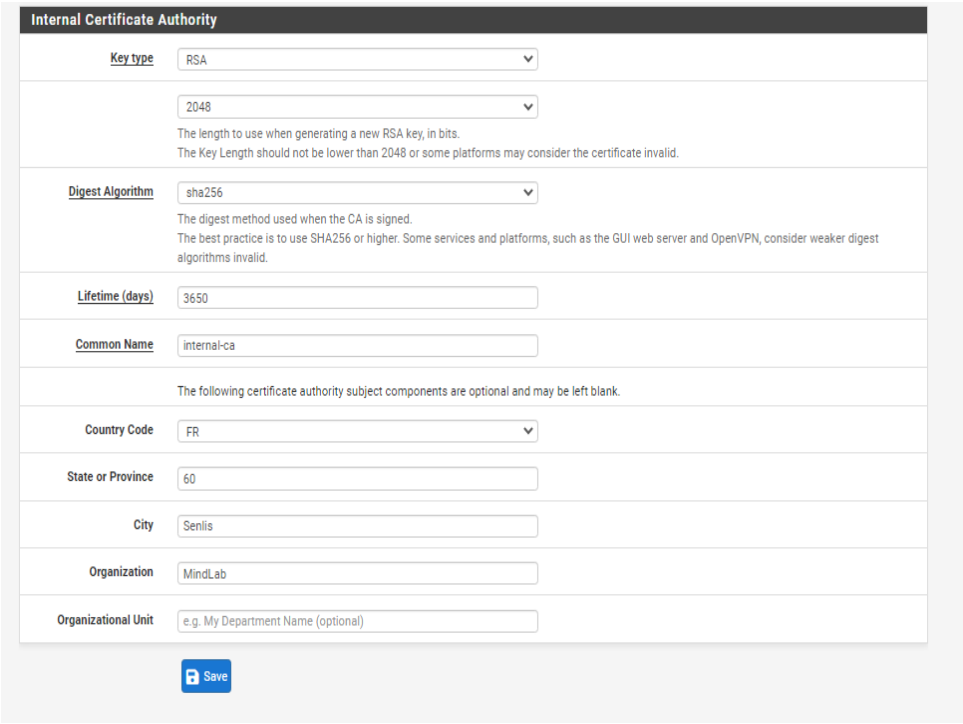
VII. Test du proxy transparent et filtrage

7.1. Mise en place d'une blacklist

Pour valider le bon fonctionnement du proxy, on configure une blacklist via l'onglet ACLs de Squid. On y ajoute le domaine horizon21.fr (site en HTTP simple, idéal pour le test sans encore traiter le HTTPS).



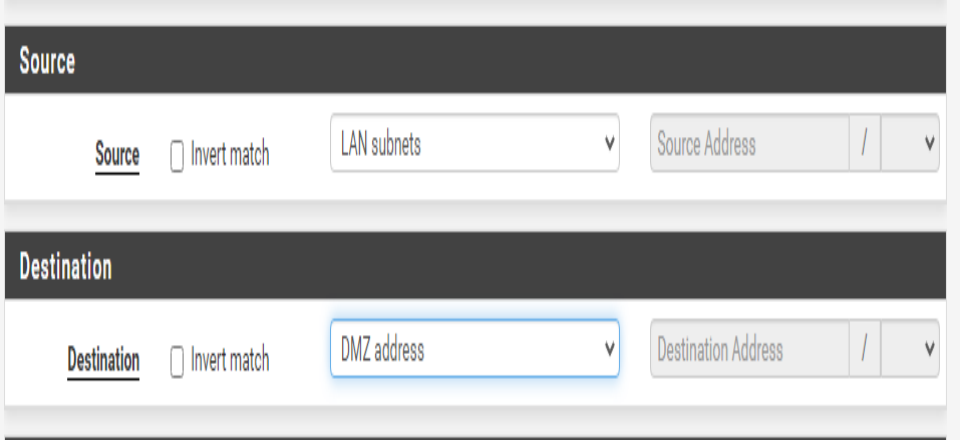
Onglet ACLs de Squid avec liste des sous-réseaux autorisés



Ajout du domaine horizon21.fr dans la blacklist

7.2. Validation du filtrage HTTP

Depuis un poste client du LAN, la tentative d'accès au site bloqué retourne immédiatement une page d'erreur générée par Squid : "ERROR — The requested URL could not be retrieved" avec le motif Access Denied. Cette page confirme que le trafic transite bien par le proxy et que la règle de filtrage est appliquée.



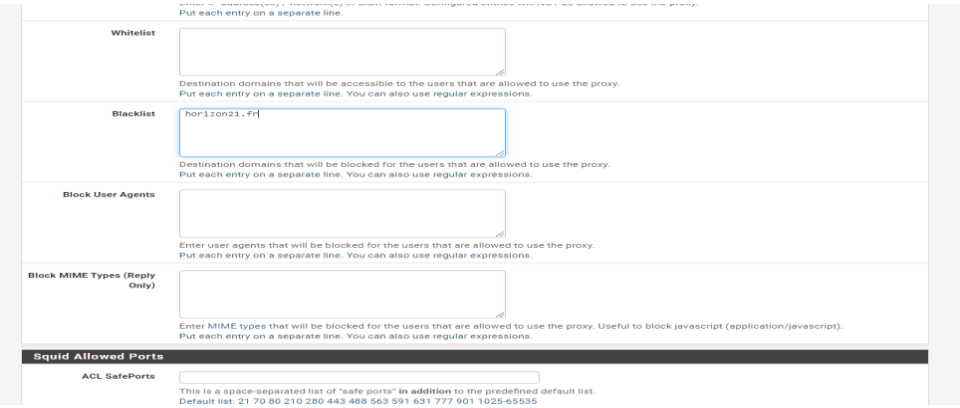
Page d'erreur Squid : accès au domaine bloqué refusé

VIII. Filtrage HTTPS avec interception SSL

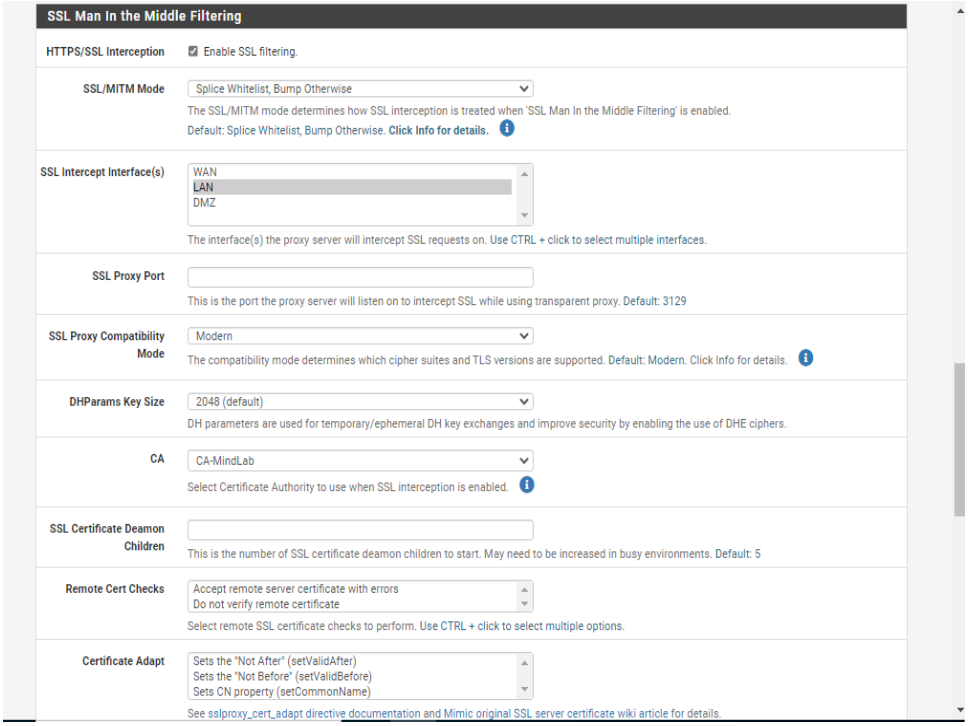
À ce stade, le proxy ne filtre que le trafic HTTP. Or, plus de 95% du trafic Web actuel est en HTTPS. Pour étendre le filtrage au HTTPS, il faut activer le mode SSL Bump (interception SSL), qui nécessite la création d'une autorité de certification interne.

8.1. Création de l'autorité de certification

L'autorité de certification (CA) interne est créée via System > Cert. Manager > CAs > Add. Elle servira à signer les certificats que Squid présentera aux clients à la place des certificats originaux des sites visités.



Création de l'autorité de certification CA-MindLab

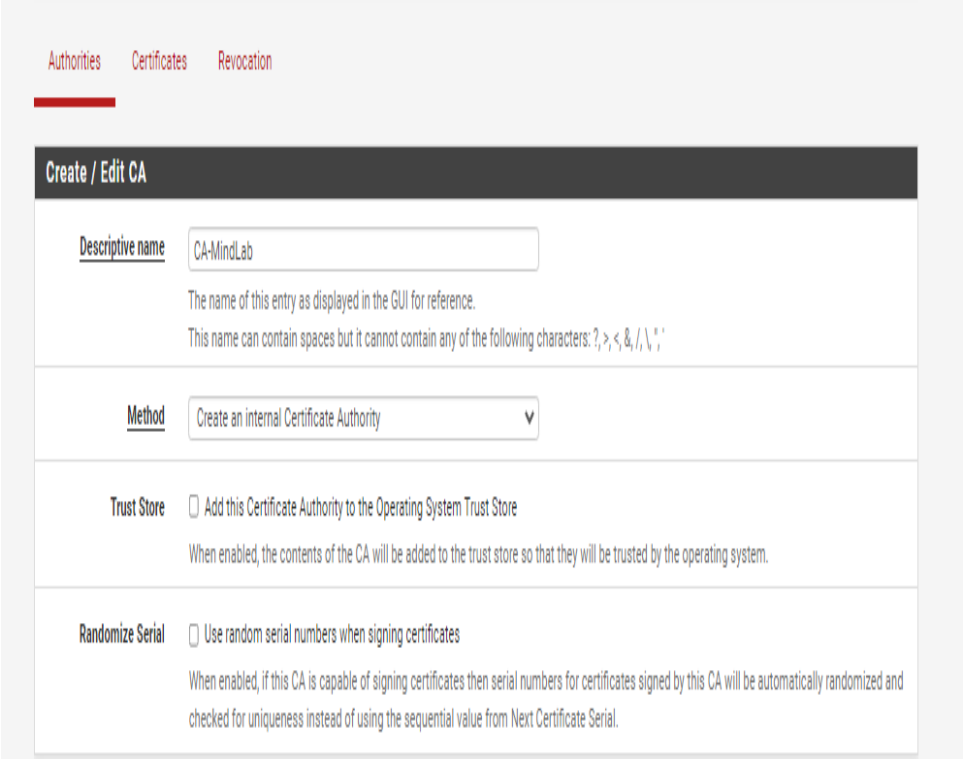


Paramètres de la CA interne : RSA 2048 bits, SHA-256, validité 10 ans

Les paramètres retenus pour la CA sont : type de clé RSA 2048 bits (équilibre sécurité/performance), algorithme de signature SHA-256, durée de vie 10 ans (3650 jours), et localisation à Senlis pour cohérence avec MindLab.

8.2. Activation du SSL Bump

Dans la configuration Squid, l'option Enable SSL filtering active l'interception. Le mode SSL/MITM retenu est Splice Whitelist, Bump Otherwise : les sites de la liste blanche sont laissés en chiffrement direct (cas des sites bancaires sensibles), tous les autres passent par l'inspection SSL.



Configuration du SSL Man In The Middle Filtering avec CA-MindLab

8.3. Ajustement de la résolution DNS

Pour que le proxy transparent HTTPS fonctionne correctement, le DNS du domaine doit transmettre ses requêtes via pfSense. Sur le contrôleur de domaine, on ajoute pfSense (192.168.80.1) comme redirecteur DNS dans les propriétés du serveur DNS. Sans cette étape, certains sites HTTPS retournent une erreur ERR_SSL_PROTOCOL_ERROR.

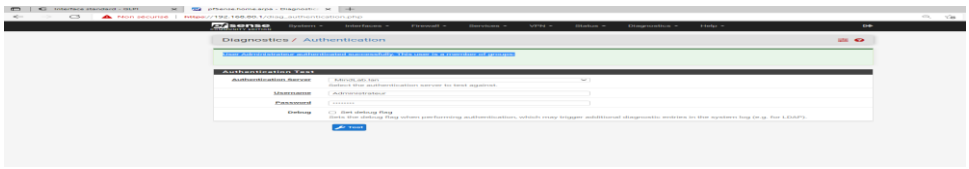
8.4. Validation du blocage HTTPS

On ajoute un domaine HTTPS (par exemple un réseau social) à la blacklist Squid, puis on tente d'y accéder depuis un poste client. Le navigateur affiche désormais un avertissement de certificat (signé par CA-MindLab et non par l'autorité originale du site), confirmant que l'interception SSL fonctionne et que la règle de blocage est bien appliquée.

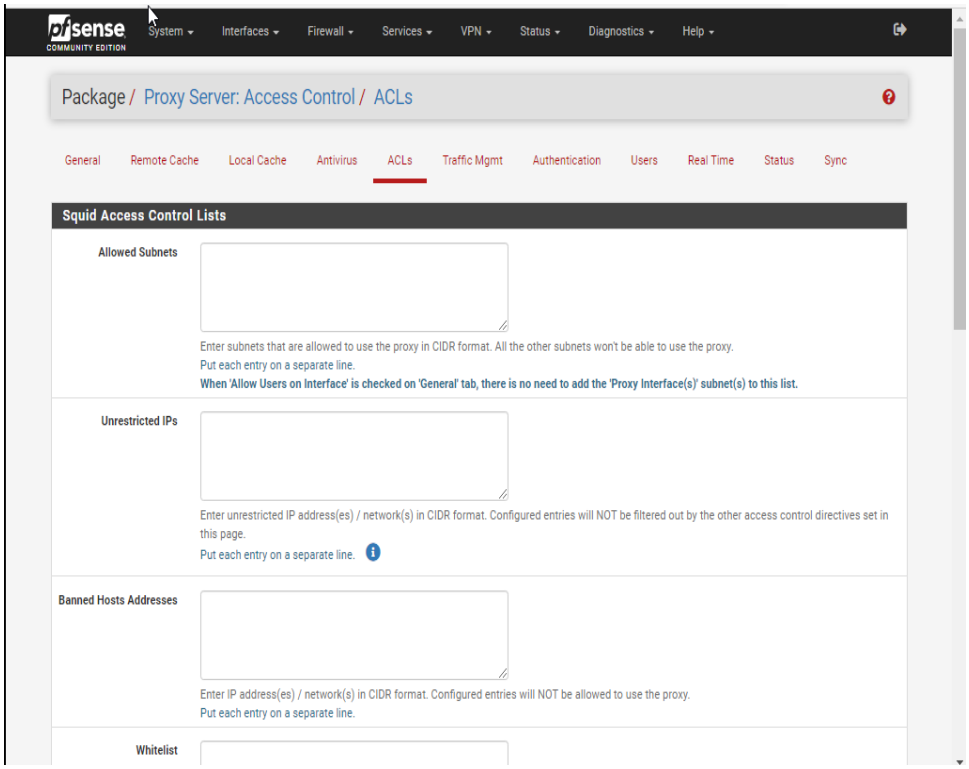
IX. Liaison LDAP avec l'Active Directory

9.1. Configuration du serveur d'authentification

La liaison LDAP permet d'authentifier les administrateurs de pfSense avec leurs comptes Active Directory, évitant la duplication des comptes. La configuration s'effectue via System > User Manager > Authentication Servers > Add.



Création du serveur d'authentification MindLab.lan de type LDAP



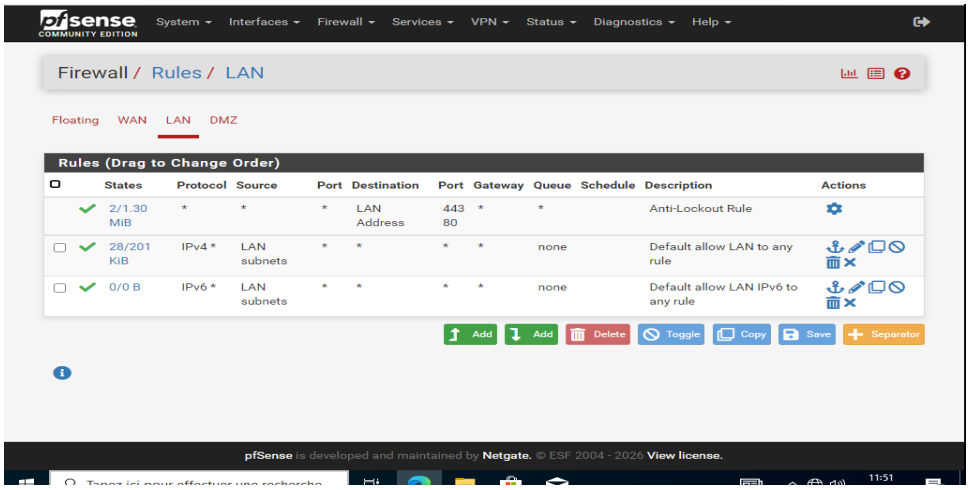
Paramètres LDAP : adresse, port 389, transport TCP, Base DN

Les paramètres clés sont : Hostname 192.168.80.4 (adresse du contrôleur de domaine), port 389 (LDAP non chiffré pour la maquette ; en production on privilégiera LDAPS sur 636), Base DN DC=MindLab,DC=lan correspondant à la racine de l'annuaire.

Le compte de service utilisé pour les requêtes (Bind credentials) est CN=pfsense.MindLab,pfSense,DC=MindLab,DC=lan. Ce compte technique est créé spécifiquement dans l'AD avec les seuls droits de lecture nécessaires.

9.2. Test de l'authentification

Le test de l'authentification s'effectue via Diagnostics > Authentication. On sélectionne le serveur MindLab.lan, on saisit un identifiant et un mot de passe utilisateur valide du domaine, puis on clique sur Test.



Test d'authentification réussi : utilisateur Administrateur authentifié

Le message "User Administrateur authenticated successfully" confirme que pfSense parvient à interroger l'AD, à trouver l'utilisateur et à valider son mot de passe. La liaison LDAP est opérationnelle.

9.3. Bascule de l'authentification système

Pour que la connexion à l'interface Web pfSense utilise l'AD au lieu de la base locale, on définit MindLab.lan comme serveur d'authentification dans System > User Manager > Settings. Désormais, les administrateurs se connectent avec leurs comptes du domaine.

X. Configuration de CrowdSec

CrowdSec est un IPS (Intrusion Prevention System) open-source et communautaire qui vient compléter le filtrage stateful de pfSense par une détection comportementale. Il analyse en temps réel les journaux du pare-feu pour repérer les comportements suspects (scans de ports, tentatives de force brute, exploitation de vulnérabilités) et bannit automatiquement les adresses IP malveillantes via le firewall bouncer.

10.1. Installation du paquet CrowdSec

L'installation s'effectue depuis le gestionnaire de paquets de pfSense, via le menu System > Package Manager > Available Packages. On recherche "crowdsec" puis on clique sur Install. Le paquet déploie à la fois l'agent CrowdSec (analyse des logs), la Local API (LAPI) et le firewall bouncer qui applique les décisions de blocage.

10.2. Paramétrage de CrowdSec

La configuration s'effectue via Services > CrowdSec. CrowdSec est livré préconfiguré et opérationnel dès l'installation, ce qui constitue un atout majeur pour un déploiement rapide. Les options activées par défaut sont :

- Remediation component (firewall bouncer) : Enable coché — alimente les blocklists du pare-feu pfSense

- Log processor (CrowdSec agent) : Enable coché — lit les logs de pfSense et de ses paquets pour détecter les menaces
- Local API : Enable coché — expose une API locale sur 127.0.0.1:8080 pour la communication interne entre l'agent et le bouncer

Aucune modification n'est strictement nécessaire pour démarrer ; il suffit de cliquer sur Save si la configuration n'est pas déjà appliquée. Pour des environnements plus complexes (plusieurs pfSense en cluster), on peut exposer la LAPI sur l'IP du LAN au lieu de 127.0.0.1.

10.3. Vérification du statut

Le bon fonctionnement de CrowdSec se contrôle dans Status > CrowdSec Status. L'onglet Machines doit afficher l'entrée "pfsense" en statut Validé, ce qui confirme que l'agent communique correctement avec la LAPI. L'onglet Bouncers doit lister "pfsense-firewall" en valide, signe que le firewall bouncer est bien enregistré et prêt à appliquer les décisions de blocage.

Les onglets Alerts et Decisions permettent ensuite de visualiser respectivement les détections en temps réel et les bannissements actifs. À ce stade, ils sont vides, ce qui est attendu en l'absence de trafic suspect.

XI. Kali Linux — Tests de sécurité

Pour valider l'efficacité de CrowdSec dans un scénario réaliste, on déploie une machine virtuelle Kali Linux jouant le rôle d'attaquant externe. Kali est une distribution dédiée aux tests d'intrusion qui embarque tous les outils nécessaires : Nmap pour la cartographie réseau, Hydra pour les attaques par dictionnaire, Metasploit pour l'exploitation de vulnérabilités, etc.

11.1. Création de la VM Kali

La machine Kali est déployée dans VMware avec les paramètres suivants : système invité Debian 12.x 64 bits, nom KALI-01, 2 vCPU et 4 Go de RAM, disque de 80 Go. Le point critique est le choix de l'interface réseau : VMnet8 (NAT), c'est-à-dire le même réseau que l'interface WAN de pfSense. Cela simule un attaquant externe qui tenterait d'atteindre l'entreprise depuis Internet.

L'installation de Kali suit la procédure standard : choix de la langue, partitionnement automatique, création du compte utilisateur (login : quentin, mot de passe : Kz747bt!) et installation de l'environnement graphique XFCE (léger et adapté à une machine de test).

11.2. Simulation d'un scan de ports avec Nmap

Nmap est l'outil de référence pour cartographier un réseau et identifier les services exposés sur une machine cible. Un scan de ports est typiquement la première étape d'une attaque réelle : l'attaquant cherche à identifier les services vulnérables avant de tenter une exploitation.

Depuis le terminal Kali, on lance la commande suivante pour scanner l'interface WAN de pfSense :

```
nmap -Pn 192.168.70.1
```

L'option -Pn désactive la phase préliminaire de découverte par ping, qui pourrait être bloquée par pfSense. L'IP 192.168.70.1 doit être remplacée par l'IP WAN réelle de pfSense, visible dans Status > Interfaces (elle dépend du DHCP du réseau VMnet8 NAT).

11.3. Vérification de la détection par CrowdSec

Quelques secondes après le lancement du scan, on retourne sur l'interface pfSense dans Status > CrowdSec Status > Decisions. L'IP de la machine Kali apparaît dans la liste des bannissements, accompagnée du motif "firewallservices/pf-scan-multi_ports" qui correspond au scénario CrowdSec déclenché par la détection d'un scan de ports multiple sur un même hôte.

La durée du ban par défaut est de 4 heures, ce qui suffit largement à décourager un attaquant automatisé tout en limitant le risque de blocage légitime en cas de faux positif. Pendant cette période, toute tentative de connexion depuis l'IP bannie est bloquée par pfSense avant même d'atteindre les services exposés.

Ce test démontre que la chaîne CrowdSec → firewall bouncer → règles pfSense fonctionne de bout en bout : la détection comportementale identifie l'attaque, la décision de blocage est propagée à pfSense, et la règle de pare-feu correspondante est appliquée automatiquement, sans aucune intervention humaine.

XII. Compétences BTS SIO mobilisées

Ce projet mobilise les compétences du bloc 2 du référentiel BTS SIO option SISR : "Administration des systèmes et des réseaux". Le tableau ci-dessous synthétise les compétences travaillées et les sections du dossier qui en attestent.

Compétence	Mise en œuvre dans le projet
Concevoir une solution d'infrastructure réseau	Choix de l'architecture en trois zones (LAN/DMZ/WAN), définition du plan d'adressage IP, sélection des solutions techniques (pfSense, Squid, OpenVPN, CrowdSec), rédaction du cahier des charges (sections II et III).
Installer, tester et déployer une solution d'infrastructure réseau	Installation de pfSense 2.7.2 sur VMware, configuration des trois interfaces réseau, déploiement des paquets Squid et CrowdSec, création de l'autorité de certification interne, mise en place du VPN OpenVPN (sections III à VIII et X).
Exploiter, dépanner et superviser une solution d'infrastructure réseau	Définition et application des règles de pare-feu sur les trois interfaces, gestion des ACLs Squid, supervision via les logs pfSense, Squid et CrowdSec, dépannage de l'erreur ERR_SSL_PROTOCOL_ERROR rencontrée lors du paramétrage HTTPS (sections V, VII, VIII et X).
Gérer le patrimoine informatique	Documentation complète de la configuration, traçabilité des accès via journalisation Squid et CrowdSec, intégration LDAP pour la gestion centralisée des comptes administrateurs (sections IX et X).
Assurer la cybersécurité d'une solution d'infrastructure	Segmentation réseau LAN/DMZ, principe du moindre privilège dans les règles de pare-feu, interception SSL pour le filtrage HTTPS, authentification centralisée via Active Directory, détection

Compétence	Mise en œuvre dans le projet
	comportementale des attaques avec CrowdSec, validation par tests d'intrusion depuis Kali Linux (sections V, VIII, IX, X et XI).

XIII. Conclusion

À l'issue de ce projet, l'entreprise MindLab dispose d'une infrastructure de sécurité réseau complète, multicouche et validée par des tests d'intrusion. Le pare-feu pfSense filtre tous les flux entre les zones LAN, DMZ et Internet selon le principe du moindre privilège : seuls les flux explicitement autorisés transitent, et la segmentation réseau cantonne un éventuel attaquant à la zone qu'il aurait compromise.

Le proxy Squid apporte une couche de contrôle applicatif sur la navigation Web. Grâce à l'interception SSL via une autorité de certification interne, il filtre aussi bien le HTTP que le HTTPS, journalise toutes les requêtes pour la traçabilité, et applique des listes blanches et noires en fonction de la politique de l'entreprise. La liaison LDAP avec l'Active Directory complète le dispositif en centralisant l'authentification des administrateurs sur leurs comptes du domaine.

CrowdSec ajoute une dimension proactive et comportementale à cette défense périmétrique. Là où pfSense applique des règles statiques et où Squid filtre des domaines connus, CrowdSec détecte les comportements suspects (scans de ports, force brute, exploitation de CVE) et bannit dynamiquement les IP malveillantes. Les tests menés depuis Kali Linux ont validé l'intégration de bout en bout : un simple scan Nmap a déclenché une décision de bannissement automatique, propagée du moteur CrowdSec aux règles du pare-feu pfSense en quelques secondes.

Plusieurs axes d'amélioration peuvent être envisagés pour une mise en production. D'abord, le passage à LDAPS (LDAP sur SSL) renforcerait la confidentialité des échanges entre pfSense et l'Active Directory. Ensuite, la connexion de CrowdSec à la communauté centrale (CAPI) permettrait de bénéficier des blocklists collaboratives mondiales en plus des détections locales. Enfin, la mise en haute disponibilité de pfSense via CARP éviterait toute interruption de service en cas de panne du pare-feu principal, et le déploiement d'un IDS comme Suricata viendrait compléter CrowdSec sur la détection des charges malveillantes au niveau paquet.

Sur le plan personnel, ce projet a été l'occasion d'approfondir des compétences techniques essentielles au métier de technicien systèmes et réseaux : conception d'architecture sécurisée, manipulation fine du filtrage stateful, gestion de PKI interne, intégration entre solutions open-source et environnement Microsoft, et démarche de validation par tests offensifs. Les difficultés rencontrées (notamment l'erreur SSL lors du proxy transparent HTTPS) ont également été formatrices, en exigeant une démarche méthodique de diagnostic et de résolution. Ce PPE m'a permis de mettre en pratique l'ensemble des compétences du bloc SISR dans un scénario proche de la réalité professionnelle.