BTS Services informatiques aux organisations - SISR

Session 2026

E4 – Support et mise à disposition de services informatiques

Coefficient 4

DESCRIPTION DE LA REALISATION PROFESSIONNELLE

NOM et prénom du candidat : Aoudani Noeh	

Contexte de la réalisation professionnelle

L'entreprise dispose d'une infrastructure informatique virtualisée sous environnement VMware ESXi, hébergeant plusieurs services internes et exposés sur Internet (web, messagerie, cloud).
Avec l'évolution des besoins, notamment l'ajout de services accessibles depuis l'extérieur, il est devenu nécessaire de sécuriser les flux réseau tout en garantissant leur accessibilité.
L'absence de segmentation réseau et de filtrage avancé pouvait entraîner des risques de sécurité, notamment en cas d'exposition directe des serveurs.
La problématique était donc de mettre en place une solution permettant de contrôler les accès, isoler les différents environnements (clients, serveurs, DMZ) et sécuriser les communications.
Pour répondre à ce besoin, une solution basée sur le pare-feu pfSense a été déployée afin d'assurer le routage, la segmentation réseau via VLAN, la gestion des règles firewall et la publication sécurisée des services.
Cette solution permet également de proposer un accès distant sécurisé grâce à la mise en place d'un VPN.

Intitulé de la réalisation professionnelle

Mise en place et sécurisation d'une infrastructure réseau segmentée avec pfSense

Période de réalisation : Février 2026 **Lieu : Joigny**
Modalité : Individuelle

Principale(s) activité(s) concernée(s) :
Gérer le patrimoine informatique
Mettre à disposition des utilisateurs un service informatique
Organiser son développement professionnel

Conditions de réalisation

- **Ressources présentes Environnement virtualisé sous VMware ESXi**

Réseau interne non segmenté ou peu sécurisé

Services hébergés nécessitant un accès externe (web, mail)

Absence de pare-feu centralisé avancé

- **Résultats attendus**

Mise en place d'un pare-feu pfSense fonctionnel
Segmentation du réseau via VLAN

Configuration des règles de filtrage (firewall)

Publication sécurisée des services via NAT

Mise en place d'un accès distant sécurisé (VPN)

- **Durée de réalisation 5 jours**

Modalités d'accès à cette réalisation professionnelle.
https://site.jjba.fr. Compte d'accès : aucun. Mot de passe : BTSsiosisr

Partie 1 – Procédure de mise en œuvre.

L'infrastructure mise en place repose sur l'utilisation d'un pare-feu **pfSense** virtualisé sous environnement **VMware ESXi**.

Ce pare-feu constitue le point central de l'architecture réseau et assure :

- le routage inter-VLAN
- la sécurisation des flux entrants et sortants
- la gestion des accès distants via VPN
- la publication des services hébergés en DMZ

L'architecture réseau est segmentée en plusieurs VLANs afin d'isoler les différents types de flux :

- **VLAN 10 – Administration / Tools** : 10.89.10.0/24
- **VLAN 20 – Serveurs** : 10.89.20.0/24
- **VLAN 30 – Stockage** : 10.89.30.0/28
- **VLAN 40 – DMZ** : 10.89.40.0/28
- **VLAN Clients** : 10.89.89.0/24
- **Réseau VPN** : 10.89.5.0/24

Le réseau global interne est défini en **10.89.0.0/16**.

Le pare-feu pfSense dispose de deux interfaces principales :

- **WAN** : 10.196.216.188:7443
- **LAN (gateway interne)** : 10.89.X0.1

Les services exposés vers Internet sont placés dans la **DMZ**, notamment :

- un serveur Docker (10.89.40.4)
- un serveur de messagerie Grommunio (10.89.40.5)

Le pare-feu a été déployé sous forme de machine virtuelle sur un hyperviseur ESXi.

Étapes principales :

1. Création d'une VM pfSense :
    - 2 interfaces réseau (WAN / LAN)

    - allocation des ressources (CPU / RAM adaptées)
2. Installation de pfSense via image ISO
3. Attribution des interfaces :
    - WAN → réseau externe
    - LAN → réseau interne
4. Configuration initiale :
    - IP LAN : 10.89.X0.1
    - Activation de l'accès Web (port 7443 côté WAN)

Afin de segmenter le réseau, plusieurs VLANs ont été créés sur pfSense.

Chaque VLAN est associé à :

- une interface logique
- un plan d'adressage spécifique

Cette segmentation permet :

- d'isoler les services critiques
- de limiter les flux réseau
- de renforcer la sécurité globale

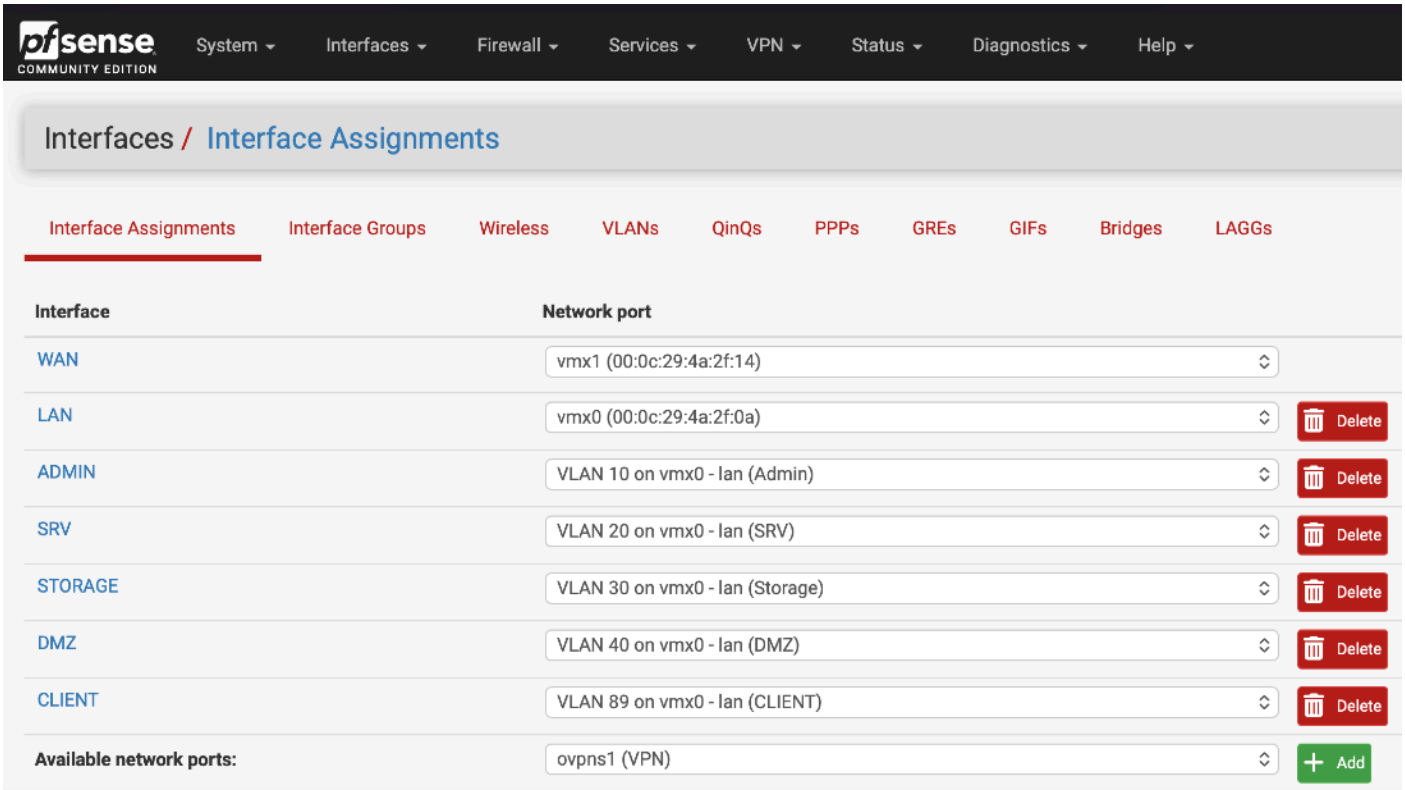
Exemple :

- VLAN 40 (DMZ) → héberge les services exposés
- VLAN 10 → réservé à l'administration

Le NAT a été configuré afin de rendre accessibles certains services internes depuis Internet.

Règles principales :

- Redirection des ports de messagerie vers Grommunio :
    - Ports : 25, 465, 587, 8443, 143, 110
    - Destination : 10.89.40.5
- Redirection des ports web vers Docker :
    - Ports : 80, 443, 22
    - Destination : 10.89.40.4
- Redirection spécifique :



- Port 8888 → 10.89.40.4:80

Ces règles permettent d'assurer l'accès aux services :

- web (sites hébergés)
- messagerie
- administration spécifique

Des alias ont été créés afin de simplifier la gestion des règles :

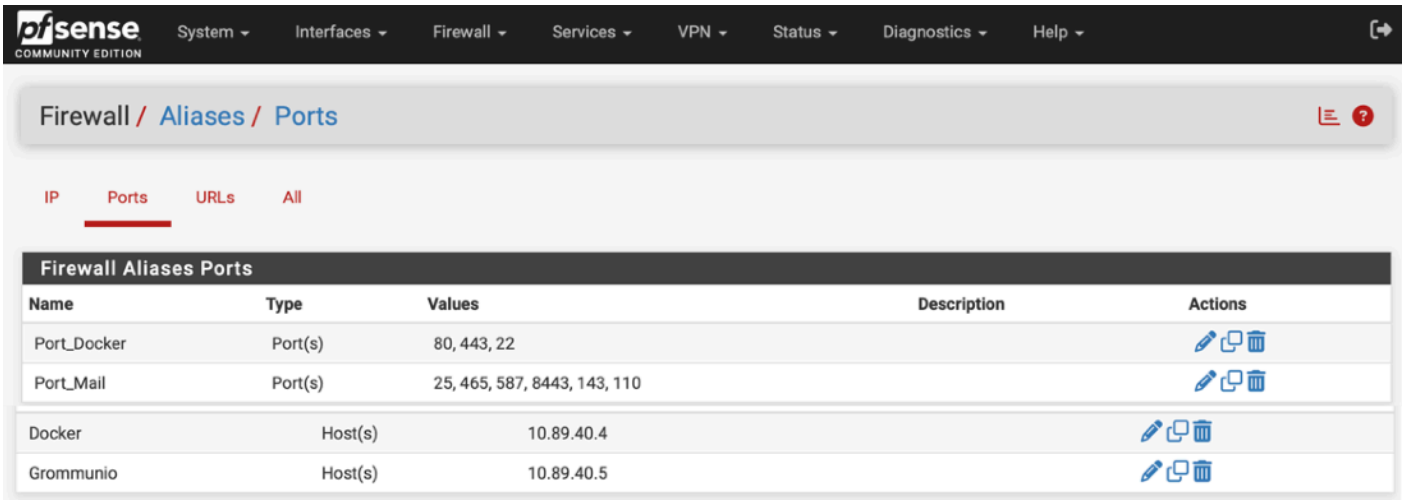
- **DOCKER_HOST** → 10.89.40.4
- **GROMMUNIO_HOST** → 10.89.40.5
- **PORT_DOCKER** → 80, 443, 22
- **PORT_MAIL** → 25, 465, 587, 8443, 143, 110

L'utilisation des alias permet :

- une meilleure lisibilité
- une maintenance simplifiée
- une réduction des erreurs de configuration

Règles Floating

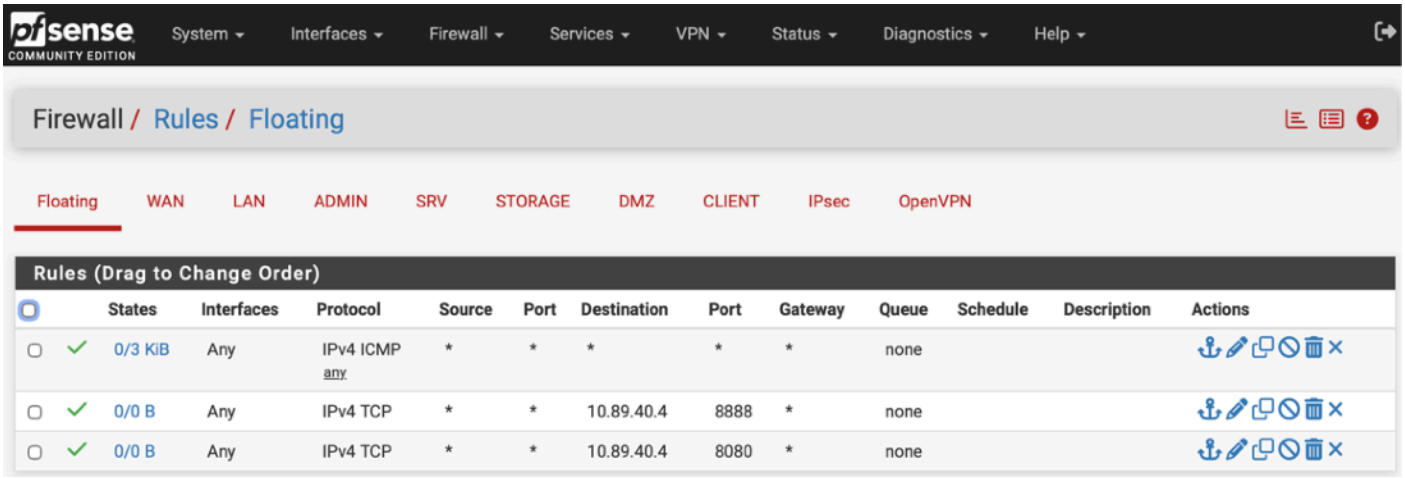
- Autorisation ICMP (diagnostic réseau)
- Autorisation accès spécifiques vers Docker :



- port 8888
- port 8080

Ces règles permettent notamment :

- les tests réseau (ping)
- l'accès à certaines interfaces web



Règles WAN

Les règles WAN autorisent uniquement les flux nécessaires :

- Accès administration (port 7443)
- Accès services web (Docker)
- Accès services mail (Grommunio)
- Accès VPN :
  - UDP 1194 (OpenVPN)

Tout autre trafic est implicitement bloqué.

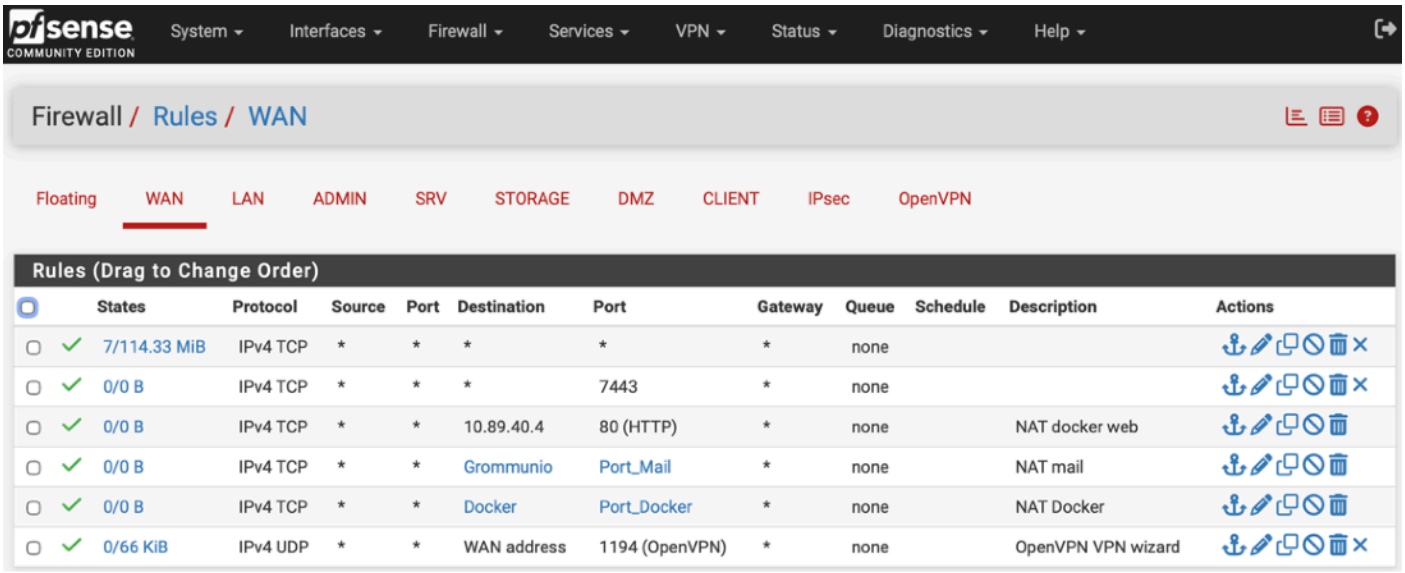
Règles LAN

- Règle anti-lockout (accès à pfSense)
- Autorisation complète :

- LAN → ANY (IPv4 et IPv6)

Cela permet :

- une connectivité complète pour les utilisateurs internes
- une gestion simplifiée du réseau local



Mise en place du VPN (OpenVPN)

Un serveur **OpenVPN** a été configuré sur pfSense afin de permettre un accès distant sécurisé à l'infrastructure réseau.

Création de l'autorité de certification (CA)

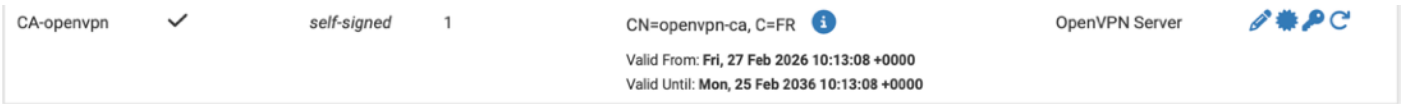
Afin de sécuriser les échanges VPN, une autorité de certification interne a été mise en place sur pfSense.

Étapes réalisées :

- Création d'une **CA (Certificate Authority)**
- Génération d'un certificat racine
- Utilisation de cette CA pour signer les certificats utilisateurs et serveur

Cela permet :

- d'authentifier les clients VPN
- de garantir la confidentialité des communications

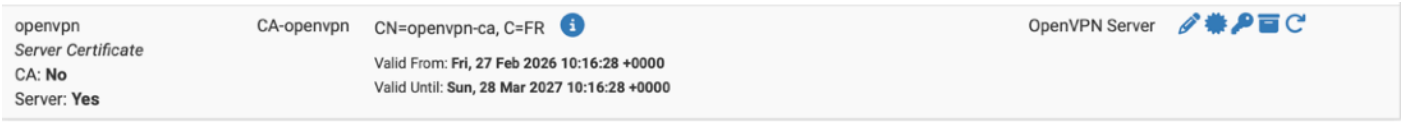


Création du certificat serveur

Un certificat serveur a été généré pour OpenVPN :

- Type : certificat serveur
- Autorité : CA interne créée précédemment
- Utilisation : authentification du serveur VPN

Ce certificat est utilisé pour sécuriser le tunnel VPN (chiffrement SSL/TLS)



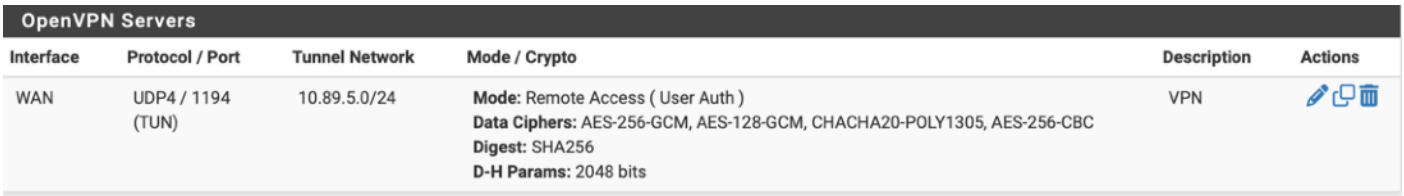
Configuration du serveur OpenVPN

Le serveur OpenVPN a été configuré avec les paramètres suivants :

- **Protocole** : UDP
- **Port** : 1194
- **Réseau VPN** : 10.89.5.0/24
- **IPv4 Local network(s)** : 10.89.0.0/16
- **DNS Server** : 10.89.10.1
- **Domaine** : jjba.lan

Ces paramètres permettent :

- aux clients VPN d'accéder à l'ensemble du réseau interne
- d'utiliser le DNS interne pour la résolution des noms



Intégration avec l'annuaire Active Directory

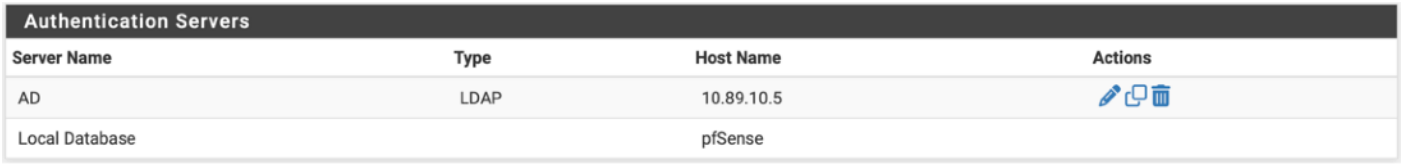
Afin de centraliser l'authentification des utilisateurs, pfSense a été configuré pour utiliser un annuaire Active Directory.

Étapes réalisées :

- Ajout d’un serveur d’authentification LDAP dans pfSense
- Connexion au contrôleur de domaine (AD)
- Configuration des paramètres :
  - IP du serveur AD
  - Base DN (domaine jjba.lan)
  - Compte de liaison (bind)
- Test de connexion à l’annuaire

Cela permet :

- d’utiliser les comptes utilisateurs du domaine
- de centraliser la gestion des accès VPN
- d’éviter la duplication des comptes



Authentication Servers

Server Name	Type	Host Name	Actions
AD	LDAP	10.89.10.5	
Local Database		pfSense	

Création des utilisateurs VPN

Les utilisateurs VPN sont authentifiés via l’Active Directory.

Chaque utilisateur :

- possède un compte dans le domaine
- peut se connecter au VPN avec ses identifiants

Possibilité de restreindre l’accès :

- par groupe AD
- par règles pfSense

Export des configurations clients

Les configurations VPN ont été exportées via l’outil :

- **OpenVPN Client Export (plugin pfSense)**

Cela permet de générer :

- fichiers `.ovpn`
- configurations automatiques pour les clients

Simplifie fortement le déploiement côté utilisateur

Fonctionnement du VPN

Une fois connecté :

- Le client reçoit une IP : 10.89.5.X
- Il accède aux ressources internes :
  - serveurs (10.89.20.0/24)
  - DMZ (10.89.40.0/28)
- Il utilise le DNS interne (10.89.10.1)

Sécurisation de l'infrastructure

Plusieurs mécanismes de sécurité ont été mis en place :

- segmentation réseau via VLAN
- isolation des services en DMZ
- filtrage strict des flux WAN
- utilisation d'un VPN pour accès distant
- limitation des ports exposés

De plus :

- seuls les services nécessaires sont publiés
- les règles firewall sont restrictives
- les accès sont contrôlés via alias
- l'authentification VPN est centralisée via Active Directory
- les communications VPN sont chiffrées via certificats

Partie 2 – Validation.

Tests de bon fonctionnement

Afin de valider l'infrastructure mise en place avec pfSense, plusieurs tests ont été réalisés portant sur :

- la connectivité réseau
- l'accès aux services exposés
- le bon fonctionnement du NAT
- la sécurité des flux

Test de connectivité réseau

Des tests de connectivité ont été effectués entre les différents VLANs.

Résultats :

- Les machines du LAN accèdent correctement aux autres réseaux autorisés
- Les VLANs sont correctement segmentés
- Les accès inter-VLAN sont contrôlés via les règles pfSense

Des tests ICMP (ping) ont permis de vérifier :

- la disponibilité des hôtes (ex : 10.89.40.4 et 10.89.40.5)
- la bonne communication réseau

Conclusion :
Le routage inter-VLAN fonctionne correctement et respecte la segmentation définie.
Test du NAT (publication des services)
Des tests ont été réalisés depuis l'extérieur du réseau afin de valider les redirections NAT configurées.

Accès aux services web (Docker)

- Accès via HTTP (port 80) et HTTPS (port 443)
- Redirection correcte vers : 10.89.40.4

Test spécifique :

- Accès via le port 8888 redirigé vers 10.89.40.4:80

Résultat :

- Les services web sont accessibles depuis Internet
- Les redirections NAT fonctionnent correctement

Accès aux services de messagerie (Grommunio)

Tests réalisés sur les ports :

- SMTP : 25, 465, 587

- Webmail : 8443
- IMAP / POP : 143, 110

Résultat :

- Les ports sont accessibles depuis l'extérieur
- Les services répondent correctement

Conclusion :
La publication des services via NAT est fonctionnelle et conforme aux besoins.

Test des règles Firewall
Des tests ont été effectués pour vérifier le filtrage des flux :

Depuis Internet (WAN)

- Seuls les ports explicitement autorisés sont accessibles :
  - 80 / 443 (web)
  - ports mail
  - 7443 (administration)
  - 1194 (VPN)
- Les autres ports sont bloqués

Résultat :

- Le pare-feu bloque correctement les accès non autorisés

Depuis le réseau interne (LAN)

- Accès libre vers Internet
- Accès aux services internes autorisé

Résultat :

- La règle « LAN to ANY » fonctionne correctement

Test du VPN (OpenVPN)

Un test de connexion VPN a été réalisé depuis un poste externe.

Vérifications :

- Connexion au serveur OpenVPN (UDP 1194)
- Attribution d'une IP dans le réseau : 10.89.5.0/24
- Accès aux ressources internes

Résultat :

- Connexion VPN établie avec succès
- Accès aux serveurs internes fonctionnel

Conclusion :
Le VPN permet un accès distant sécurisé à l'infrastructure.

Validation des accès aux services
Les services hébergés sont accessibles via les noms de domaine :

- site.jjba.fr
- nextcloud.jjba.fr
- traefik.jjba.fr

Vérifications :

- Résolution DNS fonctionnelle
- Accès via navigateur web
- Certificats HTTPS valides (Let's Encrypt)

Résultat :

- Les services sont accessibles publiquement
- Les connexions sont sécurisées

Validation de la solution

Les objectifs fixés ont été atteints :

- segmentation réseau fonctionnelle via VLAN
- sécurisation des flux grâce au firewall pfSense
- publication des services via NAT opérationnelle
- accès distant sécurisé via VPN
- accessibilité des services web et mail depuis Internet

L'infrastructure répond au besoin de :

- sécurisation
- organisation réseau
- accessibilité des services

Analyse des résultats

La solution mise en place repose sur pfSense en tant que pare-feu central.

Les tests réalisés montrent que :

- le filtrage réseau est efficace
- les flux sont maîtrisés
- les services sont accessibles de manière contrôlée
- le VPN apporte une solution sécurisée pour l'administration distante

L'utilisation des VLANs permet une isolation logique des différents environnements, notamment la DMZ qui protège le réseau interne.

Partie 3 – Veille technologique.

Analyse critique de la solution
La solution mise en place repose sur l'utilisation de pfSense comme pare-feu central afin d'assurer la sécurité et la gestion des flux réseau.

Avantages

- **Solution open source** : pfSense est gratuit et largement utilisé en entreprise
- **Interface web intuitive** facilitant la configuration
- **Gestion avancée du firewall** (règles, NAT, alias)
- **Support des VLANs** permettant une segmentation efficace du réseau
- **Intégration VPN (OpenVPN)** native et simple à mettre en œuvre
- **Grande flexibilité** pour s'adapter à différents besoins

La mise en place d'une **DMZ** et de plusieurs VLANs permet :

- une meilleure isolation des services exposés
- une réduction des risques en cas de compromission

Limites identifiées

Malgré ses avantages, certaines limites ont été observées :

- **Absence d'IDS/IPS configuré** (détection d'intrusion)
- **Interface WAN accessible (port 7443)** pouvant représenter un risque
- **Règles LAN très permissives (LAN to ANY)**

- **Manque de supervision avancée** (logs, alertes)
- **Pas de filtrage applicatif (niveau 7)**

Ces points peuvent représenter des failles potentielles dans un contexte professionnel plus exigeant.

Propositions d'amélioration

Plusieurs axes d'amélioration peuvent être envisagés afin de renforcer l'infrastructure :

Sécurisation

- Restreindre l'accès à l'interface pfSense (filtrage IP)
- Désactiver l'accès WAN à l'administration
- Mettre en place une authentification renforcée (2FA)

DS / IPS

Intégration d'un système de détection d'intrusion comme :

- Snort
- Suricata

Ces outils permettent :

- la détection d'attaques réseau
- le blocage automatique de comportements suspects

Supervision

Mise en place d'outils de monitoring :

- Zabbix
- Grafana

Objectifs :

- surveiller les performances
- détecter les anomalies
- recevoir des alertes en temps réel

Journalisation

- Centralisation des logs (Syslog)
- Analyse des événements de sécurité

- Traçabilité des connexions VPN et accès WAN

Amélioration des règles réseau

- Remplacer la règle **LAN to ANY** par des règles plus restrictives
- Filtrer les flux inter-VLAN
- Appliquer le principe du **moindre privilège**

Veille technologique

Une veille a été réalisée autour des solutions de pare-feu et de sécurité réseau.

Solutions alternatives à pfSense

OPNsense

- Fork de pfSense
- Interface plus moderne
- Mises à jour fréquentes
- Intégration native de Suricata

Alternative crédible avec une meilleure ergonomie

FortiGate

- Solution propriétaire (Fortinet)
- Fonctionnalités avancées :
    - filtrage applicatif
    - antivirus
    - IPS intégré

Très utilisé en entreprise mais coûteux

Cisco ASA

- Solution historique Cisco
- Très robuste
- Configuration plus complexe

Adapté aux grandes infrastructures

Choix de la solution

Le choix de pfSense reste pertinent dans ce projet car :

- adapté à un environnement virtualisé
- gratuit et open source
- suffisamment complet pour une PME
- bonne gestion des VLANs et du NAT
- facilité de mise en œuvre

Conclusion

La solution mise en place avec pfSense répond aux besoins initiaux en matière de :

- sécurisation des flux réseau
- segmentation via VLAN
- publication des services
- accès distant sécurisé

Elle offre une base solide pour une infrastructure réseau professionnelle.

Cependant, des améliorations peuvent être apportées, notamment :

- en matière de sécurité (IDS/IPS)
- de supervision
- et de durcissement des règles firewall

Cette veille technologique a permis d'identifier des alternatives et des axes d'évolution afin de rendre l'infrastructure plus robuste, sécurisée et adaptée à un environnement réel d'entreprise.