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, Les Ateliers De Joigny, dispose d'un site web commercial (site traditionnel) et souhaite héberger deux nouveaux services web sur un même serveur avec des certificats différents.

Cette évolution doit permettre d'améliorer l'ajout de plusieurs sites, répondre à des enjeux d'optimisation de performance, de limitation des ralentissements et de simplification de la maintenance. Elle nécessite un mécanisme capable d'aiguiller automatiquement les requêtes vers le bon service en fonction du nom de domaine.

L'entreprise a fait le choix de la conteneurisation avec Docker. Traefik a été retenu comme solution de reverse proxy , pour sa gestion centralisée du routage et des certificats SSL.

Intitulé de la réalisation professionnelle

Mise en œuvre d'une infrastructure conteneurisée avec Reverse Proxy Traefik

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

Principale(s) activité(s) concernée(s) :
Développer la présence en ligne de l'organisation
Organiser son développement professionnel
Mettre à disposition des utilisateurs un service informatique
Gérer le patrimoine informatique

Conditions de réalisation **Ressources initiales :** 1 VM (4 vCPU, 8 GB RAM) avec Debian et Docker Compose installés. **Résultats attendus :** Dashboard Traefik accessible, site WordPress opérationnel en HTTPS (Let's Encrypt), et routage fonctionnel via noms de domaine. **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.

Liste des outils utilisés

- Conteneurisation : Debian, Docker, Docker Compose
- Reverse Proxy : Traefik (image officielle)
- Application : WordPress, MySQL/MariaDB (images Docker)
- Réseau / Sécurité : Let's Encrypt (Auto-SSL), Docker Networks

Présentation de l'architecture

L'infrastructure mise en place repose sur une architecture conteneurisée utilisant Docker.

Un serveur unique héberge plusieurs services isolés sous forme de conteneurs :

- Un reverse proxy Traefik

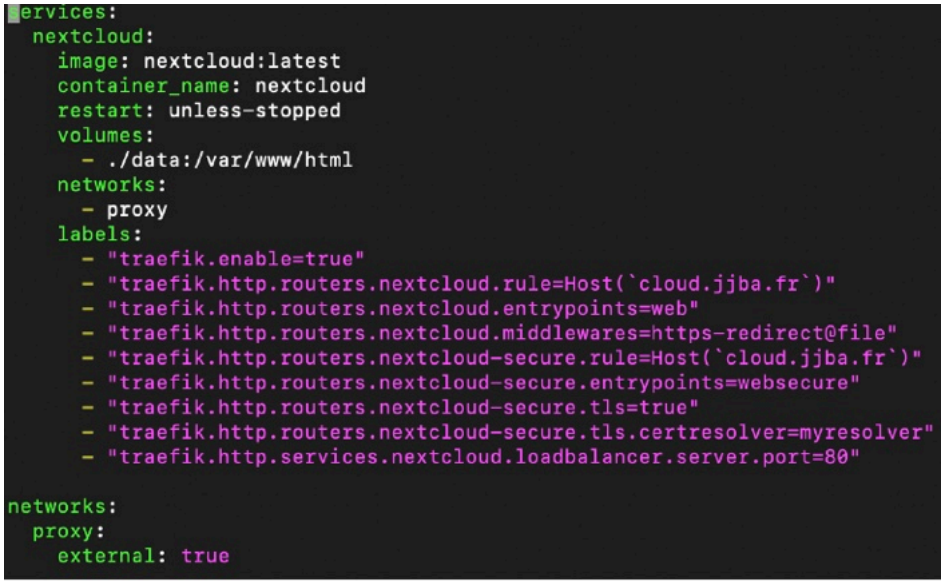
- Un site web portfolio basé sur WordPress
- Une plateforme de stockage cloud Nextcloud

Le reverse proxy Traefik permet de centraliser la gestion des accès et d'orienter automatiquement les requêtes vers le bon service en fonction du nom de domaine.

Chaque service est accessible via un sous-domaine distinct :

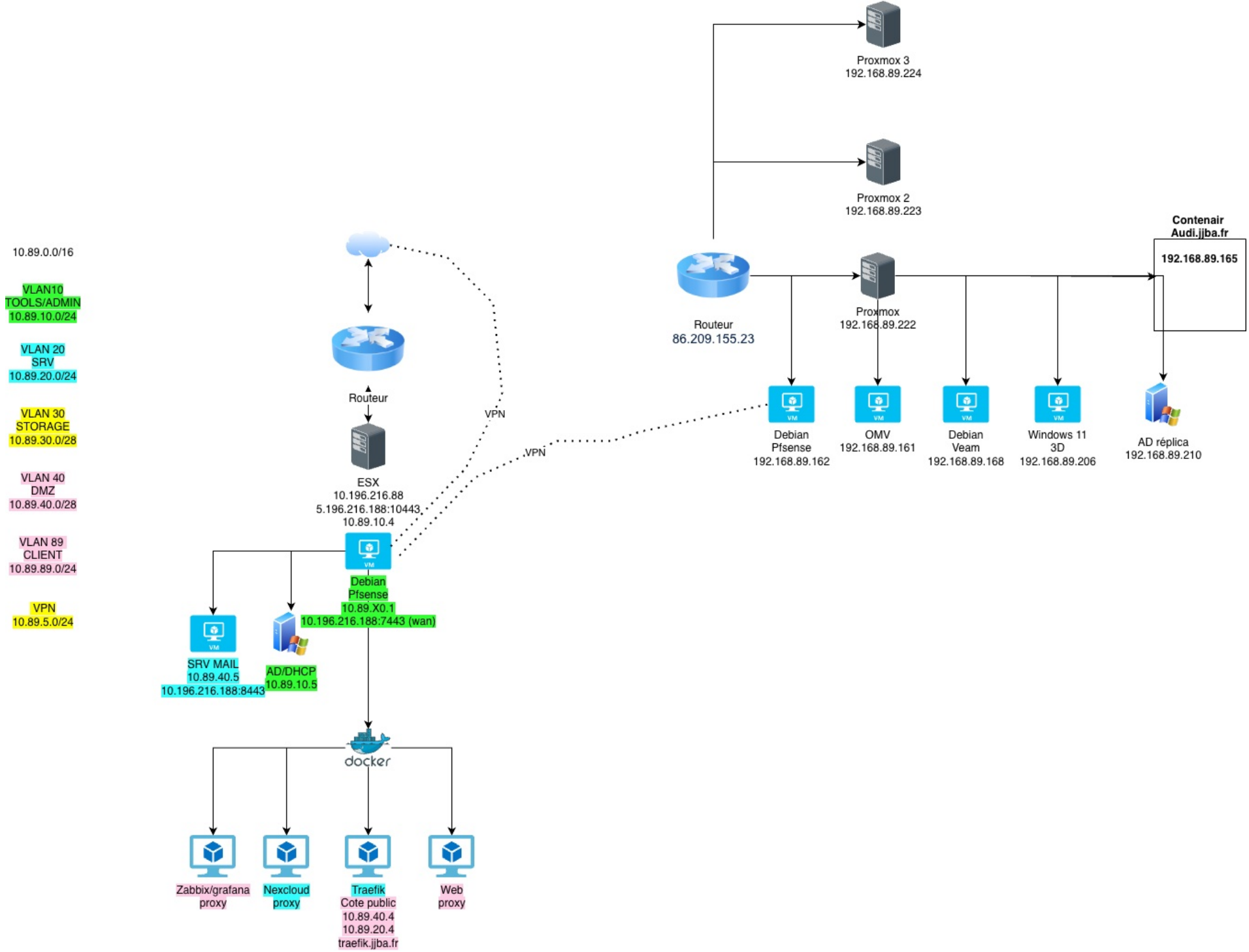
- Portfolio : site.jjba.fr
- Cloud : cloud.jjba.fr
- Dashboard Traefik : traefik.jjba.fr

Cette architecture permet une meilleure organisation, une isolation des services et une maintenance simplifiée.



```
services:
  nextcloud:
    image: nextcloud:latest
    container_name: nextcloud
    restart: unless-stopped
    volumes:
      - ./data:/var/www/html
    networks:
      - proxy
    labels:
      - "traefik.enable=true"
      - "traefik.http.routers.nextcloud.rule=Host(`cloud.jjba.fr`)"
      - "traefik.http.routers.nextcloud.entrypoints=web"
      - "traefik.http.routers.nextcloud.middlewares=https-redirect@file"
      - "traefik.http.routers.nextcloud-secure.rule=Host(`cloud.jjba.fr`)"
      - "traefik.http.routers.nextcloud-secure.entrypoints=websecure"
      - "traefik.http.routers.nextcloud-secure.tls=true"
      - "traefik.http.routers.nextcloud-secure.tls.certresolver=myresolver"
      - "traefik.http.services.nextcloud.loadbalancer.server.port=80"

networks:
  proxy:
    external: true
```


10.89.0.0/16
VLAN10
TOOLS/ADMIN
10.89.10.0/24
VLAN 20
SRV
10.89.20.0/24
VLAN 30
STORAGE
10.89.30.0/28
VLAN 40
DMZ
10.89.40.0/28
VLAN 89
CLIENT
10.89.89.0/24
VPN
10.89.5.0/24
Routeur
ESX
10.196.216.88
5.196.216.188:10443
10.89.10.4
VPN
Debian
Pfsense
10.89.X0.1
10.196.216.188:7443 (wan)
SRV MAIL
10.89.40.5
10.196.216.188:8443
AD/DHCP
10.89.10.5
docker
Zabbix/grafana
proxy
Nexcloud
proxy
Traefik
Cote public
10.89.40.4
10.89.20.4
traefik.jjba.fr
Web
proxy
Proxmox 3
192.168.89.224
Proxmox 2
192.168.89.223
Routeur
86.209.155.23
Proxmox
192.168.89.222
Contenair
Audi.jjba.fr
192.168.89.165
Debian
Pfsense
192.168.89.162
OMV
192.168.89.161
Debian
Veam
192.168.89.168
Windows 11
3D
192.168.89.206
AD réplica
192.168.89.210

Étapes clés de l'installation

1. Création du réseau Docker

Un réseau Docker externe (nommé par exemple *proxy*) a été créé afin de permettre la communication entre Traefik et les différents conteneurs.

Ce réseau facilite le routage des services sans exposer directement les ports des applications.

2. Configuration de Traefik (docker-compose.yml)

Définition des entrypoints

Dans la configuration de Traefik, plusieurs entrypoints ont été définis afin de gérer les flux réseau entrants.

Trois points d'entrée principaux sont configurés :

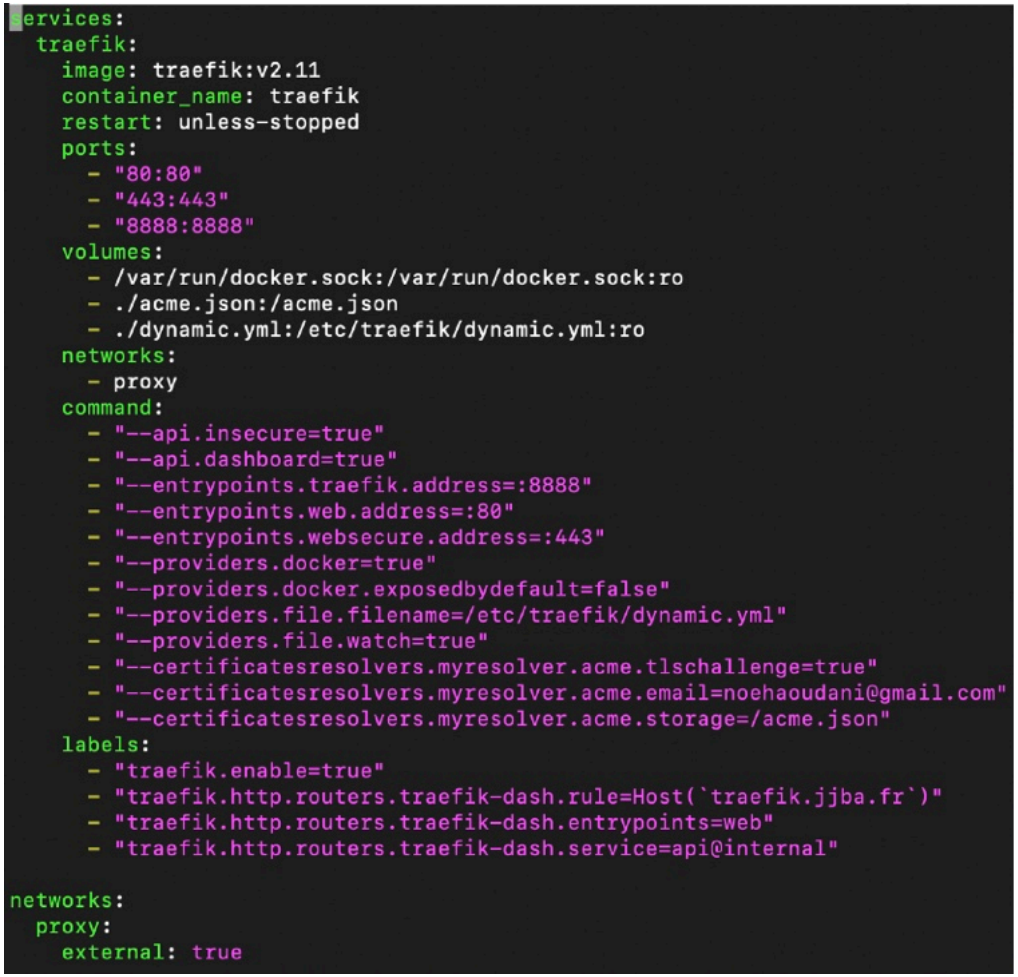
- web (port 80) : réception des requêtes HTTP
- websecure (port 443) : réception des requêtes HTTPS
- traefik (port 8888) : accès au dashboard d'administration

Ces entrypoints sont définis via les paramètres suivants :

--entrypoints.web.address=:80
--entrypoints.websecure.address=:443
--entrypoints.traefik.address=:8888

Le port 80 permet de rediriger automatiquement les utilisateurs vers HTTPS (port 443), garantissant la sécurisation des échanges.

Le port 8888 est utilisé pour accéder à l'interface de supervision de Traefik.



```yaml
services:
  traefik:
    image: traefik:v2.11
    container_name: traefik
    restart: unless-stopped
    ports:
      - "80:80"
      - "443:443"
      - "8888:8888"
    volumes:
      - /var/run/docker.sock:/var/run/docker.sock:ro
      - ./acme.json:/acme.json
      - ./dynamic.yml:/etc/traefik/dynamic.yml:ro
    networks:
      - proxy
    command:
      - "--api.insecure=true"
      - "--api.dashboard=true"
      - "--entrypoints.traefik.address=:8888"
      - "--entrypoints.web.address=:80"
      - "--entrypoints.websecure.address=:443"
      - "--providers.docker=true"
      - "--providers.docker.exposedbydefault=false"
      - "--providers.file.filename=/etc/traefik/dynamic.yml"
      - "--providers.file.watch=true"
      - "--certificatesresolvers.myresolver.acme.tlschallenge=true"
      - "--certificatesresolvers.myresolver.acme.email=noehaoudani@gmail.com"
      - "--certificatesresolvers.myresolver.acme.storage=/acme.json"
    labels:
      - "traefik.enable=true"
      - "traefik.http.routers.traefik-dash.rule=Host(`traefik.jjba.fr`)"
      - "traefik.http.routers.traefik-dash.entrypoints=web"
      - "traefik.http.routers.traefik-dash.service=api@internal"

networks:
  proxy:
    external: true
```

Configuration du provider Docker

Le provider Docker est activé afin de permettre à Traefik de détecter automatiquement les conteneurs.

Grâce à ce mécanisme, les services sont configurés dynamiquement via des labels Docker, sans configuration manuelle complexe.

Paramétrage des certificats SSL

Un certificate resolver a été configuré afin de générer automatiquement des certificats SSL via Let's Encrypt.

Cela permet :

- une sécurisation automatique des services
- un renouvellement automatique des certificats
- une simplification de la gestion HTTPS

3. Déploiement du site WordPress

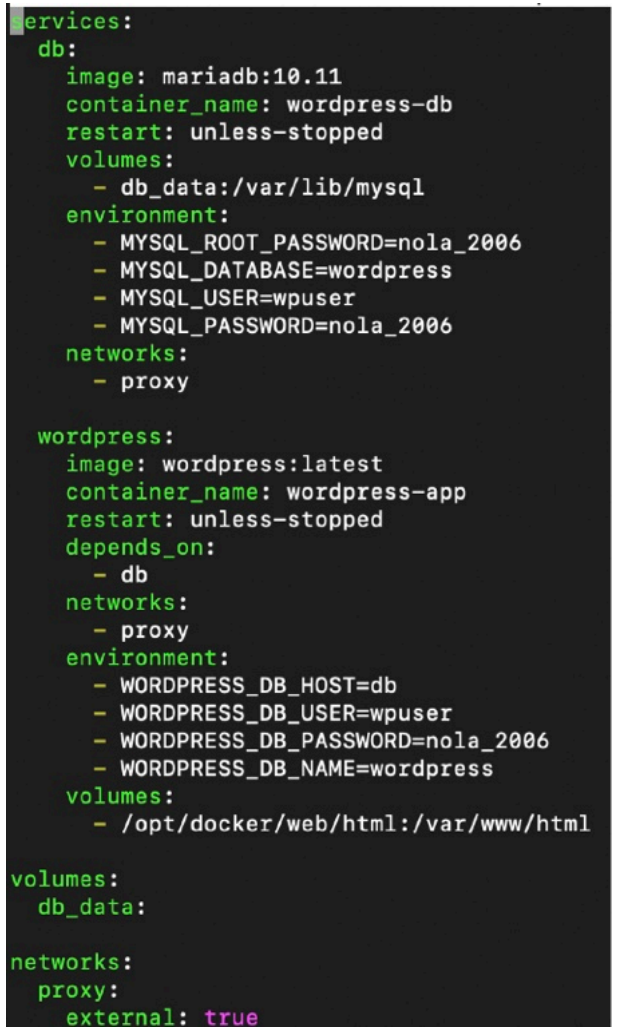
Un conteneur WordPress a été déployé pour héberger le site portfolio.

Une page personnalisée a été créée en intégrant directement du code HTML, permettant une personnalisation complète du site.

Le conteneur est relié au réseau Docker afin d'être accessible via Traefik.

Des labels Docker ont été utilisés pour :

- définir le nom de domaine (site.jjba.fr)
- activer le routage via Traefik
- sécuriser l'accès en HTTPS



```
services:
  db:
    image: mariadb:10.11
    container_name: wordpress-db
    restart: unless-stopped
    volumes:
      - db_data:/var/lib/mysql
    environment:
      - MYSQL_ROOT_PASSWORD=nola_2006
      - MYSQL_DATABASE=wordpress
      - MYSQL_USER=wpuser
      - MYSQL_PASSWORD=nola_2006
    networks:
      - proxy

  wordpress:
    image: wordpress:latest
    container_name: wordpress-app
    restart: unless-stopped
    depends_on:
      - db
    networks:
      - proxy
    environment:
      - WORDPRESS_DB_HOST=db
      - WORDPRESS_DB_USER=wpuser
      - WORDPRESS_DB_PASSWORD=nola_2006
      - WORDPRESS_DB_NAME=wordpress
    volumes:
      - /opt/docker/web/html:/var/www/html

volumes:
  db_data:

networks:
  proxy:
    external: true
```

4. Lancement des services

Les différents services ont été démarrés à l'aide de la commande suivante :

docker-compose up -d

Cette commande permet de lancer l'ensemble des conteneurs en arrière-plan.

Partie 2 – Validation.

Tests de bon fonctionnement

Plusieurs tests ont été réalisés afin de valider le bon fonctionnement de l'infrastructure mise en place avec Traefik.

Dashboard Traefik

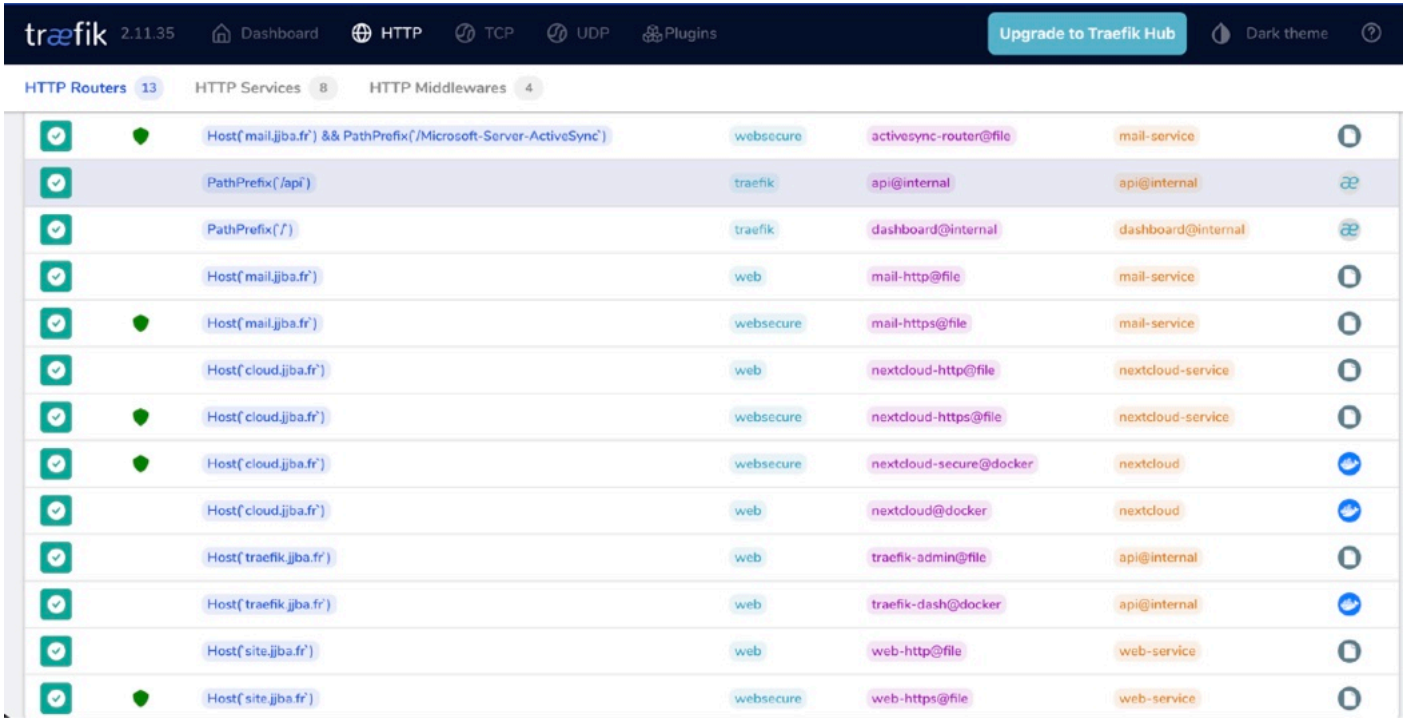
Le dashboard de Traefik a été consulté afin de vérifier que les différents conteneurs sont correctement détectés.

Les routers et services Docker apparaissent actifs et fonctionnels, ce qui confirme la bonne communication entre les conteneurs.

Accès HTTPS

Un test d'accès au site WordPress a été réalisé via le navigateur.

La présence du cadenas dans la barre d'adresse confirme que le certificat SSL est valide et correctement appliqué grâce à Let's Encrypt.



Test de routage

Des tests ont été effectués via les différents sous-domaines afin de vérifier le routage mis en place par Traefik.

Chaque service est correctement accessible :

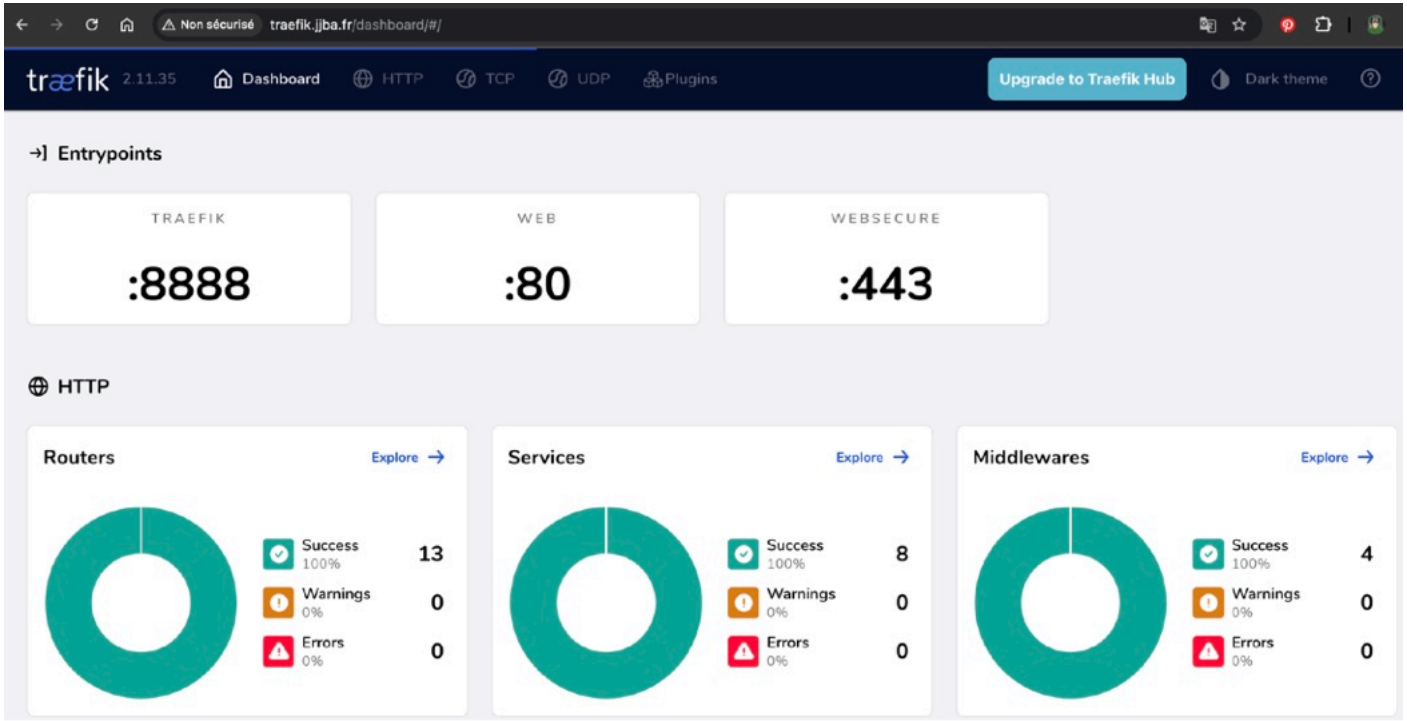
- site.jjba.fr redirige vers le conteneur WordPress
- cloud.jjba.fr redirige vers le conteneur Nextcloud
- traefik.jjba.fr permet d’accéder au dashboard

Ces tests confirment que le routage dynamique fonctionne correctement.

Preuves et analyse

Preuve : Dashboard Traefik

Une capture du dashboard montre que les routes sont actives et correctement configurées.



Accès aux services

Les services déployés sont accessibles via les adresses suivantes :

- Portfolio : https://site.jjba.fr
- Cloud : https://cloud.jjba.fr
- Dashboard Traefik : http://traefik.jjba.fr

Le site portfolio est accessible publiquement sans authentification.

La plateforme Nextcloud nécessite une authentification utilisateur pour accéder aux fichiers.

L'interface d'administration de Traefik permet de visualiser les routes, services et certificats actifs.

Tous les services accessibles publiquement sont sécurisés via le protocole HTTPS grâce à l'intégration de certificats SSL générés automatiquement par Let's Encrypt.

Validation de la solution

Les objectifs fixés en début de projet ont été atteints.

Le reverse proxy Traefik est opérationnel et permet un routage dynamique des requêtes en fonction des noms de domaine.

Les différents services déployés sont fonctionnels :

- le site portfolio est accessible en HTTPS
- la plateforme Nextcloud est opérationnelle et sécurisée
- le dashboard Traefik permet de superviser l'ensemble de l'infrastructure

Les certificats SSL sont générés automatiquement via Let's Encrypt et sont correctement appliqués.

Le système mis en place est évolutif : il est possible d’ajouter de nouveaux services simplement en déployant de nouveaux conteneurs et en configurant des labels Docker.

Partie 3 – Veille technologique.

Analyse des résultats

La solution mise en place repose sur une infrastructure conteneurisée utilisant Docker et un reverse proxy Traefik.

Les tests réalisés ont permis de valider le bon fonctionnement global du système :

- les services sont accessibles via leurs sous-domaines respectifs
- le routage des requêtes est correctement assuré par Traefik
- les certificats SSL sont générés et appliqués automatiquement via Let's Encrypt
- les applications déployées, notamment WordPress et Nextcloud, sont opérationnelles

L’utilisation de Docker permet une isolation efficace des services ainsi qu’une simplification du déploiement et de la maintenance.

Le reverse proxy Traefik apporte une gestion centralisée des accès ainsi qu’une automatisation du routage et de la sécurisation HTTPS.

Analyse critique

La solution présente plusieurs avantages :

- déploiement rapide et reproductible grâce à Docker

- isolation des services limitant les conflits entre applications
- gestion automatique des certificats SSL via Let's Encrypt
- routage dynamique simplifié avec Traefik

Cependant, certaines limites ont été identifiées :

- la configuration initiale de Traefik peut être complexe à prendre en main
- le dashboard Traefik est exposé en mode non sécurisé (api.insecure=true)
- absence de système de sauvegarde automatisé pour les données (WordPress / Nextcloud)
- absence de supervision avancée des services (monitoring, alertes)

Propositions d’amélioration

Plusieurs axes d’amélioration peuvent être envisagés afin d’optimiser la solution :

Sécurisation

- désactiver le mode insecure du dashboard Traefik
- mettre en place une authentification (basique ou via middleware)
- restreindre l’accès au dashboard par adresse IP

Sauvegardes

- mise en place de sauvegardes automatiques des volumes Docker
- export régulier des bases de données (WordPress et Nextcloud)

Supervision

- ajout d’un outil de monitoring comme Prometheus
- visualisation des métriques avec Grafana

Évolutivité

- ajout de nouveaux services via Docker
- possibilité de déployer d’autres applications web en utilisant le même reverse proxy

Veille technologique

Une veille technologique a été réalisée autour des solutions de reverse proxy et de conteneurisation.

Plusieurs alternatives à Traefik ont été étudiées :

- Nginx Proxy Manager : solution disposant d’une interface graphique facilitant la configuration
- HAProxy : solution performante mais plus complexe à configurer

Cette veille a permis de confirmer le choix de Traefik pour ce projet, notamment grâce à :

- son intégration native avec Docker
- sa configuration dynamique via les labels
- sa gestion automatique des certificats SSL

Conclusion

La solution mise en place répond aux besoins initiaux en proposant une infrastructure web fonctionnelle, sécurisée et évolutive.

L’utilisation conjointe de Docker et de Traefik permet de simplifier le déploiement et la gestion de plusieurs services web sur un même serveur.

Des améliorations peuvent néanmoins être apportées, notamment en matière de sécurité et de supervision, afin de rendre l’infrastructure encore plus robuste et professionnelle.

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 :

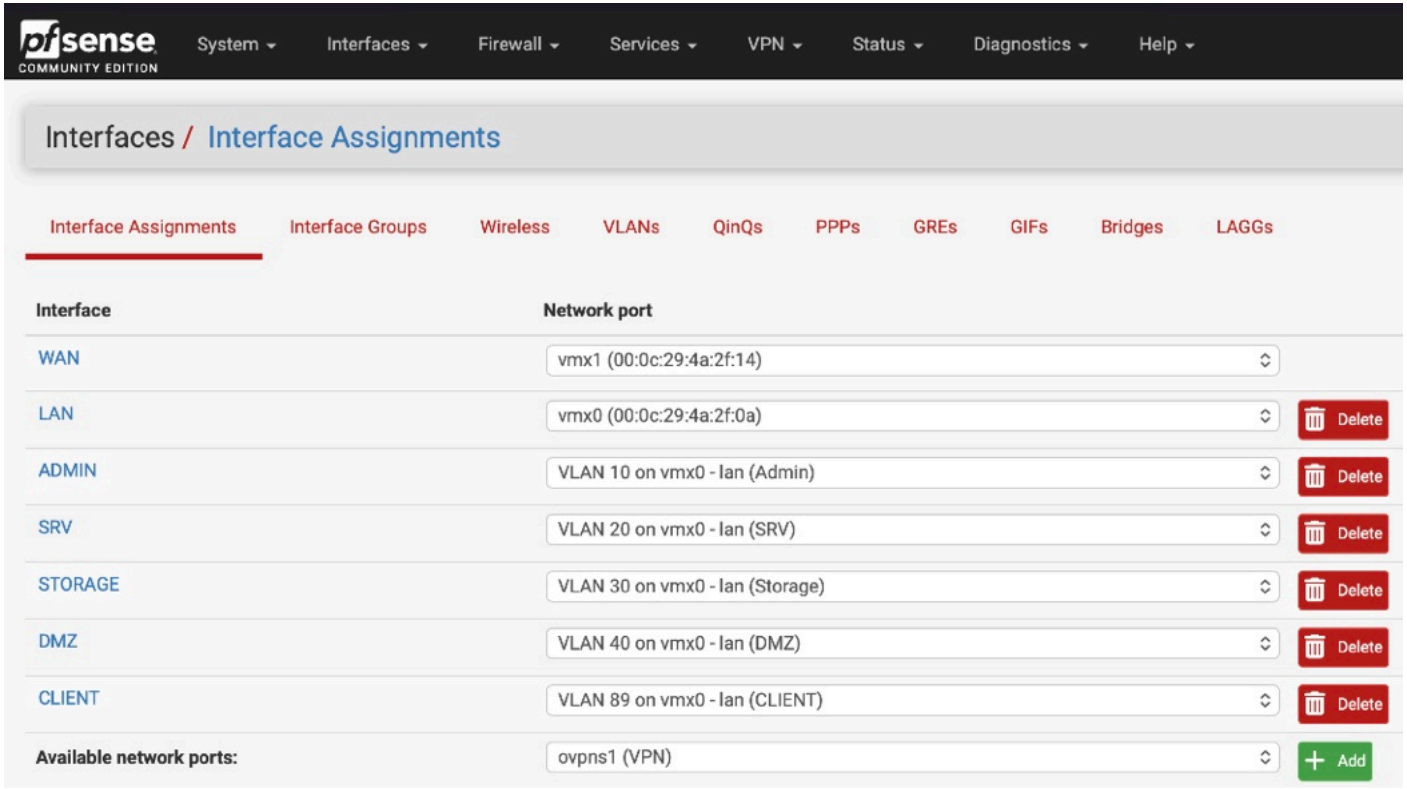
- d'isoler les services critiques

- 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 :

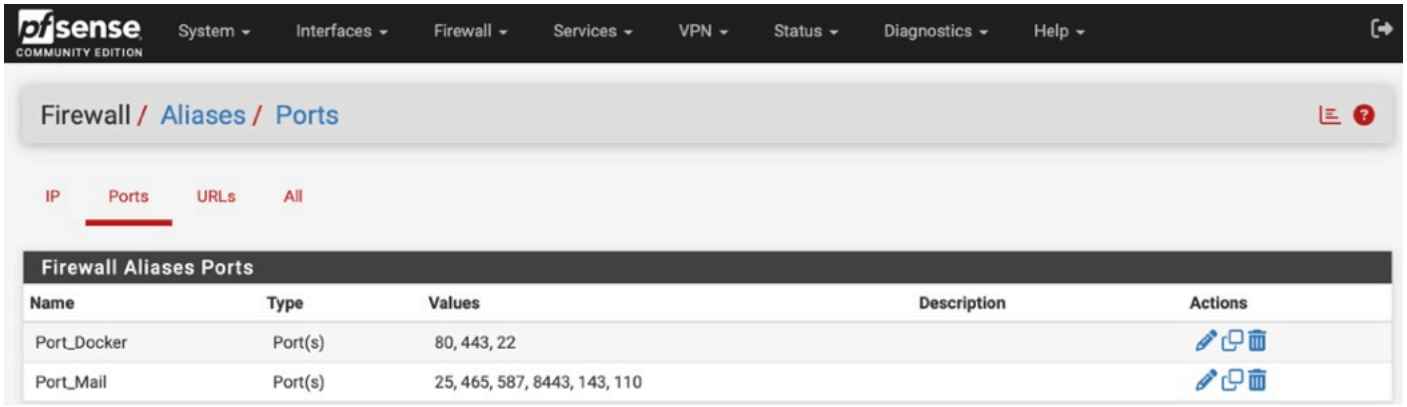
- Redirection des ports de messagerie vers Grommunio :
  - Ports : 25, 465, 587, 8443, 143, 110
  - Destination : 10.89.40.5
- Redirection des ports web vers Docker :
  - Ports : 80, 443, 22
  - Destination : 10.89.40.4
- Redirection spécifique :
  - Port 8888 → 10.89.40.4:80

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

- web (sites hébergés)
- messagerie
- administration spécifique

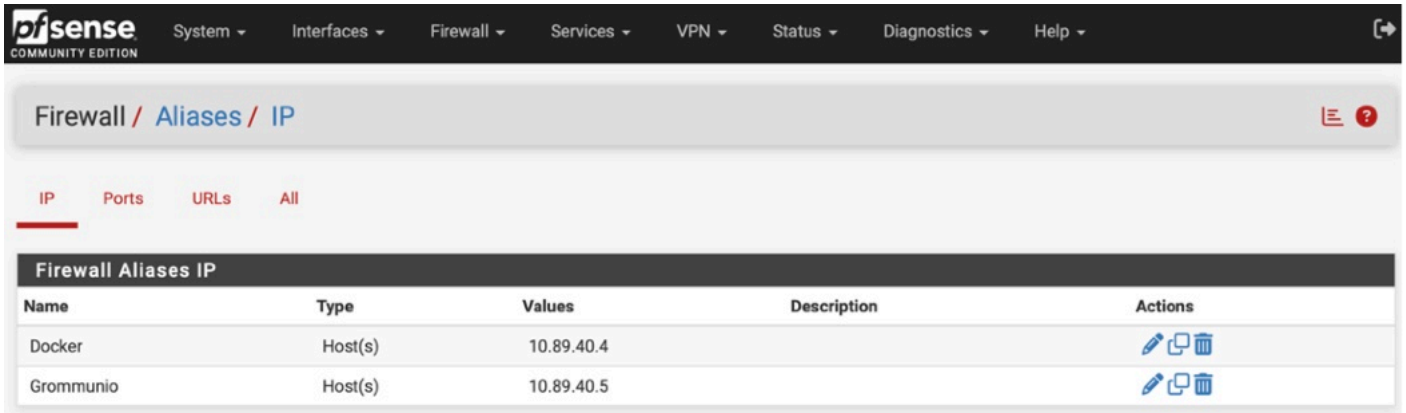
Des alias ont été créés afin de simplifier la gestion des règles :

- **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



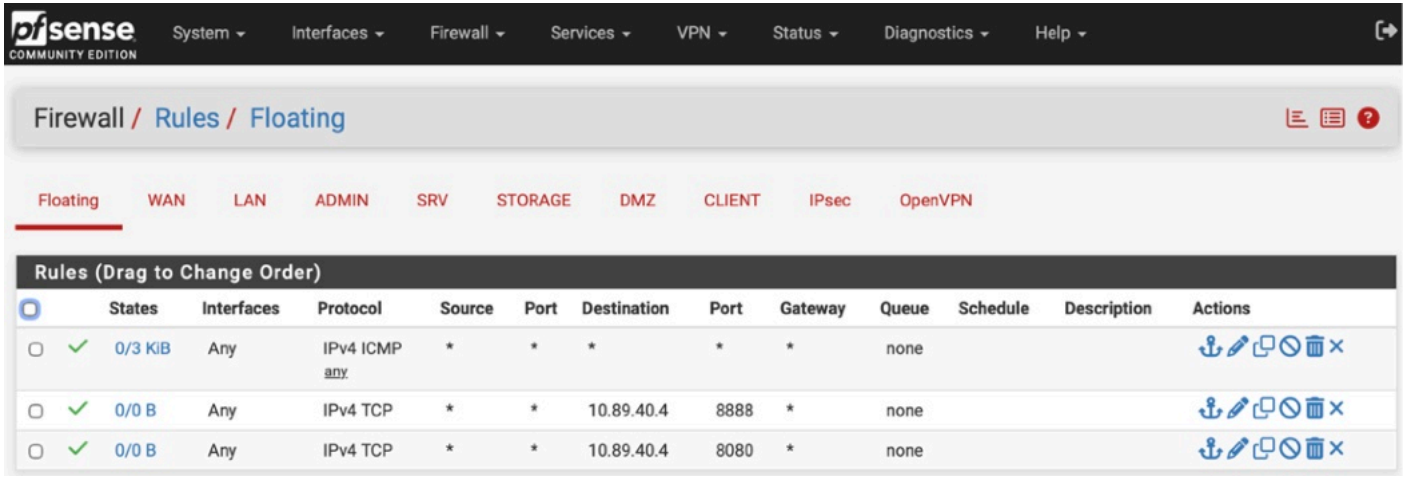
Règles Floating

- 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)

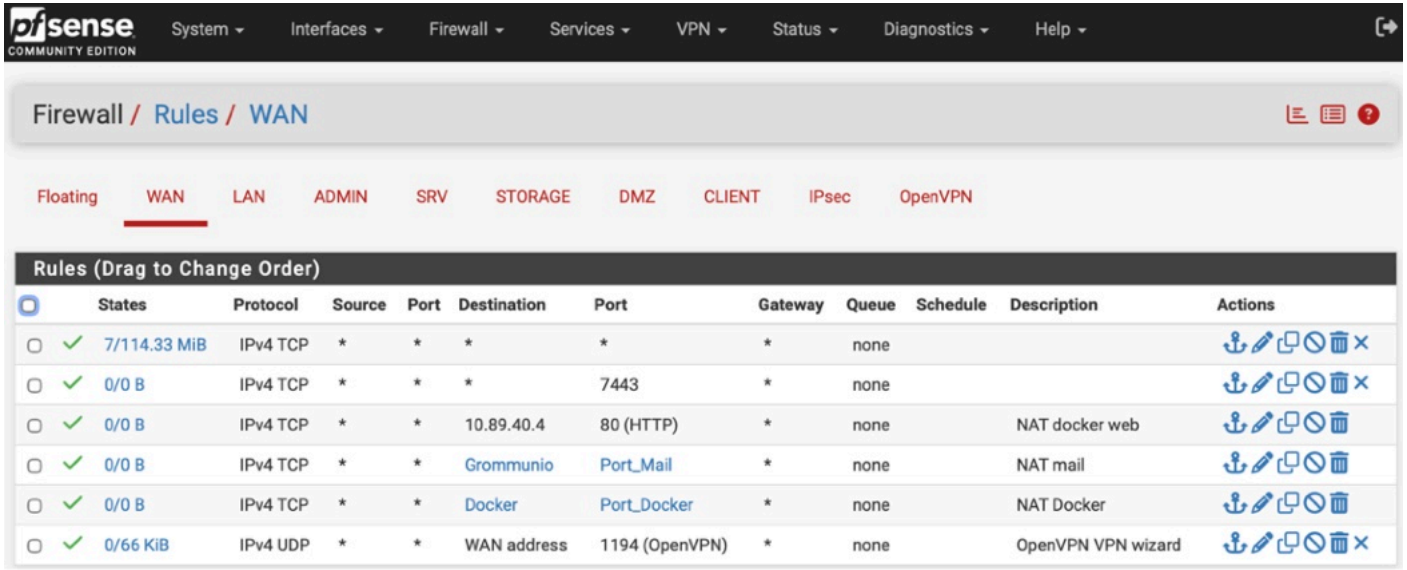
Tout autre trafic est implicitement bloqué.

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)

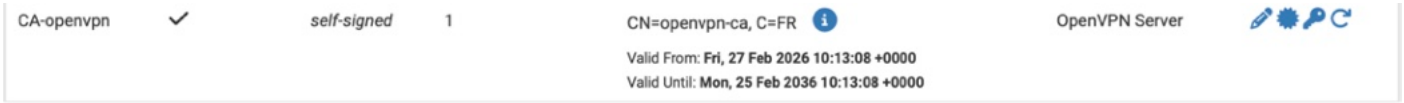
Afin de sécuriser les échanges VPN, une autorité de certification interne a été mise en place sur pfSense.

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)

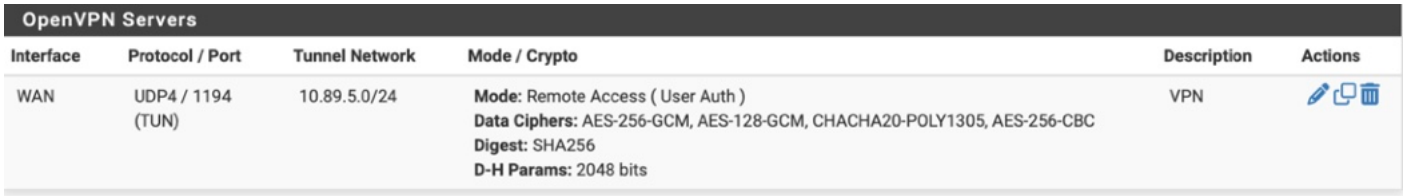
Configuration du serveur OpenVPN

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



OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.89.5.0/24	**Mode:** Remote Access (User Auth) **Data Ciphers:** AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC **Digest:** SHA256 **D-H Params:** 2048 bits	VPN	

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.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	**SESSION 2026**
Épreuve E5 - Administration des systèmes et des réseaux (option SISR)	
ANNEXE 8-A : Outil d'aide à l'appréciation de l'environnement technologique mobilisé par la personne candidate	

CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE

En référence à l'annexe II.E « Environnement technologique pour la certification » du référentiel du BTS SIO

Identification	**N° candidat : 2248078501 Nom: Aoudani Prenom: Noeh**	**SISR**

1. Environnement commun aux deux options

1.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Un service d'authentification	Mise en place d'un Active Directory	
Un SGBD	Mise en place d'une Base de donnée MariaDB	
Un accès sécurisé à internet	Mise en place d'un Pfsense	
Un environnement de travail collaboratif	Mise en place d'un NextCloud	
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (*open source)*	Mise en place d'un Active Directory ainsi que d'un GLPI	

ANNEXE 8-A (suite) : Modèle d'attestation de respect de l'annexe II.E – « Environnement technologique pour la certification » du référentiel Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution de sauvegarde	Mise en place d'un Veeam	
Des ressources dont l'accès est sécurisé et soumis à habilitation	Mise en place d'un Active Directory	
Deux types de terminaux dont un mobile (type *smartphone* ou encore tablette)	Mise en place d'un OpenVPN sur un Pc portable sur un téléphone	

1.2 Des outils sont mobilisés pour la gestion de la sécurité :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Gestion des incidents	Mise en place d'un GLPI	
Détection et prévention des intrusions	Mise en place Zabbix ainsi que d'un Grafana	
Chiffrement	Mise en place de Let's encrypt et d'un VPN	
Analyse de trafic	Mise en place de Snort	

Rappel : les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.

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

ANNEXE 8-A (suite) : Modèle d'attestation de respect de l'annexe II.E « Environnement technologique pour la certification » du référentiel

2. Éléments spécifiques à l'option « Solutions d'infrastructure, systèmes et réseaux » (SISR)

Rappel de l'annexe II.E du référentiel : **« *Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.* »**

2.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

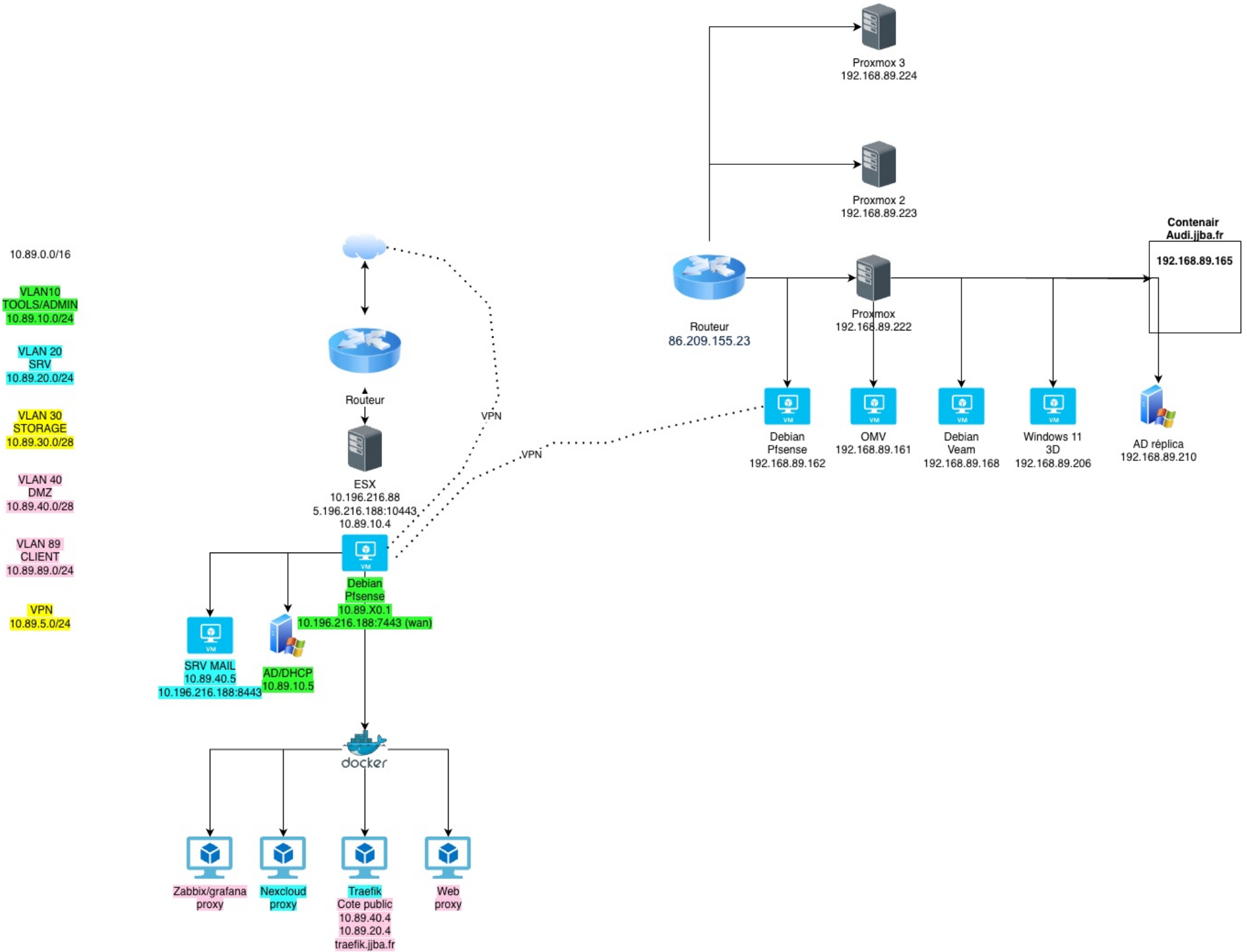
Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Un réseau comportant plusieurs périmètres de sécurité	Mise en place de VLANs	

Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Mise en place d’un Active Directory répliqué	
Un logiciel d'analyse de trames	Mise en place de Wireshark	
Un logiciel de gestion des configurations	Mise en place d’un Active Directory	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	Mise en place d’OpenVPN	
Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	Mise en place Zabbix ainsi que d'un Grafana	
Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	Mise en place Zabbix ainsi que d'un Grafana d’un DFS et d’un AD Répliqué	
Éléments	**Description de l’implantation dans le centre d’examen (nom du service ou de l’outil et caractéristiques techniques)**	**Remarques de la commission d’interrogation**
Une solution garantissant la continuité d'un service	Réplication de l’ad sur le Proxmox chez moi	
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	Réplication de l’ad sur le Proxmox chez moi	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d’interconnexion	Mise en place du Veeam sur le Proxmox chez moi	

2.2 La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :

Éléments	**Description de l’implantation dans le centre d’examen (nom du service ou de l’outil et caractéristiques techniques)**	**Remarques de la commission d’interrogation**
Une solution permettant la connexion sécurisée entre deux sites distants	Mise en place d’OpenVPN	
Une solution permettant le déploiement des solutions techniques d'accès	Mise en place d’un GLPI de WDS et d’une GPO	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de *scripting*	Mise en place d’un docker	
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	Mise en place de Snort	

Infrastructure réseau :


10.89.0.0/16
VLAN10
TOOLS/ADMIN
10.89.10.0/24
VLAN 20
SRV
10.89.20.0/24
VLAN 30
STORAGE
10.89.30.0/28
VLAN 40
DMZ
10.89.40.0/28
VLAN 89
CLIENT
10.89.89.0/24
VPN
10.89.5.0/24
Routeur
ESX
10.196.216.88
5.196.216.188:10443
10.89.10.4
VPN
Debian
Pfsense
10.89.X0.1
10.196.216.188:7443 (wan)
SRV MAIL
10.89.40.5
10.196.216.188:8443
AD/DHCP
10.89.10.5
docker
Zabbix/grafana
proxy
Nexcloud
proxy
Traefik
Cote public
10.89.40.4
10.89.20.4
traefik.jjba.fr
Web
proxy
VPN
Routeur
86.209.155.23
Proxmox 3
192.168.89.224
Proxmox 2
192.168.89.223
Proxmox
192.168.89.222
Contenair
Audi.jjba.fr
192.168.89.165
Debian
Pfsense
192.168.89.162
OMV
192.168.89.161
Debian
Veam
192.168.89.168
Windows 11
3D
192.168.89.206
AD réplica
192.168.89.210