ANNEXE IV - PAGE DE GARDE DU DOSSIER PROFESSIONNEL

BREVET DE TECHNICIEN SUPERIEUR SERVICES INFORMATIQUES AUX ORGANISATIONS

Session 2026

DOSSIER PROFESSIONNEL

NOM : HAMOUD

Prénom : Mouhamed Messaoud

Établissement de formation (sur un seul des deux exemplaires du dossier)

Visa du représentant de l'équipe pédagogique attestant la réalité des activités professionnelles décrites dans le dossier (sur un seul des deux exemplaires du dossier) :

Nom et qualité du signataire	Date	Signature
RAGOT Mélanie Chargée de mission pédagogique	24/04/2026	Mewo 7, rue Edouard Belin 57070 Metz S.A.S. au capital de 20.000€ SIRET 82047291800011 - APE 85422 03 87 78 08 08 - contact@mewo.fr www.mewo.fr

Attestation sur l'honneur pour les candidats individuels (sur un seul des deux exemplaires du dossier) :

Je soussigné(e), Nom HAMOUD, Prénom Mouhamed M, certifie que les activités décrites ainsi que les différentes informations reproduites dans ce dossier reflètent les activités professionnelles que j'ai personnellement réalisées au cours de ma formation.

Fait à Metz
Date Le 24/04/2026

Signature

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS SESSION 2026

ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : A**
Nom, prénom : HAMOUD Mouhamed Messaoud	**N° candidat : 2544756783**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date : 22/04/2026**

Organisation support de la réalisation professionnelle

L'entreprise **SHAMOUD IT** est une ESN dynamique spécialisée dans l'infogérance réseau et le développement web pour le compte de PME.
Pour répondre à sa croissance, l'organisation a structuré son activité sur deux sites géographiques distincts A et B que j'ai dû interconnecter de manière totalement sécurisée. En tant que technicien réseau, ma mission principale a consisté à concevoir une architecture robuste s'appuyant sur deux pare-feu pfSense pour garantir la confidentialité des données entre le siège social, le site secondaire et les collaborateurs nomades.
Pour assurer la réplication de l'Active Directory et la communication entre les sous-réseaux LAN A et LAN B, j'ai mis en place un tunnel **VPN IPsec Site-to-Site** permettant un routage transparent et chiffré des flux métiers. En complément, pour répondre aux besoins de mobilité des développeurs, j'ai déployé une solution **VPN Client-to-Site** offrant un accès distant sécurisé aux ressources critiques de l'entreprise. Cette infrastructure intègre également une zone **DMZ** isolée pour les accès publics, assurant ainsi une segmentation stricte des réseaux conformément aux bonnes pratiques de sécurité informatique.

Intitulé de la réalisation professionnelle

Mise en œuvre d'une infrastructure réseau multisites sécurisée par tunnels **VPN IPsec** et **OpenVPN**

Période de réalisation : Janvier 2026 – Mai 2026 **Lieu :** Campus MEWO Metz

Modalité : ☒ **Seul(e)** ☐ **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[1] (ressources fournies, résultats attendus)

L'infrastructure a été déployée au sein d'un environnement virtualisé s'appuyant sur un hyperviseur **VMware ESXi** fourni par l'établissement. Pour mener à bien cette réalisation, j'ai disposé d'un pool de machines virtuelles comprenant :

- 2 serveurs **Windows Server 2025,**
- 2 pare-feu **PfSense 2.7**
- 2 machines **Debian Server 12**
- 1 machines **Debian Server 13**
- 2 postes clients sous **Windows 11 Professionnel**

Le réseau a été segmenté physiquement et logiquement pour isoler les zones WAN, LAN A, LAN B et la DMZ.

Les résultats attendus pour cette mission étaient les suivants :

- **Établissement d'un tunnel VPN IPsec fonctionnel** entre le Site A et le Site B, permettant une communication transparente et chiffrée entre les deux réseaux locaux pour la réplication des données.
- **Mise en service d'un accès VPN Client-to-Site** opérationnel, autorisant un utilisateur distant à s'authentifier et à accéder aux ressources internes (LAN et DMZ) depuis une connexion Internet publique.
- **Isolation stricte des flux** grâce au pare-feu, garantissant que seuls les protocoles autorisés transitent par les tunnels VPN.
- **Validation de la connectivité de bout en bout** via des tests de continuité (ping et réplication AD) prouvant l'efficacité de l'interconnexion sécurisée.
- **Disponibilité et supervision des services** critiques à travers l'infrastructure VPN, confirmant que le tunnel supporte la charge des flux de monitoring et d'administration.

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

Description des ressources documentaires, matérielles et logicielles utilisées[2]

- **Ressources logicielles et matérielles**

L'environnement technique repose sur la solution de virtualisation **VMware ESXi 8.0**. Le parc de machines virtuelles est organisé comme suit :

● **Infrastructure Réseau :** Deux pare-feu **pfSense 2.7.2** assurant les fonctions de routage, filtrage, serveur DHCP et points de terminaison pour les tunnels **VPN IPsec** (Site-to-Site) et **OpenVPN** (Client-to-Site).

● **Services d'Annuaire :** Deux serveurs **Windows Server 2025** configurés en contrôleurs de domaine (AD DS) pour assurer la gestion centralisée des utilisateurs et la réplication des objets via le tunnel IPsec.

● **Services Linux :** Trois serveurs **Debian 12/13** dédiés à la supervision avec **Zabbix,** à l'inventaire avec **GLPI**, à l'authentification avec le serveur **RADIUS** et au serveur DMZ permettant un accès sécurisé depuis l'extérieur sans exposer le réseau local.

● **Postes Clients :** Deux machines **Windows 11 Professionnel** utilisées pour valider l'intégration au domaine et les tests de connectivité distante.

● **Outils de conception :** Utilisation de l'application **draw.io** pour la modélisation de l'architecture réseau et la réalisation du schéma de principe.

- **Plan d'adressage réseau**

● **Windows Server 1 HS-SRV1 :** 10.11.19.17 /28

● **Windows Server 2 HS-SRV2 :** 10.11.20.18 /28

● **PfSense 1 :**

Interface Web : https://10.11.19.28:444

WAN A : 10.10.101.19 /16

LAN_A : 10.11.19.16 /28

DMZ_A : 10.11.19.0 /28

Interface Web DMZ : http://10.11.19.2 & http://10.10.101.19

● **PfSense 2 :**

Interface Web : http://10.11.20.27

WAN B : 10.10.101.20 /16

LAN_B : 10.11.20.16 /28

● **Debian 1 GLPI/RADIUS :** 10.11.19.20 /28

● **Debian 2 ZABBIX :** 10.11.19.21 /28

● **Debian 3 DMZ :** 10.11.19.2 /28

● **Postes clients :** DHCP

- **Ressources documentaires**

Pour la réalisation, j'ai exploité les documentations suivantes :

● https://noob2pro.fr pour la mise en place du VPN IPsec, de l'OpenVPN, de la méthode AGDLP, de GPO, du serveur Zabbix et de la réplication AD.

● https://all-it-network.com pour la mise en place de GLPI, du serveur FreeRADIUS et la configuration de l'AD.

Modalités d'accès aux productions et à leur documentation

L'ensemble de l'infrastructure est hébergé sur un serveur **VMware ESXi** accessible via l'interface Web sur le réseau de l'établissement.

Accès à l'hyperviseur :

URL : https://10.10.255.249 Identifiant : SISR-10 Mot de passe : aQWwsAs6Sa4=

Accès aux machines virtuelles :

Équipement	Rôle	Système	Identifiant	Mot de passe
PfSense 1 https://10.11.19.28:444	Firewall / VPN	FreeBSD	admin	Hamoud6905_
PfSense 2 http://10.11.19.27	Firewall / VPN	FreeBSD	admin	Hamoud6905_
WSERV1 10.11.19.17 /28	Contrôleurs de domaine	Win Server 2025	Administrateur	Hamoud6905_
WSERV2 10.11.20.18 /28	Contrôleurs de domaine	Win Server 2025	Administrateur	Hamoud6905_
UBNT1 – GLPI / RADIUS http://10.11.19.20	Inventaire / Authentification centralisée	Debian 12	glpi	Hamoud6905_
UBNT2 - ZABBIX http://10.11.19.21/zabbix	Supervision	Debian 13	Admin	zabbix
UBNT3 - DMZ http://10.11.19.2	Bastion / Services	Debian 12	serveurdmz	Hamoud6905_
W101	Postes de test	Win 11 Pro	drh1, it2	Hamoud6905_
W102	Postes de test	Win 11 Pro	W11-Client2	Hamoud6905_

Accès aux machines virtuelles :

Un profil de connexion OpenVPN (.ovpn) est disponible sur le bureau du **Windows Server HS-SRV1**. Ce profil simule l'accès d'un collaborateur nomade via l'autorité de certification interne du pfSense.

- **Utilisateur VPN (Base locale) :** shamoud_vpn
- **Mot de passe :** Hamoud6905_

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

La mission a consisté à bâtir une architecture réseau hautement sécurisée et segmentée pour l'entreprise **SHAMOUD IT**. La réalisation s'est articulée autour de quatre phases techniques majeures :

1. **Segmentation et Isolation des réseaux (Networking)**

En m'appuyant sur l'hyperviseur **VMware ESXi** mis à disposition par l'établissement, j'ai configuré les commutateurs virtuels pour isoler les flux. J'ai installé deux pare-feu **PfSense** pour assurer le routage. Une attention particulière a été portée à la **zone DMZ**, rendue accessible depuis l'extérieur via une règle de **NAT (Port Forwarding)** sur l'adresse IP WAN du pfSense, permettant ainsi d'exposer les services nécessaires tout en protégeant le cœur du réseau.

2. **Mise en œuvre du tunnel VPN IPsec (Site-to-Site)** Pour l'interconnexion permanente des deux sites, j'ai configuré un tunnel **IPsec** entre les deux passerelles PfSense.

- **Sécurisation :** Paramétrage de l'authentification par clé partagée (PSK) et chiffrement AES-256.
- **Objectif métier :** Ce tunnel permet la **réplication Active Directory** entre les contrôleurs de domaine (HS-SRV1 et HS-SRV2) et le monitoring des équipements distants de manière transparente.

3. **Déploiement du service VPN nomade (Client-to-Site)** J'ai configuré un serveur **OpenVPN** sur le site principal pour les collaborateurs nomades.

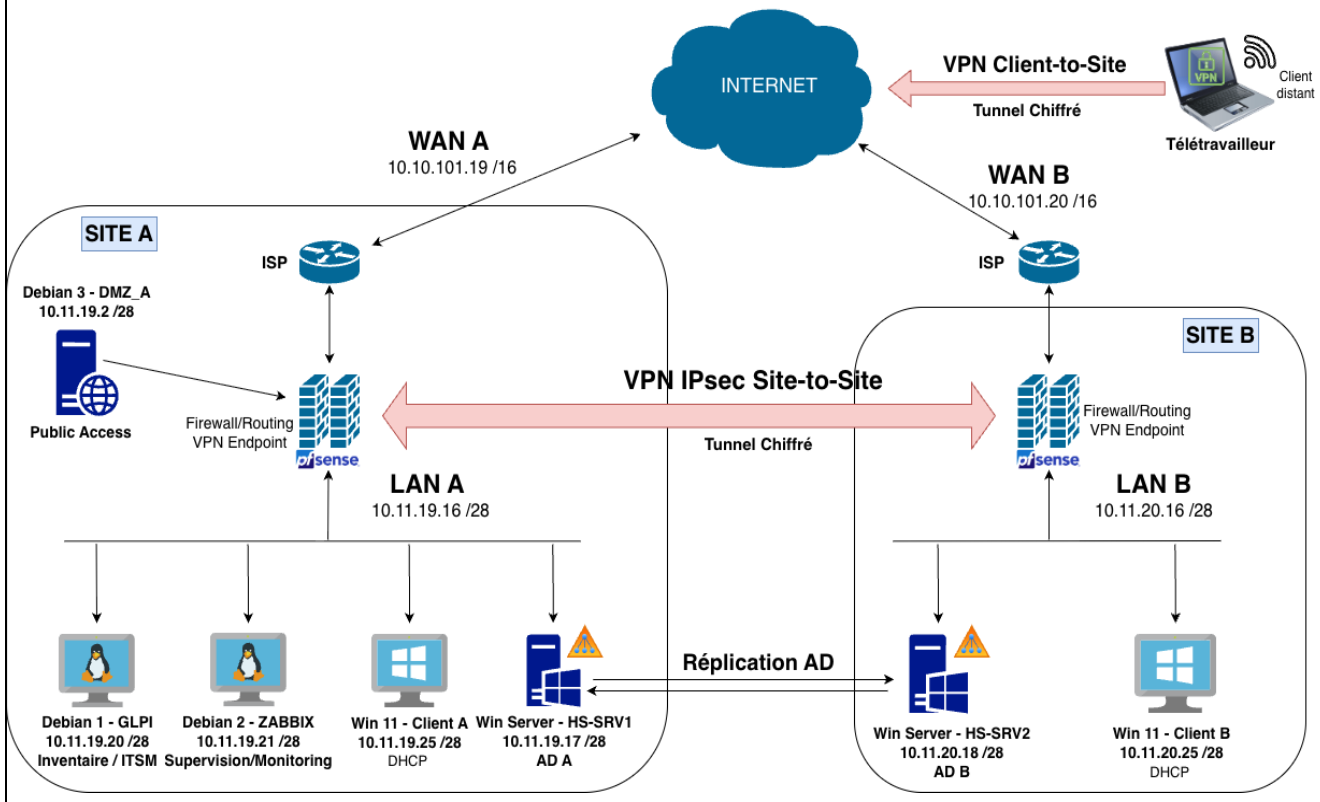
- **Authentification :** Mise en place d'une autorité de certification interne et gestion des certificats clients.
- **Accès distant :** Ce tunnel permet aux techniciens d'accéder en toute sécurité au LAN (pour l'administration) et à la DMZ depuis n'importe quelle connexion Internet.

4. **Durcissement (Hardening) et Supervision**

- **Sécurisation DMZ :** La machine **Debian 13** a été déployée **sans interface graphique (mode console uniquement)** afin de réduire les ressources consommées et de minimiser drastiquement la surface d'attaque.
- **Supervision :** Le serveur **Zabbix**, positionné stratégiquement dans le **LAN A**, assure la surveillance de l'intégralité de l'infra (serveurs, tunnels VPN, interfaces PfSense) via les flux autorisés à travers le pare-feu.

Projet **SHAMOUD**

Mise en oeuvre d'une infrastructure réseau
avec VPN sécurisé et supervision centralisée



BTS SERVICES INFORMATIQUES AUX ORGANISATIONS SESSION 2026

ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : B**
Nom, prénom : HAMOUD Mouhamed Messaoud	**N° candidat : 2544756783**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date : 25/04/2026**

Organisation support de la réalisation professionnelle

L'entreprise **SHAMOUD IT** est une ESN dynamique spécialisée dans l'infogérance réseau et le développement web pour le compte de PME.
Dans le cadre de l'interconnexion de ses deux sites géographiques, l'organisation a dû faire face à une problématique de gestion des identifiants pour ses collaborateurs nomades. En tant que technicien réseau, ma mission a consisté à renforcer la sécurité des accès distants en déployant une solution d'**authentification centralisée RADIUS**.
L'objectif était de s'affranchir d'une gestion locale des utilisateurs sur les pare-feu pfSense, peu évolutive, au profit d'un serveur **FreeRADIUS** installé sur une machine **Debian**. Cette architecture permet de centraliser la base des comptes utilisateurs et de sécuriser les demandes de connexion aux tunnels VPN via le protocole **RADIUS**. Désormais, lorsqu'un développeur nomade sollicite un accès **Client-to-Site**, le pare-feu délègue l'authentification au serveur RADIUS, garantissant ainsi un contrôle strict et unifié des accès aux ressources critiques de l'entreprise, conformément aux bonnes pratiques de sécurité informatique.

Intitulé de la réalisation professionnelle
Sécurisation et centralisation de l'authentification réseau via un serveur **RADIUS (**FreeRADIUS)

Période de réalisation : Janvier 2026 – Mai 2026 **Lieu :** Campus MEWO Metz
Modalité : ☒ **Seul(e)** ☐ **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[1] (ressources fournies, résultats attendus)

L'infrastructure a été déployée au sein d'un environnement virtualisé s'appuyant sur un hyperviseur **VMware ESXi** fourni par l'établissement. Pour mener à bien cette réalisation, j'ai disposé d'un pool de machines virtuelles comprenant :

- 2 serveurs **Windows Server 2025,**
- 2 pare-feu **PfSense 2.7**
- 2 machines **Debian Server 12**
- 1 machine **Debian Server 13**
- 2 postes clients sous **Windows 11 Professionnel**

Le réseau a été segmenté physiquement et logiquement pour isoler les zones WAN, LAN A, LAN B et la DMZ.

Les résultats attendus pour cette mission étaient les suivants :

- **Centralisation de l'authentification :** Migration réussie de la gestion des comptes utilisateurs depuis la base locale pfSense vers un serveur unique FreeRADIUS sur Debian.
- **Sécurisation des échanges AAA :** Établissement d'une liaison de confiance entre le pare-feu (NAS) et le serveur RADIUS via l'utilisation d'un secret partagé (Shared Secret).
- **Accessibilité distante via RADIUS :** Mise en service d'un accès VPN Client-to-Site où l'authentification des collaborateurs est déléguée au serveur RADIUS, garantissant l'accès aux ressources du LAN et de la DMZ.
- **Traçabilité et contrôle des accès :** Capacité à monitorer les tentatives de connexion en temps réel (via le mode debug et les logs système) pour identifier et bloquer les accès non autorisés.
- **Disponibilité et supervision des services** critiques à travers l'infrastructure VPN, confirmant que le tunnel supporte la charge des flux de monitoring et d'administration.

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

Description des ressources documentaires, matérielles et logicielles utilisées[2]

- **Ressources logicielles et matérielles**

L'environnement technique repose sur la solution de virtualisation **VMware ESXi 8.0**. Le parc de machines virtuelles est organisé comme suit :

● **Infrastructure Réseau :** Deux pare-feu **pfSense 2.7.2** assurant les fonctions de routage, filtrage, serveur DHCP et points de terminaison pour les tunnels **VPN IPsec** (Site-to-Site) et **OpenVPN** (Client-to-Site).

● **Services d'Annuaire :** Deux serveurs **Windows Server 2025** configurés en contrôleurs de domaine (AD DS) pour assurer la gestion centralisée des utilisateurs et la réplication des objets via le tunnel IPsec.

● **Services Linux :** Trois serveurs **Debian 12/13** dédiés à l'authentification avec le serveur **RADIUS,** à la supervision avec **Zabbix,** à l'inventaire avec **GLPI**, et au serveur **DMZ** permettant un accès sécurisé depuis l'extérieur sans exposer le réseau local.

● **Postes Clients :** Deux machines **Windows 11 Professionnel** utilisées pour valider l'intégration au domaine et les tests de connectivité distante.

● **Outils de conception :** Utilisation de l'application **draw.io** pour la modélisation de l'architecture réseau et la réalisation du schéma de principe.

- **Plan d'adressage réseau**

● **Windows Server 1 HS-SRV1 :** 10.11.19.17 /28

● **Windows Server 2 HS-SRV2 :** 10.11.20.18 /28

● **PfSense 1 :**

Interface Web : https://10.11.19.28:444

WAN A : 10.10.101.19 /16

LAN_A : 10.11.19.16 /28

DMZ_A : 10.11.19.0 /28

Interface Web DMZ : http://10.11.19.2 & http://10.10.101.19

● **PfSense 2 :**

Interface Web : http://10.11.20.27

WAN B : 10.10.101.20 /16

LAN_B : 10.11.20.16 /28

● **Debian 1 GLPI/RADIUS :** 10.11.19.20 /28

● **Debian 2 ZABBIX :** 10.11.19.21 /28

● **Debian 3 DMZ :** 10.11.19.1 /28

● **Postes clients :** DHCP

- **Ressources documentaires**

Pour la réalisation, j'ai exploité les documentations suivantes :

● https://noob2pro.fr pour la mise en place du VPN IPsec, de l'OpenVPN, de la méthode AGDLP, de GPO, du serveur Zabbix et de la réplication AD.

● https://all-it-network.com pour la mise en place de GLPI, du serveur FreeRADIUS et la configuration de l'AD.

Modalités d'accès aux productions et à leur documentation

L'ensemble de l'infrastructure est hébergé sur un serveur **VMware ESXi** accessible via l'interface Web sur le réseau de l'établissement.

Accès à l'hyperviseur :

URL : https://10.10.255.249 **Identifiant :** SISR-10 **Mot de passe :** aQWwsAs6Sa4=

Accès aux machines virtuelles :

Équipement	Rôle	Système	Identifiant	Mot de passe
PfSense 1 https://10.11.19.28:444	Firewall / VPN	FreeBSD	admin	Hamoud6905_
PfSense 2 http://10.11.19.27	Firewall / VPN	FreeBSD	admin	Hamoud6905_
WSERV1 10.11.19.17 /28	Contrôleurs de domaine	Win Server 2025	Administrateur	Hamoud6905_
WSERV2 10.11.20.18 /28	Contrôleurs de domaine	Win Server 2025	Administrateur	Hamoud6905_
UBNT1 – GLPI / RADIUS http://10.11.19.20	Inventaire / Authentification centralisée	Debian 12	glpi	Hamoud6905_
UBNT2 - ZABBIX http://10.11.19.21/zabbix	Supervision	Debian 13	Admin	zabbix
UBNT3 - DMZ http://10.11.19.2	Bastion / Services	Debian 12	serveurdmz	Hamoud6905_
W101	Postes de test	Win 11 Pro	drh1, it2	Hamoud6905_
W102	Postes de test	Win 11 Pro	W11-Client2	Hamoud6905_

Accès aux machines virtuelles :

Un profil de connexion OpenVPN (.ovpn) est disponible sur le bureau du **Windows Server HS-SRV1** pour simuler l'accès d'un collaborateur nomade.

- **Utilisateur VPN (Base RADIUS) :** shamoud_radius
- **Mot de passe :** Hamoud6905_

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

La mission a consisté à bâtir une architecture réseau hautement sécurisée et segmentée pour l'entreprise **SHAMOUD IT**. La réalisation s'est articulée autour de quatre phases techniques majeures :

1. **Segmentation et Isolation des réseaux (Networking)**

En m'appuyant sur la machine **Debian 12** déjà présente dans le LAN A , j'ai procédé à l'installation et à la configuration du service **FreeRADIUS**. L'objectif était de déporter la base des utilisateurs du pare-feu vers un serveur dédié afin de respecter les principes de segmentation et de gestion centralisée des identités.

2. **Configuration de la liaison de confiance (RADIUS AAA)**

Pour permettre au pare-feu d'interroger le serveur Debian, j'ai configuré les paramètres **AAA** (Authentication, Authorization, Accounting) :

- **Côté Serveur :** Déclaration du pfSense comme client autorisé (NAS) dans le fichier /**clients.conf** via l'utilisation d'un Secret Partagé (Shared Secret) pour chiffrer les échanges.
- **Côté Annuaire :** Création des comptes utilisateurs dans le fichier /**users** avec des attributs de mot de passe sécurisés (Cleartext-Password).

3. **Intégration au service VPN Nomade (Networking & Sécurité)**

J'ai modifié la configuration du serveur **OpenVPN** sur le **pfSense 2.7** pour basculer le mode d'authentification :

- **Délégation :** Remplacement de la base de données locale par le serveur RADIUS externe.
- **Filtrage :** Mise en œuvre de règles de pare-feu sur le pfSense pour autoriser spécifiquement le flux **UDP 1812** entre l'interface du pare-feu et le serveur Debian en DMZ/LAN.

4. **Diagnostic, Tests et Validation**

- **Analyse des flux :** Utilisation du mode **Debug (freeradius -X)** sur la Debian pour valider la bonne réception des paquets "Access-Request" envoyés par le pfSense.
- **Validation finale :** La validation finale a été réalisée depuis le **Windows Server 2025 (HS-SRV1)** faisant office de poste d'administration. L'installation du client **OpenVPN Connect** sur ce serveur a permis de confirmer le bon fonctionnement de l'authentification RADIUS et l'accès aux ressources distantes, simulant ainsi le comportement d'un collaborateur nomade tout en restant dans un cadre de contrôle d'infrastructure.

Projet **SHAMOUD**
Architecture d'authentification centralisée
RADIUS pour l'accès VPN Nomade