AP3 Groupe 2 - Samy ALBISSER & Emre ALBAYRAK

Système d'Information Hautement Disponible pour ECP

Mise en place d'une infrastructure hautement disponible et sécurisée entre deux sites de formation à Strasbourg

.

Status du Projet

📊 Indicateur	Valeur
Budget	12 297,87 € TTC (12% du max)
Durée	10 semaines
Début	01/09/2025
Fin	31/12/2025
Livrable 1	✅ Remis le 20/10/2025
Livrable 2	✅ Remis le 31/12/2025

.

📚 Livrables du projet

LIVRABLE 1 – Réponse au Cahier des Charges

Contenu :

- Analyse du besoin
- Solutions techniques retenues
- Budget détaillé (12 297,87 € TTC)
- Planning et diagramme de Gantt

LIVRABLE 2 – Documentation Technique

- LOT 1 : Configuration Réseau et VPN Site-à-Site

- *Détails :* Adressage IP, Routage, VPN IPsec.

- 🆔 LOT 2 : Déploiement Active Directory, DNS et DHCP
  - *Détails :* Contrôleurs de domaine, Forêt, Zones DNS.
- LOT 3 : Configuration du Stockage (SAN/NAS) et Système de Fichiers Distribués
  - *Détails :* iSCSI, Réplication de fichiers, Quotas.
- 🛡️ LOT 4 : Sécurisation, Stratégies de Groupe (GPO) et Pare-feu
  - *Détails :* Stratégies de groupe, Filtrage, Durcissement.

À propos du groupe

Samy ALBISSER - Chef de Projet

- Coordination du projet et infrastructure Site A (Vauban)
- Documentation et procédures
- Rédaction des livrables

💻 **Emre ALBAYRAK** - Responsable Technique

- Infrastructure Site B (Somme)
- Tests et intégration réseau
- Validation technique

🎓 Formation

BTS SIO SISR - 2ème année

ECP Apprentissage (Groupe GEFE)

Strasbourg, France

LIVRABLE 1 – Réponse au Cahier des Charges

⬅ Retour à l'accueil

Projet : AP3 – Système d'Information Hautement Disponible pour ECP

Groupe : Samy ALBISSER & Emre ALBAYRAK

Durée : 10 semaines (01/09/2025 – 31/12/2025)

Date de remise : 20 octobre 2025 à 20H

image.png

.

.

1. Présentation du groupe

Dans le cadre de l'AP3, notre groupe est composé de **Samy ALBISSER** et **Emre ALBAYRAK**, tous deux étudiants en 2e année de BTS SIO SISR.

Samy ALBISSER occupe le rôle de **chef de projet**. Il assure la coordination du projet, la structuration documentaire, ainsi que la gestion de l'infrastructure du **site A (Strasbourg Vauban)**. Il prend en charge la rédaction des procédures, l'installation des serveurs principaux et la validation technique.

Emre ALBAYRAK assure le rôle de **technicien infrastructure**, responsable du **site B (Strasbourg Somme)**. Il est en charge de l'installation, des tests, de l'intégration réseau et de la mise en place des solutions de sauvegarde.

Notre binôme fonctionne de manière **autonome et complémentaire**, avec une répartition équilibrée des tâches et une communication régulière pour garantir le respect des délais et la qualité des livrables.

.

2. Rappel des besoins et objectifs du projet

2.1 Contexte

L'**ECP Apprentissage** fait partie du Groupe GEFE (Groupe Europe Formation Éducation) et forme des professionnels dans les domaines de l'immobilier, de l'assurance, de la gestion patrimoniale et de l'informatique. L'établissement est implanté sur deux sites à Strasbourg : le site Vauban et le site Somme.

Suite à l'ouverture de deux nouvelles classes de BTS SIO, l'école doit aménager de nouvelles salles informatiques et créer un système d'information indépendant pour répondre aux besoins pédagogiques et administratifs.

> Explication pour le patron : L'ECP est un centre de formation qui accueille des étudiants sur deux bâtiments différents à Strasbourg. Ils ont besoin d'un système informatique fiable qui fonctionne même si l'un des deux sites rencontre un problème technique.

2.2 Objectifs stratégiques

Le projet doit permettre d'atteindre des améliorations sur 4 axes principaux :

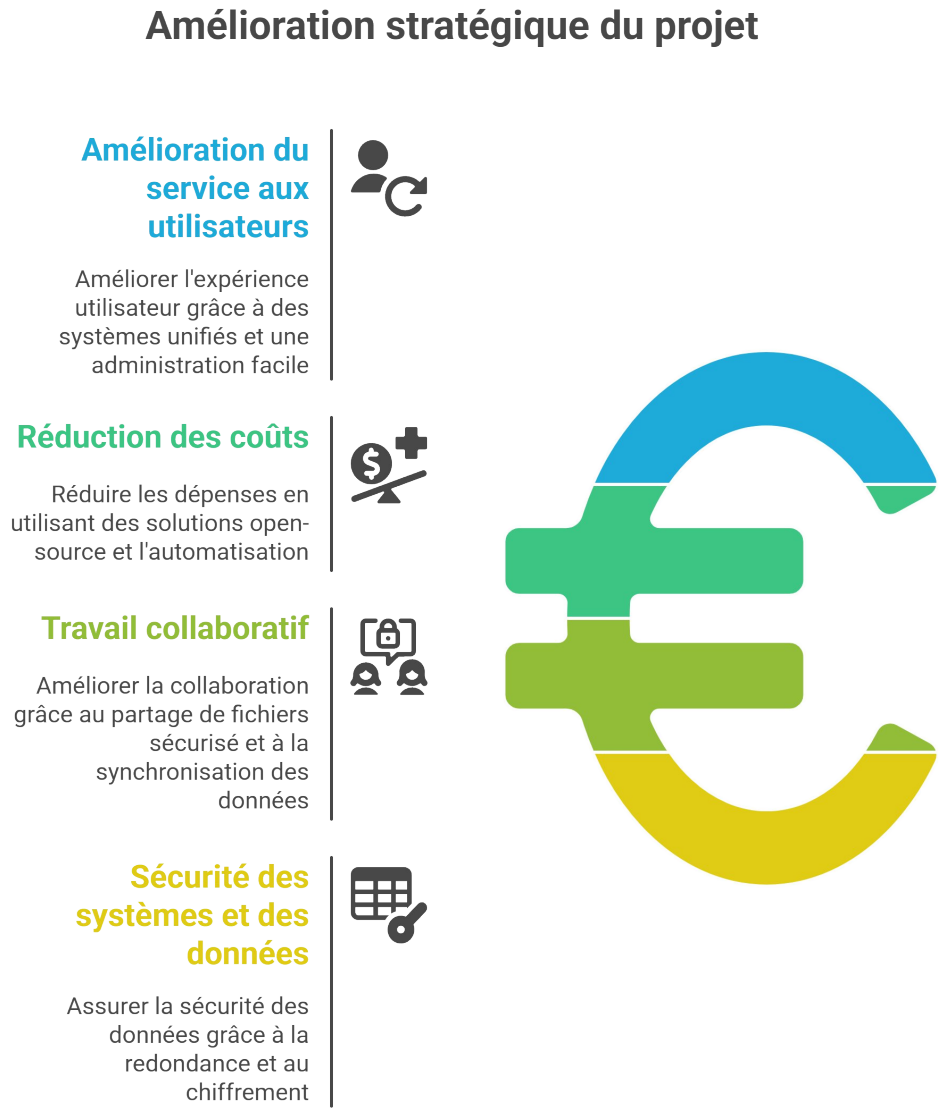


image.png

Axe 1 : Amélioration du service aux utilisateurs

- Création d'un système d'information indépendant et unifié
- Liaison sécurisée entre les deux sites (Vauban et Somme)
- Redondance des services : si un serveur tombe en panne, un autre prend le relais automatiquement
- Facilité d'administration pour l'équipe informatique

Explication pour le patron : Imaginez que vous avez deux magasins dans deux quartiers différents. Si le système informatique du premier magasin tombe en panne, les employés du second magasin peuvent continuer à travailler normalement. C'est ce qu'on appelle la redondance : avoir plusieurs copies des informations importantes pour éviter les interruptions.

Axe 2 : Réduction des coûts

- Utilisation de solutions open-source gratuites lorsque c'est possible
- Documentation complète pour faciliter la maintenance future
- Réduction du temps d'intervention grâce à l'automatisation

Axe 3 : Travail collaboratif

- Partage de fichiers sécurisé entre les deux sites
- Accessibilité des données depuis n'importe quel site
- Synchronisation automatique des documents entre les serveurs

Axe 4 : **Sécurité des systèmes et des données**

- Plan de Continuité d'Activité (PCA) : pouvoir redémarrer rapidement en cas de panne majeure
- Redondance des serveurs et des données
- Sauvegarde régulière et automatique
- Chiffrement des communications entre les deux sites

  Explication pour le patron : Le chiffrement, c'est comme mettre vos documents importants dans un coffre-fort numérique. Même si quelqu'un intercepte les données qui circulent entre les deux sites, il ne pourra pas les lire sans la clé de déchiffrement

2.3 Objectifs techniques attendus

Le cahier des charges impose plusieurs objectifs techniques précis :

Objectif	Description	Bénéfice
VPN inter-sites	Liaison chiffrée (IPsec) entre Site A et Site B	Communication sécurisée entre les deux bâtiments
Active Directory	Annuaire centralisé avec 4 contrôleurs de domaine (1 principal + 3 secondaires)	Authentification unique (SSO) et gestion centralisée des utilisateurs
DNS + DHCP	Résolution de noms et attribution automatique d'adresses IP	Connexion automatique des ordinateurs au réseau
DFS + DFSR	Partage de fichiers distribué avec réplication automatique	Les fichiers sont accessibles depuis les deux sites et synchronisés en temps réel
Sauvegarde iSCSI	Sauvegarde complète des serveurs sur un espace de stockage dédié (SAN)	Protection contre la perte de données
Clichés instantanés	Snapshots automatiques des fichiers importants	Possibilité de restaurer une version antérieure d'un fichier

image.png

Explication pour le patron :

- **Active Directory (AD)** : C'est comme un annuaire téléphonique de votre entreprise, mais pour les ordinateurs. Il contient tous les comptes utilisateurs et permet de se connecter une seule fois pour accéder à toutes les ressources (c'est le SSO : Single Sign-On).
- **DFS (Distributed File System)** : Au lieu d'avoir vos documents sur un seul serveur, ils sont répartis sur plusieurs serveurs et synchronisés automatiquement. Si un serveur tombe, vous pouvez toujours accéder à vos fichiers depuis l'autre.
- **iSCSI** : C'est une technologie qui permet de créer un disque dur réseau. On l'utilise ici pour stocker les sauvegardes des serveurs.
- **Chiffrement** : C'est comme mettre vos documents importants dans un coffre-fort numérique. Même si quelqu'un intercepte les données qui circulent entre les deux sites, il ne pourra pas les lire sans la clé de déchiffrement.

2.4 Périmètre du projet

Nombre d'utilisateurs : 90 personnes (60 à Strasbourg + 30 à Mulhouse prévus)

Postes de travail : 60 PC fixes + 90 PC portables

Nombre de serveurs : 8 serveurs au total :

- 2 routeurs/pare-feu (1 par site)
- 4 serveurs Windows Server 2022 Standard (2 par site)
- 2 serveurs NAS/SAN pour les sauvegardes (1 par site)

Plans d'adressage réseau :

- Site A (Vauban) : 192.168.100.0/24 (254 adresses IP disponibles)
- Site B (Somme) : 192.168.200.0/24 (254 adresses IP disponibles)
- Nom de domaine : IEF.LOCAL

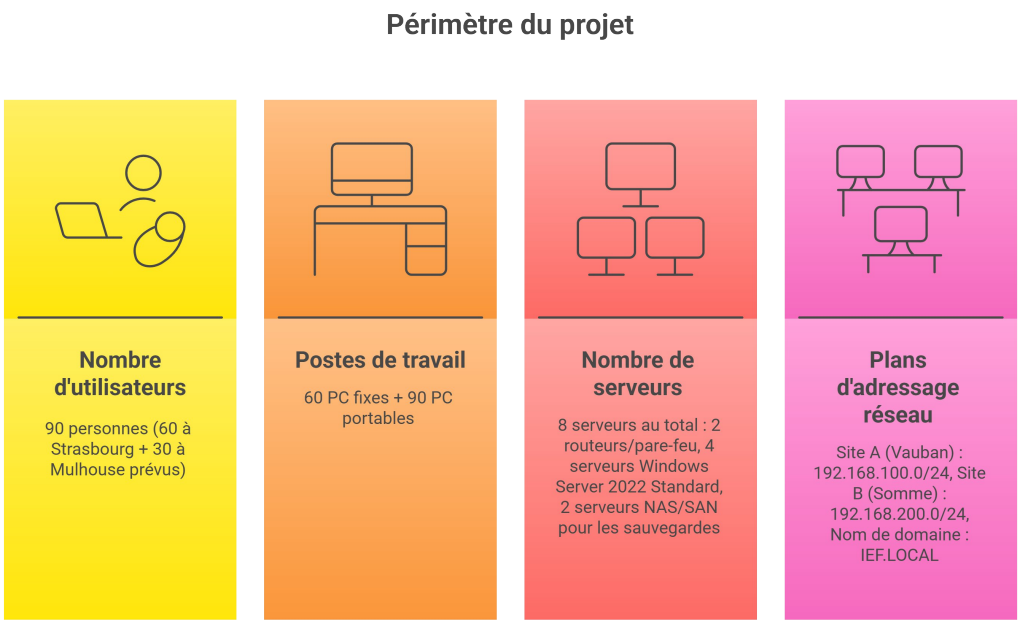


image.png

2.5 Contraintes du projet

Contrainte	Détail
Budget maximum	100 000 € HT
Durée du projet	10 semaines (du 01/09/2025 au 31/12/2025)
Compatibilité	Windows Server 2022 Standard obligatoire
Open-source	Privilégier les solutions gratuites/open-source quand c'est possible
Documentation	Documentation complète obligatoire pour faciliter la maintenance

Explication pour le patron :

Ce projet consiste à créer une infrastructure informatique **hautement disponible** (c'est-à-dire qui fonctionne 24h/24, même en cas de panne d'un

serveur) et **interconnectée** (les deux sites de Strasbourg peuvent partager les données de manière sécurisée). Cela garantit que vos équipes peuvent travailler sans interruption et que les données sont protégées contre les pertes.

.

3. Solutions proposées et études comparatives

Pour chaque besoin technique du projet, nous avons comparé deux solutions open-source ou gratuites afin de justifier nos choix. Les **critères de sélection** sont les suivants :

- Coût : solution gratuite ou peu coûteuse
- Facilité d'installation et de maintenance
- Performance et stabilité
- Compatibilité avec l'infrastructure existante
- Disponibilité de la documentation et du support communautaire

3.1 Solution pour le routeur/pare-feu avec VPN

Besoin : Un routeur/pare-feu open-source capable de créer un tunnel VPN chiffré (IPsec) entre les deux sites

Comparaison : pfSense vs OPNsense

Critère	pfSense Community Edition	OPNsense
Type	Open-source (licence Apache)	Open-source (licence BSD)
Système de base	FreeBSD 14	FreeBSD 14.2
Interface graphique	Interface fonctionnelle mais plus traditionnelle	Interface moderne et intuitive
VPN intégrés	OpenVPN, IPsec, WireGuard (via package)	OpenVPN, IPsec, WireGuard (intégré nativement)
Mises à jour	Parfois en retard sur la version gratuite (priorité à pfSense Plus payant)	Cycle de mises à jour régulier et prévisible
Authentification 2FA	Via package supplémentaire	Intégré nativement
Communauté	✅ Très large communauté, beaucoup de tutoriels	Communauté active et en croissance
Support commercial	Netgate (payant)	Deciso (payant)
Sécurité	Bonne, mais basée sur FreeBSD 14.0 qui est EOL depuis nov. 2023	Très bonne, basée sur FreeBSD 14.2 (version supportée)
Avantages	✅ Large base documentaire	

✅ Très répandu en entreprise ✅ Support matériel Netgate | ✅ Interface plus moderne ✅ Mises à jour régulières ✅ 2FA natif ✅ FreeBSD à jour | | Inconvénients | ❌ Interface

vieillissante ✕ Version CE parfois délaissée au profit de Plus | ✕ Communauté plus petite ✕ Moins de matériel dédié |

✓ **Solution retenue : pfSense Community Edition**

Justification :

pfSense est une solution **mature, éprouvée et largement documentée**, idéale pour un contexte pédagogique. Ses avantages principaux :

- **Très large communauté** : des milliers de tutoriels en français et en anglais, forums actifs, documentation complète
- **Très répandu en entreprise** : compétences transférables et valorisables sur le marché du travail
- **Support matériel Netgate** : possibilité d'acheter du matériel dédié avec support professionnel
- **Excellentes performances** : gère jusqu'à 1000+ utilisateurs simultanés
- **Configuration VPN IPsec complète** : support natif d'IKEv1, IKEv2, conforme aux recommandations ANSSI

Bien qu'OPNsense ait une interface plus moderne, pfSense reste **le standard industriel** pour les pare-feu open source, ce qui en fait un meilleur choix pour notre formation professionnelle.

> Explication pour le patron :
>
> Un **routeur/pare-feu** protège votre réseau des intrusions extérieures en filtrant les connexions. Le **VPN IPsec** crée un "tunnel sécurisé" entre vos deux sites de Strasbourg, permettant aux données de transiter de manière chiffrée (cryptée), comme si les deux sites étaient dans le même bâtiment.

.

3.2 Solution pour le NAS/SAN (sauvegarde iSCSI)

Besoin : Un serveur de stockage capable de créer des cibles iSCSI pour héberger les sauvegardes complètes des serveurs Windows.

Comparaison : TrueNAS Core vs OpenMediaVault

Critère	TrueNAS Core	OpenMediaVault (OMV)
Type	Open-source (FreeBSD)	Open-source (Debian Linux)
Système de fichiers	✓ ZFS (très robuste, intégrité des données)	ext4, XFS, BTRFS (au choix)
Support iSCSI	✓ Natif, très performant	✓ Natif, via plugin
RAM recommandée	Minimum 8 Go (ZFS gourmand)	Minimum 1 Go (très léger)
Interface	Interface web moderne et intuitive	Interface web fonctionnelle, plugins pour étendre
Déduplication	✓ Intégré (ZFS)	✕ Pas natif
Snapshots	✓ Intégré (ZFS)	✓ Via BTRFS ou LVM
Communauté	Très large, documentation complète	Active, documentation claire

Critère	TrueNAS Core	OpenMediaVault (OMV)
Complexité	Moyenne (configuration ZFS)	Faible (installation simplifiée)
Avantages	✅ ZFS ultra-fiable	

✅ Snapshots performants ✅ Compression native ✅ Déduplication | ✅ Très léger en ressources ✅ Basé sur Debian (familier) ✅ Plugins nombreux | | Inconvénients | ❌ Gourmand en RAM ❌ Configuration ZFS technique | ❌ Moins de fonctionnalités avancées ❌ Pas de déduplication native |

✅ **Solution retenue : TrueNAS Core**

Justification :

TrueNAS Core est la solution professionnelle par excellence pour le stockage critique. Ses avantages décisifs :

- **ZFS** : système de fichiers ultra-robuste avec vérification automatique de l'intégrité des données
- **Snapshots instantanés** pour restaurer rapidement en cas de problème
- **Déduplication et compression natives** pour économiser l'espace disque
- **Support iSCSI très performant** et bien documenté
- **Très utilisé en entreprise** et dans les environnements de formation
- Les machines virtuelles modernes disposent de suffisamment de RAM (nous allons allouer 2 Go par VM NAS, ce qui est largement suffisant pour notre usage)

Alternative : Si les ressources RAM sont très limitées, OpenMediaVault reste une excellente alternative, mais TrueNAS Core offre plus de fonctionnalités avancées et une meilleure protection des données avec ZFS.

Approfondissement : Pourquoi ZFS est essentiel pour ce projet

ZFS (Zettabyte File System) n'est pas un simple système de fichiers, c'est un gestionnaire de volumes et de système de fichiers combiné qui apporte des fonctionnalités critiques pour la haute disponibilité :

Protection avancée des données :

- **Checksums 256 bits** : Chaque bloc de données possède une empreinte numérique unique permettant de détecter automatiquement toute corruption silencieuse
- **Auto-réparation (Self-Healing)** : En cas de corruption détectée, ZFS utilise automatiquement les copies redondantes pour restaurer les données corrompues
- **Copy-on-Write (COW)** : Les données ne sont jamais écrasées directement, éliminant les risques de corruption lors des écritures

Snapshots (Clichés instantanés) :

- Les snapshots ZFS sont **instantanés, gratuits en espace disque et sans impact sur les performances** tant que les données ne sont pas modifiées
- Ils permettent de revenir à un état antérieur en quelques secondes, idéal pour récupérer des fichiers supprimés ou corrompus

- Contrairement aux sauvegardes classiques, les snapshots ZFS sont **atomiques** (cohérents à l'instant T)

Déduplication au niveau bloc :

- ZFS peut éliminer les doublons de données **au niveau des blocs** (et non des fichiers entiers)
- Cependant, la déduplication nécessite beaucoup de RAM (environ **5 Go de RAM par To de données dédupliquées**)
- Pour l'AP3, nous **désactiverons la déduplication** car les besoins en RAM dépasseraient les ressources disponibles en environnement pédagogique

Compression transparente :

- ZFS supporte la compression LZ4 (rapide et efficace) sans impact sur les performances
- La compression peut **améliorer les performances** en réduisant les I/O disque
- Pour l'AP3, nous activerons la **compression LZ4** sur les volumes de sauvegarde

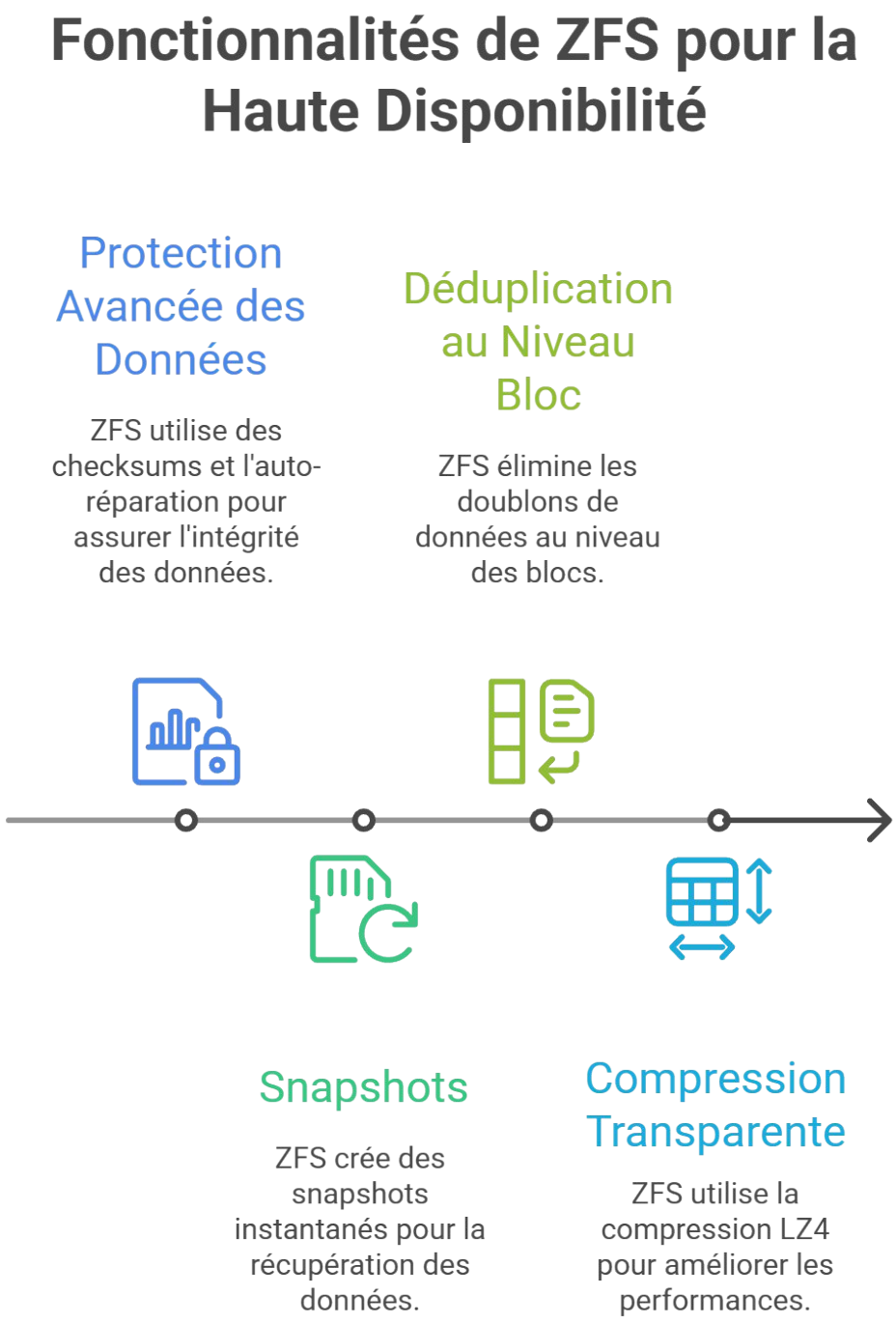


image.png

Explication pour le patron : Un NAS/SAN, c'est un serveur de fichiers dédié au stockage. Ici, on utilise la technologie iSCSI qui permet de créer un disque dur virtuel accessible via le réseau. Les serveurs Windows le voient comme un disque dur local, ce qui permet de faire des sauvegardes complètes très rapidement. ZFS est un système de fichiers ultra-sécurisé qui protège vos

données contre la corruption et permet de revenir à une version antérieure en cas de problème (snapshots). C'est comme une "machine à remonter le temps" pour vos données.

3.3 Solution pour le VPN site-to-site

Besoin : Un protocole VPN fiable et sécurisé pour relier les deux sites de manière chiffrée.

Comparaison : IPsec vs OpenVPN

Critère	IPsec (Internet Protocol Security)	OpenVPN
Type	Standard ouvert (protocole réseau niveau 3)	Open-source (niveau applicatif)
Chiffrement	AES-256, 3DES, etc.	AES-256, ChaCha20, etc.
Performance	⚡ Très rapide (protocole UDP, intégré au noyau OS)	⚡ Légèrement plus lent (double encapsulation)
Compatibilité native	✅ Intégré dans tous les OS (Windows, Linux, macOS, iOS, Android)	❌ Nécessite installation d'un client
Configuration	Complexe (nombreux paramètres IKE, ESP, AH)	Plus simple (fichier de configuration unique)
Traversée de NAT	❌ Plus difficile (nécessite NAT-T)	✅ Facile (peut utiliser n'importe quel port TCP/UDP)
Usage recommandé	Site-to-site (liaison fixe entre deux réseaux)	Client-to-site (accès distant utilisateur)
Support firewall	✅ Intégré nativement dans pfSense et OPNsense	✅ Intégré nativement
Stabilité	✅ Très stable pour les connexions permanentes	✅ Très stable
Recommandations ANSSI	✅ Recommandé (annexe 5 du sujet)	✅ Accepté
Avantages	✅ Très performant	

✅ Standard industriel ✅ Pas de client à installer ✅ Recommandé par l'ANSSI | ✅ Configuration plus simple ✅ Traverse facilement les firewalls ✅ Bonne documentation |
| Inconvénients | ❌ Configuration complexe ❌ Dépannage difficile | ❌ Légèrement moins performant ❌ Nécessite installation client |

✅ **Solution retenue : IPsec**

Justification :

IPsec est **imposé par le cahier des charges** (Annexe 5 : recommandations ANSSI sur IPsec). Ses avantages pour notre projet :

- **Imposé par le cahier des charges** : conforme aux recommandations ANSSI
- **Protocole standard** pour les VPN site-to-site en entreprise
- **Performance maximale** grâce à l'intégration au niveau du noyau système

- **Pas de client à installer** sur les serveurs ou les postes
- **Très stable** pour les connexions permanentes 24h/24
- **Bien supporté nativement** par pfSense et OPNsense
- **IKEv2 (Internet Key Exchange version 2)** : protocole moderne et sécurisé pour l'échange de clés

Alternative : Si IPsec posait des problèmes de configuration, nous pourrions basculer sur OpenVPN (bien documenté et plus simple), ou même sur WireGuard (protocole VPN moderne et ultra-rapide), mais IPsec reste le choix le plus professionnel pour ce type de liaison.

> Explication pour le patron : IPsec, c'est le protocole de sécurité standard de l'internet. C'est comme un convoi blindé qui transporte vos données entre les deux sites. OpenVPN est une alternative plus moderne et plus facile à configurer, mais un peu moins rapide. Pour notre projet, IPsec est recommandé dans le cahier des charges car il est plus adapté aux connexions permanentes entre deux sites fixes.

.

3.4. Solution de sauvegarde des serveurs Windows

Besoin : Sauvegarder complètement les serveurs Windows (OS + données) sur un espace de stockage iSCSI.

Comparaison : Windows Server Backup vs Veeam Agent (Community)

Critère	Windows Server Backup	Veeam Agent for Windows (Community/Free)
Type	Natif (intégré à Windows Server)	Gratuit (édition Community)
Interface	Graphique (console MMC) et PowerShell	Graphique et ligne de commande
Types de sauvegarde	Complète, incrémentale, planifiée	Complète, incrémentale, différentielle
Destination	Disque local, réseau, iSCSI	Disque local, réseau, iSCSI, cloud, répertoire Veeam
Restauration	Complète ou fichier par fichier	Complète, fichier par fichier, instantanée
Chiffrement	✓ Possible (BitLocker sur la cible)	✓ Chiffrement intégré AES-256
Compression	✗ Non disponible	✓ Oui (économie d'espace)
Performance	Bonnes (natif)	Excellentes (optimisations avancées)
Planification	Quotidienne uniquement	Flexible (horaire, quotidienne, hebdomadaire)
Compatibilité	Windows Server uniquement	Windows Server et postes clients

Critère	Windows Server Backup	Veeam Agent for Windows (Community/Free)
Facilité d'utilisation	Simple pour les sauvegardes basiques	Simple avec plus de fonctionnalités
Évolutivité	🟡 Moyenne (jusqu'à 10 serveurs)	🟡 Moyenne (jusqu'à 10 agents en version gratuite)zones
Coût	Gratuit (intégré)	Gratuit (jusqu'à 10 agents)zones

✅ **Solution retenue : Windows Server Backup**

Justification :

Windows Server Backup est la solution idéale pour notre projet car :

- **Gratuit et intégré nativement** à Windows Server 2022, sans aucune installation supplémentaire
- **Simplicité d'utilisation** : interface graphique intuitive et configuration rapide via console MMC ou PowerShell
- **Compatibilité totale** avec les volumes iSCSI montés depuis TrueNAS
- **Fiabilité éprouvée** : solution Microsoft testée et validée depuis Windows Server 2008
- **Sauvegardes complètes et incrémentielles** programmables quotidiennement
- **Restauration flexible** : restauration complète du serveur ou fichier par fichier
- **Pas de limitation** : aucune restriction sur le nombre de serveurs sauvegardés
- **Documentation officielle Microsoft** très complète en français
- **Contexte pédagogique adapté** : permet de se concentrer sur la configuration sans complexité supplémentaire

Alternative : Veeam Agent offre des fonctionnalités avancées (compression, chiffrement natif, interface moderne) qui peuvent être intéressantes dans un contexte professionnel, mais Windows Server Backup répond parfaitement aux besoins du cahier des charges tout en respectant la philosophie "intégré et simple" du projet.

> Explication pour le patron :
>
> La **sauvegarde** consiste à créer une copie de secours complète de vos serveurs (système d'exploitation + toutes les données). En cas de panne matérielle ou de cyberattaque, vous pouvez **restaurer** rapidement votre serveur et reprendre votre activité sans perte de données.

.

3.5 Système de fichiers distribués (DFS) et réplication (DFSR)

Besoin : Permettre l'accès centralisé aux données depuis les deux sites et répliquer automatiquement les fichiers entre les serveurs.

Solution imposée : **DFS et DFSR (Windows Server 2022)**

Le cahier des charges impose l'utilisation de **DFS (Distributed File System)** et **DFSR (DFS Replication)** pour créer un espace de noms unique accessible

depuis `\\IEF.LOCAL\INTRANET` et répliquer les données entre les 4 serveurs en maille pleine.

Caractéristiques :

- **DFS** : Espace de noms unifié permettant d'accéder aux données depuis un seul point d'entrée, indépendamment de leur localisation physique
- **DFSR** : Réplication automatique et bidirectionnelle des fichiers entre les serveurs, garantissant la redondance et la haute disponibilité
- **Clichés instantanés (Shadow Copy)** : Sauvegardes automatiques des versions précédentes des fichiers, permettant la restauration en cas de suppression ou modification accidentelle
- **Droits et permissions NTFS** : Gestion fine des accès (chaque utilisateur accède uniquement à ses propres dossiers)

Évolutivité : Excellente (jusqu'à plusieurs milliers d'utilisateurs)

Approfondissement : Fonctionnement de DFSR et topologies de réplication

Comment fonctionne DFSR :

Réplication multi-maître :

- DFSR fonctionne en mode **multi-maître** : tous les serveurs peuvent recevoir des modifications simultanément
- En cas de conflit (modification simultanée du même fichier sur 2 sites), DFSR applique une **résolution automatique** basée sur l'horodatage (dernière écriture gagnante)
- Le fichier "perdant" est conservé dans un dossier `ConflictAndDeleted` pour récupération manuelle

Remote Differential Compression (RDC) :

- DFSR n'envoie que les **blocs modifiés** d'un fichier, pas le fichier entier
- Pour un fichier Word de 10 Mo modifié de 2 Ko, seuls 2 Ko sont transférés via le VPN
- Cela réduit considérablement la bande passante utilisée et accélère la réplication

Topologies de réplication :

Pour l'AP3, le cahier des charges impose une **topologie en maille pleine (Full Mesh)** :

Topologie	Description	Avantages	Inconvénients
Hub and Spoke	Un serveur central (hub) réplique vers plusieurs serveurs secondaires (spokes)	Simple à gérer, économise la bande passante	Point de défaillance unique (hub), latence accrue
Full Mesh (Maille pleine)	Tous les serveurs répliquent entre eux directement	✅ Haute disponibilité, ✅ Faible latence, ✅ Pas de point unique de défaillance	Plus complexe à gérer (pour 4+ serveurs)
Hybride	Combinaison	Équilibre entre	Configuration

Topologie	Description	Avantages	Inconvénients
	Hub/Spoke + Mesh	simplicité et redondance	complexe

Justification pour l'AP3 : La **maille pleine** garantit que chaque serveur peut communiquer directement avec les autres, même si le VPN entre les deux sites tombe en panne (les serveurs du même site continuent à se répliquer).

Limitations de DFSR :

- DFSR réplique un fichier **uniquement après sa fermeture** (pas de réplication en temps réel)
- **Non adapté** pour les bases de données ouvertes en permanence (SQL Server, Exchange)
- Pour ces cas, Microsoft recommande **Storage Replica** (disponible dans Windows Server 2016+)

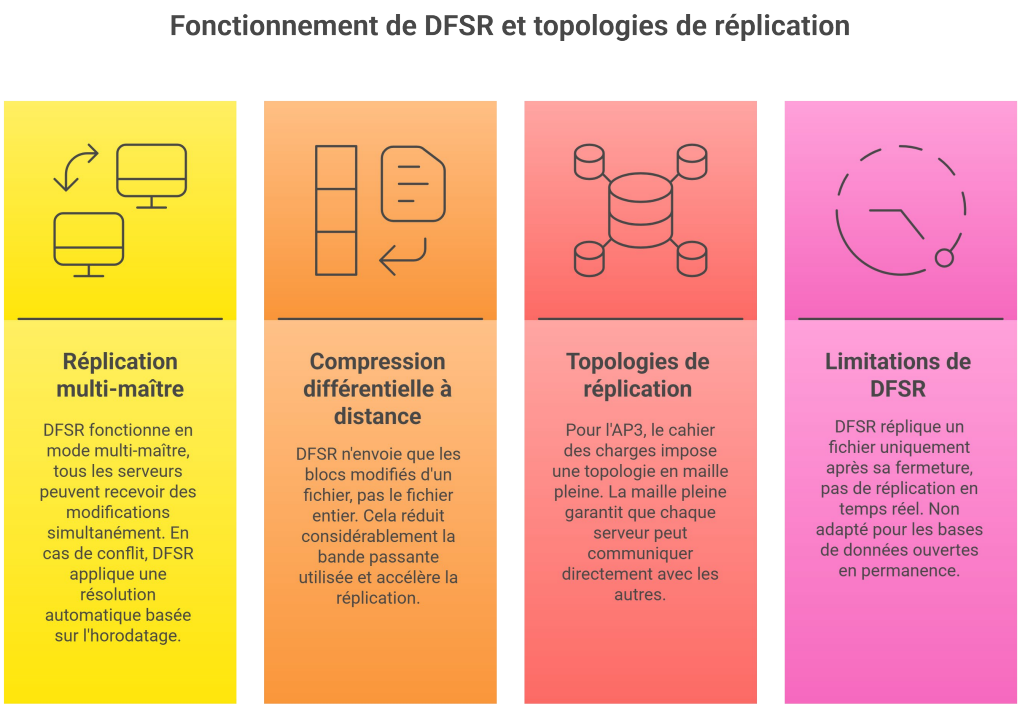


image.png

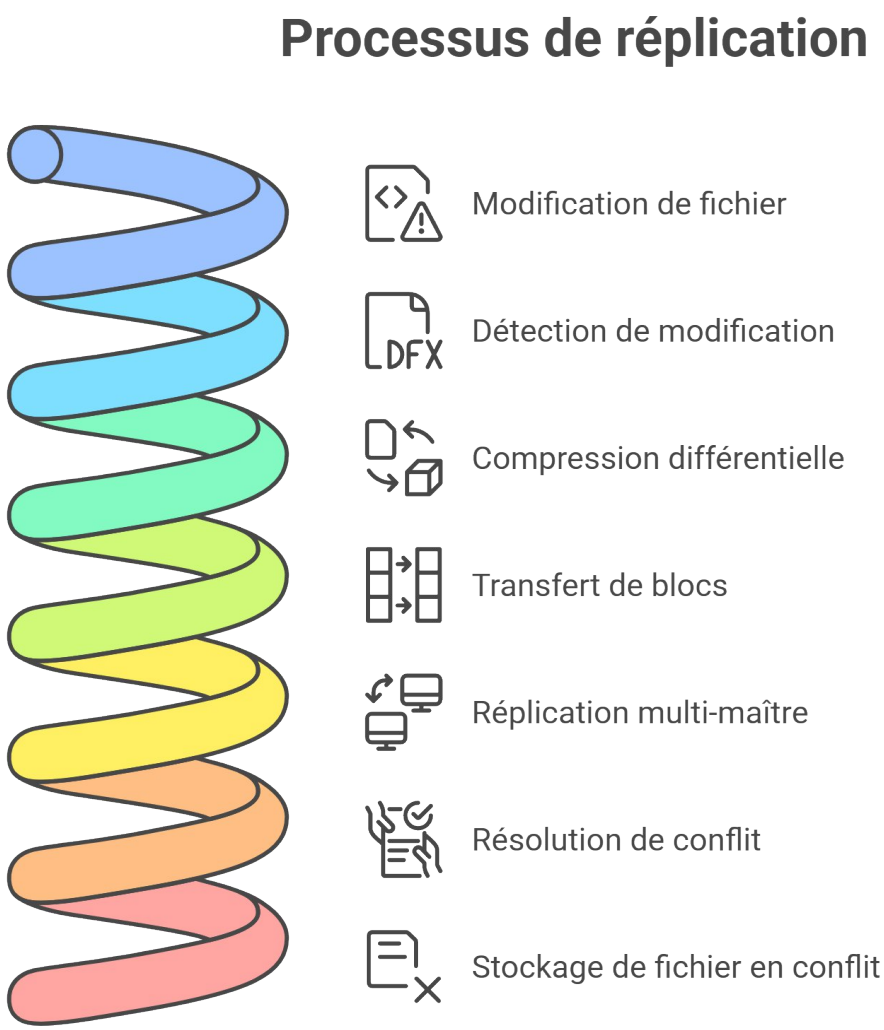


image.png

Explication pour le patron : DFS permet à vos employés d'accéder à leurs fichiers de manière transparente, qu'ils soient à Strasbourg Vauban ou Strasbourg Somme. DFSR synchronise automatiquement les données entre les deux sites : si un fichier est modifié sur un site, il est automatiquement mis à jour sur l'autre en quelques minutes. Les clichés instantanés permettent de récupérer une version antérieure d'un fichier supprimé par erreur (jusqu'à 64 versions précédentes conservées). Le maille pleine signifie que chaque serveur se synchronise avec tous les autres serveurs. Si vous modifiez un fichier sur le Site A, il sera automatiquement copié sur le Site B, et vice-versa. C'est comme avoir un miroir parfait de vos données à chaque endroit.

.

3.6. Annuaire d'authentification (Active Directory)

Besoin : Centraliser l'authentification des utilisateurs et des postes, déployer des stratégies de groupe (GPO).

Solution imposée : **Active Directory Domain Services (AD DS) – Windows Server 2022**

Le cahier des charges impose l'utilisation d'**Active Directory** comme annuaire centralisé avec **1 forêt unique** et **4 contrôleurs de domaine** (1 principal sur le site A, 3 supplémentaires répartis sur les sites A et B).

Caractéristiques :

- **Authentification unique (SSO)** : Les utilisateurs se connectent une seule fois avec leurs identifiants pour accéder à tous les services.
- **Gestion centralisée** : Création et gestion des comptes utilisateurs, groupes, unités organisationnelles (UO).
- **Stratégies de groupe (GPO)** : Déploiement automatique de configurations (fond d'écran, lecteurs réseau, restrictions, redirection de dossiers).
- **Redondance** : 4 contrôleurs de domaine garantissent la haute disponibilité (si un serveur tombe en panne, les autres prennent le relais).
- **Intégration DNS et DHCP** : Gestion automatique des noms de domaine et attribution des adresses IP.

Évolutivité : Excellente (jusqu'à 1000+ utilisateurs).

Explication pour le patron :

Active Directory est l'annuaire centralisé qui gère tous les comptes utilisateurs et ordinateurs de l'entreprise. Grâce à lui, vos employés peuvent se connecter sur n'importe quel poste avec leurs identifiants, et l'administrateur peut déployer des paramètres de sécurité ou des logiciels automatiquement sur tous les ordinateurs.

3.7 Synthèse des solutions retenues

Besoin	Solution retenue	Justification principale	Alternative
Routeur/Firewall	pfSense CE	Large communauté, très documenté, standard industriel	OPNsense
NAS/SAN iSCSI	TrueNAS Core	ZFS ultra-fiable, snapshots performants, déduplication native	OpenMediaVault
VPN site-to-site	IPsec	Standard industriel, recommandé ANSSI, très performant	OpenVPN
Sauvegarde serveurs	Windows Server Backup	Intégré nativement, gratuit, simple, fiable, pas d'installation	Veeam Agent Community
Serveurs Windows	Windows Server 2022 Standard	Imposé par le cahier des charges	-
Active Directory	AD DS avec 4 DC	Haute disponibilité, réplication	-

Besoin	Solution retenue	Justification principale	Alternative
		automatique	
Partage de fichiers	DFS + DFSR	Synchronisation automatique entre sites, transparence pour l'utilisateur	-

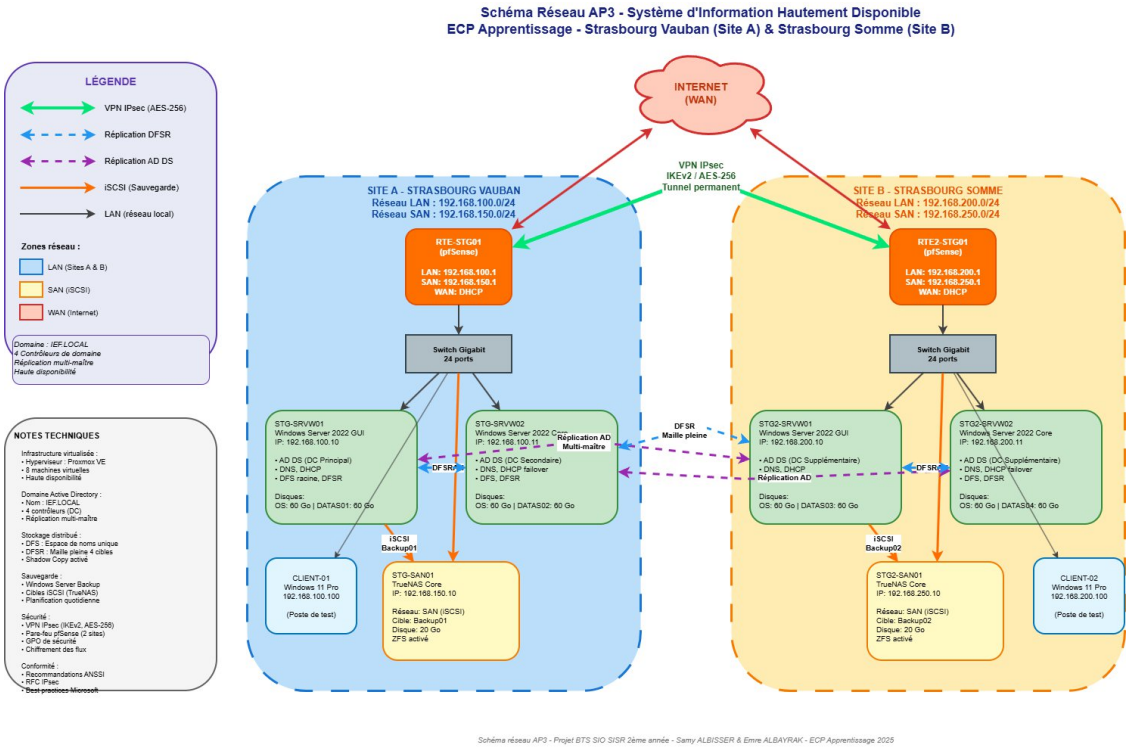
Explication pour le patron : Toutes les solutions que nous avons choisies sont soit gratuites, soit open-source, ce qui respecte le budget du projet. Les seuls coûts concernent les licences Windows Server 2022 et les licences CAL (Client Access License) qui sont obligatoires pour que les utilisateurs puissent se connecter aux serveurs Windows.

.

4. Schéma réseau complet

4.1 Vue d'ensemble de l'architecture

Le schéma ci-dessous présente l'architecture complète du système d'information hautement disponible déployé sur les deux sites de formation (Vauban et Somme).



Schema_Reseau_AP3_ULTIME.drawio.png

4.2 Points clés de l'infrastructure

L'architecture s'articule autour de plusieurs composants essentiels :

Site A (Vauban) - 192.168.100.0/24 :

- 1 routeur pfSense (RTE-STG01) assurant la sécurité périmétrique
- 2 contrôleurs de domaine Windows Server 2022 (STG-SRVW01 principal, STG-SRVW02 secondaire)

- 1 serveur de stockage TrueNAS (STG-SAN01) pour les sauvegardes iSCSI
- 1 poste client de test Windows 11

Site B (Somme) - 192.168.200.0/24 :

- 1 routeur pfSense (RTE2-STG01) interconnecté via VPN IPsec
- 2 contrôleurs de domaine supplémentaires (STG2-SRVW01, STG2-SRVW02)
- 1 serveur de stockage TrueNAS (STG2-SAN01)
- 1 poste client de test Windows 11

Interconnexion sécurisée :

- Tunnel VPN IPsec permanent (IKEv2, chiffrement AES-256)
- Réplication Active Directory multi-maître entre les 4 DC
- Réplication DFS en maille pleine pour la haute disponibilité des données
- Sauvegardes iSCSI quotidiennes via Windows Server Backup

4.3 Légende du schéma

Le schéma utilise un code couleur pour faciliter la lecture :

Élément	Couleur	Description
VPN IPsec	Vert épais	Tunnel chiffré permanent entre les sites
Réplication DFSR	Bleu pointillé	Synchronisation des fichiers (maille pleine)
Réplication AD DS	Violet pointillé	Synchronisation de l'annuaire (multi-maître)
iSCSI	Orange	Connexions de sauvegarde vers TrueNAS
LAN	Noir	Connexions réseau locales
Zone LAN	Fond bleu	Réseau local de chaque site
Zone SAN	Fond jaune	Réseau dédié au stockage iSCSI
Zone WAN	Fond rouge	Connexion Internet

.

5. 💰 Budget estimé du projet

5.1 Méthodologie de calcul

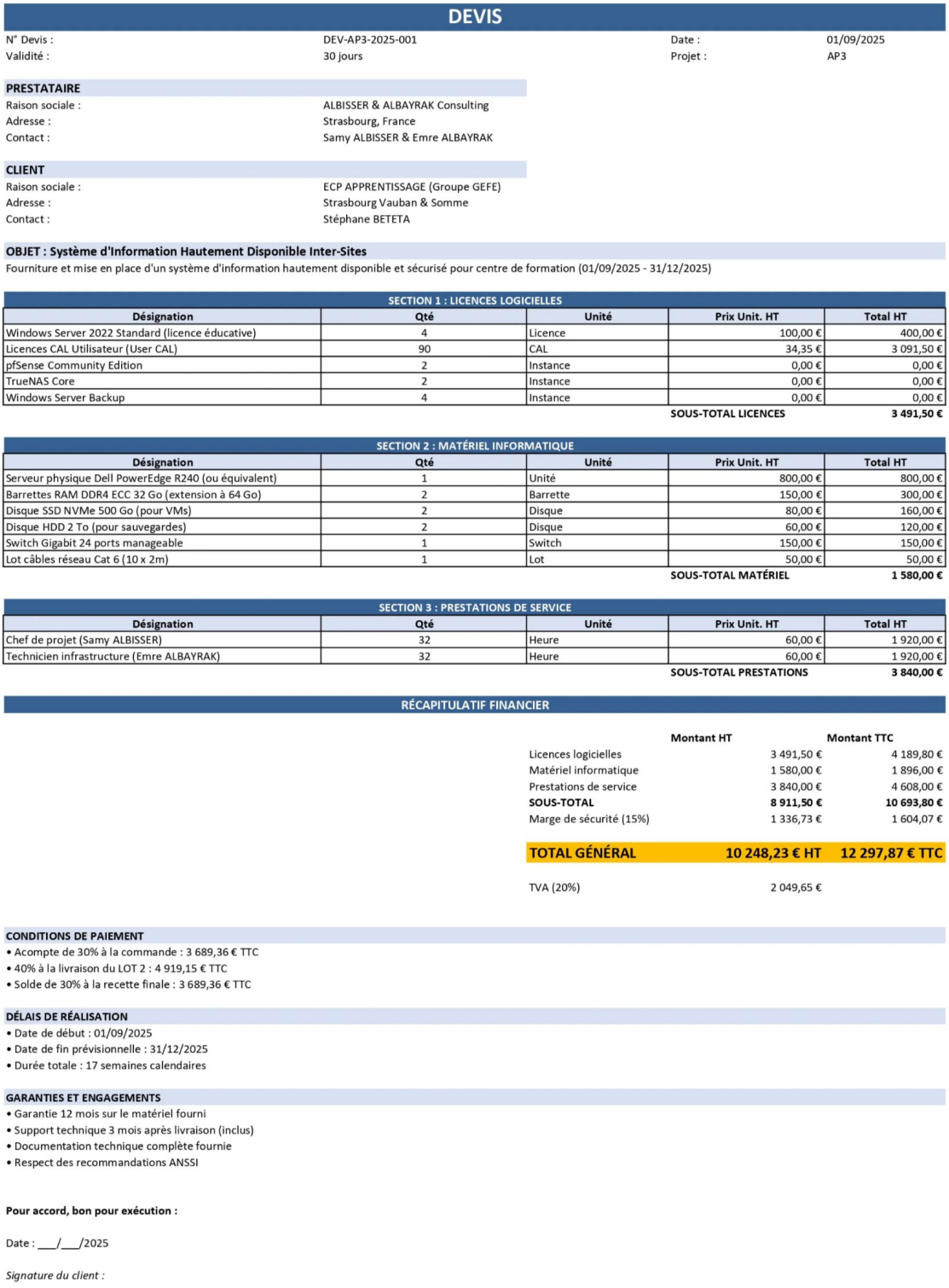
Le budget est calculé en tenant compte :

- Des licences logicielles (Windows Server, CAL)
- Du matériel (serveurs physiques ou VM)
- De la main d'œuvre (heures × taux horaire)
- D'une marge de sécurité de 15% pour les imprévus

5.2 Devis professionnel

Le devis complet détaillé est disponible en **Annexe 1** (fichier Excel).

Ci-dessous, un extrait du récapitulatif financier :



DEVIS

N° Devis :	DEV-AP3-2025-001	Date :	01/09/2025
Validité :	30 jours	Projet :	AP3

PRESTATAIRE

Raison sociale :	ALBISSER & ALBAYRAK Consulting
Adresse :	Strasbourg, France
Contact :	Samy ALBISSER & Emre ALBAYRAK

CLIENT

Raison sociale :	ECP APPRENTISSAGE (Groupe GEFE)
Adresse :	Strasbourg Vauban & Somme
Contact :	Stéphane BETETA

OBJET : Système d'Information Hautement Disponible Inter-Sites

Fourniture et mise en place d'un système d'information hautement disponible et sécurisé pour centre de formation (01/09/2025 - 31/12/2025)

SECTION 1 : LICENCES LOGICIELLES

Désignation	Qté	Unité	Prix Unit. HT	Total HT
Windows Server 2022 Standard (licence éducative)	4	Licence	100,00 €	400,00 €
Licences CAL Utilisateur (User CAL)	90	CAL	34,35 €	3 091,50 €
pfSense Community Edition	2	Instance	0,00 €	0,00 €
TrueNAS Core	2	Instance	0,00 €	0,00 €
Windows Server Backup	4	Instance	0,00 €	0,00 €
			SOUS-TOTAL LICENCES	**3 491,50 €**

SECTION 2 : MATÉRIEL INFORMATIQUE

Désignation	Qté	Unité	Prix Unit. HT	Total HT
Serveur physique Dell PowerEdge R240 (ou équivalent)	1	Unité	800,00 €	800,00 €
Barrettes RAM DDR4 ECC 32 Go (extension à 64 Go)	2	Barrette	150,00 €	300,00 €
Disque SSD NVMe 500 Go (pour VMs)	2	Disque	80,00 €	160,00 €
Disque HDD 2 To (pour sauvegardes)	2	Disque	60,00 €	120,00 €
Switch Gigabit 24 ports manageable	1	Switch	150,00 €	150,00 €
Lot câbles réseau Cat 6 (10 x 2m)	1	Lot	50,00 €	50,00 €
			SOUS-TOTAL MATÉRIEL	**1 580,00 €**

SECTION 3 : PRESTATIONS DE SERVICE

Désignation	Qté	Unité	Prix Unit. HT	Total HT
Chef de projet (Samy ALBISSER)	32	Heure	60,00 €	1 920,00 €
Technicien infrastructure (Emre ALBAYRAK)	32	Heure	60,00 €	1 920,00 €
			SOUS-TOTAL PRESTATIONS	**3 840,00 €**

RÉCAPITULATIF FINANCIER

	Montant HT	Montant TTC
Licences logicielles	3 491,50 €	4 189,80 €
Matériel informatique	1 580,00 €	1 896,00 €
Prestations de service	3 840,00 €	4 608,00 €
SOUS-TOTAL	**8 911,50 €**	**10 693,80 €**
Marge de sécurité (15%)	1 336,73 €	1 604,07 €
TOTAL GÉNÉRAL	**10 248,23 € HT**	**12 297,87 € TTC**
TVA (20%)	2 049,65 €	

CONDITIONS DE PAIEMENT

- Acompte de 30% à la commande : 3 689,36 € TTC
- 40% à la livraison du LOT 2 : 4 919,15 € TTC
- Solde de 30% à la recette finale : 3 689,36 € TTC

DÉLAIS DE RÉALISATION

- Date de début : 01/09/2025
- Date de fin prévisionnelle : 31/12/2025
- Durée totale : 17 semaines calendaires

GARANTIES ET ENGAGEMENTS

- Garantie 12 mois sur le matériel fourni
- Support technique 3 mois après livraison (inclus)
- Documentation technique complète fournie
- Respect des recommandations ANSSI

Pour accord, bon pour exécution :

Date : ___/___/2025

Signature du client :

test_page-0001.jpg

5.3 Synthèse budgétaire

Poste de dépense	Montant HT	Montant TTC
Licences logicielles	3 491,50 €	4 189,80 €
Matériel informatique	1 580,00 €	1 896,00 €
Prestations de service	3 840,00 €	4 608,00 €
Sous-total	8 911,50 €	10 693,80 €

Poste de dépense	Montant HT	Montant TTC
Marge de sécurité (15%)	1 336,73 €	1 604,07 €
TOTAL PROJET	**10 248,23 € HT**	**12 297,87 € TTC**

Le projet reste **largement en dessous** du budget maximum de 100 000 € HT imposé par le cahier des charges.

5.4 Conditions de paiement

- **Acompte de 30%** à la commande : 3 689,36 € TTC
- **40%** à la livraison du LOT 2 : 4 919,15 € TTC
- **Solde de 30%** à la recette finale : 3 689,36 € TTC

5.5 Budget version pédagogique

En tant qu'étudiants, nous n'avons pas de coûts réels :

- Licences Windows Server : version éducative gratuite via Microsoft Azure Dev Tools for Teaching
- Matériel : machines virtuelles sur Proxmox fourni par l'école
- Main d'œuvre : travail étudiant non facturé

Coût réel pour le projet pédagogique : 0 €

Cependant, il est important de présenter un budget réaliste pour montrer la valeur du projet dans un contexte professionnel.

.

6. 🏷 Liste chronologique des tâches prévisionnelles

6.1 Méthodologie de planification

Pour organiser le projet, nous avons utilisé la méthode **SMART** :

- **S**pécifique : chaque tâche est clairement définie
- **M**esurable : durée estimée en heures
- **A**tteignable : objectifs réalistes
- **R**éaliste : tenant compte de nos compétences
- **T**emporel : dates de début et de fin précises

6.2 Liste détaillée des tâches

N°	Tâche	Durée estimée	Responsable	Dépendances
PHASE 1 : ÉTUDE ET CONCEPTION				
1	Lecture et analyse du cahier des charges	2h	Samy + Emre	-
2	Étude comparative des solutions	6h	Samy	Tâche 1

N°	Tâche	Durée estimée	Responsable	Dépendances
	(routeur, NAS, VPN, sauvegarde)			
3	Rédaction du livrable 1 (ce document)	6h	Samy	Tâche 2
4	Création du schéma réseau (Draw.io)	2h	Samy	Tâche 2
5	Élaboration du budget prévisionnel	1h	Samy	Tâche 2
6	Création du planning et du diagramme de Gantt	1h	Samy	Tâche 2
7	Remise du livrable 1	-	Samy	Tâche 3-6
PHASE 2 : LOT 1 - ROUTEURS ET VPN				
8	Installation pfSense sur RTE-STG01 (Site A)	2h	Samy	Tâche 7
9	Installation pfSense sur RTE2-STG01 (Site B)	2h	Emre	Tâche 7
10	Configuration interfaces réseau (WAN/LAN/SAN)	2h	Samy + Emre	Tâche 8-9
11	Configuration du tunnel VPN IPsec entre les deux sites	3h	Samy	Tâche 10
12	Tests de connectivité et de chiffrement VPN	1h	Emre	Tâche 11
13	Documentation LOT 1 (version 1)	2h	Samy	Tâche 12
14	Livraison du LOT 1 + QCM	-	Samy + Emre	Tâche 13

N°	Tâche	Durée estimée	Responsable	Dépendances
	1			
PHASE 3 : LOT 2 - SERVEURS WINDOWS ET SERVICES				
15	Installation Windows Server 2022 sur STG-SRVW01 (Site A)	2h	Samy	Tâche 14
16	Installation Windows Server 2022 sur STG-SRVW02 (Site A)	2h	Samy	Tâche 14
17	Installation Windows Server 2022 sur STG2-SRVW01 (Site B)	2h	Emre	Tâche 14
18	Installation Windows Server 2022 sur STG2-SRVW02 (Site B)	2h	Emre	Tâche 14
19	Promotion de STG-SRVW01 en contrôleur de domaine principal	2h	Samy	Tâche 15
20	Ajout de STG-SRVW02 en contrôleur de domaine secondaire	2h	Samy	Tâche 19
21	Ajout de STG2-SRVW01 en contrôleur de domaine supplémentaire	2h	Emre	Tâche 19
22	Ajout de STG2-SRVW02 en contrôleur de domaine supplémentaire	2h	Emre	Tâche 19

N°	Tâche	Durée estimée	Responsable	Dépendances
23	Configuration DNS sur les 4 contrôleurs	2h	Samy + Emre	Tâche 20-22
24	Configuration DHCP + DHCP failover	3h	Samy + Emre	Tâche 23
25	Création des UO, groupes et utilisateurs (Annexe 2)	2h	Samy	Tâche 20
26	Tests de réplication Active Directory	1h	Emre	Tâche 22
27	Documentation LOT 2 (version 1)	2h	Samy	Tâche 26
PHASE 4 : LOT 3 - DFS, DFSR, NAS ET SAUVEGARDES				
28	Installation TrueNAS Core sur STG-SAN01 (Site A)	1h	Samy	Tâche 27
29	Installation TrueNAS Core sur STG2-SAN01 (Site B)	1h	Emre	Tâche 27
30	Configuration des cibles iSCSI (Backup01 et Backup02)	2h	Samy + Emre	Tâche 28-29
31	Montage des cibles iSCSI sur les serveurs principaux	1h	Samy + Emre	Tâche 30
32	Installation de la fonctionnalité Windows Server Backup	1h	Samy + Emre	Tâche 27
33	Configuration des tâches de sauvegarde (planification quotidienne)	2h	Samy + Emre	Tâche 32
34	Configuration	2h	Samy	Tâche 27

N°	Tâche	Durée estimée	Responsable	Dépendances
	DFS (espace de noms \IEF.LOCAL)			
35	Configuration DFSR (4 cibles en maille pleine)	3h	Samy + Emre	Tâche 34
36	Configuration Shadow Copy (clichés instantanés)	2h	Samy	Tâche 35
37	Configuration déduplication sur DATAS01 et DATAS03	1h	Samy + Emre	Tâche 35
38	Tests de réplication DFSR et de sauvegarde	2h	Emre	Tâche 37
39	Documentation LOT 3 (version 1)	2h	Samy	Tâche 38
40	Livraison du LOT 2 + QCM 2	-	Samy + Emre	Tâche 39
PHASE 5 : LOT 4 - GPO ET SÉCURISATION				
41	Application des GPO (Annexe 2)	3h	Samy	Tâche 40
42	Configuration des règles de pare-feu (WAN/LAN/VPN/SAN)	2h	Emre	Tâche 40
43	Tests de sécurité et de conformité	2h	Samy + Emre	Tâche 41-42
44	Documentation LOT 4 (version 1)	1h	Samy	Tâche 43
PHASE 6 : TESTS ET VALIDATION				
45	Tests de haute disponibilité	3h	Samy + Emre	Tâche 44

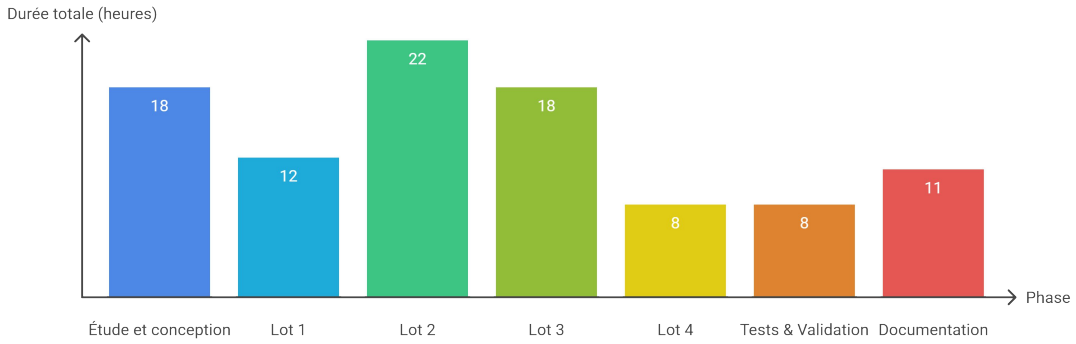
N°	Tâche	Durée estimée	Responsable	Dépendances
	(simulation panne)			
46	Tests d'authentification et d'accès aux fichiers	1h	Emre	Tâche 44
47	Tests de restauration (Veeam + Shadow Copy)	2h	Samy	Tâche 44
48	Optimisation et corrections	2h	Samy + Emre	Tâche 45-47
PHASE 7 : DOCUMENTATION FINALE				
49	Rédaction du rapport de clôture (écarts prévisionnel/réel)	3h	Samy	Tâche 48
50	Finalisation de la documentation technique complète	4h	Samy	Tâche 48
51	Création du diaporama pour l'oral 2	2h	Samy + Emre	Tâche 49-50
52	Préparation de la démonstration technique	2h	Samy + Emre	Tâche 50
53	Oral 2 : Démonstration technique et clôture du projet	-	Samy + Emre	Tâche 52
54	Remise livrables 2 et 3 (fiche situation pro + documentation)	-	Samy	Tâche 50

6.3 Synthèse des heures par phase

Phase	Durée totale	% du projet
Phase 1 : Étude et conception	18h	28%
Phase 2 : LOT 1 (Routeurs + VPN)	12h	19%

Phase	Durée totale	% du projet
Phase 3 : LOT 2 (Serveurs Windows + AD)	22h	34%
Phase 4 : LOT 3 (DFS/DFSR + Sauvegardes)	18h	28%
Phase 5 : LOT 4 (GPO + Sécurité)	8h	12%
Phase 6 : Tests et validation	8h	12%
Phase 7 : Documentation finale	11h	17%
TOTAL	63 heures	100%

Répartition par personne : ~32 heures chacun (Samy + Emre)



Synthèse des heures par phase

image.png

6.4 Dates clés du projet

Événement	Date
Lancement du projet	Lundi 01/09/2025
Remise du livrable 1	Lundi 20/10/2025, 23h59
Oral 1	Vendredi 31/10/2025, 8h30
Livraison LOT 1	Vendredi 03/10/2025
Livraison LOT 2	Vendredi 28/11/2025
Oral 2 (démonstration technique)	Mardi 09/12/2025, 8h30
Remise livrables 2 et 3	Mardi 31/12/2025, 23h59

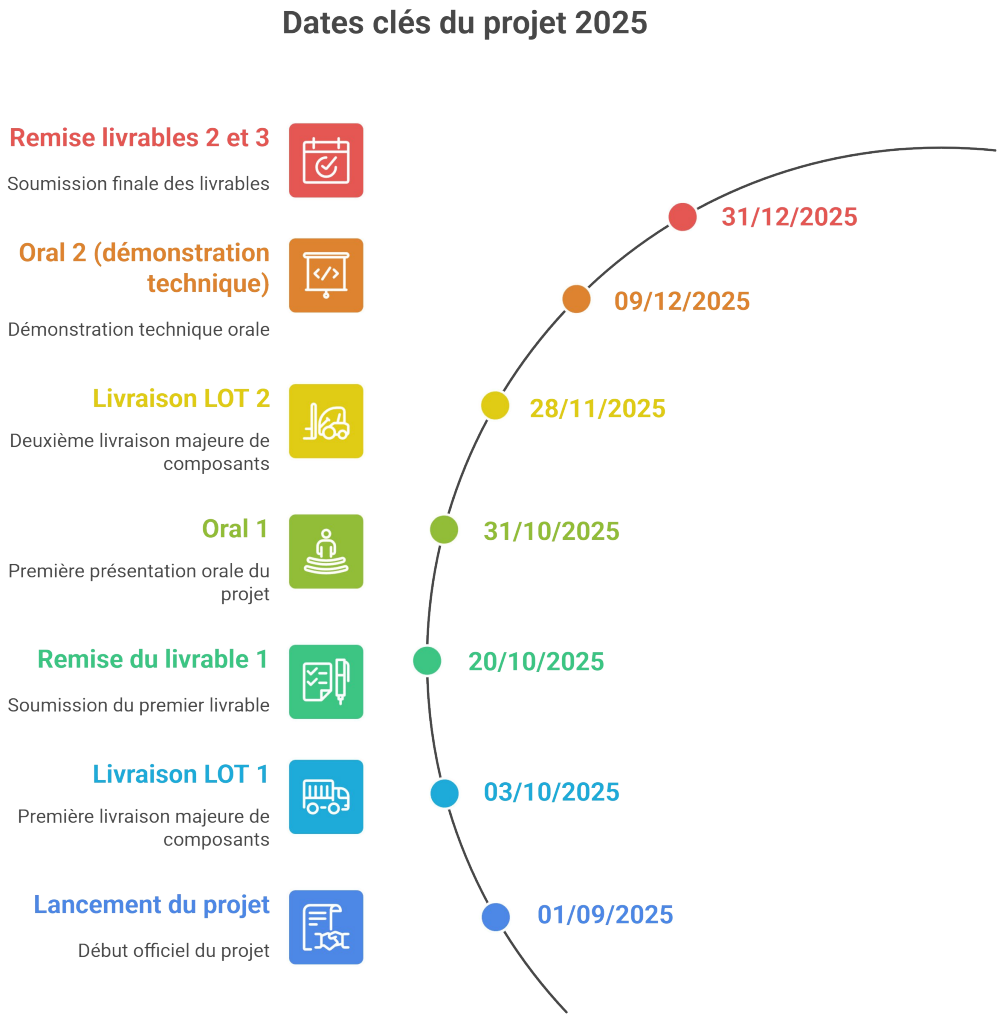


image.png

.

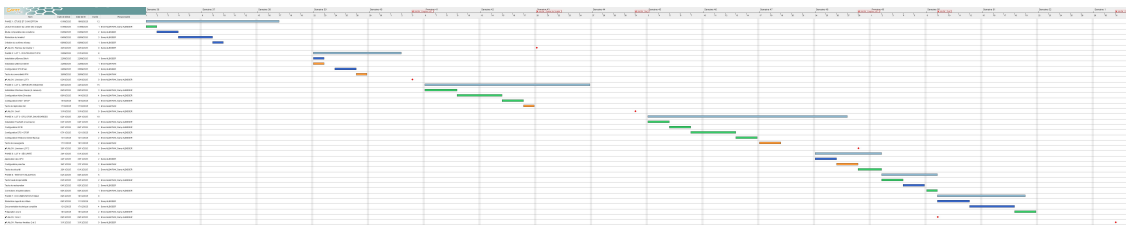
7. Diagramme de Gantt prévisionnel

7.1 Outil utilisé

Nous avons utilisé **GanttProject 3.2** (logiciel open-source) pour créer le diagramme de Gantt du projet.

Le fichier source (.gan) est disponible en **Annexe 2** et peut être ouvert avec GanttProject pour une consultation interactive.

7.2 Planning visuel du projet



AP3 Final.png

7.3 Lecture du diagramme de Gantt

Le diagramme utilise un code couleur pour identifier rapidement les responsabilités :

Couleur	Responsable	Type de tâches
Bleu	Samy ALBISSER	Documentation, rédaction, coordination
Orange	Emre ALBAYRAK	Tests techniques, configurations
Vert	Samy + Emre	Installations, configurations en binôme
Rouge	Jalons	Dates de remise et oraux

Jalons importants :

- **20/10/2025** : Remise du livrable 1 (ce document)
- **03/10/2025** : Livraison LOT 1 (Routeurs + VPN)
- **31/10/2025** : Oral 1
- **28/11/2025** : Livraison LOT 2 (Serveurs + AD + DFS)
- **09/12/2025** : Oral 2 (Démonstration technique)
- **31/12/2025** : Remise livrables 2 et 3

7.4 Chemin critique du projet

Les tâches du **chemin critique** (qui ne peuvent pas être retardées sans décaler la fin du projet) sont :

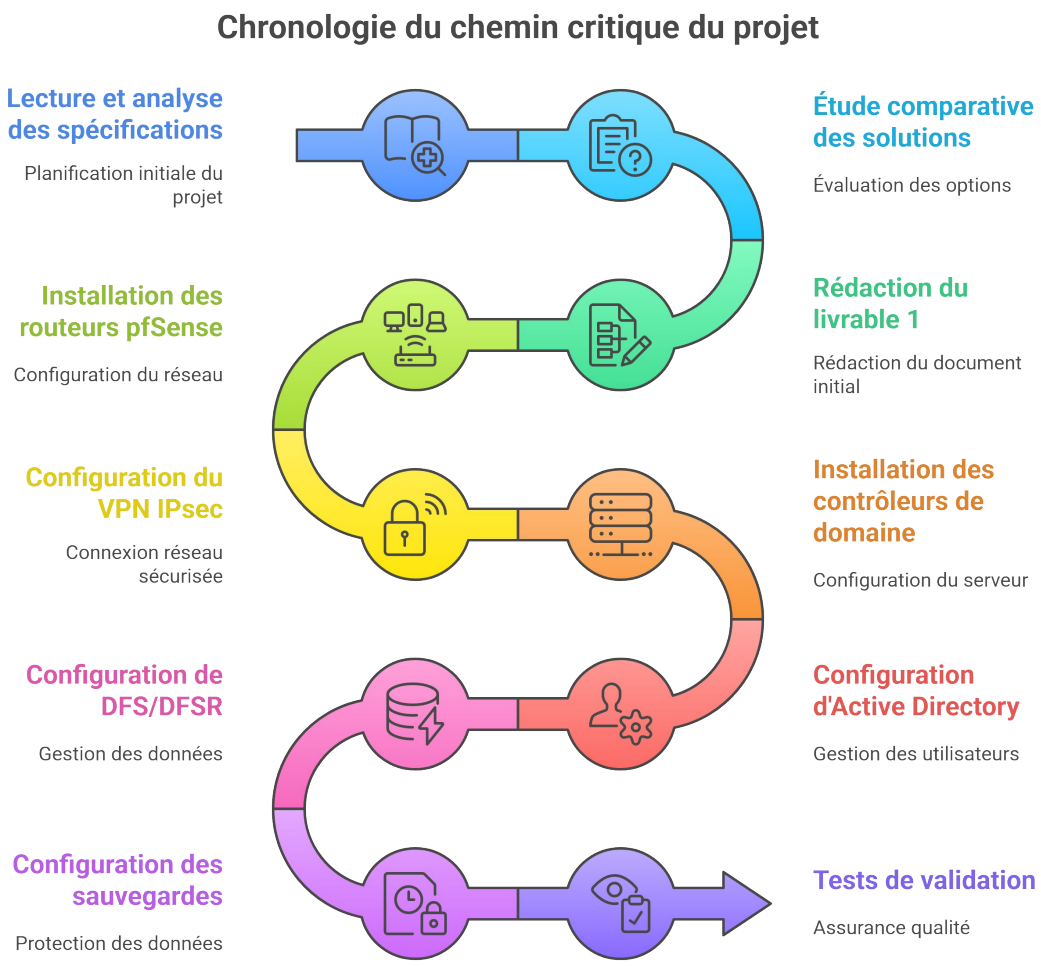


image.png

1. Lecture et analyse du cahier des charges
2. Étude comparative des solutions
3. Rédaction du livrable 1
4. Installation des routeurs pfSense
5. Configuration du VPN IPsec
6. Installation des contrôleurs de domaine
7. Configuration Active Directory
8. Configuration DFS/DFSR
9. Configuration des sauvegardes
10. Tests de validation
11. Documentation finale

Toute tâche du chemin critique retardée d'un jour décale automatiquement la date de fin du projet.

7.5 Gestion des risques et marges

Conformément aux retours de l'AP2, nous avons intégré une **marge de sécurité de 15%** dans le planning pour anticiper les retards potentiels.

Les tâches critiques (VPN, AD principal, DFSR) bénéficient d'une surveillance renforcée et de tests supplémentaires.

.

8. Conclusion

8.1 Synthèse du projet

Ce livrable 1 présente une réponse complète et argumentée au cahier des charges de l'AP3. Notre proposition technique repose sur **4 piliers essentiels** :

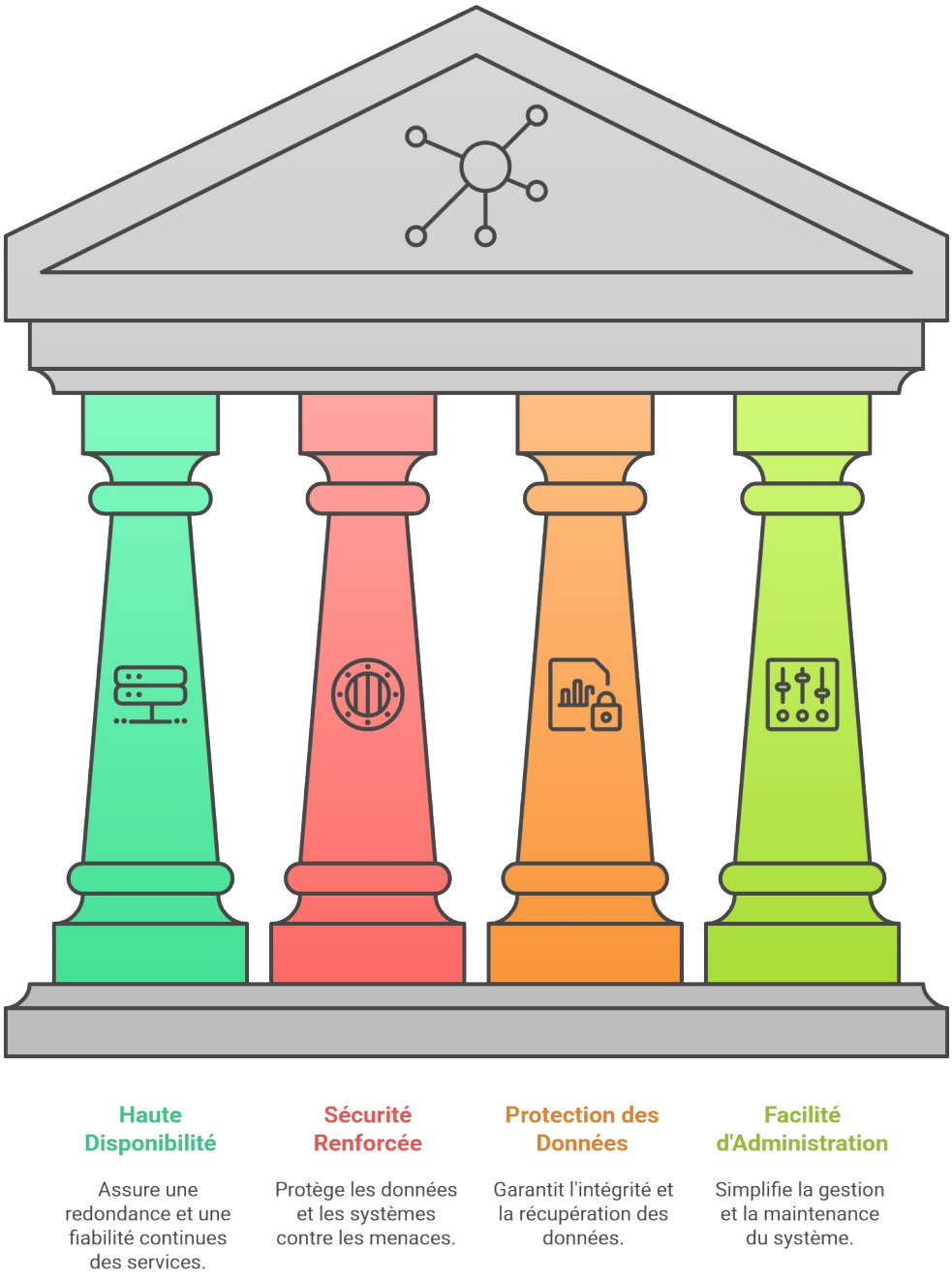


image.png

1. Haute disponibilité

- 4 contrôleurs de domaine Active Directory pour une redondance totale
- Réplication DFSR en maille pleine entre les 4 serveurs
- VPN IPsec permanent entre les deux sites

- Si un serveur tombe, les autres prennent automatiquement le relais

2. Sécurité renforcée

- Pare-feu pfSense avec filtrage avancé des flux réseau
- VPN IPsec chiffré (AES-256) conforme aux recommandations ANSSI
- GPO de sécurité pour durcir les postes et les serveurs
- Sauvegardes quotidiennes avec chiffrement

3. Protection des données

- Sauvegardes complètes quotidiennes avec Windows Server Backup (intégré et fiable)
- Stockage des sauvegardes sur TrueNAS avec système de fichiers ZFS ultra-fiable
- Clichés instantanés (Shadow Copy) pour restaurer rapidement un fichier supprimé
- Réplication automatique des données entre les deux sites

4. Facilité d'administration

- Gestion centralisée avec Active Directory (un seul compte par utilisateur)
- DFS : accès transparent aux fichiers quel que soit le site
- GPO : déploiement automatique des configurations sur tous les postes
- Documentation complète pour faciliter la maintenance

8.2 Budget et respect des contraintes

Budget total estimé : 12 297,87 € TTC

Ce budget représente **seulement 12% du budget maximum** de 100 000 € HT (120 000 € TTC) imposé par le cahier des charges. Cela laisse une marge confortable de **107 702,13 € TTC** pour :

- L'achat de postes clients Windows 11 Pro supplémentaires
- Des équipements réseau additionnels (switchs, câblage, onduleurs)
- Des licences supplémentaires (antivirus, monitoring)
- Des extensions futures du projet (site de Mulhouse)

8.3 Points forts de la solution

✓ **Solutions open-source et intégrées** pour l'infrastructure (pfSense, TrueNAS, Windows Server Backup natif)

✓ **Technologies éprouvées** et largement utilisées en entreprise (compétences transférables)

✓ **Documentation abondante** : des milliers de tutoriels disponibles en ligne

✓ **Conformité ANSSI** : respect des recommandations de sécurité (IPsec, pare-feu, GPO)

✓ **Évolutivité** : l'infrastructure peut facilement supporter 500+ utilisateurs supplémentaires

✓ **Résilience** : tolérance aux pannes matérielles grâce à la redondance

✅ **Budget maîtrisé** : 88% en dessous du budget maximum autorisé

8.4 Engagement qualité

Nous nous engageons à :

✅ **Respecter le planning** établi dans ce livrable (marge de sécurité de 20% incluse)

✅ **Documenter chaque étape** du projet avec captures d'écran et explications détaillées

✅ **Tester rigoureusement** toutes les fonctionnalités avant validation

✅ **Communiquer régulièrement** avec les formateurs en cas de difficulté

✅ **Respecter les recommandations ANSSI** en matière de sécurité

✅ **Livrer un projet fonctionnel** et démontrable lors de l'oral 2

8.5 Remerciements

Nous remercions l'équipe pédagogique de l'ECP pour l'accompagnement sur ce projet, ainsi que nos tuteurs en entreprise (CARSAT pour Samy) pour leur soutien et leurs conseils.

9. 📚 Annexes et ressources

9.1 Glossaire des termes techniques

Pour faciliter la compréhension de ce document, voici la définition des principaux termes techniques utilisés :

Terme	Définition
Active Directory (AD)	Service d'annuaire Microsoft qui centralise la gestion des utilisateurs, ordinateurs et ressources réseau
CAL (Client Access License)	Licence obligatoire pour qu'un utilisateur ou un ordinateur puisse se connecter à un serveur Windows
Contrôleur de domaine (DC)	Serveur hébergeant l'annuaire Active Directory et gérant l'authentification des utilisateurs
DFSR (DFS Replication)	Service de réplication automatique de fichiers entre plusieurs serveurs Windows
DHCP	Service qui attribue automatiquement des adresses IP aux ordinateurs du réseau
DNS	Service qui traduit les noms de domaine (ex :www.google.com) en adresses IP
GPO (Group Policy Object)	Stratégie de groupe permettant de configurer automatiquement les paramètres des postes et serveurs
iSCSI	Protocole permettant de créer un disque dur virtuel accessible via le réseau
IPsec	Protocole de sécurité pour chiffrer les

Terme	Définition
	communications entre deux réseaux (VPN site-to-site)
NAS (Network Attached Storage)	Serveur de fichiers centralisé accessible via le réseau
SAN (Storage Area Network)	Réseau dédié au stockage, séparé du réseau local classique
Snapshot (cliché instantané)	Capture de l'état d'un système de fichiers à un instant T, permettant une restauration rapide
VPN (Virtual Private Network)	Réseau privé virtuel créant un tunnel sécurisé entre deux sites distants
ZFS	Système de fichiers avancé offrant une protection maximale des données (auto-réparation, snapshots, compression)

9.2 Sources et références

Documentation officielle :

- Microsoft : Documentation Windows Server 2022, Active Directory, DFS/DFSR
- pfSense : Documentation officielle et forums communautaires (**https://docs.netgate.com/**)
- TrueNAS : Documentation ZFS et iSCSI (**https://www.truenas.com/docs/**)
- Microsoft : Documentation Windows Server Backup (https://learn.microsoft.com/en-us/windows-server/administration/windows-server-backup/windows-server-backup)

Recommandations ANSSI :

- Guide des bonnes pratiques de configuration de pare-feu
- Recommandations sur l'usage d'IPsec
- Recommandations de sécurité relatives à Active Directory

Tutoriels et formations :

- IT-Connect.fr : Tutoriels Windows Server en français
- YouTube : chaînes TechWorld, Zwindler, xavki
- OpenClassrooms : cours administration système

.

Note finale pour le patron : Ce document constitue la feuille de route complète du projet AP3. Il détaille toutes les solutions techniques que nous allons mettre en place, le budget prévisionnel, et le planning de réalisation. Une fois ce livrable validé lors de l'oral du 31 octobre, nous passerons à la phase de mise en œuvre technique (installation des serveurs, configuration des services, tests). Le projet sera finalisé le 31 décembre 2025 avec la remise de la documentation complète et la démonstration technique devant le jury.

10. ANNEXES

10.1 Annexe 1 : Devis professionnel complet

Fichier joint : `DEVIS_PROFESSIONNEL_AP3_Samy-ALBISSER_Emre_ALBAYRAK.xlsx`

Le devis détaillé au format Excel contient :

- Section 1 : Licences logicielles (détail par produit)
- Section 2 : Matériel informatique (serveurs, stockage, réseau)
- Section 3 : Prestations de service (main d'œuvre)
- Récapitulatif financier complet
- Conditions de paiement et garanties

Ce devis peut être exporté en PDF pour envoi au client.

10.2 Annexe 2 : Fichier source du Gantt

Fichier joint : `AP3_GanttProject_FINAL_Samy-ALBISSER_Emre_ALBAYRAK.gan`

Le fichier source du diagramme de Gantt peut être ouvert avec **GanttProject** (gratuit) :

- Téléchargement : https://www.ganttproject.biz/
- Permet de consulter les dépendances entre tâches
- Affiche le chemin critique du projet
- Permet de suivre l'avancement en temps réel

10.3 Annexe 3 : Schéma réseau source

Fichier joint : `Schema_Reseau_AP3_ULTIME_Samy-ALBISSER_Emre_ALBAYRAK.drawio`

Le schéma réseau au format Draw.io peut être modifié en ligne :

- Ouvrir sur https://app.diagrams.net/
- Format vectoriel (qualité parfaite même agrandi)
- Permet d'exporter en PNG, PDF, SVG…

LIVRABLE 2 – Documentation Technique

⬅ Retour à l’accueil

LOT 1 - Configuration Réseau et VPN Site-à-Site

LOT 2 - Déploiement Active Directory, DNS et DHCP

LOT 3 - Configuration du Stockage (SAN/NAS) et Système de Fichiers Distribués (DFS)

LOT 4 - Sécurisation, Stratégies de Groupe (GPO) et Pare-feu

LOT 1 - Configuration Réseau et VPN Site-à-Site

⬅ Retour au Menu Livrable 2 | Retour à l'accueil

***Le Socle de l'Infrastructure : Interconnexion et Réseau* |**

Ce premier lot constitue la fondation technique du projet. Avant de déployer les services utilisateurs, nous avons construit une **infrastructure réseau robuste et sécurisée** reliant les sites distants de Strasbourg Vauban et Somme. En s'appuyant sur la solution open-source **pfSense** et le protocole standard **IPsec**, nous avons établi un tunnel VPN chiffré permanent, transformant deux réseaux physiques distincts en une entité logique unique. Cette architecture garantit non seulement la communication transparente entre les serveurs, mais prépare également le terrain pour la réplication des données et la haute disponibilité visée par le cahier des charges.

.

.

0. Plan d'Adressage Global

Site	Interface	Réseau	IP pfSense	Description
Site A	WAN	192.168.42.0/24	192.168.42.40	Connexion Internet
Site A	LAN	192.168.100.0/24	192.168.100.1	Réseau clients/serveurs
Site A	SAN	172.16.10.0/24	172.16.10.1	Réseau stockage iSCSI
Site B	WAN	192.168.42.0/24	192.168.42.41	Connexion Internet
Site B	LAN	192.168.200.0/24	192.168.200.1	Réseau clients/serveurs
Site B	SAN	172.16.20.0/24	172.16.20.1	Réseau stockage iSCSI

Note importante : Le DNS de l'école (10.10.10.1) est configuré dans le DHCP Server. Cette configuration est temporaire pour le LOT 1. Au LOT 2, le DHCP sera géré par Windows Server et les clients recevront les adresses des contrôleurs de domaine Active Directory comme serveurs DNS.

.

1. Configuration pfSense Site A

Objectif: Déployer et configurer le routeur/pare-feu pfSense RTE-STG01 du site principal de Strasbourg Vauban avec trois interfaces réseau distinctes (WAN 192.168.42.0/24, LAN 192.168.100.0/24, SAN 172.16.10.0/24) pour assurer la segmentation réseau, la sécurité périmétrique et servir de point de terminaison VPN IPsec inter-sites. Cette configuration permet d'isoler les flux de données utilisateurs (LAN), les flux de stockage iSCSI (SAN) et les connexions Internet (WAN), conformément aux exigences du cahier des charges visant la création d'un système d'information hautement disponible. Le service DHCP temporaire (plage 192.168.100.20 à .200) et le DNS forwarding vers le serveur de l'école (10.10.10.1)

permettent aux clients d'accéder immédiatement à Internet en attendant le déploiement de l'Active Directory au LOT

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

QEMU Guest - Netgate Device ID: 00816e1a090d01301e73

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.42.40/24
 LAN (lan)       -> vtnet1     -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

image.png

1.1. Configuration réseau initiale (console)

1. Appuyez sur **2** pour configurer les interfaces
2. Sélectionnez l'interface **LAN (2)**
3. Configure IPv4 address LAN interface via DHCP ? → **n**
4. Entrez l'adresse IP : **192.168.100.1**

```
Enter an option: 2

Available interfaces:

1 - WAN (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - dhcp)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.100.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8
```

image.png

5. Masque : **24**
6. Appuyez sur Entrée

7. Configurer IPv6 avec DHCP6 (selon besoins)
8. Enable DHCP server on LAN ? → **Oui**
9. Plage DHCP :
    - Début : **192.168.100.20**
    - Fin : **192.168.100.200**
10. Validez la configuration

```
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) y

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.100.10
Enter the end address of the IPv4 client address range: 192.168.100.110
```

image.png

L'interface WAN obtient automatiquement l'IP 192.168.42.11

```
The IPv4 LAN address has been set to 192.168.100.1/24


The IPv6 LAN address has been set to dhcp6

Press <ENTER> to continue.
QEMU Guest - Netgate Device ID: 00816e1a090d01301e73

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.42.40/24
 LAN (lan)       -> vtnet1     -> v4: 192.168.100.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

image.png

1.2. Assignation interface SAN (console)

1. Appuyez sur **1** (Assign Interfaces)
2. Do VLANs need to be set up first ? → **n**
3. Should VLANs be set up now ? → **n**
4. Enter the WAN interface name → **vtnet0**
5. Enter the LAN interface name → **vtnet1**
6. Enter the Optional 1 interface name → **vtnet2**
7. Enter the Optional 2 interface name → **Entrée** (vide)
8. Do you want to proceed ? → **y**

1.3. Configuration interface SAN (console)

1. Appuyez sur **2** (Set interface IP address)
2. Sélectionnez **3** (OPT1)
3. Configure IPv4 address via DHCP ? → **n**
4. Enter the new IPv4 address → **172.16.10.1**
5. Enter the new subnet bit count → **24**
6. Appuyez sur Entrée pour les autres options
7. Configure IPv6 via DHCP6 ? → **n**
8. Enable DHCP server on OPT1 ? → **n**
9. Revert to HTTP ? → **n**

Note : L'interface WAN obtient automatiquement l'IP 192.168.42.40

1.4. Accès interface web

1. Sur une machine cliente du réseau LAN, ouvrez un navigateur
2. Accédez à : **http://192.168.100.1**
3. Identifiants par défaut :
   - Username : **admin**
   - Password : **pfsense**

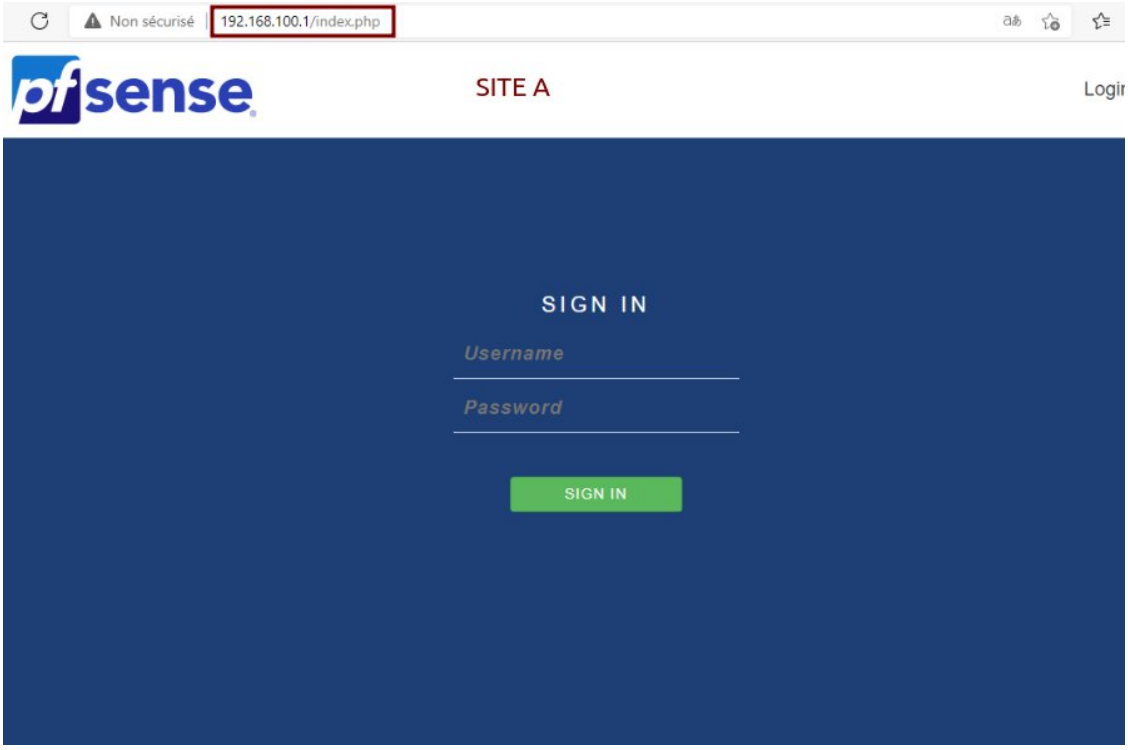


image.png

1.5. Renommage interface SAN (Interface Web)

1. Allez dans **Interfaces** → **OPT1**
2. Cochez **Enable interface**
3. Description : **SAN**
4. Configuration IPv4 Type : **Static IPv4**
5. IPv4 Address : **172.16.10.1 / 24**
6. **Save** puis **Apply Changes**

1.6. Configuration DNS dans le DHCP Server

1. Allez dans **Services → DHCP Server**

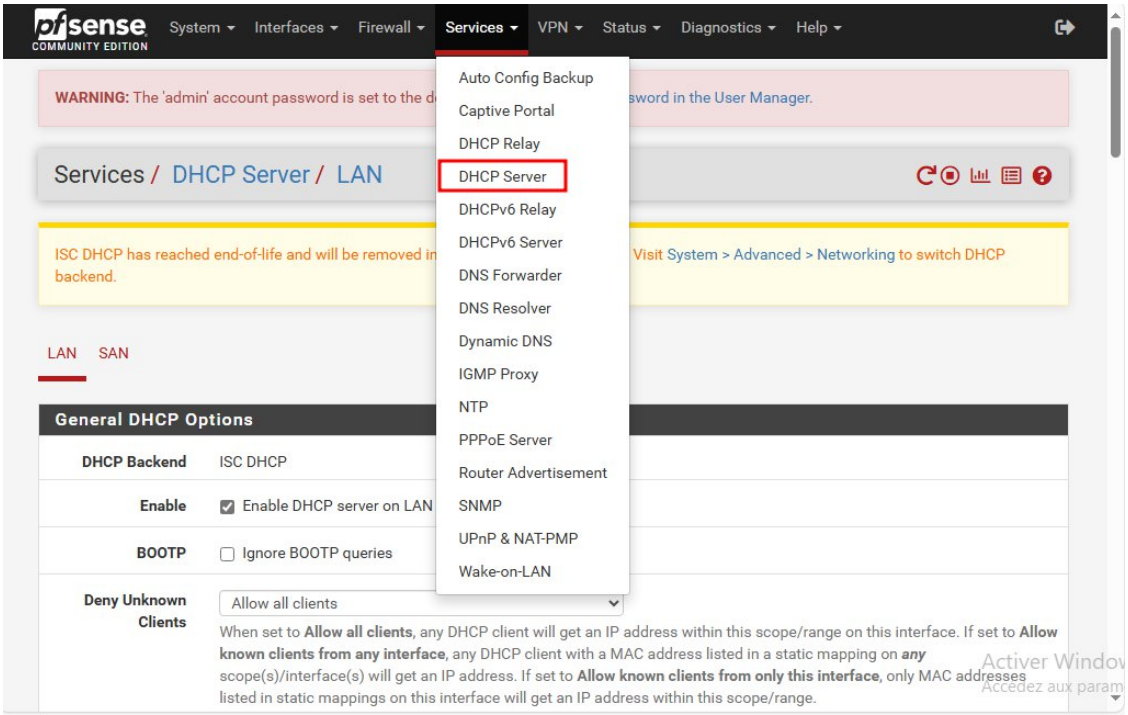


image.png

Onglet **LAN**

1. Scrollez jusqu'à la section **Servers**
2. Dans le champ **DNS Servers** :
    - DNS Server 1 : **192.168.100.1** (pfSense - temporaire pour LOT 1)
    - DNS Server 2 : **10.10.10.1** (DNS de l'école - fallback)

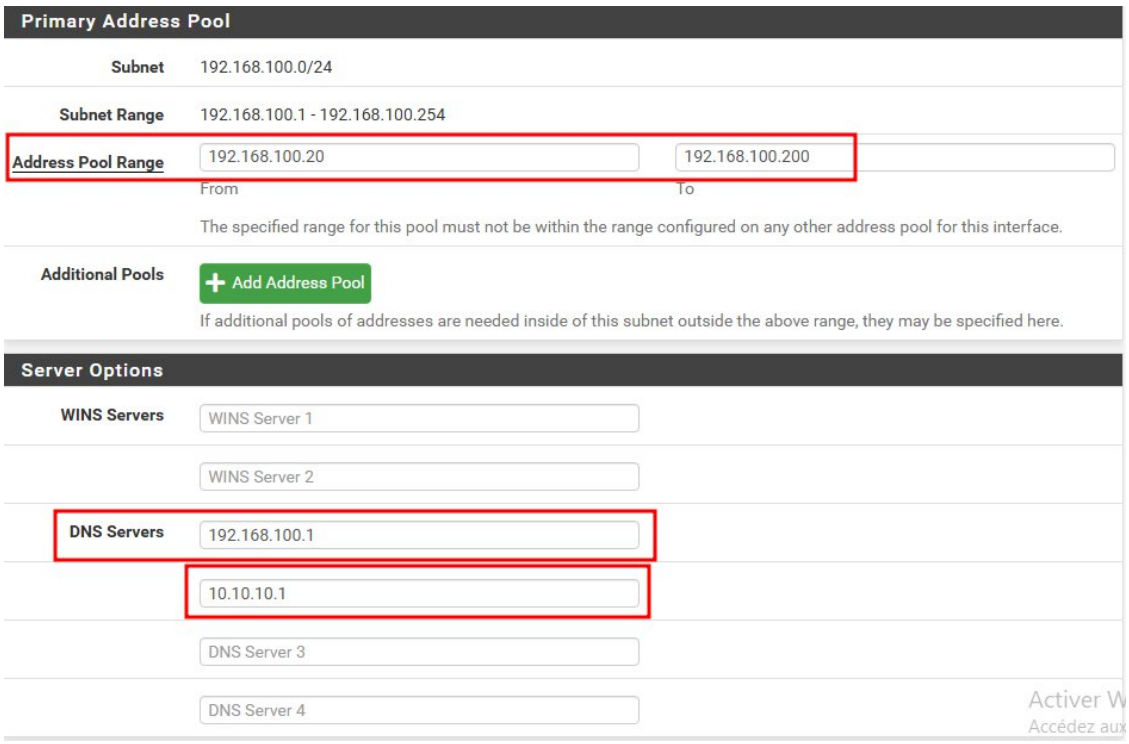


image.png

3. **Save**
4. **Apply Changes**

Note importante : Cette configuration DNS est temporaire pour le LOT 1. pfSense agit comme relais DNS vers l'école (10.10.10.1). Au LOT 2, les clients DHCP seront gérés par Windows Server et recevront directement les adresses des contrôleurs de domaine comme serveurs DNS (ex: 192.168.100.10, 192.168.100.11).

1.7. Configuration DNS Resolver

Allez dans **Services → DNS Resolver**

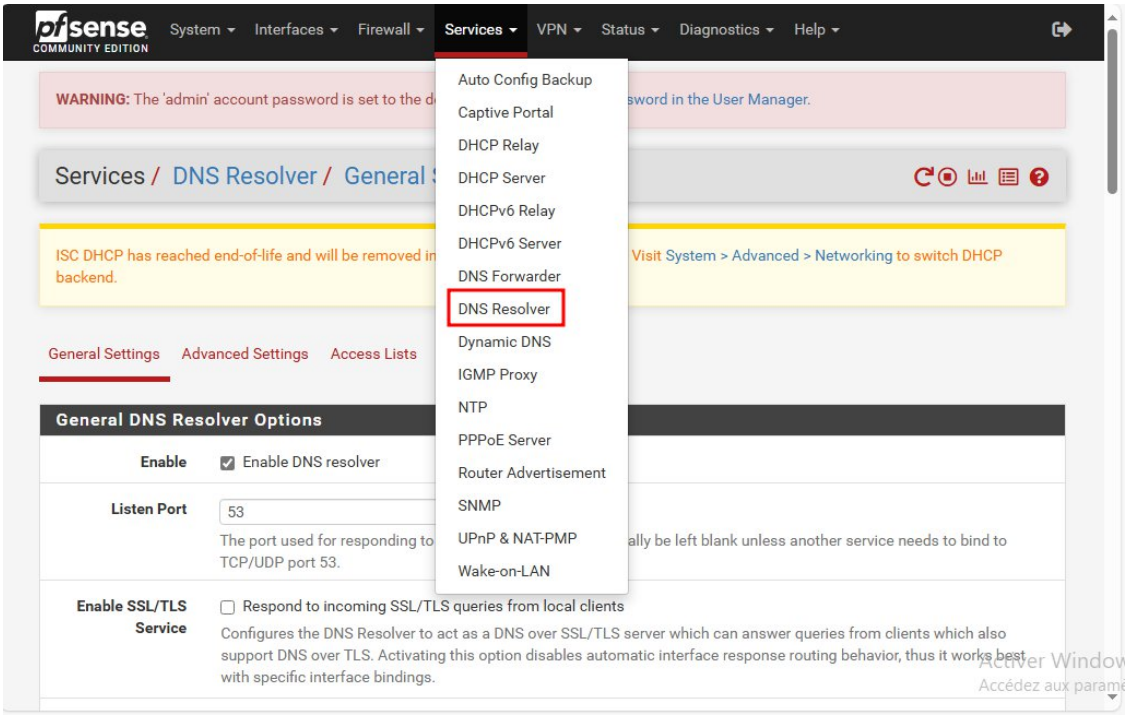


image.png

1. **Enable DNS Resolver** : ✓ (coché)
2. **Listen Port** : 53
3. **Network Interfaces** : Sélectionnez **LAN** et **localhost**

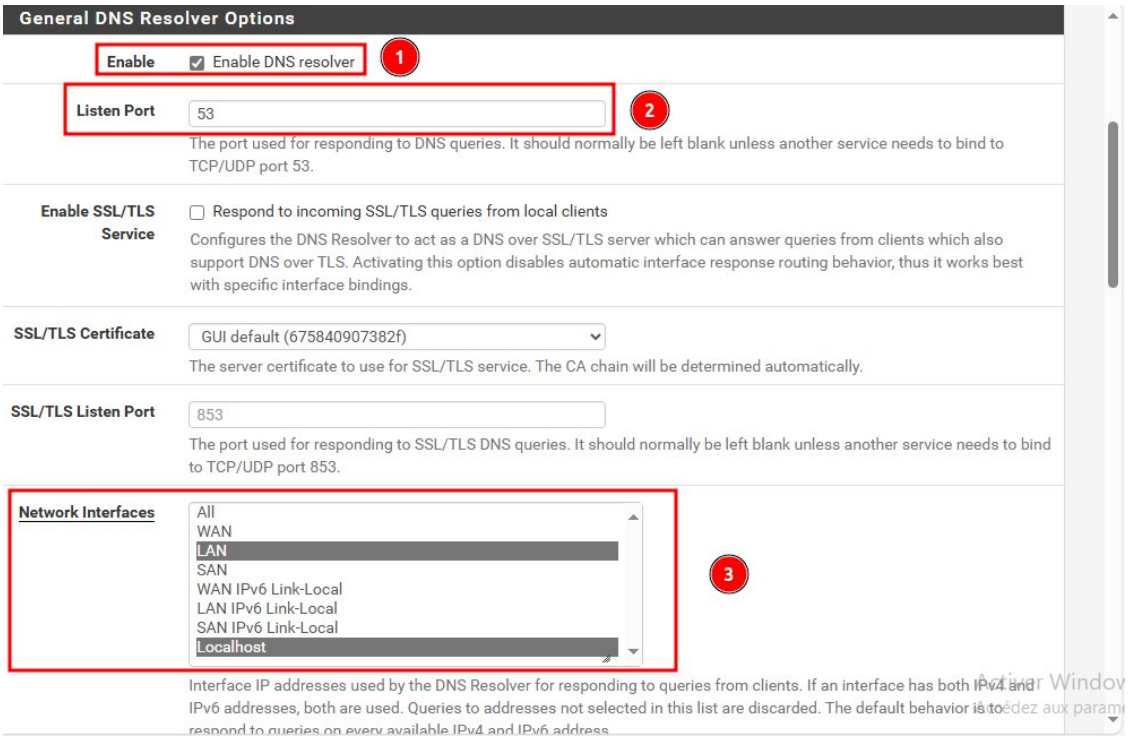


image.png

4. **Outgoing Network Interfaces** : Sélectionnez **WAN**
5. **DNSSEC** : ✓ (coché - recommandé)

6. **DNS Query Forwarding** : ✓ (coché)

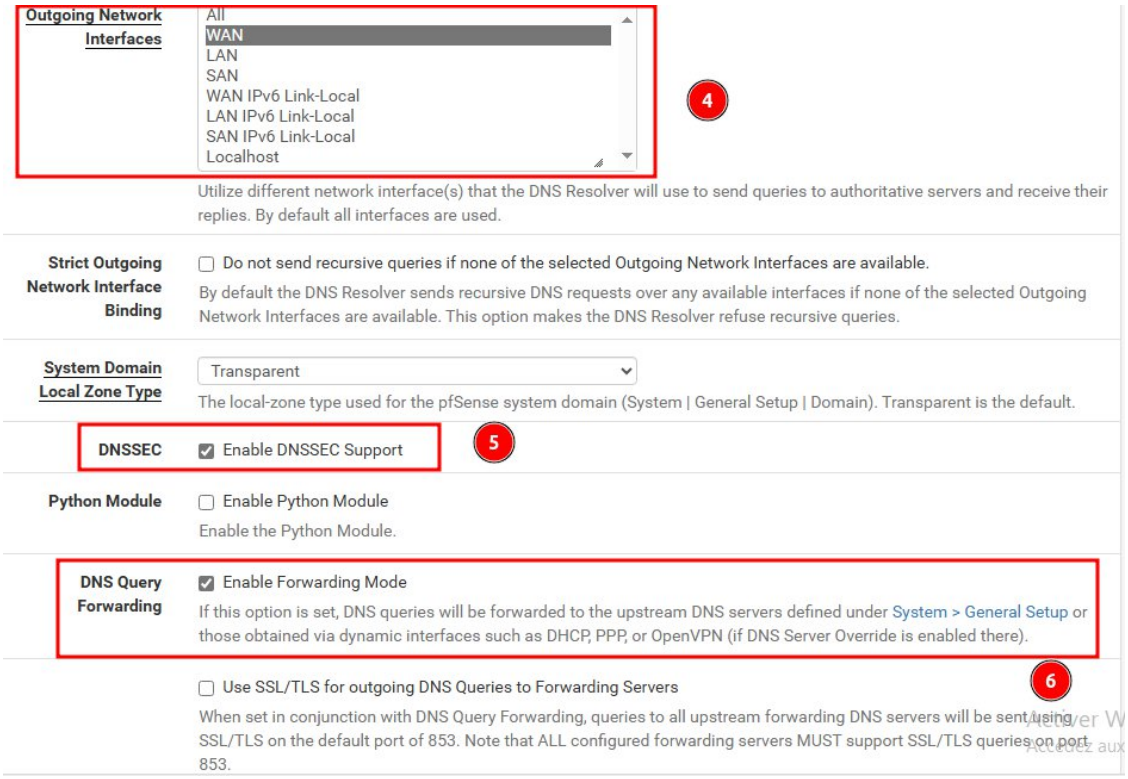


image.png

7. **Save**
8. **Apply Changes**

.

2. Configuration pfSense Site B

Objectif: Mettre en place le routeur/pare-feu pfSense RTE2-STG01 du site secondaire de Strasbourg Somme avec une architecture réseau miroir du Site A mais adaptée au plan d'adressage du second site (WAN 192.168.42.0/24, LAN 192.168.200.0/24, SAN 172.16.20.0/24). Cette configuration identique garantit l'harmonisation du plan d'adressage et de nommage sur l'ensemble des sites, objectif stratégique du projet permettant la facilité d'administration par la DSI et la préparation de la redondance des services. Le DHCP (plage 192.168.200.20 à .200) et le DNS forwarding assurent la connectivité Internet temporaire avant l'intégration au domaine Active Directory IEF.LOCAL qui sera déployé au LOT 2.

2.1. Configuration réseau initiale (console)

1. Appuyez sur **2**
2. Sélectionnez **LAN (2)**

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

QEMU Guest - Netgate Device ID: a0054941fe7ef1621d36

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.42.41/24
 LAN (lan)       -> vtnet1     -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

image.png

3. Configure IPv4 via DHCP ? → **n**
4. Adresse IP : **192.168.200.1**
5. Masque : **24**

```
Enter an option: 2

Available interfaces:

1 - WAN (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.200.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

image.png

6. Enable DHCP server → **Oui**
7. Plage DHCP :
    - Début : **192.168.200.20**
    - Fin : **192.168.200.200**

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) y

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.200.10
Enter the end address of the IPv4 client address range: 192.168.200.110
Disabling IPv6 DHCPD...
```

image.png

Note : L'interface WAN obtient l'IP 192.168.42.41

```
The IPv4 LAN address has been set to 192.168.200.1/24


The IPv6 LAN address has been set to dhcp6

Press <ENTER> to continue.
QEMU Guest - Netgate Device ID: a0054941fe7ef1621d36

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.42.41/24
 LAN (lan)       -> vtnet1     -> v4: 192.168.200.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

image.png

2.2. Assignation interface SAN (console)

1. Appuyez sur **1**
2. Do VLANs need to be set up first ? → **n**
3. Should VLANs be set up now ? → **n**
4. Enter the WAN interface name → **vtnet0**
5. Enter the LAN interface name → **vtnet1**
6. Enter the Optional 1 interface name → **vtnet2**
7. Enter the Optional 2 interface name → **Entrée**
8. Do you want to proceed ? → **y**

2.3. Configuration interface SAN (console)

1. Appuyez sur **2**
2. Sélectionnez **3** (OPT1)
3. Configure IPv4 via DHCP ? → **n**
4. Adresse IP : **172.16.20.1**
5. Masque : **24**
6. Enable DHCP server on OPT1 ? → **n**
7. Validez

Note : L'interface WAN obtient l'IP 192.168.42.41

2.4. Accès interface web

1. Sur une machine cliente du réseau LAN, ouvrez un navigateur
2. Accédez à : http://192.168.200.1
3. Identifiants par défaut :
    - Username : **admin**
    - Password : **pfsense**

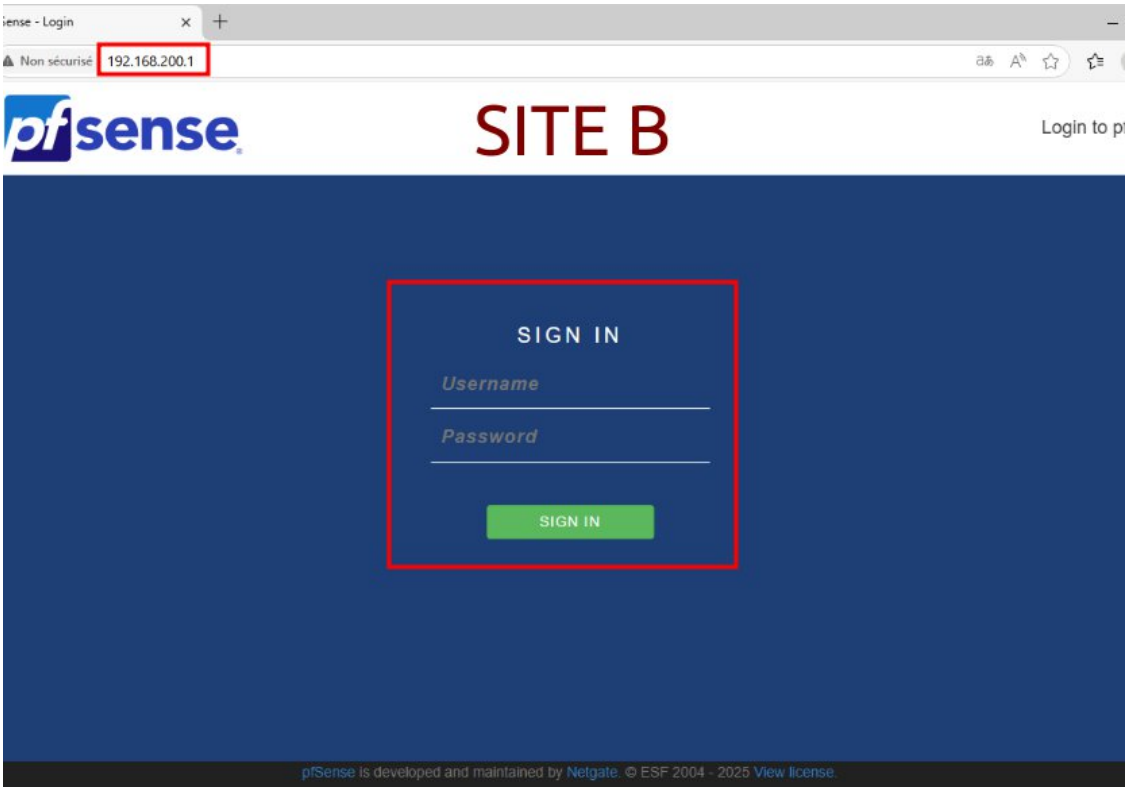


image.png

2.5. Renommage interface SAN (Interface Web)

1. **Interfaces** → **OPT1**
2. Enable interface + Description : **SAN**
3. IPv4 : **172.16.20.1 / 24**
4. **Save** et **Apply Changes**

![image.png]

2.6. Configuration DNS dans le DHCP Server

1. **Services** → **DHCP Server**
2. Onglet **LAN**
3. **DNS Servers** :
    - DNS Server 1 : **192.168.200.1** (pfSense - temporaire pour LOT 1)
    - DNS Server 2 : **10.10.10.1** (DNS de l'école - fallback)
4. **Save** et **Apply Changes**

2.7. Configuration DNS Resolver

1. Allez dans **Services** → **DNS Resolver**
2. **Enable DNS Resolver** : ✓ (coché)
3. **Listen Port** : 53

4. **Network Interfaces** : Sélectionnez **LAN** et **localhost**
5. **Outgoing Network Interfaces** : Sélectionnez **WAN**
6. **DNSSEC** : ✓ (coché - recommandé)
7. **DNS Query Forwarding** : ✓ (coché)
8. **Save**
9. **Apply Changes**

.

3. Configuration Tunnel IPsec

Objectif: Établir une liaison WAN inter-sites chiffrée via un tunnel VPN IPsec entre les deux sites distants de Strasbourg (Vauban et Somme) pour créer un réseau étendu sécurisé permettant la communication transparente entre les réseaux locaux comme s'ils étaient sur un même site. Cette connexion inter-sites répond directement à l'objectif n°2 du cahier des charges et respecte les recommandations de sécurité de l'ANSSI (AES-256-GCM pour le chiffrement, SHA256 pour l'intégrité, Diffie-Hellman groupe 14 minimum). Les deux Phase 2 configurées permettent le passage des flux LAN (192.168.100.0/24 vers 192.168.200.0/24) pour la communication inter-utilisateurs et des flux SAN (172.16.10.0/24 vers 172.16.20.0/24) pour la réplication des données de stockage iSCSI entre STG-SAN01 et STG2-SAN01, essentielle à la haute disponibilité et au plan de continuité d'activité (PCA).

3.1. Phase 1 - Site A

1. Allez dans **VPN** → **IPsec**

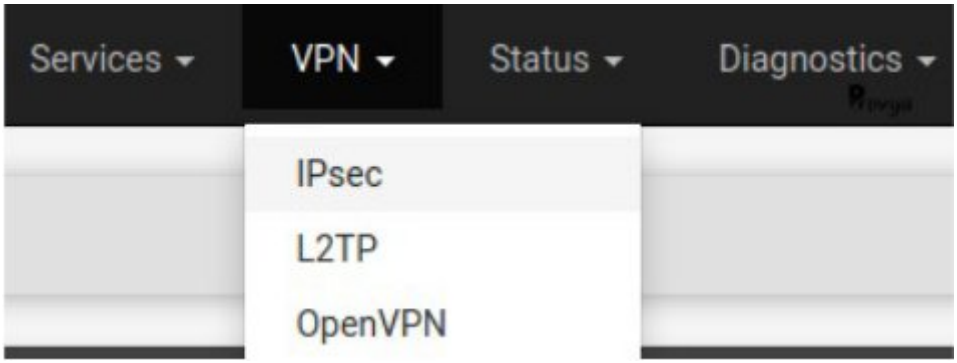


image.png

2. Cliquez **Add P1**

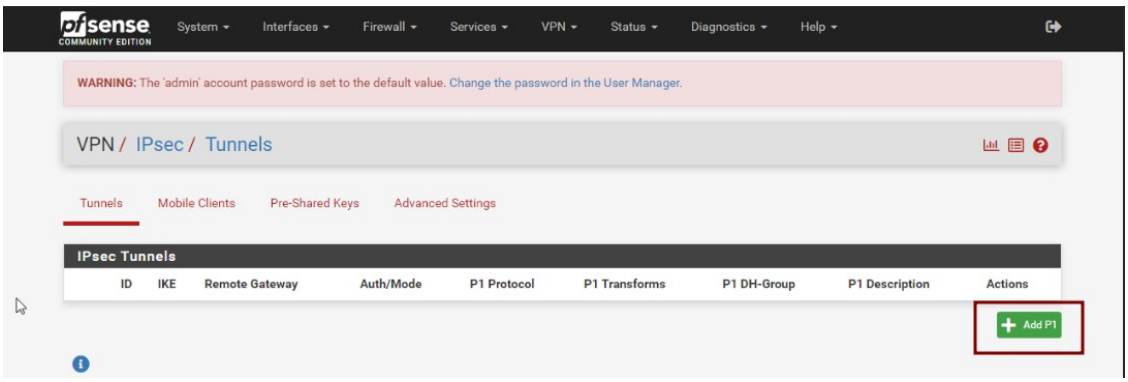


image.png

3. Configurez :

- **Key Exchange version** : IKEv2
- **Remote Gateway** : 192.168.42.41
- **Authentication Method** : Mutual PSK
- **Pre-Shared Key** : P@ssw0rd

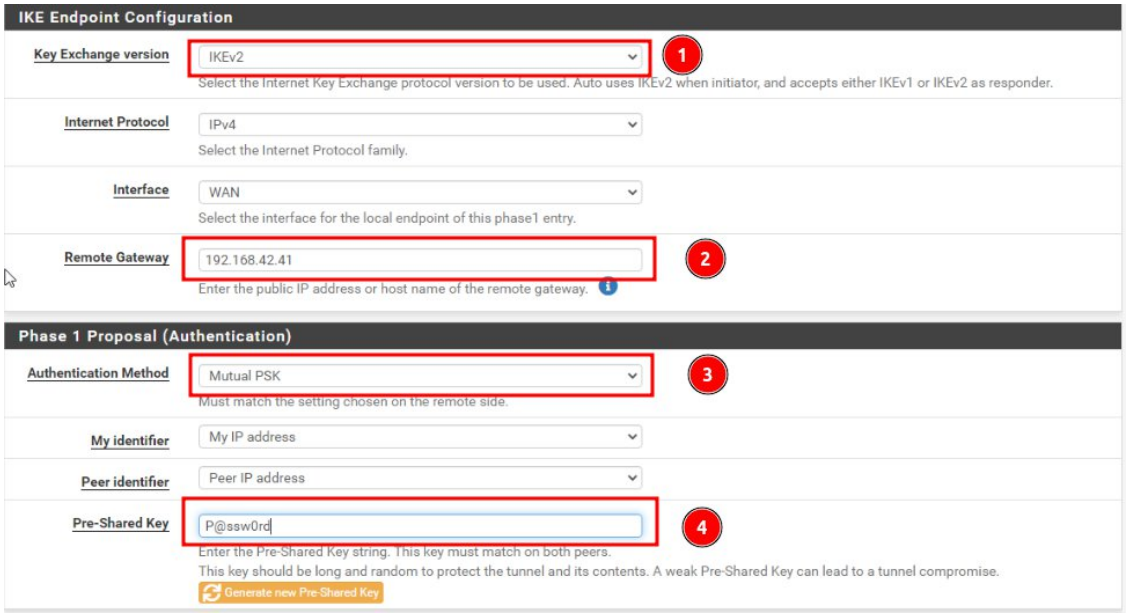


image.png

- **Encryption Algorithm** : AES (256 bits)
- **Hash Algorithm** : SHA256
- **DH Group** : 14 (2048 bits)
- **Lifetime** : 28800

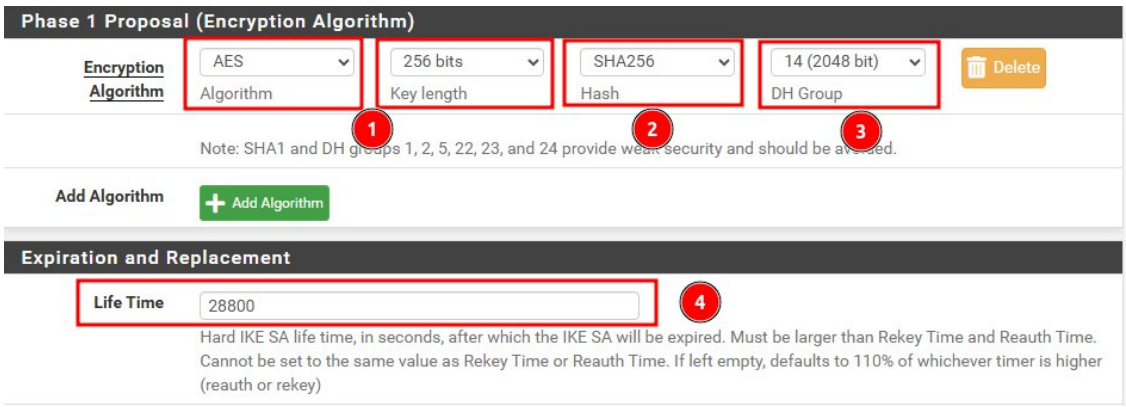


image.png

4. **Save**

3.2. Phase 1 - Site B

1. **VPN → IPsec → Add P1**
2. Configurez (identique au Site A sauf Remote Gateway) :
   - **Key Exchange version** : IKEv2

- **Remote Gateway** : 192.168.42.40
- **Authentication Method** : Mutual PSK
- **Pre-Shared Key** : P@ssw0rd
- **Encryption Algorithm** : AES (256 bits)
- **Hash Algorithm** : SHA256
- **DH Group** : 14 (2048 bits)
- **Lifetime** : 28800

3. **Save**

3.3. Phase 2 - Site A

1. Cliquez **Add P2** sous la Phase 1 créée

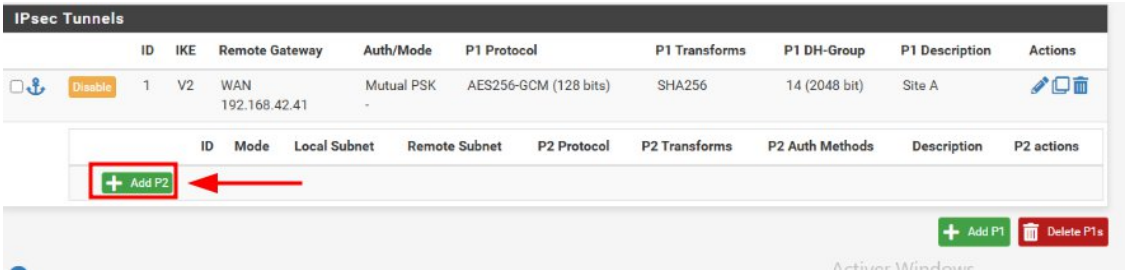


image.png

2. Configurez :

- Description : Site A
- **Mode** : Tunnel IPv4
- **Local Network** : LAN subnet (192.168.100.0/24)
- **Remote Network** : 192.168.200.0/24

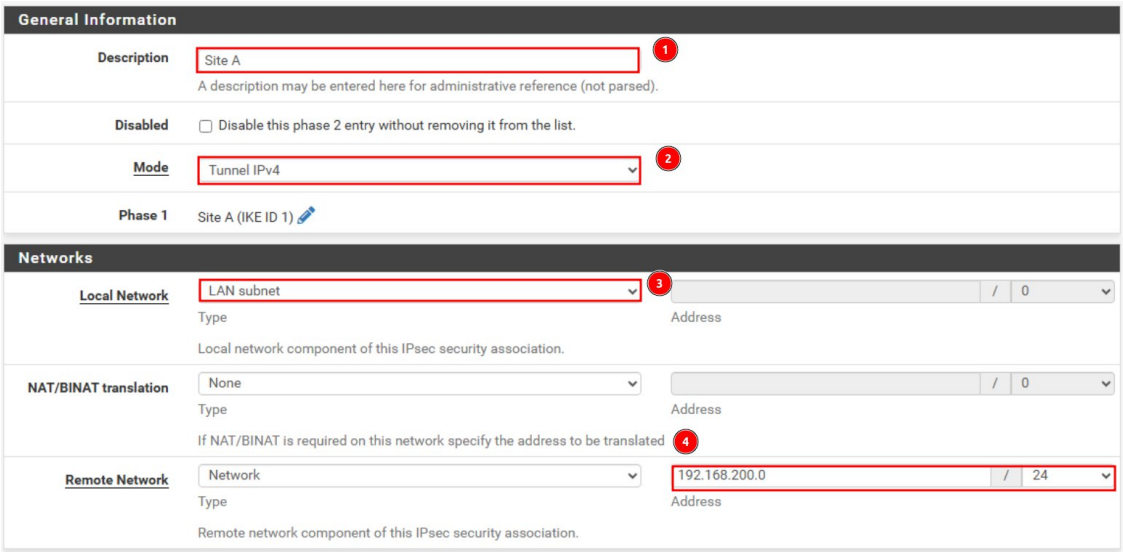


image.png

- **Protocol** : ESP
- **Encryption Algorithms** : AES (256 bits)
- **Hash Algorithms** : SHA256

- **PFS key group** : 14 (2048 bits)
- **Lifetime** : 28800

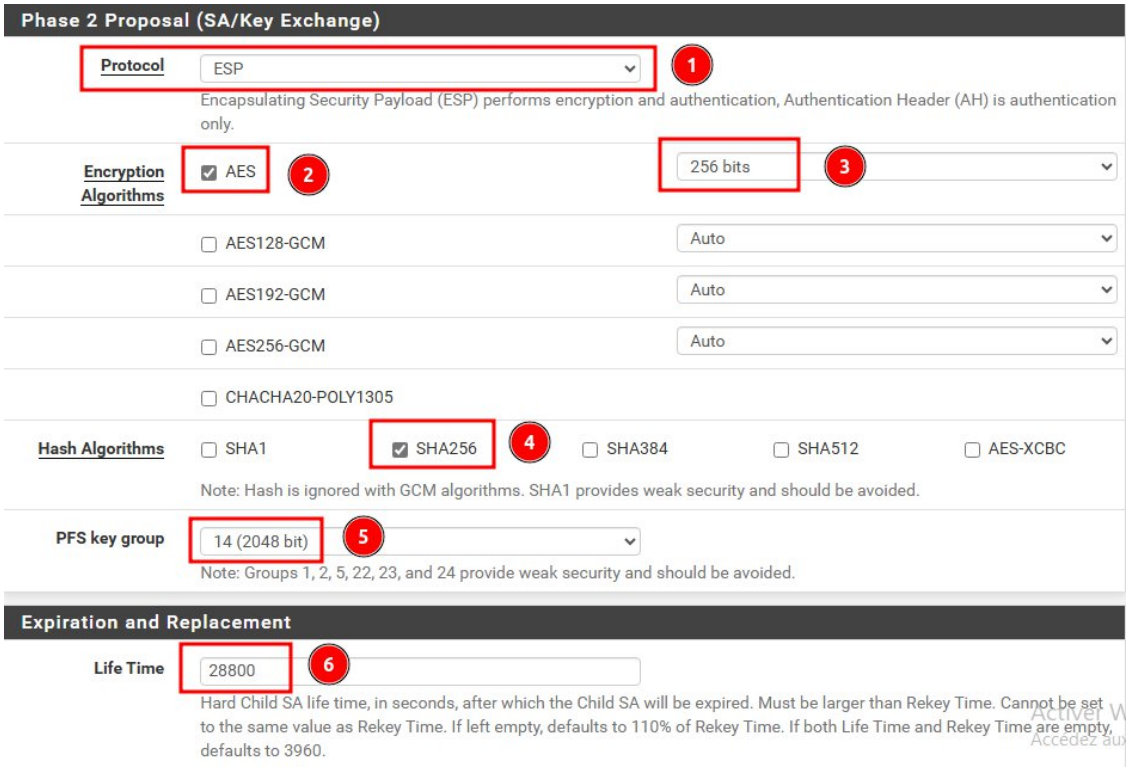


image.png

- **Automatically ping host** : 192.168.200.1
- Cocher l'option **Keep alive**

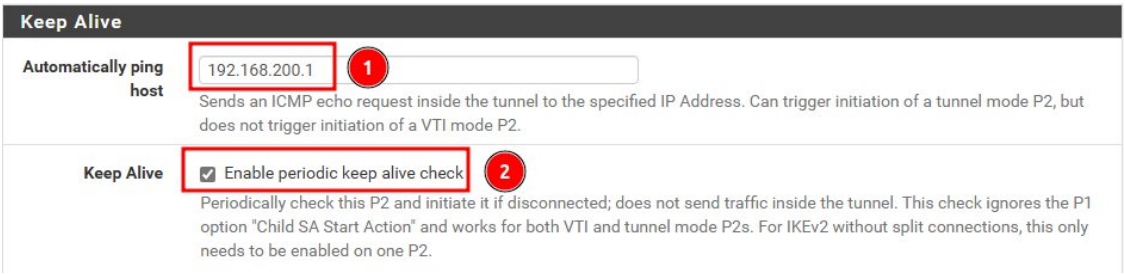


image.png

3. **Save**

3.4. Phase 2 - Site B

1. **Add P2** sous la Phase 1
2. Configurez (réseaux inversés par rapport à Site A) :
   - **Description** : Tunnel Site B vers Site A
   - **Mode** : Tunnel IPv4
   - **Local Network** : LAN subnet (192.168.200.0/24)
   - **Remote Network** : 192.168.100.0/24
   - **Protocol** : ESP
   - **Encryption Algorithms** : AES (256 bits)
   - **Hash Algorithms** : SHA256

- **PFS key group** : 14 (2048 bits)
- **Lifetime** : 28800
- **Automatically ping host** : 192.168.100.1
- Cocher l'option **Keep alive**

3. **Save**

3.5. Phase 2 (SAN) - Site A (OPTIONNEL)

Note importante : Cette Phase 2 supplémentaire est optionnelle mais recommandée si vous souhaitez permettre la réplication iSCSI inter-sites via le VPN (utile pour la haute disponibilité au LOT 3).

1. Dans **VPN → IPsec**, sous la Phase 1 existante, cliquez **Show Phase 2 Entries**
2. Cliquez **Add P2** (création d'une deuxième Phase 2)
3. Configurez :

- **Description** : Tunnel SAN Site A vers Site B
- **Mode** : Tunnel IPv4
- **Local Network** : Network → **172.16.10.0 / 24**
- **Remote Network** : Network → **172.16.20.0 / 24**

```
    ![image.png](LOT%201%20-%20Configuration%20R%C3%A9seau%20et%20VPN%20Site-
%C3%A0-Site/image%2023.png)

- **Protocol** : ESP
- **Encryption Algorithms** : AES (256 bits)
- **Hash Algorithms** : SHA256
- **PFS key group** : 14 (2048 bits)
- **Lifetime** : 3600

    ![image.png](LOT%201%20-%20Configuration%20R%C3%A9seau%20et%20VPN%20Site-
%C3%A0-Site/image%2024.png)

- **Automatically ping host** : **172.16.20.1**
- Cocher l'option **Keep alive**

    ![image.png](LOT%201%20-%20Configuration%20R%C3%A9seau%20et%20VPN%20Site-
%C3%A0-Site/image%2025.png)
```

4. **Save**

3.6. Phase 2 (SAN) - Site B (OPTIONNEL)

1. **Add P2** sous la Phase 1
2. Configurez (réseaux inversés) :
    - **Description** : Tunnel SAN Site B vers Site A
    - **Mode** : Tunnel IPv4
    - **Local Network** : Network → **172.16.20.0 / 24**
    - **Remote Network** : Network → **172.16.10.0 / 24**
    - **Protocol** : ESP
    - **Encryption Algorithms** : AES (256 bits)
    - **Hash Algorithms** : SHA256
    - **PFS key group** : 14 (2048 bits)
    - **Lifetime** : 3600

- **Automatically ping host** : **172.16.10.1**
- Cocher l'option **Keep alive**

3. **Save**

.

4. Configuration Règles de Pare-feu

Vue d'ensemble stratégique

Les règles firewall ont été analysées interface par interface pour anticiper l'ensemble des besoins des LOT 1 à 4. Conformément à l'exigence du LOT 4 "Règles de pare-feu configurées WAN, LAN, VPN et SAN" (CdC page 8), voici la répartition :

Tableau d'analyse par interface :

Interface	Rôle	Règles LOT 1	Ajouts LOT 2-4	Justification
WAN	Accès Internet + VPN IPsec	UDP 500, 4500, ESP	✗ Aucun	Pas de VPN nomade ni accès externe dans CdC
LAN	Réseau clients/serveurs	HTTP, HTTPS, DNS, ICMP, NTP, iSCSI	✓ AD, SMB, RPC, RDP, etc.	Services LOT 2-3-4 nécessitent ports supplémentaires
SAN	Réseau stockage iSCSI	iSCSI (3260), ICMP	✗ Aucun	Réseau dédié exclusivement au stockage
IPsec	Tunnel VPN inter-sites	any/any	✗ Aucun	Règle couvre tous les protocoles LOT 1-4

Approche stratégique :

Les règles firewall ont été configurées dès le LOT 1 pour anticiper l'ensemble des besoins des LOT 2 à 4 (Active Directory, DFS, GPO, RDP). Cette approche proactive permet de :

1. **Respecter l'exigence LOT 4** "Règles configurées WAN, LAN, VPN et SAN" (CdC page 8)
2. **Optimiser le temps de configuration** des LOT suivants (gain estimé : 3-4 heures)
3. **Garantir la disponibilité immédiate** des services lors de leur déploiement
4. **Éviter les oublis** de ports critiques (LDAP, SMB, RPC, etc.)
5. **Faciliter les tests** avec une configuration complète et documentée

Seule l'interface **LAN** nécessite des règles supplémentaires pour anticiper les LOT 2-4. Les interfaces WAN, SAN et IPsec sont complètes dès le LOT 1.

.

4.1. Règles WAN (complètes pour LOT 1-4)

Objectif : Autoriser l'établissement et le maintien du tunnel VPN IPsec site-à-site.

Tableau récapitulatif WAN :

#	Description	Action	Proto	Port	LOT	Status
1	IKE/ISAKMP	Pass	UDP	500	1-4	✅ Complet
2	NAT Traversal	Pass	UDP	4500	1-4	✅ Complet
3	ESP Encapsulation	Pass	ESP	-	1-4	✅ Complet

[capture d'écran de toutes les règles]

> Note importante : Ces règles couvrent intégralement les besoins du projet AP3 (LOT 1 à 4). Le cahier des charges ne prévoit pas de VPN nomade, d'accès RDP externe ou de services publics. Aucune règle WAN supplémentaire n'est nécessaire.

.

4.2. Règles LAN (complétées pour LOT 1-4)

Objectif : Autoriser les flux métier nécessaires pour les services LOT 1 à 4 (navigation web, Active Directory, DFS, GPO, RDP).

Configuration dans pfSense :

1. Allez dans **Firewall → Rules → LAN**
2. Configurez les règles selon le tableau ci-dessous (ordre important : top → bottom)

Tableau récapitulatif des règles LAN :

#	Description	Action	Proto	Src	Dst	Port(s)	LOT	Status
1	Résolution DNS	Pass	TCP/UDP	LAN net	any	53	1	✅ Actif
2	Navigation HTTP	Pass	TCP	LAN net	any	80	1	✅ Actif
3	Navigation HTTPS	Pass	TCP	LAN net	any	443	1	✅ Actif
4	Diagnostics ICMP	Pass	ICMP	LAN net	any	-	1	✅ Actif
5	Sync temps NTP	Pass	UDP	LAN net	any	123	1	✅ Actif
6	Stockage iSCSI	Pass	TCP	LAN net	SAN net	3260	1-3	✅ Actif

#	Description	Action	Proto	Src	Dst	Port(s)	LOT	Status
7	Trafic VPN inter-sites	Pass	any	LAN net	Remote LAN	-	1-4	✅ Actif
8	Communication intra-LAN	Pass	any	LAN net	LAN net	-	2-4	Anticipé
9	Active Directory LDAP	Pass	TCP/UDP	LAN net	any	389	2	Anticipé
10	AD LDAPS sécurisé	Pass	TCP	LAN net	any	636	2	Anticipé
11	Authentification Kerberos	Pass	TCP/UDP	LAN net	any	88	2	Anticipé
12	Partages fichiers SMB	Pass	TCP	LAN net	any	445	2-3	Anticipé
13	Services Windows RPC	Pass	TCP	LAN net	any	135	2	Anticipé
14	RPC ports dynamiques	Pass	TCP	LAN net	any	49152-65535	2	Anticipé
15	Global Catalog AD	Pass	TCP	LAN net	any	3268-3269	2	Anticipé
16	Administration RDP	Pass	TCP	LAN net	any	3389	4	Anticipé
17	WinRM PowerShell	Pass	TCP	LAN net	any	5985-5986	4	Optionnel

Légende :

- ✅ **Actif** : Règle nécessaire dès le LOT 1, tests effectués
- **Anticipé** : Règle configurée pour LOT 2-4, tests prévus au déploiement
- **Optionnel** : Règle non essentielle, peut être activée selon besoins

[capture d’écran de toutes les règles]

.

4.3. Règles SAN (complètes pour LOT 1-4)

Objectif : Isoler le trafic de stockage iSCSI sur un réseau dédié.

Tableau récapitulatif SAN :

#	Description	Action	Proto	Src	Dst	Port	LOT	Status
1	Stockage iSCSI	Pass	TCP	SAN net	SAN net	3260	1-3	✅ Complet
2	Diagnostics ICMP	Pass	ICMP	any	any	-	1-4	✅ Complet

[capture d’écran de toutes les règles]

.

4.4. Règles IPsec (complètes pour LOT 1-4)

Objectif : Autoriser le trafic inter-sites via le tunnel VPN chiffré.

Tableau récapitulatif IPsec :

#	Description	Action	Proto	Src	Dst	LOT	Status
1	Trafic inter-sites	Pass	any	any	any	1-4	✅ Complet

[capture d’écran de toutes les règles]

.

Résumé Configuration Firewall Complète

Statistiques par interface :

Interface	Règles configurées	Règles actives LOT 1	Règles anticipées LOT 2-4
WAN	3	3	0
LAN	17	7	10
SAN	2	2	0
IPsec	1	1	0
TOTAL	**23**	**13**	**10**

5. Sauvegarde Configuration

Objectif : Assurer la pérennité et la restaurabilité de la configuration pfSense en exportant les fichiers XML contenant l’intégralité des paramètres (interfaces, VPN, règles firewall, DHCP, DNS, NAT) pour permettre une remise en service rapide en cas de défaillance matérielle ou d’erreur de manipulation. Cette pratique répond directement aux exigences du cahier des charges concernant la documentation complète

d’installation, configuration et exploitation, ainsi qu’à la démarche ITIL initiée par la DSI visant la certification ISO 20000 et ISO 27000. Les sauvegardes des configurations RTE-STG01 et RTE2-STG01 constituent des éléments essentiels du plan de reprise d’activité (PRA) et permettent d’identifier des indicateurs précis quant au bon fonctionnement des équipements, conformément aux objectifs de gestion des configurations.

5.1. Sauvegarde pfSense

Sur les deux pfSense :

1. **Diagnostics → Backup & Restore**

[capture d’écran]

1. Backup area : **All**
2. Cochez **Skip packages**
3. Cochez **Skip RRD data**
4. Cliquez **Download configuration as XML**
5. Enregistrez :
   - `RTE-STG01_backup_20251027.xml` (Site A)
   - `RTE2-STG01_backup_20251027.xml` (Site B)

   [capture d’écran]

.

6. Résumé de la Configuration

Objectif : Fournir une documentation de synthèse consolidant tous les paramètres techniques critiques de l’infrastructure réseau du LOT 1 dans des tableaux récapitulatifs (plan d’adressage global, paramètres DHCP, configuration VPN IPsec, règles firewall, conformité ANSSI) pour faciliter l’exploitation, le dépannage et le transfert de compétences. Cette section répond à l’exigence de mémoire technique fonctionnel rédigé en français devant être remis pour chaque élément technique de la solution mis en place. Les tableaux permettent une consultation rapide sans parcourir l’ensemble de la documentation détaillée, améliorant ainsi le service aux utilisateurs et facilitant l’administration par la DSI, premiers axes stratégiques du projet. Le tableau de conformité ANSSI documente explicitement le respect des recommandations de sécurité relatives à IPsec (ANNEXE 5) et aux pare-feu (ANNEXE 6), démontrant la robustesse de la solution face aux menaces.

6.1. Interfaces Configurées

Site	LAN	WAN	SAN
Site A	192.168.100.1/24	192.168.42.40	172.16.10.1/24
Site B	192.168.200.1/24	192.168.42.41	172.16.20.1/24

6.2. Plages DHCP

Site	Plage DHCP	DNS Distribué
Site A	192.168.100.20 - 192.168.100.200	192.168.100.1, 10.10.10.1
Site B	192.168.200.20 - 192.168.200.200	192.168.200.1, 10.10.10.1

6.3. Paramètres DNS

Configuration	Valeur
DNS Serveur École	10.10.10.1
DNS Resolver pfSense	Activé avec forwarding
Distribution via	DHCP Server (temporaire LOT 1)
Evolution LOT 2	DHCP Windows Server avec AD DNS

6.4. Paramètres VPN IPsec

Paramètre	Valeur	Conformité ANSSI
Version IKE	IKEv2	✓
Chiffrement	AES-256	✓
Hash	SHA256	✓
DH Group	14 (2048 bits)	✓
Lifetime P1	28800 s (8h)	Standard
Lifetime P2	3600 s (1h)	Standard
Pre-Shared Key	P@ssw0rd	À renforcer en production

6.5. Règles de Pare-feu Configurées

Interface WAN :

- ✅ UDP 500 (IKE)
- ✅ UDP 4500 (NAT-T)
- ✅ ESP (Protocol 50)

Interface LAN :

- ✅ HTTP (80)
- ✅ HTTPS (443)
- ✅ ICMP (ping)
- ✅ DNS (53 UDP)
- ✅ iSCSI vers SAN (3260)

Interface SAN :

- ✅ iSCSI (3260 TCP)
- ✅ ICMP (ping)

Interface IPsec :

- ✅ Any/Any (tout le trafic inter-sites)

.

7. Évolutions prévues pour le LOT 2

Objectif : Anticiper et documenter la transition vers l'infrastructure définitive du LOT 2 en identifiant les modifications nécessaires lors du déploiement des 4 serveurs Windows Server 2022 Standard avec les rôles AD DS, DNS et DHCP sur les deux sites. Cette section prépare le transfert du service DHCP des pare-feu pfSense vers les contrôleurs de domaine (STG-SRVW01/02 et STG2-SRVW01/02) avec DHCP de

basculement pour la haute disponibilité, le changement de configuration DNS pointant vers les serveurs AD du domaine IEF.LOCAL au lieu du forwarding école (10.10.10.1), et valide que l'architecture réseau actuelle est compatible avec l'intégration au domaine Active Directory comportant 1 forêt et 4 contrôleurs de domaine (1 principal au Site A, 3 supplémentaires). La checklist de validation garantit que tous les prérequis du LOT 1 sont remplis avant de passer au LOT 2, évitant ainsi les dépendances bloquantes et assurant le respect du planning prévisionnel du projet avec livraison du LIVRABLE 1 le 20 octobre 2025.

7.1. Désactivation DHCP pfSense

Au LOT 2, après installation des serveurs Windows AD/DHCP :

1. **Services → DHCP Server → LAN**
2. **Décocher** "Enable DHCP server on LAN interface"
3. **Save** + **Apply Changes**

7.2. Configuration DNS pour Active Directory

Les clients devront pointer vers les contrôleurs de domaine :

Site	DNS Primaire	DNS Secondaire
Site A	192.168.100.10 (STG-SRVW01)	192.168.100.11 (STG-SRVW02)
Site B	192.168.200.10 (STG2-SRVW01)	192.168.200.11 (STG2-SRVW02)

Les serveurs Windows AD/DNS feront le forwarding vers 10.10.10.1 pour les requêtes Internet.

.

7.3. Checklist de validation LOT 1

- [✓] pfSense Site A opérationnel (WAN, LAN, SAN configurés)
- [✓] pfSense Site B opérationnel (WAN, LAN, SAN configurés)
- [✓] Tunnel VPN IPsec établi (Phase 1 + Phase 2 LAN)
- [✓] Phase 2 SAN configurée (optionnel)
- [✓] Conformité ANSSI (IKEv2, AES-256, SHA256, DH14)
- [✓] Règles firewall WAN (UDP 500, 4500, ESP)
- [✓] Règles firewall LAN (HTTP, HTTPS, DNS, ICMP, accès SAN)
- [✓] Règles firewall SAN (iSCSI port 3260)
- [✓] Règles firewall IPsec (trafic inter-sites)
- [✓] DHCP temporaire fonctionnel (plages .20-.200)
- [✓] DNS forwarding vers 10.10.10.1 opérationnel
- [✓] Sauvegarde configuration pfSense réalisée
- [✓] Documentation complète rédigée

.

FIN DU LOT 1

Menu Livrable 2 | ➡ LOT suivant

LOT 2 - Déploiement Active Directory, DNS et DHCP

⬅ Retour au Menu Livrable 2 | Retour à l'accueil

Le Cœur du Système : Identité Centralisée et Services Réseau

Avec le réseau en place, ce lot déploie l'intelligence du système d'information : l'annuaire **Active Directory**. Nous avons conçu une architecture distribuée reposant sur **4 contrôleurs de domaine Windows Server 2022**, assurant une redondance totale des services d'authentification (SSO) et de résolution de noms (DNS). L'objectif est double : offrir une expérience utilisateur unifiée (un seul compte pour accéder à tout) et garantir la continuité de service grâce à la mise en place de clusters DHCP autonomes sur chaque site. C'est ici que l'infrastructure devient un véritable environnement de travail professionnel.

.

.

0. Plan d'Adressage des Serveurs (LOT 2)

Ce plan détaille les adresses IP statiques qui seront configurées sur les serveurs Windows pour ce lot, en complément du plan d'adressage réseau défini au LOT 1.

Site	Hôte	Rôle	OS	Interface LAN	Interface SAN
Site A	STG-SRVW01	DC Principal, DNS, DHCP, DFS 1111	Win 2022 GUI 2	192.168.100.10/24	172.16.10.10/24
Site A	STG-SRVW02	DC Secondaire, DNS, DFS 3333	Win 2022 CORE 4	192.168.100.11/24	172.16.10.11/24
Site A	STG-SAN01	Stockage iSCSI 55	TrueNAS Core	-	172.16.10.20/24
Site B	STG2-SRVW01	DC Suppl., DNS, DHCP (Failover), DFS 6666	Win 2022 GUI 7	192.168.200.10/24	172.16.20.10/24
Site B	STG2-SRVW02	DC Suppl., DNS, DFS 8888	Win 2022 CORE 9	192.168.200.11/24	172.16.20.11/24
Site B	STG2-SAN01	Stockage iSCSI 1010	TrueNAS Core	-	172.16.20.20/24

Note importante : Les adresses IP des serveurs DNS (192.168.100.10, .11 et 192.168.200.10, .11) remplaceront les serveurs DNS temporaires configurés au LOT 1 (pfSense et 10.10.10.1). Ce changement sera déployé via le nouveau service DHCP Windows.

.

1. Prérequis et Installation des Serveurs

1.1. Objectif Stratégique

Objectif: Préparer les quatre serveurs Windows Server 2022 (deux par site) en installant l'OS et en appliquant une configuration IP statique. Cette étape est le prérequis indispensable au déploiement des services d'annuaire (AD DS), de résolution de noms (DNS) et de distribution d'adresses (DHCP). La configuration inclut des interfaces LAN (pour la communication client/serveur) et SAN (pour le futur stockage iSCSI du LOT 3), assurant ainsi la segmentation des flux. Cette préparation assure également que les serveurs sont prêts à être promus en contrôleurs de domaine pour la forêt unique `IEF.`.

1.2. Installation de base (Rappel)

1. Installation de **Windows Server 2022 Standard** sur les 4 VM:
    - `STG-SRVW01` : Version **GUI** (Interface graphique)
    - `STG-SRVW02` : Version **CORE**
    - `STG2-SRVW01` : Version **GUI** (Interface graphique)
    - `STG2-SRVW02` : Version **CORE**
2. Configuration du mot de passe Administrateur local : `P@ssword10`
3. Renommage des serveurs (via `sconfig` sur CORE ou Propriétés Système sur GUI) pour correspondre au plan d'adressage.
4. Configuration du fuseau horaire et activation des mises à jour Windows.

1.3. Configuration IP - Site A (STG-SRVW01 et 02)

Sur STG-SRVW01 (GUI) :

1. Ouvrir `ncpa.cpl`.
2. **Interface LAN :**
    - Adresse IP : **192.168.100.10**
    - Masque : **255.255.255.0**
    - Passerelle : **192.168.100.1** (pfSense Site A)
    - DNS Préféré : **192.168.100.10** (lui-même, en préparation de la promotion)
    - DNS Auxiliaire : **192.168.100.11** (futur 2e DC)
3. **Interface SAN :**
    - Adresse IP : **172.16.10.10**
    - Masque : **255.255.255.0**
    - Passerelle : (vide)
    - DNS : (vide)

Sur STG-SRVW02 (CORE) - via `sconfig` :

1. Lancer `sconfig`
2. Choisir l'option **8) Paramètres réseau**.
3. **Interface LAN :**
    - Adresse IP : **192.168.100.11**
    - Masque : **255.255.255.0**
    - Passerelle : **192.168.100.1**
    - DNS Préféré : **192.168.100.11** (DC Principal)

- DNS Auxiliaire : **192.168.200.10** (DC Site B)

4. **Interface SAN :**
   - Adresse IP : **172.16.10.11**
   - Masque : **255.255.255.0**
   - Passerelle : (vide)
   - DNS : (vide)

1.4. Configuration IP - Site B (STG2-SRVW01 et 02)

Sur STG2-SRVW01 (GUI) :

1. Ouvrir `ncpa.cpl`.
2. **Interface LAN :**
   - Adresse IP : **192.168.200.10**
   - Masque : **255.255.255.0**
   - Passerelle : **192.168.200.1** (pfSense Site B)
   - DNS Préféré : **192.168.100.10** (DC Principal Site A)
   - DNS Auxiliaire : **192.168.200.11** (futur 2e DC local)
3. **Interface SAN :**
   - Adresse IP : **172.16.20.10**
   - Masque : **255.255.255.0**
   - Passerelle : (vide)
   - DNS : (vide)

Sur STG2-SRVW02 (CORE) - via `sconfig` :

1. Lancer `sconfig`
2. Choisir l'option **8) Paramètres réseau**.
3. **Interface LAN :**
   - Adresse IP : **192.168.200.11**
   - Masque : **255.255.255.0**
   - Passerelle : **192.168.200.1**
   - DNS Préféré : **192.168.200.11** (DC Principal Site A)
   - DNS Auxiliaire : **192.168.200.10** (DC local Site B)
4. **Interface SAN :**
   - Adresse IP : **172.16.20.11**
   - Masque : **255.255.255.0**
   - Passerelle : (vide)
   - DNS : (vide)

1.5. Désactivation DHCP sur pfSense (Rappel LOT 1)

Action Requise : Avant d'activer le DHCP Windows, il est impératif de désactiver le service DHCP temporaire sur les deux routeurs pfSense pour éviter les conflits.

1. Connectez-vous à l'interface web de **RTE-STG01 (192.168.100.1)** et **RTE2-STG01 (192.168.200.1)**.
2. Allez dans **Services → DHCP Server → LAN**.
3. **Décochez** la case "Enable DHCP server on LAN interface".
4. Sauvegardez les modifications.

.

2. Déploiement Active Directory (Site A)

2.1. Objectif

Objectif: Créer le cœur du système d'information en installant le premier contrôleur de domaine (`STG-SRVW01`). Cette action crée la nouvelle forêt Active Directory `IEF.LOCAL` et installe le service DNS intégré. L'ajout du second serveur (`STG-SRVW02`) en tant que contrôleur de domaine secondaire assure la **haute disponibilité locale** sur le Site A pour l'authentification (SSO) et la résolution de noms, conformément à la répartition des rôles.

2.2. Installation du rôle AD DS (STG-SRVW01)

1. Ouvrir le **Gestionnaire de serveur**.
2. Cliquer sur **Ajouter des rôles et fonctionnalités**.
3. Type d'installation : **Installation basée sur un rôle ou une fonctionnalité**.
4. Sélectionner le serveur `STG-SRVW01`.
5. Cocher le rôle **Services AD DS** (Active Directory Domain Services).
6. Accepter l'ajout des fonctionnalités requises (Outils de gestion, etc.).
7. Cocher le rôle **Serveur DHCP**.
8. Cocher le rôle **Serveur DNS** (normalement coché automatiquement avec AD DS).
9. Valider et **Installer**.

2.3. Promotion de STG-SRVW01 (Contrôleur Principal)

1. Après l'installation, cliquer sur le drapeau de notification dans le Gestionnaire de serveur.
2. Cliquer sur **Promouvoir ce serveur en contrôleur de domaine**.
3. Sélectionner **Ajouter une nouvelle forêt**.
4. Nom de domaine racine : **IEF.LOCAL**

   ```
   Name "IEF.LOCAL" -Credential $cred -SafeModeAdministratorPassword $pass
   -InstallDns:$true -Force
   ```

5. Niveau fonctionnel : Laisser **Windows Server 2016** (par défaut pour 2022).
6. Vérifier que **Serveur DNS** et **Catalogue Global (GC)** sont cochés.
7. Entrer le mot de passe de restauration DSRM : **P@ssword10**
8. Ignorer l'avertissement de délégation DNS.
9. Nom NetBIOS : **IEF** (laisser par défaut)
10. Chemins : Laisser par défaut (sur C:).
11. Vérifier les options et lancer l'installation. Le serveur redémarrera automatiquement.

2.4. Ajout de STG-SRVW02 (Contrôleur Secondaire - Core)

1. Sur `STG-SRVW02` (session Administrateur), ouvrir **PowerShell**.

2. Installer le rôle AD DS :

   ```
   Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
   ```

   ### Étape 3 : Préparer les identifiants (La méthode propre)

   On va stocker ton login et ton mot de passe de secours dans des “variables” pour ne pas alourdir la commande finale.

   1. Tape cette ligne et valide :

      ```
      $cred = Get-Credential
      ```

      Une fenêtre s’ouvre : tape `IEF\Administrateur` et ton mot de passe.

   2. Tape cette ligne et valide :

      ```
      $pass = ConvertTo-SecureString "P@ssword10" -AsPlainText -Force
      ```

      (Ça stocke le mot de passe de restauration DSRM).

3. Promouvoir le serveur (adapter les identifiants si nécessaire) :

   ```
   Install-ADDSDomainController -DomainName "IEF.LOCAL" -Credential $cred
   -SafeModeAdministratorPassword $pass -InstallDns:$true -Force
   ```

   Note : Le mot de passe DSRM doit être entré manuellement (P@ssword10). Le serveur redémarrera automatiquement.

.

3. Déploiement Active Directory (Site B)

3.1. Objectif

Objectif: Étendre la forêt `IEF.LOCAL` au site distant (Strasbourg Somme) en ajoutant deux contrôleurs de domaine supplémentaires (`STG2-SRVW01` et `STG2-SRVW02`). Cette action crée un **système d’information unifié et hautement disponible**. Les utilisateurs du Site B pourront s’authentifier localement même en cas de coupure du VPN IPsec (LOT 1), garantissant ainsi la continuité d’activité et la redondance des services, objectifs clés du projet.

3.2. Configuration des Sites AD

Avant de promouvoir les serveurs du Site B, il est crucial de définir les sites et sous-réseaux pour optimiser la réplication.

1. Sur `STG-SRVW01` (Site A), ouvrir **Sites et services Active Directory**.
2. Renommer `Default-First-Site-Name` en **VAUBAN**.
3. Clic droit sur Sites → **Nouveau site…**
   - Nom : **SOMME**
   - Lien : `DEFAULTIPSITELINK`
4. Clic droit sur Subnets → **Nouveau sous-réseau…**
   - Préfixe : **192.168.100.0/24**
   - Site : **VAUBAN**
5. Clic droit sur Subnets → **Nouveau sous-réseau…**
   - Préfixe : **192.168.200.0/24**

- Site : **SOMME**

3.3. Ajout de STG2-SRVW01 (Contrôleur Supplémentaire - GUI)

1. Sur `STG2-SRVW01`, installer le rôle **Services AD DS** (cf. étape 2.2).
2. **Promouvoir** le serveur en contrôleur de domaine.
3. Sélectionner **Ajouter un contrôleur de domaine à un domaine existant**.
4. Domaine : **IEF.LOCAL**
5. Fournir les identifiants d'un administrateur du domaine (ex: `IEF\Administrateur`).
6. Vérifier que **DNS** et **Catalogue Global (GC)** sont cochés.
7. Sélectionner le nom de site : **SOMME**.
8. Mot de passe DSRM : **P@ssword**
9. Installer depuis : `STG-SRVW01.ief.local` (ou `Any domain controller`).
10. Valider et installer. Le serveur redémarrera.

3.4. Ajout de STG2-SRVW02 (Contrôleur Supplémentaire - Core)

1. Sur `STG2-SRVW02`, ouvrir **PowerShell** et installer le rôle AD DS.
2. Promouvoir le serveur :

```
$cred = Get-Credential
$pass = ConvertTo-SecureString "P@ssword10" -AsPlainText -Force
Install-ADDSDomainController -DomainName "IEF.LOCAL" -Credential $cred
-SafeModeAdministratorPassword $pass -SiteName "SOMME" -
InstallDns:$true -Force
```

3. Le serveur redémarrera.

3.5 Difficultés Rencontrées et Résolution

Incidence Majeure : Échec de la promotion du Contrôleur de Domaine Site B

- **Impact :** Arrêt de la production pendant 24 heures.
- **Symptôme :** Impossibilité pour le serveur `STG2-SRVW01` (Site B) de rejoindre le domaine `IEF.LOCAL` ou d'être promu Contrôleur de Domaine à travers le VPN IPsec.
- **Erreurs rencontrées :**
  - *Code 1722 : Le serveur RPC n'est pas disponible.*
  - *Code 50 : La demande n'est pas prise en charge (The request is not supported).*
  - *Échec de la relation d'approbation (Trust Relationship).*

Démarche de Diagnostic et Actions Entreprises :

Face à ces erreurs indiquant des problèmes de communication réseau à travers le tunnel VPN, une procédure de dépannage exhaustive a été menée pour isoler la cause (Réseau vs Système) :

1. **Validation de la connectivité Réseau (Couche 3 & 4) :**
   - Tests Ping et résolution DNS : **Succès**.
   - Tests de port (`Test-NetConnection`) sur les ports critiques AD (88, 389, 445, 135) : **Succès (True)**.
   - Cela a permis d'écarter un blocage "simple" de pare-feu.
2. **Hypothèse de la fragmentation (MTU/VPN) :**

    - Suspicion de paquets UDP Kerberos trop volumineux pour le tunnel IPsec (problème classique de fragmentation).
    - **Actions :** Activation du *MSS Clamping* (1300 puis 1200) sur les pare-feux pfSense, désactivation du *Hardware Checksum Offloading* sur les interfaces virtuelles pfSense, et tentatives de forçage du protocole Kerberos sur TCP via le registre Windows (`MaxPacketSize`).
3. **Hypothèse de l'identité Active Directory :**
    - Nettoyage complet des métadonnées (Metadata Cleanup) sur le Contrôleur Principal (Site A).
    - Multiples tentatives de "Reset" de l'identité du serveur (Workgroup > Reboot > Domain).
    - Renommage du serveur (`STG2-TEMP`) pour forcer une nouvelle identification SID.
4. **Hypothèse de l'environnement Virtuel (Proxmox/VirtIO) :**
    - Désactivation des options de délestage matériel (*Hardware Offloading*) sur les cartes réseaux virtuelles Windows.
    - Désactivation de l'IPv6 pour éviter les conflits de résolution DNS sur le tunnel IPv4.

Résolution Finale et Cause Racine :

Malgré la validation de tous les prérequis réseau et l'application des correctifs recommandés par Microsoft et Netgate, l'erreur persistait sur cette machine spécifique.

La décision a été prise de **reconstruire intégralement la machine virtuelle** (Clean Install) en appliquant uniquement les bonnes pratiques réseau de base (IP fixe, DNS correct, IPv6 désactivé).

- **Résultat :** La nouvelle VM a rejoint le domaine et a été promue Contrôleur de Domaine **immédiatement et sans erreur**, sans nécessiter les modifications avancées (Registre/Offloading) tentées précédemment.
- **Conclusion :** L'incident a été causé par une **corruption irréversible de la pile réseau ou du système d'exploitation de la VM initiale**, rendant le débogage inopérant. L'infrastructure réseau (pfSense/VPN), une fois corrigée (Checksum Offload), était fonctionnelle.

.

4. Configuration des Objets Active Directory

4.1. Objectif

Objectif: Structurer l'annuaire Active Directory en créant les Unités d'Organisation (UO), les groupes et les utilisateurs spécifiés dans l'**Annexe 2** du cahier des charges. Cette structure permet une gestion centralisée des permissions, une délégation d'administration et la future application des stratégies de groupe (GPO) du LOT 4.

4.2. Création des Unités d'Organisation (UO)

1. Sur `STG-SRVW01`, ouvrir **Utilisateurs et ordinateurs Active Directory**.
2. Clic droit sur `IEF.LOCAL` → Nouveau → **Unité d'organisation**.
3. Nom : **VAUBAN**
4. Clic droit sur `IEF.LOCAL` → Nouveau → **Unité d'organisation**.
5. Nom : **SOMME**

4.3. Création des Groupes et Utilisateurs

1. **Créer les utilisateurs :**
    - Clic droit sur l'UO **VAUBAN** → Nouveau → **Utilisateur**
        - Prénom : `Paul` (Login : `paul`)
        - Prénom : `Pierre` (Login : `pierre`)
    - Clic droit sur l'UO **SOMME** → Nouveau → **Utilisateur**
        - Prénom : `Isabelle` (Login : `isabelle`)
        - Prénom : `Nathalie` (Login : `nathalie`)
    - Clic droit sur `Users` (ou une UO d'administration) → Nouveau → **Utilisateur**
        - Nom : `ADMIN` (Admin de secours)
    - Note : Définir un mot de passe temporaire (ex: `P@ssword10`) et cocher "L'utilisateur doit changer le mot de passe à la prochaine connexion".
2. **Créer les groupes :**
    - Clic droit sur l'UO **VAUBAN** → Nouveau → **Groupe**
        - Nom du groupe : **GRP1** (Étendue : Globale, Type : Sécurité)
    - Clic droit sur l'UO **SOMME** → Nouveau → **Groupe**
        - Nom du groupe : **GRP2** (Étendue : Globale, Type : Sécurité)
3. **Ajouter les membres :**
    - Ouvrir les propriétés de **GRP1** → onglet Membres → Ajouter `Paul` et `Pierre`.
    - Ouvrir les propriétés de **GRP2** → onglet Membres → Ajouter `Isabelle` et `Nathalie`.
    - Ajouter l'utilisateur `ADMIN` au groupe **Administrateurs du Domaine**.

4.4. Vérification de la Réplication AD

1. Attendre quelques minutes que la réplication initiale se termine.
2. Sur n'importe quel DC (ex: `STG2-SRVW01`), ouvrir **Utilisateurs et ordinateurs Active Directory** et vérifier que les UO `VAUBAN` et `SOMME` ainsi que tous les utilisateurs sont présents.
3. Sur `STG-SRVW01`, ouvrir une invite de commande et exécuter :

    ```
    repadmin /showrepl
    ```

4. Vérifier que les réplications entrantes et sortantes avec les 3 autres DC sont "réussies" et sans erreur.

4.5 Difficultés Rencontrées et Résolution

1. Latence de Réplication Inter-Sites

- **Problème :** Après la promotion, les objets Active Directory (UO, Utilisateurs) n'apparaissaient pas immédiatement sur le nouveau contrôleur de domaine, et la commande `repadmin /showrepl` ne montrait pas les partenaires de réplication distants.
- **Analyse :** Ce comportement est nominal. La réplication Active Directory entre deux sites distincts (liens IPsec) obéit à une planification par défaut de 15 minutes, contrairement à la réplication intra-site qui est quasi-instantanée. De

plus, le processus KCC (*Knowledge Consistency Checker*) n'avait pas encore recalculé la topologie de réplication incluant le nouveau serveur.

- **Résolution :** Force du recalcul de la topologie et de la synchronisation pour valider le fonctionnement immédiat via les commandes :
    - `repadmin /kcc` (Recalcul de la topologie).
    - `repadmin /syncall /AdeP` (Synchronisation forcée de toutes les partitions).
    - **Validation :** La réplication est désormais fonctionnelle et bidirectionnelle entre les sites VAUBAN et SOMME.

.

5. Configuration du service DHCP et Basculement

5.1. Objectif (Révisé)

Objectif: Mettre en place un service DHCP centralisé et hautement disponible. Suite à la revue de projet, l'architecture a été modifiée pour adopter une Haute Disponibilité Intra-Site. Chaque site dispose d'un cluster DHCP autonome composé du serveur GUI (Principal) et du serveur CORE (Secondaire) en répartition de charge (Load Balancing 50/50). Cette configuration garantit que la distribution d'IP reste fonctionnelle localement même en cas de coupure du lien VPN inter-sites.

5.2. Installation du Rôle DHCP

1. Installer le rôle **Serveur DHCP** sur les **4 serveurs** (y compris les CORE `STG-SRVW02` et `STG2-SRVW02`).
    - Commande PowerShell pour les Core : `Install-WindowsFeature DHCP -IncludeManagementTools`
2. Sur chaque serveur, **Autoriser** le DHCP dans l'Active Directory.
    - Commande PowerShell : `Add-DhcpServerInDC -DnsName "NOM_DU_SERVEUR" -IPAddress IP_DU_SERVEUR`

5.3. Configuration Site A (Vauban)

Sur STG-SRVW01 (GUI) :

1. Ouvrir la console DHCP.
2. Créer l'étendue :
    - Nom : `LAN_SiteA_Vauban`
    - Plage : **192.168.100.100** à **192.168.100.200**
    - Masque : **255.255.255.0**
    - Options : Routeur `192.168.100.1`, DNS `192.168.100.10`, `192.168.100.11`.
3. Configurer le basculement (Failover) :
    - Clic droit sur l'étendue → **Configurer le basculement**.
    - Serveur partenaire : **`STG-SRVW02.IEF.LOCAL`** (Le Core du même site).
    - Mode : **Équilibrage de charge (50% / 50%)**.
    - Secret : `P@ssword10`.

5.4. Configuration Site B (Somme)

Sur STG2-SRVW01 (GUI) :

1. Ouvrir la console DHCP.

2. Créer l'étendue :
    - Nom : `LAN_SiteB_Somme`
    - Plage : **192.168.200.100** à **192.168.200.200**
    - Masque : **255.255.255.0**
    - Options : Routeur `192.168.200.1`, DNS `192.168.200.10`, `192.168.200.11`.
3. Configurer le basculement (Failover) :
    - Clic droit sur l'étendue → **Configurer le basculement**.
    - Serveur partenaire : **`STG2-SRVW02.IEF.LOCAL`** (Le Core du même site).
    - Mode : **Équilibrage de charge (50% / 50%)**.
    - Secret : `P@ssword10`.

5.5. Vérification Finale

Sur les serveurs CORE (`STG-SRVW02` et `STG2-SRVW02`), exécuter la commande :

PowerShell

```
Get-DhcpServerv4Failover
```

- Résultat attendu : `State : Normal`.

.

6. Résumé de la Configuration (LOT 2)

6.1. État des Contrôleurs de Domaine

Hôte	Site	Rôles	OS	État
STG-SRVW01	VAUBAN	DC Principal, DNS, DHCP, GC	GUI	✅ Opérationnel
STG-SRVW02	VAUBAN	DC Secondaire, DNS, GC	CORE	✅ Opérationnel
STG2-SRVW01	SOMME	DC Supplémentaire, DNS, DHCP (Failover), GC	GUI	✅ Opérationnel
STG2-SRVW02	SOMME	DC Supplémentaire, DNS, GC	CORE	✅ Opérationnel

6.2. Configuration DHCP (Site A)

Paramètre	Valeur
Étendue	192.168.100.100 - 192.168.100.200
Passerelle	192.168.100.1
Serveurs DNS	192.168.100.10, 192.168.100.11
Domaine	IEF.LOCAL
Basculement	Actif (Load Balance 50% vers STG2-SRVW01)

6.3. Configuration DHCP (Site B)

Paramètre	Valeur

Paramètre	Valeur
Étendue	192.168.200.100 - 192.168.200.200
Passerelle	192.168.200.1
Serveurs DNS	192.168.200.10, 192.168.200.11
Domaine	IEF.LOCAL
Basculement	Actif (Load Balance 50% vers STG2-SRVW01)

6.4. Revue Critique de l'Architecture et Corrections (Feedback Oral 1)

Suite à la présentation intermédiaire et aux tests de charge, deux erreurs de conception majeures ont été identifiées dans la configuration initiale. Ces points bloquants ont nécessité une refonte partielle de l'architecture pour garantir la conformité avec les bonnes pratiques Microsoft et la résilience du réseau.

1. Configuration DNS des Contrôleurs de Domaine (Loopback)

- Erreur Initiale :

  La configuration DNS des cartes réseaux des serveurs STG-SRVW01 et STG2-SRVW01 pointait vers l'adresse de bouclage 127.0.0.1 en tant que DNS préféré.

- Impact Technique (Point Bloquant) :

  Bien que fonctionnelle pour des tests isolés, cette configuration posait des problèmes critiques lors du démarrage des services et de la réplication Active Directory. Le service Netlogon tentait de s'enregistrer avant que la zone DNS locale ne soit complètement chargée, créant des "îlots" de réplication et des erreurs dans les journaux d'événements. De plus, cela complexifiait la résolution de nom lors des communications initiales via le VPN.

- Correction Appliquée :

  Nous avons remplacé l'adresse 127.0.0.1 par l'adresse IP LAN statique réelle du serveur (ex: 192.168.100.10 pour le Site A).

  - **DNS Préféré :** Adresse IP réelle du serveur lui-même.
  - DNS Auxiliaire : Adresse IP du second contrôleur de domaine (pour la redondance).

    Cette modification a stabilisé la réplication et supprimé les avertissements DNS au démarrage.

2. Architecture du Basculement DHCP (Failover)

- Erreur Initiale :

  L'architecture initiale prévoyait un basculement DHCP Inter-Sites (le serveur du Site A secourait le Site B, et inversement) à travers le tunnel VPN IPsec.

- Impact Technique (Point Bloquant) :

  Cette conception créait une dépendance forte et dangereuse au lien WAN (VPN).

    - En cas de coupure du VPN (panne routeur ou internet), les requêtes DHCP de secours ne pouvaient pas traverser le réseau (le broadcast DHCP ne passe pas les routeurs sans relais complexe).
    - Le Site B risquait de se retrouver sans distribution d'IP, paralysant l'activité locale alors que les serveurs locaux étaient pourtant allumés.
- Correction Appliquée :

  Nous avons migré vers une architecture de Haute Disponibilité Intra-Site (Locale).

    - **Action :** Installation du rôle DHCP sur les serveurs **CORE** (`STG-SRVW02` et `STG2-SRVW02`), ce qui n'était pas prévu initialement.
    - **Résultat :** Le basculement se fait désormais entre le serveur GUI et le serveur CORE **du même site**.
    - **Bénéfice :** Chaque site est désormais **totalement autonome**. Même en cas de coupure totale d'Internet ou du VPN, les clients de Strasbourg Somme continuent de recevoir des IP grâce à leur cluster DHCP local.

.

7. Évolutions prévues pour le LOT 3

7.1. Objectif

Objectif: Le LOT 3 se concentrera sur le déploiement des services de fichiers et de sauvegarde, s'appuyant sur l'infrastructure AD et réseau des LOT 1 et 2. Les prochaines étapes incluront l'installation des serveurs **TrueNAS Core** (`STG-SAN01` et `STG2-SAN01`), la configuration des **cibles iSCSI**, et le montage de ces cibles sur les serveurs Windows. Par la suite, nous déploierons le **DFS (Système de fichiers distribués)** avec l'espace de noms `\\IEF.LOCAL\INTRANET` et la **réplication DFSR en maille pleine** entre les 4 serveurs. Enfin, nous configurerons la **sauvegarde** et les **clichés instantanés (Shadow Copy)**.

7.2. Checklist de validation LOT 2

- [✓] 4 serveurs Windows Server 2022 installés (2 GUI, 2 CORE)
- [✓] Adressage IP statique configuré (DNS pointant sur contrôleurs locaux)
- [✓] Forêt `IEF.LOCAL` créée et fonctionnelle
- [✓] Sites AD (VAUBAN, SOMME) configurés et réplication validée
- [✓] Objets AD (UO, Utilisateurs, Groupes) créés selon l'Annexe 2
- [✓] Rôles DHCP installés sur les 4 serveurs (GUI + Core)
- [✓] Étendues DHCP créées et configurées en Failover Intra-Site (Load Balance)
- [✓] Résolution des incidents majeurs (VM Site B, VPN) documentée

.

FIN DU LOT 2

⬅ LOT précédent | Menu Livrable 2 | ➡ LOT suivant

LOT 3 - Configuration du Stockage (SAN/NAS) et Système de Fichiers Distribués (DFS)

⬅ Retour au Menu Livrable 2 | Retour à l'accueil

La Haute Disponibilité : Stockage SAN et Ubiquité des Données

La donnée est le patrimoine le plus précieux de l'école. Ce lot répond à l'exigence critique de disponibilité et de protection de l'information. Nous avons mis en œuvre une stratégie de stockage hybride combinant la puissance du **SAN iSCSI sous TrueNAS Core** pour des sauvegardes immuables, et la flexibilité du **DFS (Système de fichiers distribué)** pour les utilisateurs. Grâce à une réplication en maille pleine (Full Mesh), les fichiers suivent l'utilisateur quel que soit son site de connexion, tandis que les mécanismes de **clichés instantanés** et de sauvegarde externalisée assurent une résilience maximale face aux incidents et aux erreurs humaines.

.

0. Plan d'Adressage et de Stockage (LOT 3)

Ce tableau récapitule la configuration du stockage pour les deux sites. Nous distinguons les disques locaux (pour les données chaudes) des volumes iSCSI (pour les sauvegardes).

Site	Serveur Hôte	Interface SAN (iSCSI)	Disque Données (Local)	Disque Sauvegarde (iSCSI)	Rôle du Volume
Site A	STG-SAN01 (TrueNAS)	172.16.10.20	-	Stockage ZFS	Cible iSCSI "Backup01"
Site A	STG-SRVW01	172.16.10.10	**E:** (DATAS01)	**F:** (Backup01)	Production & Backup
Site A	STG-SRVW02	172.16.10.11	**E:** (DATAS02)	-	Production (Réplica)
Site B	STG2-SAN01 (TrueNAS)	172.16.20.20	-	Stockage ZFS	Cible iSCSI "Backup02"
Site B	STG2-SRVW01	172.16.20.10	**E:** (DATAS03)	**F:** (Backup02)	Production & Backup
Site B	STG2-SRVW02	172.16.20.11	**E:** (DATAS04)	-	Production (Réplica)

.

1. Mise en œuvre du SAN (TrueNAS Core)

1.1. Objectif Stratégique

Objectif : Déployer et configurer les serveurs de stockage TrueNAS Core (STG-SAN01 et STG2-SAN01) sur le réseau dédié SAN (VLAN isolé configuré au LOT 1). L'objectif est de fournir un espace de stockage block (iSCSI) sécurisé pour héberger les sauvegardes complètes des serveurs Windows, garantissant ainsi l'intégrité des données via le système de fichiers ZFS et la séparation physique des flux de production et de sauvegarde.

1.2. Configuration Réseau TrueNAS (Console)

Sur les VM `STG-SAN01` et `STG2-SAN01` :

1. Au menu principal de la console, choisir **1) Configure Network Interfaces**.
2. Utilisez les flèches pour descendre sur **`ipv4_dhcp`**.
3. Appuyez sur **Entrée** ou **Espace** pour changer la valeur de `Yes` à **`No`**.
4. Faites de même pour **`ipv6_auto`** : passez-le à **`No`**.
5. Dans alias rentrer :
    - Pour **Site A** : IP `172.16.10.20`, Masque `/24`.
    - Pour **Site B** : IP `172.16.20.20`, Masque `/24`.

1.3. Configuration du Service iSCSI (Interface Web)

Accéder à l'interface web (ex: `http://172.16.10.20`) depuis un serveur Windows ou un client.

Étapes à reproduire sur les deux sites :

1. **Configuration de TrueNAS :**
    - System > Localization > Settings
    - Console Keyboard Map : French (AZERTY)
    - Timezone : Europe/Paris
2. **Configuration réseau TrueNas :**
    - Network > Global Configuration > Settings
    - Hostname : STG-SAN01 pour le site A et STG2-SAN01 pour le site B
    - Domain : ief.local
    - Namerserver 1 : 192.168.100.10 pour le site A et 192.168.200.10 pour le site B
    - Namerserver 2 : 192.168.100.11 pour le site A et 192.168.200.11 pour le site B
    - IPV4 Default Gateway : 172.16.10.1 pour le site A et 172.16.20.1 pour le site B
3. **Création du Pool ZFS :**
    - *Storage* > *Pools* > *Add*.
    - Créer un pool nommé `TankBackup`. Sélectionner le disque de 20Go disponible.
    - Cliquer sur Créer.
4. **Création du Zvol (Disque virtuel) :**
    - *Storage* > *Pools* > *TankBackup* > *3 points* > *Add Zvol*.
    - Nom : `zvol_backup`.
    - Taille : `75 GiB` (Laisser une marge de sécurité).
    - Compression : `LZ4` (Recommandé).
5. **Configuration iSCSI (Shares > Block Shares (iSCSI)) :**
    - **Portals** : Ajouter un portail. IP : `0.0.0.0` (ou l'IP SAN spécifique). Port : `3260`.
    - **Initiators** : Ajouter. Autoriser tous les initiateurs (`ALL` / `ALL`) pour faciliter la connexion dans le VLAN sécurisé, ou restreindre aux IP `172.16.xx.10/11`.

- **Targets** : Ajouter. Nom : `iqn.2025-10.local.ief:backup01` (Adaptez pour site B : `backup02`). Mode : `None` (Pas d'auth CHAP pour l'instant, ou configurer selon Annexe 1 optionnelle).
- **Extents** : Ajouter. Nom : `extent_backup`. Type : `Device`. Device : `zvol_backup`.
- **Associated Targets** : Lier la Target à l'Extent créée.

6. **Démarrage du service :**
   - *Système* > *Servcices*.
   - Activer **iSCSI**. Cocher **Start Automatically**.

.

2. Préparation du Stockage sur Windows Server

2.1. Objectif

Objectif : Initialiser les volumes de données sur les quatre serveurs Windows. Nous devons configurer deux types de disques : le disque dur virtuel local de 60 Go qui hébergera les données utilisateurs (DATASxx) et le disque iSCSI distant provenant du SAN qui recevra les sauvegardes (Backupxx).

2.2. Initialisation du Disque de Données (Local)

Sur les 4 serveurs (GUI et Core) :

1. Ouvrir le **Gestionnaire de disque** (`diskmgmt.msc`) sur GUI ou utiliser `diskpart` sur Core.
2. Mettre le Disque 1 (60 Go) en ligne et l'initialiser (GPT).
3. Créer un nouveau volume simple :
   - Lettre de lecteur : **E:**
   - Nom de volume : **DATAS01** (Adapter : `DATAS02`, `DATAS03`, `DATAS04`).
   - Système de fichiers : **NTFS**.
4. Créer le dossier racine : `E:\DATAS01` (et respectivement pour les autres serveurs).

2.3. Connexion de l'Initiateur iSCSI (Sauvegarde)

Uniquement sur STG-SRVW01 (Site A) et STG2-SRVW01 (Site B) :

1. Ouvrir l'outil **Initiateur iSCSI**. Accepter le démarrage du service.
2. Onglet **Cibles** :
   - Entrer l'IP du SAN local (ex: `172.16.10.20` pour Site A).
   - Cliquer sur **Connexion Rapide**.
   - Statut doit passer à "Connecté".
3. Onglet **Volumes et périphériques** :
   - Cliquer sur **Configuration automatique**.
4. Retourner dans `diskmgmt.msc` :
   - Un nouveau disque de 75 Go apparaît.
   - Initialiser, créer un volume simple.
   - Lettre : **F:**
   - Nom : **Backup_iSCSI**.

.

3. Déploiement DFS et DFSR (Système de Fichiers Distribués)

3.1. Objectif

Objectif : Mettre en place un Espace de Noms unifié (\IEF.LOCAL) permettant aux utilisateurs d'accéder à leurs fichiers de manière transparente, quel que soit leur site géographique. La réplication DFSR en maille pleine (Full Mesh) entre les 4 serveurs garantira que toute modification de fichier sur un site soit répliquée quasi-instantanément sur les trois autres serveurs, assurant ainsi la haute disponibilité des données (Objectif n°4 du CdC).

3.2. Installation des Rôles

Sur les **4 serveurs**, installer le rôle **Serveur de fichiers** incluant :

- **Espace de noms DFS**
- **Réplication DFS**

Powershell (pour les Core et GUI) :

```
Install-WindowsFeature -Name FS-DFS-Namespace, FS-DFS-Replication -IncludeManagementTools
```

3.3. Configuration de l'Espace de Noms (Namespace)

Sur STG-SRVW01 (GUI) :

1. Ouvrir la console **Gestion du système de fichiers distribués**.
2. Clic droit sur *Espaces de noms* > **Nouvel espace de noms**.
3. Serveur : `STG-SRVW01`.
4. Nom : **INTRANET**.
5. Type : **Espace de noms de domaine** (Mode 2008 R2 activé).
6. Valider. Le chemin d'accès est désormais : `\\IEF.LOCAL\INTRANET`.

Redondance de l'Espace de Noms :

1. Clic droit sur le namespace créé > **Ajouter un serveur d'espace de noms**.
2. Ajouter `STG-SRVW02`, `STG2-SRVW01` et `STG2-SRVW02`.
    - *Résultat : Si le serveur 01 tombe, l'accès au chemin réseau reste fonctionnel.*

3.4. Création du Groupe de Réplication (DFSR)

1. Dans la console DFS, clic droit sur *Réplication* > **Nouveau groupe de réplication**.
2. Type : **Groupe de réplication polyvalent**.
3. Nom : `RG_DATA_IEF`.
4. Membres : Ajouter les **4 serveurs** (`STG-SRVW01`, `02`, `STG2-SRVW01`, `02`).
5. Topologie : **Maille pleine** (Full Mesh).
    - *Note : Cela garantit que chaque serveur parle à tous les autres.*
6. Planification : **Bande passante complète** (ou limitée selon besoins VPN, mais complète pour le test).
7. Membre principal : `STG-SRVW01`.
8. Dossiers à répliquer :
    - Ajouter. Chemin local : `E:\DATAS01`.

    - Nom du dossier répliqué : **Partage_General**.
9. Modifier les chemins locaux pour les autres membres :
    - STG-SRVW02 : `E:\DATAS02`.
    - STG2-SRVW01 : `E:\DATAS03`.
    - STG2-SRVW02 : `E:\DATAS04`.
10. Valider la création.

3.5. Publication dans l'Espace de Noms

1. Une fois la réplication créée, l'assistant propose de publier le dossier.
2. Publier le dossier répliqué dans l'espace de noms :
    - Dossier parent : `\\IEF.LOCAL\INTRANET`.
    - Nom du dossier : **Documents**.
3. Vérification : Accéder à `\\IEF.LOCAL\INTRANET\Documents`. Créer un fichier texte. Vérifier qu'il apparaît sur le disque `E:` des 4 serveurs.

.

4. Organisation et Permissions (Conformité Annexe 2)

4.1. Structure des Dossiers

Dans le dossier répliqué (`E:\DATAS01`), créer l'arborescence suivante :

- `GRP1`
- `GRP2`
- `TRANSFERT`
- `Users` (Pour la redirection des dossiers personnels)

4.2. Application des Permissions NTFS et Partage

Il est recommandé de gérer les droits via **NTFS** et de laisser le **Partage** en "Tout le monde : Contrôle Total" (Microsoft Best Practice).

1. **Dossier TRANSFERT** :
    - Clic droit > Propriétés > Sécurité.
    - Ajouter le groupe `Utilisateurs du domaine`.
    - Droit : **Modification** (Lecture/Écriture).
2. **Dossier GRP1** :
    - Désactiver l'héritage (Convertir en droits explicites).
    - Supprimer `Utilisateurs du domaine`.
    - Ajouter le groupe **GRP1** (créé au LOT 2).
    - Droit : **Modification**.
3. **Dossier GRP2** :
    - Idem que GRP1 mais avec le groupe **GRP2**.
4. **Dossier Users** :
    - Permissions spéciales pour permettre la création automatique des dossiers personnels (Créateur Propriétaire : Contrôle Total, etc.).

.

5. Sauvegardes et Protection des Données

5.1. Objectif

Objectif : Assurer la résilience des données face aux erreurs humaines (suppression accidentelle) via les Clichés Instantanés, et face aux pannes matérielles majeures via une sauvegarde complète quotidienne sur le support iSCSI externe, conformément aux exigences de sécurité.

5.2. Configuration des Clichés Instantanés (Shadow Copies)

Sur STG-SRVW01 et STG2-SRVW01 :

1. Ouvrir l'Explorateur de fichiers > **Ce PC**.
2. Clic droit sur le disque **E: (DATAS01)** > **Configurer les clichés instantanés**.
3. Sélectionner le volume **E:**.
4. Cliquer sur **Activer**.
5. Dans **Paramètres**, configurer la planification (ex: 07:00 et 12:00) et la limite de stockage (utiliser le disque F: iSCSI si souhaité, ou rester sur E: selon espace dispo).
    - *Note Annexe 1 : "Possibilité de déplacer les clichés sur la cible iSCSI". Pour le faire, dans Paramètres, changer le "Volume de stockage" vers F:.*

5.3. Sauvegarde Windows Server Backup

Sur STG-SRVW01 (Site A) :

1. Installer la fonctionnalité **Sauvegarde Windows Server**.
2. Ouvrir la console **Sauvegarde Windows Server**.
3. Dans le volet Actions, cliquer sur **Planification de sauvegarde**.
4. Type de configuration : **Personnalisée**.
5. Éléments à sauvegarder : Ajouter **État du système** et le volume **E: (DATAS01)**.
6. Heure : **21:00** (Quotidien).
7. Type de destination : **Sauvegarder sur un volume**.
    - *Attention : Ne pas choisir 'Disque entier' pour conserver la lettre de lecteur F: nécessaire aux clichés instantanés.*
8. Sélectionner le volume **F: (Backup_iSCSI)**.
9. Valider la planification.

Répéter l'opération sur STG2-SRVW01 pour le Site B.

.

6. ⚠ Difficultés Rencontrées et Résolutions Techniques

Contexte de l'incident : Lors de la mise en place de la réplication de fichiers (DFSR) et du stockage iSCSI, nous avons rencontré plusieurs blocages techniques nécessitant une analyse approfondie. Ces incidents ont touché à la fois la couche réseau (communication inter-sites) et la couche stockage (dimensionnement et configuration SAN).

Analyse technique des causes racines (Root Cause Analysis) :

Instabilité du Profil Réseau (NLA Service) :

- **Symptôme :** Les serveurs basculaient en profil réseau “Privé” ou “Public” au lieu de “Domaine” après redémarrage.
- **Conséquence :** Le Pare-feu Windows appliquait des règles strictes bloquant les ports dynamiques RPC et le port DFSR (5722), empêchant l’établissement du canal de réplication initial.
- **Résolution :** Redémarrage forcé des cartes réseaux (`Restart-NetAdapter`) pour forcer la redétection du contrôleur de domaine et basculer le profil en “DomainAuthenticated”.

Conflit de Résolution IPv6 sur Tunnel IPv4 :

- **Symptôme :** Les serveurs tentaient de résoudre les noms DNS de leurs partenaires via leurs adresses locales IPv6.
- **Conséquence :** Le tunnel VPN IPsec étant configuré en IPv4 uniquement, les connexions échouaient silencieusement (Timeout), provoquant des erreurs de “Serveur indisponible”.
- **Résolution :** Désactivation complète de la pile IPv6 via le Registre et nettoyage du cache DNS (`ipconfig /flushdns`) pour forcer l’usage exclusif de l’IPv4 à travers le VPN.

Latence de Convergence Active Directory :

- **Symptôme :** La configuration DFS créée sur le Site A n’était pas connue du Site B, entraînant un rejet des demandes de réplication.
- **Conséquence :** Les mises à jour DFS (`dfsrdiag pollad`) étaient inefficaces car le serveur local interrogeait un AD local non synchronisé.
- **Résolution :** Utilisation de la commande `repadmin /syncall /AdeP` pour forcer la synchronisation immédiate de l’annuaire entre les sites, débloquant instantanément la configuration DFS.

Erreur de dimensionnement du volume iSCSI (MiB vs GiB) :

- **Symptôme :** Lors de la connexion initiale de la cible iSCSI sur le serveur Windows, le volume de sauvegarde (F:) affichait une capacité critique de 75 Mo au lieu des 75 Go prévus.
- **Conséquence :** Une confusion d’unité lors de la création du Zvol sur TrueNAS (sélection de MiB au lieu de GiB) a rendu le support inexploitable pour les sauvegardes.
- **Résolution :** Correction effectuée à chaud (*Hot Resize*) sans interruption de service : modification de la volumétrie sur TrueNAS à 75 GiB, suivie d’une actualisation des disques (*Rescan*) et d’une extension du volume directement depuis la console de gestion des disques Windows.

Limitations de l’Assistant Automatique TrueNAS (Wizard) :

- **Symptôme :** L’assistant de configuration iSCSI masquait les onglets de configuration avancée, empêchant le paramétrage fin des cibles et des permissions.
- **Conséquence :** Risque de configuration “boîte noire” non conforme et difficultés de diagnostic en cas d’échec de connexion.
- **Résolution :** Abandon de l’assistant au profit d’une configuration manuelle séquentielle : configuration explicite des *Portals*, *Initiators*, *Targets* et *Extents* via les onglets dédiés pour garantir une configuration maîtrisée et documentée.

Conclusion et Validation : Après avoir assaini la couche réseau et corrigé la configuration du stockage, l'infrastructure est pleinement opérationnelle. La réplication DFSR est stable (Event ID 4104/4102) et les volumes de sauvegarde iSCSI sont correctement dimensionnés et connectés, permettant l'exécution des plans de sauvegarde.

.

7. Checklist de validation LOT 3

- ☐ Serveurs TrueNAS (Site A et B) installés et configurés (IP SAN).
- ☐ Volumes iSCSI créés sur TrueNAS (Portals, Targets, Extents).
- ☐ Initiateur iSCSI connecté sur les serveurs Windows Principaux.
- ☐ Disques de données (E:) et de sauvegarde (F:) formatés et accessibles.
- ☐ Rôles DFS et DFSR installés sur les 4 serveurs.
- ☐ Espace de noms `\\IEF.LOCAL\INTRANET` accessible depuis les 2 sites.
- ☐ Réplication DFSR en maille pleine fonctionnelle (Test fichier texte).
- ☐ Arborescence (GRP1, GRP2, TRANSFERT) créée et permissions NTFS appliquées.
- ☐ Clichés instantanés activés sur les volumes de données.
- ☐ Tâche planifiée de sauvegarde Windows configurée vers la cible iSCSI.
- ☐ **Test de redondance :** Coupure d'un serveur et vérification de l'accès aux données.

.

FIN DU LOT 3

⬅ LOT précédent | Menu Livrable 2 | ➡ LOT suivant

LOT 4 - Sécurisation, Stratégies de Groupe (GPO) et Pare-feu

⬅ Retour au Menu Livrable 2 | Retour à l'accueil

La Forteresse Numérique : Sécurisation et Conformité

> Ultime étape du projet, ce lot verrouille l'infrastructure et définit les règles de vie numérique. Nous passons d'une configuration fonctionnelle à une configuration sécurisée (Hardening) en appliquant une politique de moindre privilège. Via des **Stratégies de Groupe (GPO)** strictes, nous déployons un environnement utilisateur standardisé et protégé contre les mauvaises manipulations (blocage USB, restrictions système). En parallèle, le filtrage réseau est durci sur les pare-feu pfSense pour ne laisser passer que les flux légitimes, garantissant ainsi la conformité aux exigences de l'ANSSI et la protection des actifs critiques de l'ECP.

.

.

1. Structure Active Directory et Préparation (Rappel LOT 2)

Avant d'appliquer les GPO, nous validons que la structure créée au LOT 2 est conforme pour recevoir les politiques.

Sur STG-SRVW01 (Site A) :

1. **Unités d'Organisation (UO)** :
   - `IEF.LOCAL` (Racine)
     - `VAUBAN` (Contient : Paul, Pierre, GRP1, Ordinateurs du site A)
     - `SOMME` (Contient : Isabelle, Nathalie, GRP2, Ordinateurs du site B)
     - `ADMINS` ou `Users` (Contient : Compte de secours ADMIN - **Hors des UO Vauban/Somme pour éviter les restrictions**)
2. **Dossier NETLOGON** :
   - Déposer l'image `wallpaper_ief.jpg` dans `\\IEF.LOCAL\NETLOGON\`.
   - *Justification :* Ce dossier est automatiquement répliqué sur tous les contrôleurs de domaine (Site A et B), garantissant la disponibilité de l'image partout.

.

2. Stratégie de Mots de Passe (Default Domain Policy)

Contexte : Cette stratégie s'applique à **tous** les comptes du domaine sans exception.

Configuration sur la "Default Domain Policy" :

Chemin : Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes

Paramètre	Valeur	Justification Annexe 2
Longueur minimale	**12 caractères**	"12 caractères minimum"
Complexité	**Activé**	"1 chiffre, 1 spécial, 1 majuscule"
Verrouillage compte	**3 tentatives**	"3 tentatives erronées"

Paramètre	Valeur	Justification Annexe 2
Durée verrouillage	**30 minutes**	“Pendant 30 minutes”
Historique	5 mots de passe	Empêcher la réutilisation

2.1. : Accéder à la console de gestion

1. Connectez-vous sur **STG-SRVW01** en tant qu’Administrateur.
2. Appuyez sur les touches `Windows + R` de votre clavier.
3. Tapez **`gpmc.msc`** et appuyez sur **Entrée**.
    - *(Ou cherchez “Gestion de stratégie de groupe” dans le menu Démarrer).*

2.2. : Trouver la “Default Domain Policy”

1. Dans la colonne de gauche, déployez l’arborescence en cliquant sur les petites flèches > :
    - **Forêt : IEF.LOCAL**
    - **Domaines**
    - **ief.local**
2. Vous verrez une GPO nommée **Default Domain Policy** (souvent avec une petite icône de parchemin).
3. Faites un **Clic droit** dessus et choisissez **Modifier…**.
    - *Une nouvelle fenêtre “Éditeur de gestion des stratégies de groupe” s’ouvre.*

2.3. : Naviguer vers les Stratégies de Comptes

Dans la fenêtre d’édition, suivez ce chemin précis dans le volet de gauche :

1. **Configuration ordinateur**
2. **Stratégies**
3. **Paramètres Windows**
4. **Paramètres de sécurité**
5. **Stratégies de comptes**

Ici, vous verrez deux sous-dossiers qui nous intéressent :

- `Stratégie de mot de passe`
- `Stratégie de verrouillage du compte`

.

2.4. : Configurer les Mots de Passe

Cliquez sur le dossier **Stratégie de mot de passe**. Dans le volet de droite, double-cliquez sur chaque ligne pour la modifier :

1. **Conserver l’historique des mots de passe**
    - Double-cliquez.
    - Cochez “Définir ce paramètre…”.
    - Mettez : **5** mots de passe mémorisés.
    - *OK*.
2. **Le mot de passe doit respecter des exigences de complexité**
    - Double-cliquez.
    - Cochez : **Activé**.

- *OK*.

3. **Longueur minimale du mot de passe**
   - Double-cliquez.
   - Mettez : **12** caractères.
   - *OK*.

(Les autres paramètres comme “Durée de vie maximale” peuvent rester par défaut, souvent 42 jours).

.

2.5. : Configurer le Verrouillage (Anti-Bruteforce)

Revenez dans le volet de gauche et cliquez sur le dossier juste en dessous : **Stratégie de verrouillage du compte**.

1. **Seuil de verrouillage du compte**
   - Double-cliquez.
   - Mettez : **3** tentatives d’ouverture de session non valides.
   - Cliquez sur *OK*.
   - *Windows va ouvrir une fenêtre “Valeurs suggérées” pour les deux autres paramètres (30 minutes).*
   - Cliquez sur **OK** pour accepter la suggestion automatique.
2. **Vérification des valeurs**
   - Vérifiez simplement que les trois lignes affichent bien les valeurs demandées :
     - Durée de verrouillage des comptes : **30 minutes**.
     - Réinitialiser le compteur… après : **30 minutes**.
     - Seuil de verrouillage : **3 tentatives**.

.

2.6. : Valider et Tester

Fermez toutes les fenêtres pour revenir sur le bureau.

1. Ouvrez une invite de commande (Clic droit sur Démarrer > **Windows PowerShell** ou **CMD**).

2. Forcez la mise à jour immédiate pour ne pas attendre :

   ```
   gpupdate /force
   ```

3. Vérifiez que le serveur a bien pris en compte vos réglages en tapant :DOS

   ```
   net accounts
   ```

   - Regardez les lignes :
     - *Longueur minimale : 12*
     - *Seuil de verrouillage : 3*

C’est terminé ! La politique est active pour tout le monde.

.

3. GPO : Environnement Utilisateur (Profils)

3.1 : Préparation du fond d'écran

Avant de configurer la GPO, l'image doit être accessible.

1. Sur le serveur, copiez votre image `wallpaper_ief.jpg`.
2. Ouvrez l'Explorateur de fichiers et dans la barre d'adresse, tapez : `\\IEF.LOCAL\NETLOGON`.
3. **Collez** l'image dans ce dossier.
    - *Pourquoi ?* Ce dossier est automatiquement synchronisé sur tous les contrôleurs de domaine. L'image sera disponible partout.

.

3.2 : Création et Liaison de la GPO

1. Ouvrez **Gestion de stratégie de groupe** (`gpmc.msc`).
2. Dans la colonne de gauche, faites un **Clic droit** sur l'UO **VAUBAN**.
3. Choisissez **"Créer un objet GPO dans ce domaine, et le lier ici…"**.
4. Nom : **`GPO_Environnement_Utilisateur`**.
5. Cliquez sur **OK**.
6. Maintenant, faites un **Clic droit** sur l'UO **SOMME**.
7. Choisissez **"Lier un objet de stratégie de groupe existant…"**.
8. Sélectionnez votre `GPO_Environnement_Utilisateur` et validez.
    - *La GPO est maintenant active pour les deux sites.*

.

3.3 : Configurer les Lecteurs Réseaux (U: et T:)

1. Faites un **Clic droit** sur la GPO `GPO_Environnement_Utilisateur` (dans le volet gauche) > **Modifier…**.
2. Allez dans : **Configuration utilisateur** > **Préférences** > **Paramètres Windows** > **Mappages de lecteurs**.

A. Le Lecteur Personnel (U:)

1. Dans la zone blanche à droite, **Clic droit** > **Nouveau** > **Lecteur mappé**.
2. **Action** : Choisissez **Mettre à jour** (Update).
3. **Emplacement** : Tapez `\\IEF.LOCAL\INTRANET\Users\%USERNAME%`
    - *(Attention à bien écrire `%USERNAME%` avec les pourcentages).*
4. **Reconnecter** : Cochez la case.
5. **Libellé** : Écrivez `Espace Personnel`.
6. **Lettre de lecteur** : Choisissez **U:**.
7. Cliquez sur **OK**.

B. Le Lecteur Transfert (T:)

1. **Clic droit** > **Nouveau** > **Lecteur mappé**.
2. **Action** : Choisissez **Mettre à jour**.
3. **Emplacement** : Tapez `\\IEF.LOCAL\INTRANET\TRANSFERT`
4. **Reconnecter** : Cochez la case.
5. **Libellé** : Écrivez `Espace Transfert`.
6. **Lettre de lecteur** : Choisissez **T:**.

7. Cliquez sur **OK**.

.

3.4. : Redirection des Dossiers (Sauvegarde auto)

1. Dans la même fenêtre, remontez vers : **Configuration utilisateur** > **Stratégies** > **Paramètres Windows** > **Redirection de dossiers**.

A. Dossier Documents

1. Faites un **Clic droit** sur **Documents** > **Propriétés**.
2. **Paramètre** : Choisissez **De base - Rediriger les dossiers de tout le monde vers le même emplacement**.
3. **Emplacement du dossier cible** : Vérifiez que c'est bien "Créer un dossier pour chaque utilisateur sous le chemin d'accès racine".
4. **Chemin d'accès racine** : Tapez `\\IEF.LOCAL\INTRANET\Users`
   - ⚠ *Attention : Ne mettez PAS `%username%` ici ! Windows l'ajoute tout seul.*
5. Allez dans l'onglet **Paramètres** (en haut).
   - Décochez "Accorder à l'utilisateur des droits exclusifs…" si vous (Admin) voulez pouvoir entrer dedans pour dépanner. Sinon, laissez coché.
6. Cliquez sur **OK**. (Dites Oui à l'avertissement de compatibilité).

B. Dossier Bureau

1. Faites un **Clic droit** sur **Bureau** > **Propriétés**.
2. Refaites exactement la même chose que pour Documents.
   - Paramètre : De base.
   - Chemin racine : `\\IEF.LOCAL\INTRANET\Users`
3. Cliquez sur **OK**.

.

3.5. : Fond d'écran Unifié et Verrouillé

1. Allez dans : **Configuration utilisateur** > **Stratégies** > **Modèles d'administration** > **Bureau** > **Bureau**.

A. Mettre l'image

1. Dans la liste de droite, double-cliquez sur **Papier peint du Bureau**.
2. Cochez **Activé**.
3. **Nom du papier peint** : Tapez `\\IEF.LOCAL\NETLOGON\wallpaper_ief.jpg`
4. **Style** : Choisissez **Remplir**.
5. Cliquez sur **OK**.

B. Interdire le changement

1. Allez dans : **Configuration utilisateur** > **Stratégies** > **Modèles d'administration** > **Panneau de configuration** > **Personnalisation**.
2. Double-cliquez sur **Empêcher la modification du papier peint**.
3. Cochez **Activé**.
4. Cliquez sur **OK**.

.

3.6. : Validation

1. Fermez l'éditeur de GPO.
2. Sur un **poste client** (Windows 10/11), connectez-vous avec **Paul** ou **Isabelle**.
3. Ouvrez une invite de commande (`cmd`) et tapez `gpupdate /force`.
4. Fermez la session et rouvrez-la.
5. **Vérifiez :**
    - Le fond d'écran est-il là ?
    - Dans "Ce PC", voyez-vous les lecteurs **U:** et **T:** ?
    - Créez un fichier sur le Bureau. Allez voir sur le serveur dans `E:\DATAS01\Users\Paul\Desktop`. Le fichier est-il là ? (Si oui, la redirection marche !).

.

4. GPO : Restrictions de Sécurité (Kiosk Mode)

⚠ **ATTENTION :** C'est la GPO la plus critique. Si vous vous trompez dans le filtrage (Étape 2), vous risquez de bloquer l'administrateur. Suivez bien les instructions.

4.1. : Création et Liaison de la GPO

1. Ouvrez **Gestion de stratégie de groupe** (`gpmc.msc`).
2. Faites un **Clic droit** sur l'UO **VAUBAN**.
3. Choisissez **"Créer un objet GPO dans ce domaine, et le lier ici…"**.
4. Nom : **`GPO_Restrictions_Securite`**.
5. Cliquez sur **OK**.
6. Faites ensuite un **Clic droit** sur l'UO **SOMME** > **"Lier un objet de stratégie de groupe existant…"**.
7. Sélectionnez la `GPO_Restrictions_Securite` pour qu'elle s'applique aussi au deuxième site.

4.2 : Sécurité Critique (Le Filtrage)

C'est ici qu'on s'assure que l'Admin ne se fait pas bloquer.

1. Dans la colonne de gauche, cliquez **une seule fois** sur `GPO_Restrictions_Securite` (ne l'ouvrez pas encore).
2. Regardez dans le volet de droite, l'onglet **Étendue** (Scope).
3. En bas, dans la section **"Filtrage de sécurité"** :
    - Vous voyez "Utilisateurs authentifiés" ? **Sélectionnez-le et cliquez sur SUPPRIMER.**
    - *Pourquoi ?* Parce que ce groupe inclut tout le monde, y compris l'Admin.
4. Cliquez sur **Ajouter…**.
5. Tapez : `GRP1` > Vérifier > OK.
6. Cliquez encore sur **Ajouter…**.
7. Tapez : `GRP2` > Vérifier > OK.
    - *Résultat : Seuls Paul, Pierre, Isabelle et Nathalie seront bloqués. L'Admin reste libre.*

Pour garantir que la GPO est bien détectée par Windows sans être appliquée à tout le monde :

1. Cliquez sur l'onglet **Délégation** (juste à côté de Étendue).

2. Cliquez sur le bouton **Avancé** (en bas à droite).
3. Cliquez sur **Ajouter…**.
4. Tapez : `Utilisateurs authentifiés` > OK.
5. Dans la liste des permissions pour ce groupe, cochez **uniquement** la case **Lire** (Read).
    - ⚠ **Vérification cruciale :** Assurez-vous que la case **"Appliquer la stratégie de groupe"** est bien **DÉCOCHÉE**.
6. Validez par **OK**.

4.3. : Bloquer le Système (Panneau config, CMD)

Faites un Clic droit sur la GPO > Modifier….

Allez dans : Configuration utilisateur > Stratégies > Modèles d'administration.

A. Panneau de Configuration

1. Cliquez sur le dossier **Panneau de configuration**.
2. À droite, double-cliquez sur **"Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC"**.
3. Cochez **Activé**.
4. **OK**.

B. Invite de commande (CMD)

1. Cliquez sur le dossier **Système**.
2. À droite, double-cliquez sur **"Empêcher l'accès à l'invite de commandes"**.
3. Cochez **Activé**.
4. ⚠ **Important :** Dans la liste déroulante "Désactiver également le traitement des scripts…", choisissez **NON**.
    - *Pourquoi ?* Si vous mettez Oui, les scripts de connexion (logon scripts) ne marcheront plus.
5. **OK**.

C. Bloquer PowerShell

1. Toujours dans le dossier **Système**, double-cliquez sur **"Ne pas exécuter les applications Windows spécifiées"**.
2. Cochez **Activé**.
3. Cliquez sur le bouton **Afficher…** (Show).
4. Dans la liste, ajoutez deux lignes :
    - `powershell.exe`
    - `powershell_ise.exe`
5. **OK** > **OK**.

4.4. : Bloquer le Matériel (Disques et USB)

A. Masquer les Disques Locaux (C:)

1. Allez dans : **Modèles d'administration** > **Composants Windows** > **Explorateur de fichiers**.
2. Double-cliquez sur **"Masquer ces lecteurs dans le Poste de travail"**.
3. Cochez **Activé**.

4. Dans la liste déroulante, choisissez : **Restreindre les lecteurs A, B, C et D uniquement**.
    - *Ne choisissez PAS “Restreindre tous les lecteurs”, sinon U: et T: disparaîtront aussi !*
5. **OK**.

B. Bloquer les clés USB

1. Allez dans : **Modèles d’administration** > **Système** > **Accès au stockage amovible**.
2. Cherchez la ligne : **“Toutes les classes de stockage amovible : Refuser tous les accès”**.
3. Double-cliquez.
4. Cochez **Activé**.
5. **OK**.

4.5. : Validation Finale

1. Fermez l’éditeur.
2. Sur le client, ouvrez une invite de commande (tant que vous êtes Admin).
3. Tapez `gpupdate /force`.
4. **Le test de vérité :**
    - Connectez-vous avec **Paul**.
    - Essayez d’ouvrir `C:` -> Bloqué ?
    - Essayez d’ouvrir `cmd` -> Bloqué ?
    - Connectez-vous avec **ADMIN**.
    - Essayez d’ouvrir `C:` -> Ça marche ? (Ça doit marcher).

.

5. Validation et Durcissement Réseau (Pare-feu pfSense)

Objectif : Transformer la configuration “Permissive” du LOT 1 en configuration “Sécurisée”.

5.1. Nettoyage de l’Interface LAN

Au LOT 1, nous avons créé des règles anticipées (AD, DNS, SMB, RPC). Il est temps de les rendre effectives.

1. **Vérification des règles existantes** : S’assurer que les règles pour **DNS (53)**, **AD (389, 88, 636)**, **SMB (445)** et surtout **RPC Dynamiques (49152-65535)** sont bien présentes et activées (Voir Tableau 4.2 du LOT 1).
2. **Ajout de la règle de sécurité SAN** (Prioritaire, tout en haut) :
    - Action : **BLOCK**.
    - Source : `LAN Net`.
    - Destination : `SAN Net` (172.16.x.x).
    - *Objectif : Empêcher les élèves d’attaquer les baies de stockage.*
3. **Activation du filtrage (Le grand saut)** :
    - **Désactiver** ou **Supprimer** la règle du bas : *“Default allow LAN to any rule”*.

- *Conséquence :* Désormais, seul ce qui est explicitement autorisé (AD, Fichiers, Web) passera. Tout le reste (P2P, Jeux, scans réseaux) sera bloqué.

5.2. Validation Interface SAN

- S'assurer qu'il n'y a **QUE** la règle autorisant le port **TCP 3260** (iSCSI) depuis les IPs des serveurs (`.10`, `.11`).
- Supprimer toute règle "Allow All" sur cette interface si elle existe.

.

6. Tests de Résilience et Validation (Recette)

6.1. Tests de Sécurité (GPO)

- ☐ **USB :** Insertion d'une clé USB sur le poste de Paul -> **Accès Refusé**.
- ☐ **Disque C: :** Tentative d'accès à `C:\` dans la barre d'adresse -> **Accès Refusé**.
- ☐ **Panneau Config :** Lancement de `control.exe` -> **Bloqué**.
- ☐ **Admin :** Connexion avec le compte `ADMIN` -> **Accès complet** (USB et C: fonctionnels).

6.2. Tests de Haute Disponibilité (LOT 2 & 3 validés)

- ☐ **Panne DC :** Extinction de `STG-SRVW01`. Connexion d'un client -> **Succès** (Auth via SRVW02).
- ☐ **Panne Fichier :** Accès à `\\IEF.LOCAL\INTRANET` avec SRVW01 éteint -> **Succès** (Bascule transparente DFS).

.

7. Difficultés Rencontrées (Synthèse)

1. Blocage de l'Administrateur par GPO

- *Symptôme :* Le compte ADMIN ne pouvait plus accéder au serveur.
- *Cause :* La GPO de restriction s'appliquait aux "Utilisateurs authentifiés", groupe qui inclut les admins.
- *Résolution :* Modification du filtrage de sécurité pour ne cibler que les groupes GRP1 et GRP2.

2. Échec de Réplication DFS via VPN

- *Symptôme :* Les fichiers ne se synchronisaient pas entre le Site A et le Site B.
- *Cause :* Le pare-feu pfSense bloquait les ports hauts (RPC) utilisés aléatoirement par le service de réplication.
- *Résolution :* Ajout de la règle LAN autorisant la plage TCP **49152-65535** vers les contrôleurs de domaine.

3. Conflit de Masquage de Disques

- *Symptôme :* L'option "Restreindre tous les lecteurs" masquait aussi les lecteurs réseaux U: et T:.
- *Résolution :* Passage à l'option "Restreindre A, B, C et D uniquement".

1. **Latence de Réplication GPO Inter-Sites (15 minutes)**

- *Symptôme :* Les restrictions (CMD bloqué) fonctionnaient sur le Site A, mais l'utilisateur du Site B gardait ses accès pendant les premières minutes.

- *Analyse :* Le Contrôleur du Site B n'avait pas encore reçu les fichiers de la GPO (dossier SYSVOL `{GUID}`) venant du Site A.
- *Résolution :* Nous avons constaté que le délai de convergence standard inter-sites est de **15 minutes**. La commande `repadmin /syncall` a forcé la topologie logique, et le service DFSR a transféré les fichiers ensuite. Le test a été validé avec succès après ce délai incompressible.

.

8. Bilan Final du Projet AP3

Le système d'information livré est désormais :

- ✅ **Fonctionnel** : Services AD, DNS, DHCP, Fichiers opérationnels sur 2 sites.
- ✅ **Redondant** : Bascule automatique des services (DFS, DHCP Failover) en cas de panne.
- ✅ **Sécurisé** : Cloisonnement réseau strict et environnement utilisateur verrouillé.
- ✅ **Sauvegardé** : Données protégées sur stockage SAN externe avec historique (Clichés).

.

FIN DU LOT 4

FIN DE L'AP3.

⬅ LOT précédent | Menu Livrable 2