BTS Services Informatiques aux Organisations

Option SISR - Solutions d'Infrastructure, Systèmes et Réseaux

ÉPREUVE E6

Cybersécurité des services informatiques

PROJET GSB

Infrastructure Active Directory Redondante

avec Proxmox et pfSense

Candidat	Anis (Binôme avec Younes)
Formation	BTS SIO Option SISR
Établissement	Lycée Théodore Aubanel - Avignon
Session	2025 - 2026

SOMMAIRE

1. INTRODUCTION

1.1 Présentation de l'entreprise GSB

Le laboratoire Galaxy Swiss Bourdin (GSB) est issu de la fusion en 2009 entre le géant américain Galaxy, spécialisé dans le secteur des maladies virales (SIDA, hépatites), et le conglomérat européen Swiss Bourdin, travaillant sur des médicaments plus conventionnels.

L'entité Galaxy Swiss Bourdin Europe a établi son siège administratif à Paris, tandis que le siège social de la multinationale est situé à Philadelphie, Pennsylvanie, aux États-Unis. L'entreprise compte 480 visiteurs médicaux en France métropolitaine et 60 dans les départements et territoires d'outre-mer, répartis en 6 secteurs géographiques.

GSB vient d'acquérir de nouveaux locaux à Avignon et souhaite moderniser son système d'information. Notre mission consiste à mettre en place l'infrastructure réseau complète de ce nouveau site.

1.2 Contexte du projet

Ce projet s'inscrit dans le cadre de l'épreuve E6 du BTS SIO option SISR. Il consiste à mettre en place une infrastructure réseau sécurisée et redondante pour le Local 1 de GSB Avignon, incluant :

- Une infrastructure virtualisée sur deux serveurs Proxmox
- Un pare-feu pfSense avec segmentation réseau par VLANs
- Un Active Directory redondant avec deux contrôleurs de domaine
- Un serveur web MediaWiki en zone DMZ
- Des services DHCP et DNS automatisés
- Un proxy filtrant pour contrôler l'accès Internet

1.3 Objectifs techniques

> **Objectifs du projet**
>
> Déployer une infrastructure complète, sécurisée et hautement disponible, respectant les bonnes pratiques Microsoft (modèle Tiering) et les principes de sécurité réseau.

- Assurer la haute disponibilité avec réplication Active Directory
- Segmenter le réseau par VLANs pour isoler les flux
- Implémenter le modèle de sécurité Tiering (Tier0, Tier1, Tier2)
- Filtrer le trafic web avec un proxy Squid/SquidGuard
- Documenter l'ensemble pour faciliter la maintenance

1.4 Organisation du travail

Le projet est réalisé en binôme (Binôme 2 - Local 1) avec gestion de projet via Jira (méthode Kanban). Chaque membre dispose de sa propre infrastructure complète pour pouvoir passer l'épreuve E6 individuellement. La redondance Active Directory est assurée par la jonction du DC de Younes au domaine principal.

Membre	Infrastructure personnelle	Proxmox
Anis	pfSense, AD Principal (DC1), DHCP, DMZ, VM Admin	Proxmox A

Younes	pfSense, AD Secondaire (DC2 - rejoint le domaine d'Anis)	Proxmox B

Organisation pour l'épreuve E6

Chacun passe l'épreuve individuellement avec sa propre infrastructure. La partie redondance est réalisée en commun : le DC de Younes rejoint le domaine GSBLocal1.local créé par Anis, permettant de démontrer la réplication Active Directory.

2. ARCHITECTURE GLOBALE

2.1 Vue d'ensemble

L'infrastructure repose sur deux serveurs Proxmox interconnectés via un trunk 802.1Q, assurant la redondance des services critiques. Le pare-feu pfSense gère 7 interfaces réseau pour segmenter le trafic.

2.2 Composants de l'infrastructure

Composant	Description	Rôle
Proxmox A (Anis)	Hyperviseur principal (10.110.0.1)	pfSense, AD principal (DC1), VM Admin, DMZ
Proxmox B (Younes)	Hyperviseur secondaire (10.110.0.2)	pfSense, AD secondaire (DC2 - rejoint domaine)
pfSense	Pare-feu / Routeur pfSense 2.7.2	7 interfaces, NAT, Proxy, DNS
Active Directory	Domaine GSBLocal1.local	Authentification, GPO, DNS intégré
Serveur DMZ	Debian + Nginx	Serveur web (futur MediaWiki)
Switches Cisco	2x Catalyst 2960+ Series	VLANs, Trunk 802.1Q (Fa0/23)

3. DÉTAIL DES MACHINES VIRTUELLES

3.1 VM pfSense - Pare-feu et Routeur

> **Rôle**
> Cœur de la sécurité réseau : routage inter-VLAN, filtrage, NAT, proxy web, DNS.

Paramètre	Valeur
Nom de la VM	pfSense-GSB
Système d'exploitation	pfSense 2.7.2 (FreeBSD)
Mémoire RAM	2048 MB
Processeur	2 vCPU
Stockage	20 GB
Interfaces réseau	7 interfaces (WAN, LAN, DMZ, 4 VLANs)
Hébergement	Proxmox 1

3.2 VM SRV-AD-GSB - Contrôleur de Domaine Principal

> **Rôle**
> Active Directory, DNS intégré, serveur DHCP. Authentification centralisée du domaine GSBLocal1.local.

Paramètre	Valeur
Nom de la VM	SRV-AD-GSB (AD-A)
Système d'exploitation	Windows Server 2022 Standard
Mémoire RAM	4096 MB
Processeur	2 vCPU
Stockage	40 GB
Bridge Proxmox	vmbr1 - VLAN Tag 50
Adresse IP	172.21.50.25/24
Domaine	GSBLocal1.local (GSBLOCAL1)
Rôles installés	AD DS, DNS, DHCP
Outil de déploiement	Hello-My-Dir v1.1.2.3

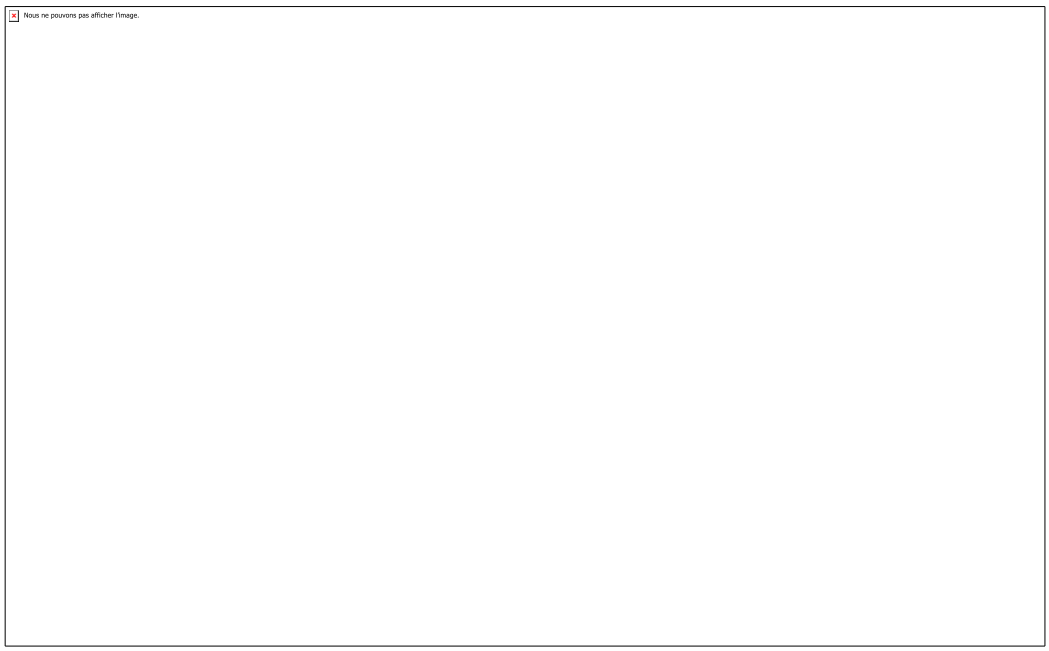

Figure 1 : Active Directory Users and Computers - Structure du domaine avec Tiering (Tier0, Tier1, Tier2)

3.3 VM SRV-AD-GSB-2 - Contrôleur de Domaine Secondaire (Younes)

Rôle

Le DC secondaire appartient à Younes et rejoint le domaine GSBLocal1.local créé par Anis. Cela permet de démontrer la redondance AD : si le DC1 tombe, le DC2 prend automatiquement le relais.

Paramètre	Valeur
Nom de la VM	SRV-AD-GSB-2
Système d'exploitation	Windows Server 2022 Standard
Adresse IP	172.21.50.24/24
Rôle AD	Contrôleur de domaine additionnel (DC2)
Domaine rejoint	GSBLocal1.local (domaine d'Anis)
Services	AD DS (Replica), DNS (répliqué)
Propriétaire	Younes (binôme)
Hébergement	Proxmox B (Younes)

3.4 VM Serveur DMZ - Serveur Web

Rôle

Serveur web Nginx dans la zone démilitarisée, destiné à héberger MediaWiki pour la documentation interne GSB.

Paramètre	Valeur
Nom de la VM	SRV-DMZ
Système d'exploitation	Debian 12
Adresse IP	172.21.200.1/24
Passerelle	172.21.200.254 (pfSense)
Service installé	Nginx (serveur web)

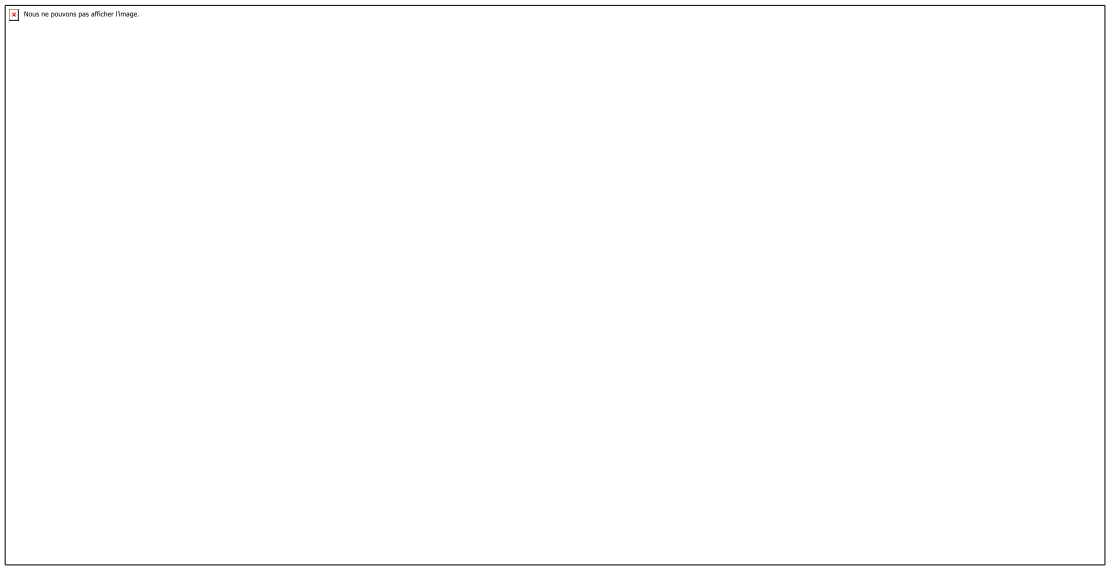

Figure 2 : Configuration réseau du serveur DMZ (/etc/network/interfaces)

Figure 3 : Service Nginx actif et test curl localhost

3.5 VM Admin - Poste d'Administration

Rôle

> Poste d'administration avec RSAT pour gérer l'AD, accès pfSense et RDP vers les serveurs.

Paramètre	Valeur
Nom de la VM	VM-ADMIN
Système d'exploitation	Windows 10/11 Pro
Bridge Proxmox	vmbr1 - VLAN Tag 99
Adresse IP	172.21.99.10/24
Outils installés	RSAT, Navigateur, Client RDP

4. PLAN D'ADRESSAGE IP ET VLANs

4.1 Tableau d'adressage global

L'infrastructure utilise le préfixe 172.21.x.0/24 pour tous les réseaux internes, conformément aux recommandations du projet GSB Local 1.

Réseau	VLAN	Plage IP	Gateway	Usage
WAN	-	10.110.0.0/8	10.110.0.1	Accès Internet/Proxmox
LAN	-	172.21.1.0/24	172.21.1.1	Réseau principal
DMZ	-	172.21.200.0/24	172.21.200.254	Zone démilitarisée
MANAGEMENT	99	172.21.99.0/24	172.21.99.1	Administration
SERVAD	50	172.21.50.0/24	172.21.50.1	Serveurs AD
UTILISATEURS	30	172.21.30.0/24	172.21.30.1	Postes utilisateurs
VISITEURS	150	172.21.150.0/24	172.21.150.1	Invités (Internet only)

4.2 VLAN 99 - MANAGEMENT

Équipement	Adresse IP	Masque	Type
pfSense (Gateway)	172.21.99.1	/24	Statique
VM Admin	172.21.99.10	/24	Statique

4.3 VLAN 50 - SERVAD (Serveurs Active Directory)

Équipement	Adresse IP	Masque	Type
pfSense (Gateway)	172.21.50.1	/24	Statique
SRV-AD-GSB-2 (DC2)	172.21.50.24	/24	Statique
SRV-AD-GSB (DC1)	172.21.50.25	/24	Statique

4.4 VLAN 30 - UTILISATEURS

Équipement	Adresse IP	Masque	Type
pfSense (Gateway)	172.21.30.1	/24	Statique
Postes utilisateurs	172.21.30.10-199	/24	DHCP

4.5 VLAN 150 - VISITEURS

Équipement	Adresse IP	Masque	Type
pfSense (Gateway)	172.21.150.1	/24	Statique
Postes visiteurs	172.21.150.10-99	/24	DHCP

4.6 DMZ - Zone Démilitarisée

Équipement	Adresse IP	Masque	Type
pfSense (Gateway)	172.21.200.254	/24	Statique
Serveur Web (Nginx)	172.21.200.1	/24	Statique

5. CONFIGURATION PFSENSE

5.1 Interfaces réseau

pfSense gère 7 interfaces réseau pour segmenter le trafic et appliquer des politiques de sécurité différenciées.

Interface	Device	Adresse IP	VLAN	Description
WAN	vtnet0	10.110.0.254/8	-	Connexion Internet
LAN	vtnet1	172.21.1.1/24	-	Réseau principal
DMZ	vtnet2	172.21.200.254/24	-	Zone démilitarisée
MANAGEMENT	vtnet1.99	172.21.99.1/24	99	Administration
SERVAD	vtnet1.50	172.21.50.1/24	50	Serveurs AD
UTILISATEURS	vtnet1.30	172.21.30.1/24	30	Postes utilisateurs
VISITEURS	vtnet1.150	172.21.150.1/24	150	Invités isolés

5.2 Configuration de l'interface DMZ

L'interface DMZ est configurée sur vtnet2 avec l'adresse 172.21.200.254/24. Cette zone héberge le serveur web accessible depuis l'extérieur.

Figure 4 : Configuration interface DMZ - Paramètres généraux

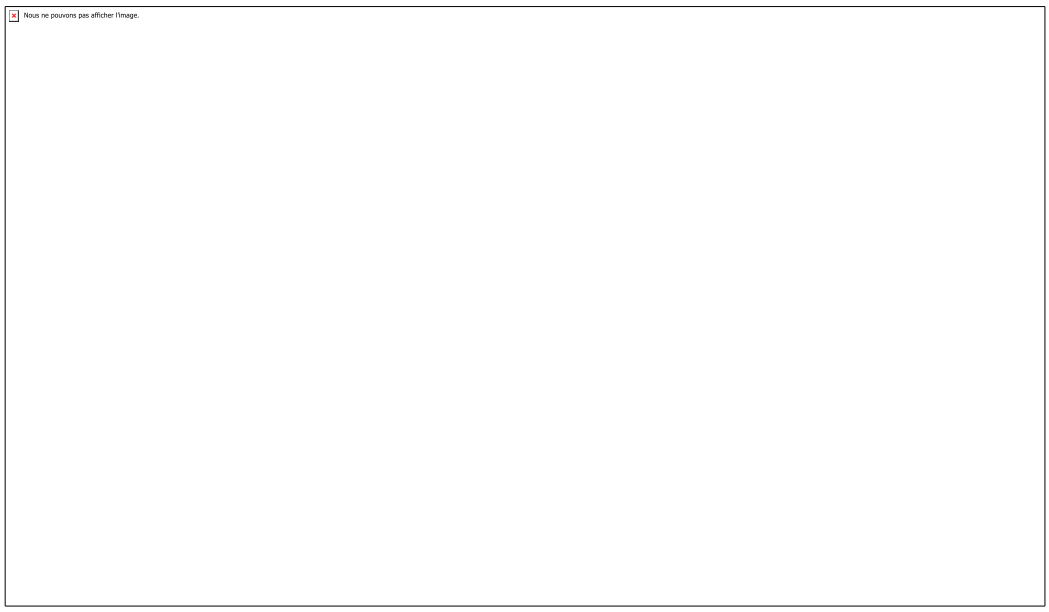

Figure 5 : Configuration interface DMZ - Adresse IP statique 172.21.200.254/24

5.3 Proxy Squid et SquidGuard

Le proxy Squid avec SquidGuard permet de filtrer le trafic web et bloquer l'accès à certaines catégories de sites (réseaux sociaux, contenu adulte, malware).

Paramètre	Valeur
Port d'écoute	3128
Mode transparent	Oui (sur LAN)
Cache disque	500 MB
Cache mémoire	64 MB
Catégories bloquées	Réseaux sociaux, contenu adulte, malware

Figure 6 : Packages installés - Squid et SquidGuard

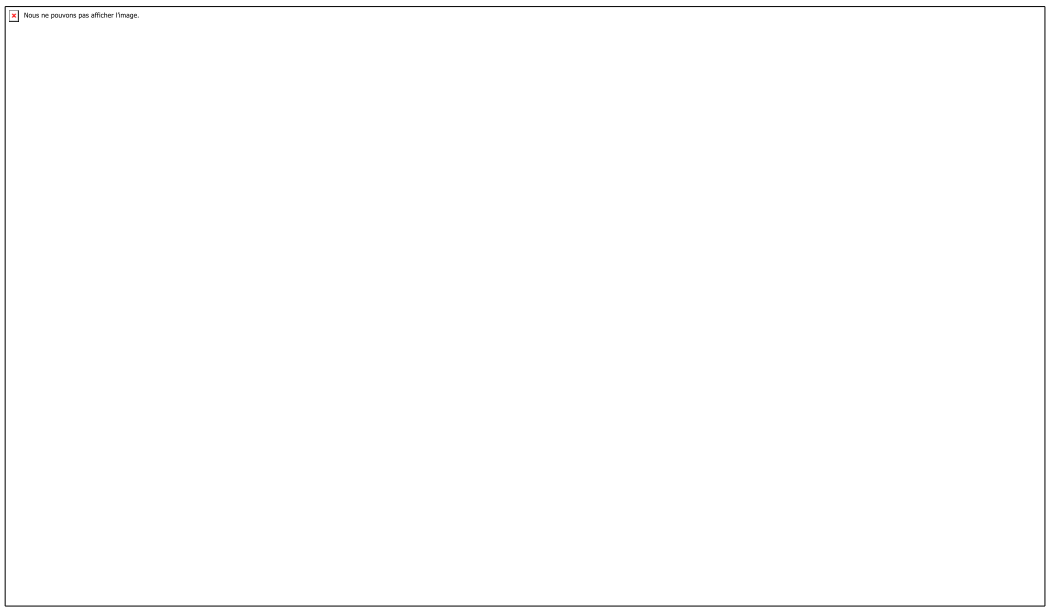

Figure 7 : SquidGuard - Téléchargement des blacklists (69 catégories)

5.4 Test du filtrage - Blocage de Facebook

Le filtrage SquidGuard a été testé en bloquant l'accès à facebook.com. Les captures suivantes montrent le résultat avant et après activation du blocage.

Figure 8 : Facebook accessible AVANT activation du blocage

Figure 9 : Facebook BLOQUÉ après activation de SquidGuard (ERR_CONNECTION_REFUSED)

5.5 Règles de pare-feu

Les règles suivent le principe du moindre privilège : tout est bloqué par défaut, seuls les flux nécessaires sont autorisés.

VLAN VISITEURS (150) - Isolé

Action	Source	Destination	Port	Description
✗ **Block**	VISITEURS net	RFC1918	Any	Bloquer réseaux privés
✓ **Pass**	VISITEURS net	Internet	Any	Internet uniquement

6. CONFIGURATION ACTIVE DIRECTORY

6.1 Installation avec Hello-My-Dir

L'Active Directory a été déployé à l'aide de l'outil Hello-My-Dir v1.1.2.3 qui automatise l'installation et applique les bonnes pratiques de sécurité Microsoft, notamment le modèle Tiering.

Figure 10 : Hello-My-Dir - Installation du domaine GSBLocal1.com avec niveau fonctionnel Windows 2016

6.2 Informations du domaine

Paramètre	Valeur
Nom de domaine DNS	GSBLocal1.local
Nom NetBIOS	GSBLOCAL1
Niveau fonctionnel forêt	Windows Server 2016
Niveau fonctionnel domaine	Windows Server 2016
DC Principal (DC1)	SRV-AD-GSB (172.21.50.25)
DC Secondaire (DC2)	SRV-AD-GSB-2 (172.21.50.24)

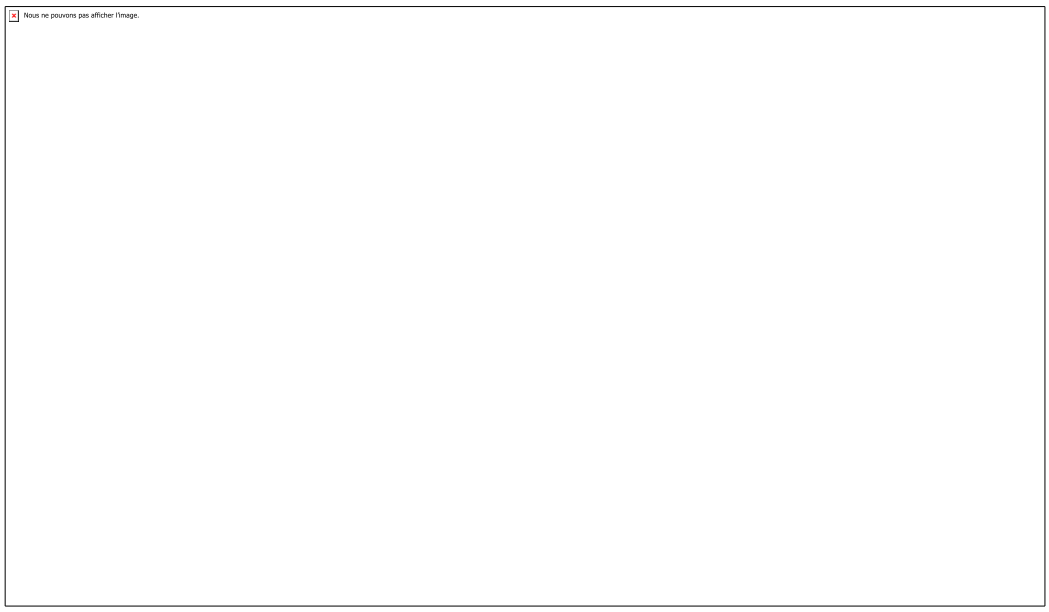

Figure 11 : Écran de connexion Windows Server - Domaine GSBLOCAL1

6.3 Modèle de sécurité Tiering

Principe du Tiering

Le modèle Tiering segmente les comptes administratifs en 3 niveaux pour limiter la propagation d'une compromission. Un compte Tier 0 ne doit jamais se connecter sur une machine Tier 1 ou Tier 2, et inversement.

Tier	Périmètre	Exemples de systèmes
Tier 0	Contrôle total du SI	Domain Controllers, PKI, serveurs AD
Tier 1	Administration serveurs	Serveurs Windows/Linux, hyperviseurs
Tier 2	Postes utilisateurs	Postes de travail, laptops

6.4 Structure organisationnelle

Hello-My-Dir a créé automatiquement l'unité d'organisation Secured-Accounts avec la structure Tiering :

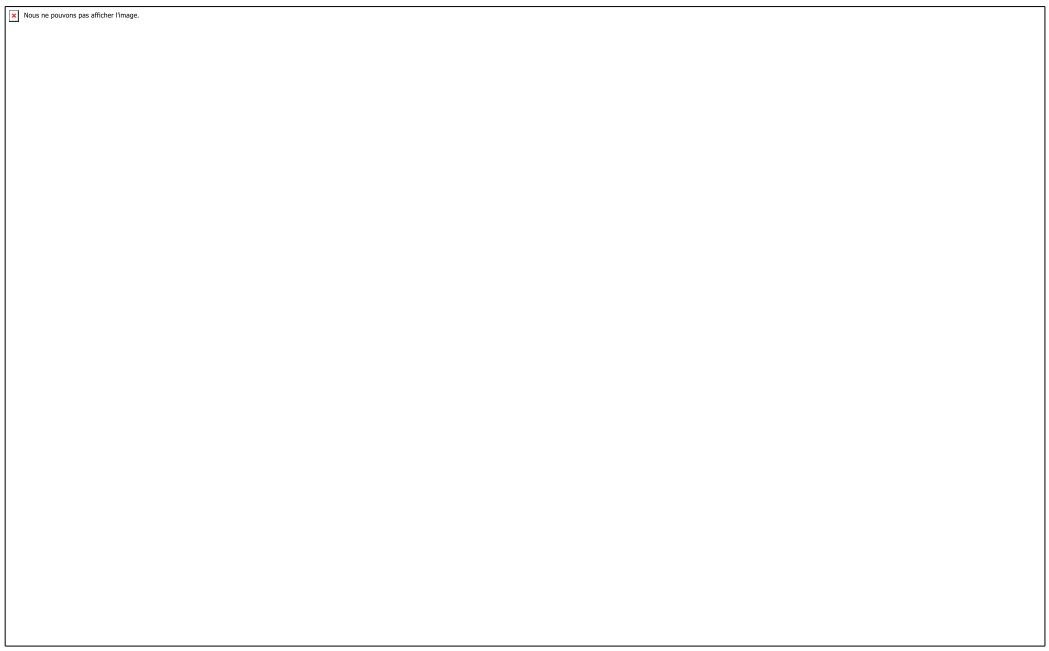

Figure 12 : Structure AD - OU Secured-Accounts avec Tier0, Tier1, Tier2

6.5 Groupes de sécurité créés

Groupe	Fonction
LS-DLG-DomainJoin-Extended	Délégation pour joindre des ordinateurs au domaine
LS-SEC-Tier0-Admins	Administrateurs Tier 0 (contrôleurs de domaine)
LS-SEC-Tier1-Admins	Administrateurs Tier 1 (serveurs)
LS-SEC-Tier2-Admins	Administrateurs Tier 2 (postes)
DHCP Administrators	Gestion complète du service DHCP

7. CONFIGURATION DHCP

7.1 Installation et autorisation

Le service DHCP est hébergé sur le contrôleur de domaine principal (SRV-AD-GSB). Il a été installé via PowerShell et autorisé dans l'Active Directory.

Figure 13 : Installation du rôle DHCP et création des groupes de sécurité

Commandes PowerShell utilisées

```
Install-WindowsFeature DHCP -IncludeManagementTools
netsh dhcp add securitygroups
Restart-Service DHCPServer
Add-DhcpServerInDC -DnsName 'AD-A' -IPAddress 172.21.50.25
Get-DhcpServerInDC
```

Figure 14 : Autorisation DHCP dans AD et vérification avec Get-DhcpServerInDC

7.2 Étendue LAN (172.21.1.0/24)

Paramètre	Valeur
Nom de l'étendue	LAN
Réseau	172.21.1.0/24
Plage d'adresses	172.21.1.50 - 172.21.1.200
Passerelle (003)	172.21.1.1 (pfSense)
Serveur DNS (006)	172.21.50.25 (AD)
Durée du bail	8 heures

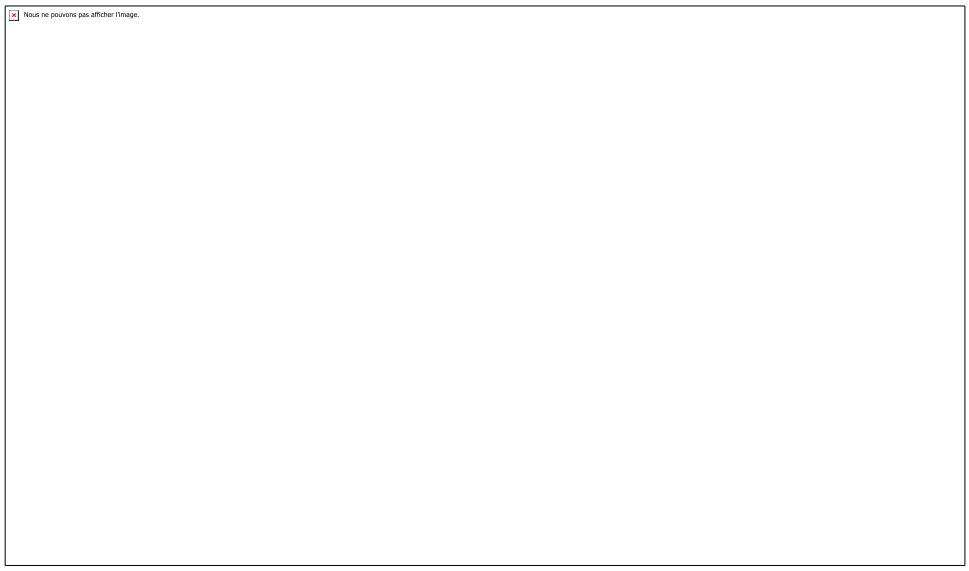

Figure 15 : Assistant nouvelle étendue - Nom LAN

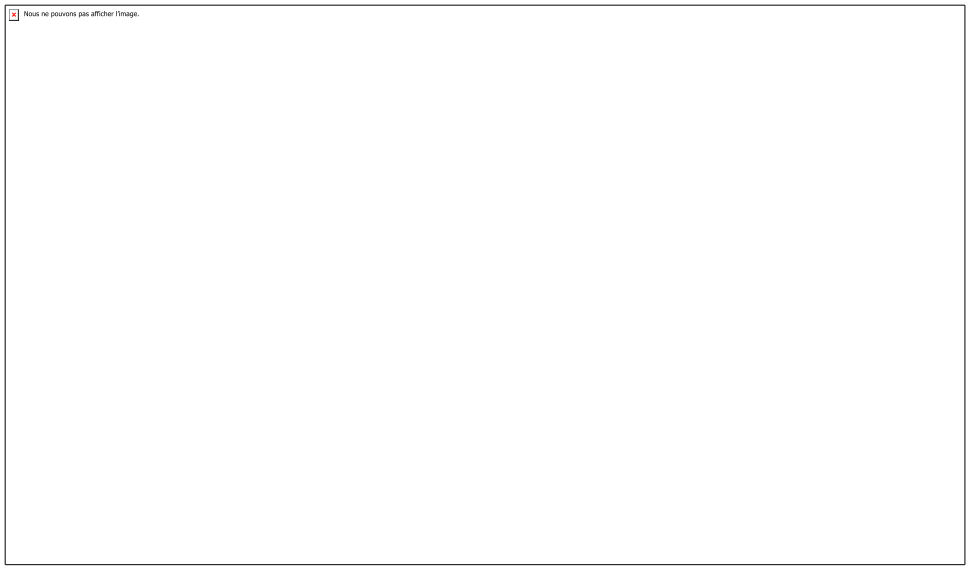

Figure 16 : Étendue LAN - Plage 172.21.1.50 à 172.21.1.200

7.3 Étendue UTILISATEURS (172.21.30.0/24)

Paramètre	Valeur

Nom de l'étendue	UTILISATEURS
Réseau	172.21.30.0/24
Plage d'adresses	172.21.30.10 - 172.21.30.199
Passerelle (003)	172.21.30.1 (pfSense)
Serveur DNS (006)	172.21.50.25 (AD)

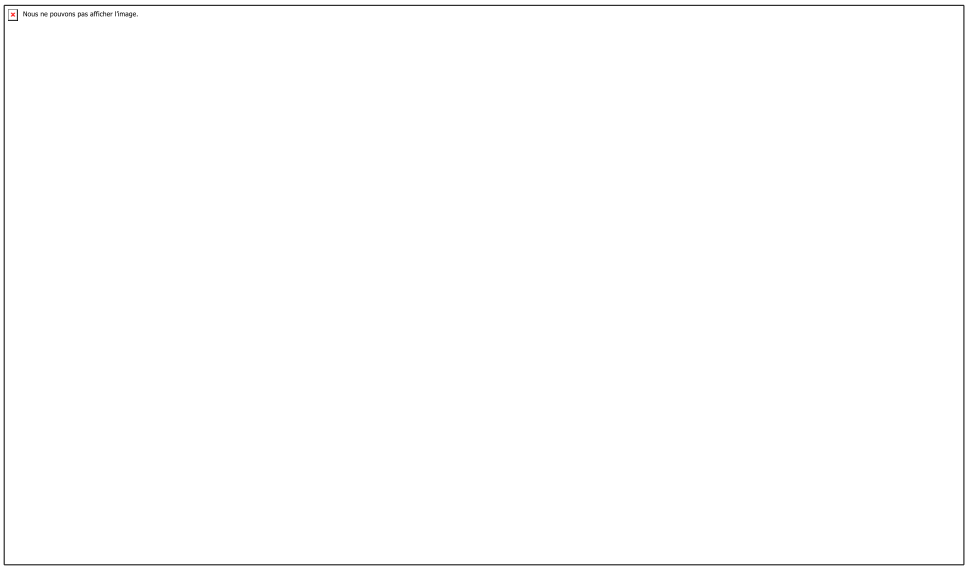

Figure 17 : Étendue UTILISATEURS - Plage 172.21.30.10 à 172.21.30.199

7.4 Étendue VISITEURS (172.21.150.0/24)

Paramètre	Valeur
Nom de l'étendue	VISITEURS
Réseau	172.21.150.0/24
Plage d'adresses	172.21.150.10 - 172.21.150.99
Passerelle (003)	172.21.150.1 (pfSense)
Serveur DNS (006)	172.21.150.1 (pfSense - isolé)
Durée du bail	4 heures (plus court)

Figure 18 : Étendue VISITEURS - Plage 172.21.150.10 à 172.21.150.99

Sécurité VLAN Visiteurs

Les visiteurs reçoivent le DNS de pfSense (172.21.150.1) et non celui de l'AD pour les isoler du réseau interne. Le bail plus court libère rapidement les adresses.

8. REDONDANCE ET HAUTE DISPONIBILITÉ

8.1 Principe de la redondance

> **Organisation binôme**
>
> Anis crée le domaine GSBLocal1.local sur son DC principal. Younes, depuis son infrastructure, promeut son serveur en DC secondaire et rejoint le domaine d'Anis. Les deux DC répliquent automatiquement les données AD.

Cette architecture permet de démontrer la haute disponibilité : si le DC d'Anis tombe en panne, le DC de Younes peut continuer à authentifier les utilisateurs et vice-versa.

8.2 Architecture redondante

Composant	Propriétaire	Rôle	IP
DC1 (SRV-AD-GSB)	Anis	DC Principal	172.21.50.25
DC2 (SRV-AD-GSB-2)	Younes	DC Additionnel	172.21.50.24

Service	Mécanisme	Avantage
Active Directory	Réplication multi-master	Continuité d'authentification
DNS	Zones intégrées AD	Résolution DNS permanente
Données utilisateurs	Réplication temps réel	Données toujours synchronisées

8.3 Configuration du trunk inter-switches

La connexion entre les deux Proxmox est assurée par un lien trunk 802.1Q sur le port FastEthernet 0/23 des deux switches Cisco.

Paramètre	Valeur
Port Switch 1 (Anis)	FastEthernet 0/23
Port Switch 2 (Younes)	FastEthernet 0/23
Mode	Trunk 802.1Q
VLANs autorisés	1, 30, 50, 99, 150
VLAN natif	1

Configuration Cisco IOS

```
interface fastEthernet 0/23
  description TRUNK vers Switch binome
  switchport mode trunk
  switchport trunk allowed vlan 1,30,50,99,150
  switchport trunk native vlan 1
  no shutdown
```

8.4 Jonction du DC de Younes au domaine

Une fois le trunk configuré et la communication établie entre les deux infrastructures, Younes promeut son serveur Windows Server en contrôleur de domaine additionnel :

```
# Sur le serveur de Younes - Promotion en DC additionnel
Install-ADDSDomainController `
    -DomainName 'GSBLocal1.local' `
    -Credential (Get-Credential GSBLOCAL1\Administrateur) `
    -InstallDns `
    -Force
```

Après la jonction

Les deux DC répliquent automatiquement : utilisateurs, groupes, GPO, zones DNS. La commande repadmin /replsummary permet de vérifier l'état de la réplication.

9. TESTS ET VALIDATION

9.1 Tests de connectivité réseau

Test	Méthode	Résultat
Connectivité inter-VLANs	Ping entre VLANs autorisés	✓ OK
Isolation VISITEURS	Ping vers réseaux internes	✓ Bloqué
Accès Internet	Ping 8.8.8.8 depuis chaque VLAN	✓ OK
Filtrage proxy (Facebook)	Accès https://facebook.com	✓ Bloqué
Accès serveur DMZ	HTTP vers 172.21.200.1	✓ OK

9.2 Tests Active Directory

Test	Commande/Méthode	Résultat
Résolution DNS domaine	nslookup GSBLocal1.local	✓ OK
Connexion au domaine	Login GSBLOCAL1\Administrateur	✓ OK
Réplication AD DC1-DC2	repadmin /replsummary	✓ OK
Jonction poste au domaine	Add-Computer -DomainName	✓ OK

9.3 Tests DHCP

Test	Vérification	Résultat
Attribution IP LAN	Plage 172.21.1.50-200	✓ OK
Attribution IP UTILISATEURS	Plage 172.21.30.10-199	✓ OK
Attribution IP VISITEURS	Plage 172.21.150.10-99	✓ OK
Options DHCP (GW, DNS)	ipconfig /all	✓ OK

10. COMPÉTENCES MOBILISÉES

10.1 Compétences du référentiel BTS SIO

Bloc	Compétence	Application dans le projet
B2	Administrer les systèmes	Windows Server 2022, AD DS, DHCP, DNS
B2	Administrer les réseaux	VLANs, routage pfSense, switches Cisco
B2	Gérer environnement virtualisé	VMs sur Proxmox VE
B3	Protéger les données	Segmentation réseau, DMZ, pare-feu
B3	Sécuriser les équipements	Modèle Tiering, GPO, proxy filtrant
B3	Assurer haute disponibilité	Redondance AD, réplication DNS

10.2 Compétences techniques acquises

- Virtualisation : Création et gestion de VMs sur Proxmox VE
- Pare-feu : Configuration avancée pfSense (interfaces, VLANs, règles, NAT, proxy)
- Active Directory : Déploiement domaine avec modèle Tiering et Hello-My-Dir
- Services réseau : DNS intégré AD, DHCP multi-étendues avec relay
- Réseau : Segmentation VLANs, trunk 802.1Q sur switches Cisco
- Haute disponibilité : Réplication AD multi-master entre deux DC
- Filtrage web : Proxy Squid + SquidGuard avec blacklists
- Scripting : PowerShell pour l'administration Windows Server

10.3 Compétences transversales

- Travail en équipe : Collaboration en binôme avec répartition des tâches
- Gestion de projet : Utilisation de Jira (méthode Kanban)
- Documentation : Rédaction de documentation technique professionnelle
- Résolution de problèmes : Diagnostic et correction des erreurs

11. CONCLUSION ET PERSPECTIVES

11.1 Bilan du projet

Ce projet a permis de déployer une infrastructure réseau d'entreprise complète et sécurisée pour le site GSB Avignon, répondant aux exigences de sécurité, disponibilité et maintenabilité.

Objectif	Statut
Infrastructure virtualisée Proxmox avec 7 réseaux segmentés	✓ Réalisé
Pare-feu pfSense avec filtrage et proxy Squid/SquidGuard	✓ Réalisé
Active Directory redondant avec 2 contrôleurs de domaine	✓ Réalisé
Modèle de sécurité Tiering (Tier0, Tier1, Tier2)	✓ Réalisé
Services DHCP avec 3 étendues (LAN, UTILISATEURS, VISITEURS)	✓ Réalisé
Serveur web Nginx en zone DMZ	✓ Réalisé
Documentation technique complète	✓ Réalisé

11.2 Difficultés rencontrées et solutions

- Configuration VLAN pfSense : Résolu par création d'interfaces VLAN sur le bridge trunk
- Communication inter-sites : Résolu par configuration correcte du trunk 802.1Q
- Autorisation DHCP dans AD : Résolu par Add-DhcpServerInDC
- Filtrage proxy : Résolu par téléchargement des blacklists SquidGuard

11.3 Évolutions possibles

- Déploiement complet de MediaWiki sur le serveur DMZ
- Configuration DNS sur Active Directory (à faire)
- GPO avancées : Déploiement de logiciels, restrictions de sécurité
- Sauvegardes automatiques : Windows Server Backup, Veeam
- Certificats SSL/TLS : PKI interne avec AD CS
- Monitoring : Déploiement de Zabbix ou PRTG
- VPN : Configuration OpenVPN sur pfSense pour accès distant
- Portail captif : Configuration pour le VLAN Visiteurs

FIN DU DOCUMENT

Documentation E6 - Projet GSB

Réalisé par Anis - BTS SIO SISR

Binôme avec Younes - Local 1

Lycée Théodore Aubanel - Avignon - Session 2025-2026