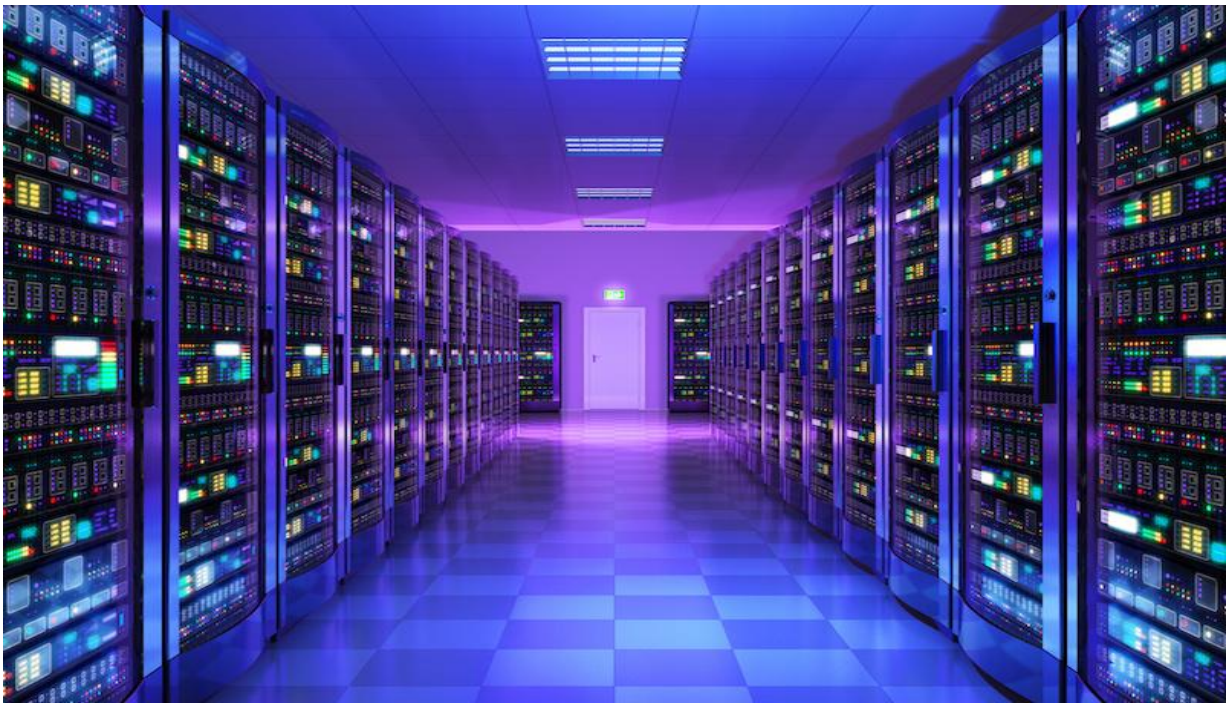
IRATNI Hocine N°Candidat : 02049749590

Dossier E6:
SUPPORT ET MISE A DISPOSITION DES SERVICES INFORMATIQUES



Portfolio : https://iratnihocine.com

Enterprise : Sauvegarde13, CPRPF

Table Des Matières

Table des matières

1. INTRODUCTION

1.1 CONTEXTE DES RÉALISATIONS

Le présent dossier s'inscrit dans le cadre du BTS SIO option SISR et a pour objectif de présenter la mise en place d'une infrastructure réseau complète pour une PME fictive. Les travaux ont été réalisés au sein du centre de formation **IFC Marseille**, à l'aide des ressources matérielles et logicielles disponibles sur place ainsi que d'outils accessibles en ligne, détaillés dans la section 1.2.

L'entreprise fictive, **DIGITEX**, est une petite société spécialisée dans la distribution en ligne de solutions numériques. Elle regroupe une dizaine de collaborateurs et vient récemment d'emménager dans de nouveaux locaux. Afin d'assurer le bon fonctionnement de son activité, la direction a souhaité mettre en place un **Système d'Information (SI)** adapté à ses besoins organisationnels (répartition des services, outils collaboratifs, messagerie, gestion des utilisateurs, etc.) tout en garantissant un haut niveau de fiabilité et de sécurité.

Dans ce contexte, ma mission consiste à concevoir, déployer et maintenir l'infrastructure réseau de l'entreprise. Ce dossier présente les différentes étapes de la mise en place de cette solution, organisées autour de deux réalisations principales.

1.2 RESSOURCES MATÉRIELLES ET LOGICIELLES

Pour la réalisation de ce projet, j'ai utilisé les équipements mis à disposition par le centre de formation **IFC Marseille**, ainsi que plusieurs solutions logicielles étudiées au cours de la formation. Ces ressources ont permis de concevoir, tester et administrer l'infrastructure réseau présentée dans ce dossier.

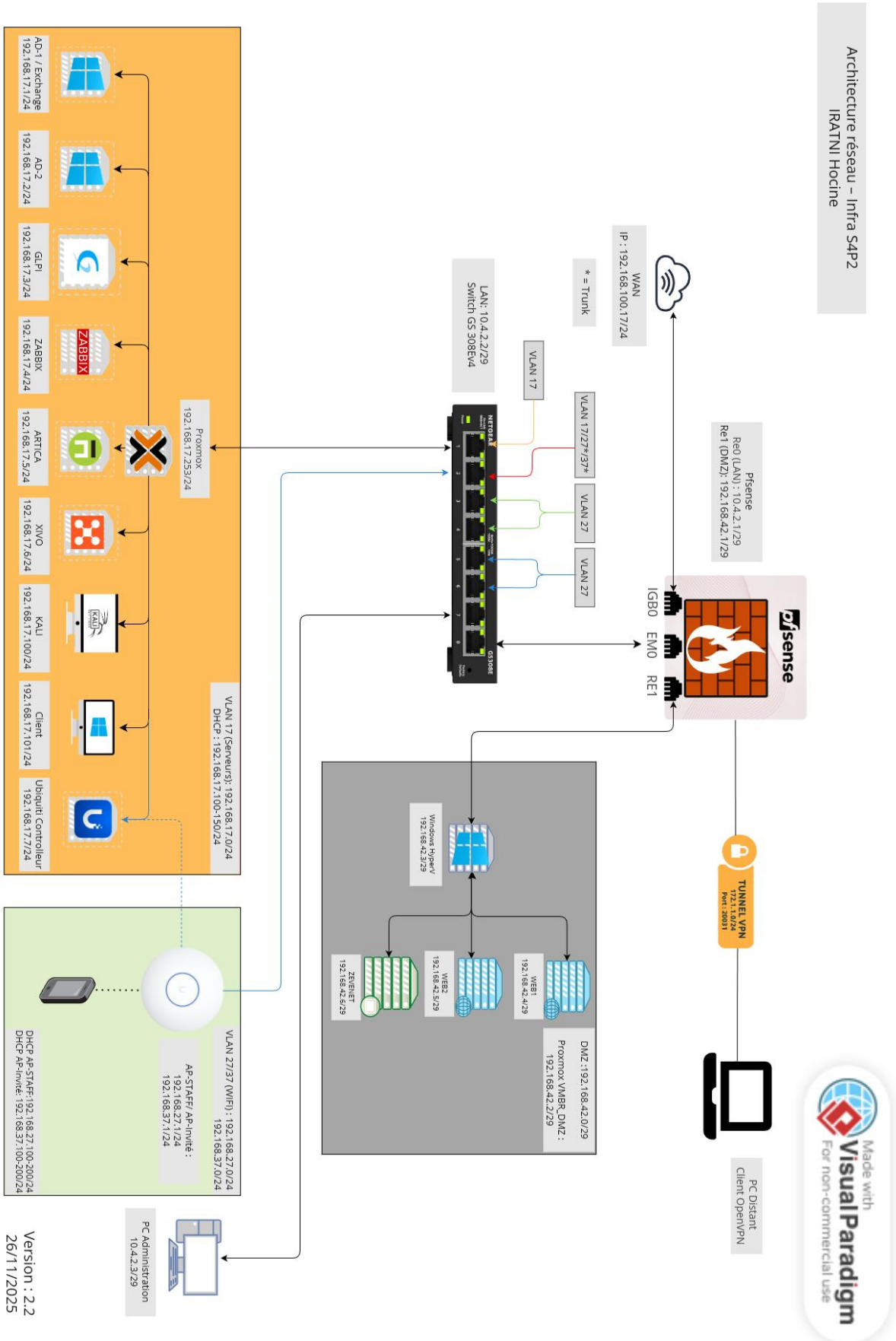
Ressources matérielles :

- Un poste fixe (clavier + souris USB) utilisé comme machine d'administration de l'infrastructure ;
- Un ordinateur portable servant de poste client afin de simuler l'activité des utilisateurs du SI ;
- Un PC équipé d'un disque dur de grande capacité (1 To) dédié à un serveur **Proxmox VE**, utilisé pour héberger et gérer les serveurs virtualisés ;
- Un espace de stockage supplémentaire pour la sauvegarde des machines virtuelles via **Proxmox Backup Server** ;
- Un PC attribué à un serveur **pfSense** (routeur/pare-feu), doté de trois cartes réseau (3 ports Ethernet) ;
- Un PC configuré en serveur **Hyper-V**, destiné à héberger des services accessibles depuis l'extérieur (ex. serveur web) ;
- Trois écrans VGA/HDMI ;
- Une prise Ethernet murale connectée au réseau WAN de l'établissement, simulant l'accès Internet de l'entreprise ;
- Des câbles Ethernet RJ45 en nombre suffisant ;
- Un commutateur **Netgear GS308Ev4** (8 ports, compatible VLAN 802.1Q) ;
- Deux multiprises ;
- Des clés USB (≥ 30 Go) pour l'installation des systèmes d'exploitation sur les machines physiques.

Ressources logicielles :

- Un serveur NAS commun aux étudiants du BTS SIO, contenant cours, procédures, logiciels et ressources pédagogiques ;
- Outil **Netgear Switch Discovery Tool (v1.2.103)**;
- Interface web d'administration du switch **Netgear GS308Ev4**;
- **Balena Etcher (v1.18.11)** pour la création de supports bootables ;
- Solution routeur/pare-feu **pfSense (v2.8.1)** avec son interface d'administration web ;
- Module de détection/prévention d'intrusions **Snort IDS** intégré à pfSense ;
- Environnement de virtualisation **Proxmox VE (v9.0.1)** et son interface web d'administration
- Serveur de sauvegarde **Proxmox Backup Server (v4.0)** ;
- **Windows Server 2025** et ses rôles Active Directory / LDAPS ;
- Solution de messagerie **Microsoft Exchange 2019 (CU15)** ;
- Distributions **Linux Debian 13/12** et **Ubuntu 24.04.03 LTS** ;
- SGBD **MariaDB** et **MySQL** ;
- Solution de supervision réseau **Zabbix (7.4 LTS)** et agent Zabbix (7.0.x) ;
- Proxy **Artica 4.50** (ISO communautaire basé sur Debian 10) et son interface web ;
- Interface d'administration **UniFi** et portail captif intégré ;
- Solution de gestion de parc informatique **GLPI (v11.0)** ;
- Client VPN **OpenVPN (v2.6.7)** ;
- **RDP (Remote Desktop)** pour l'administration des serveurs AD et Hyper-V ;

1.3. SCHEMA LOGIQUE DE L'INFRASTRUCTURE ENVISAGÉE



2. PREMIÈRE REALISATION – FICHE REA 1

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026** **ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)** **Épreuve E5 - Administration des systèmes et des réseaux (option SISR)**

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 1**
Nom, prénom : IRATNI Hocine	**N° candidat : 02049749590**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** 06 / 06 / 2026
Organisation support de la réalisation professionnelle : Organisation fictive « DIGITEX » - Plot « S4P2 » IFC Marseille	
Intitulé de la réalisation professionnelle : Conception et mises en place d'une infrastructure réseau – Structure et configuration physique et logique des équipements réseaux et périphérique pour répondre aux critères de sécurité et organisationnelle de DIGITEX	
Période de réalisation : 10/2024 – 05/2026 **Lieu :** Centre de Formation IFC MARSEILLE, Plot S4P2 **Modalité :** ☒ **Seul(e)** ☐ **En équipe**	
Compétences travaillées ☒ Concevoir une solution d'infrastructure réseau ☒ Installer, tester et déployer une solution d'infrastructure réseau ☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau	

Conditions de réalisation[1] (ressources fournies, résultats attendus)

Ressources fournies :

- **Un PC avec clavier et souris USB, utilisé comme base pour construire et configurer l'infrastructure, et pour l'administration de celle-ci ;**
- **Un PC portable utilisé comme PC Client pour simuler des utilisateurs du SI (Système d'Information) de l'organisation ;**
- **Un PC avec un disque dur attribué à un serveur PROXMOX VE (environnement de virtualisation utilisé pour héberger et administrer des serveurs virtualisés) ;**
- **Un espace disque de stockage dédié aux serveurs virtuels PROXMOX sur un serveur de sauvegarde PROXMOX BACKUP ;**
- **Un PC avec un disque dur attribué à un serveur PFSENSE (routeur/Firewall) possédant 3 cartes dont une a 2 interface réseaux et donc 4 ports Ethernet ;**
- **Un PC avec un disque dur attribué à un serveur HYPER-V pour la virtualisation qui sera utilisé pour serveurs accessible de l'extérieur du réseau et mise à disposition de réseaux externes (comme un serveur WEB par exemple) ;**
- **Trois écrans VGA/HDMI ;**
- **Une prise Ethernet murale, reliée au réseau WAN de l'établissement IFC Marseille, représentant l'arrivée internet de l'organisation ;**
- **Des câbles Ethernet RJ45 en nombre suffisant ;**
- **Un switch NETGEAR GS308Ev4 à 8 ports ;**
- **Deux multiprises ;**
- **Des clés USB pour les installations de systèmes d'exploitation**
- **Un serveur NAS commun aux BTS SIO de l'établissement auquel nous avons accès via des identifiants personnels contenant des ressources indispensables à notre progression (cours, procédures, travaux d'autres étudiants, logiciels, etc.) ;**
- **Différentes solutions logicielles et applicatives disponible au téléchargement sur le WEB (voir ressources logicielles utilisées' dans la section 'description des ressources').**

Résultats attendus :

- **Un réseau local (LAN) qui soit :**

- Opérationnel - un routeur assure les communications entre les périphériques, ils peuvent communiquer entre eux, et accéder aux ressources du réseau local ainsi qu'à internet ;

- Sécurisé - un par un pare-feu situé entre le réseau local et l'extérieur filtre les échanges avec l'extérieur pour sécuriser le réseau local, ses serveurs et ses périphériques ;

- Cloisonné - le commutateur cœur de réseau partage ses ports à plusieurs réseaux locaux virtuels (VLAN) en fonction de critères organisationnelles et de sécurité informatique, le routeur gère les Communications inter-vlan et le pare-feu filtre les communications des sous-réseaux (entre eux et vers l'extérieur, de même que l'accès aux machines administratives du réseau).

- **Un environnement et des ressources de virtualisation :**

  Un environnement de virtualisation est mis en place (pour des questions de pratique, de simplicité de gestion et d'économie de ressources), un serveur physique PROXMOX est installé et configuré dans le réseau local permettant de créer et administrer des machines virtuelles, utilisé pour héberger différents serveurs du SI de l'organisation.

- **Des ressources informatiques gérées et mise à disposition des utilisateurs à travers Windows Active Directory (AD) :**
  Un environnement de travail Windows est mis à disposition des utilisateurs, avec l'accès à des dossiers partagés, des GPO (stratégies de groupes) permettant d'appliquer des règles, de donner l'accès à des ressources, de gérer les droits des utilisateurs sur leur environnement de travail et sur l'accès aux ressources. Cet environnement est possible par la mise en place d'un serveur Windows contrôleur de domaine (et sa réplique pour redondance), ainsi qu'un la création d'un domaine Active Directory, permettant à un ou plusieurs administrateurs de gérer les ressources numériques de l'organisation.
- **Un système de supervision des machines de l'infrastructure réseau :**
  Les machines sensibles du domaine contenant des données nécessaires au fonctionnement de l'organisation peuvent être supervisées au niveau matériel et logiciel de manière centralisé, sur un serveur Zabbix Supervision. C'est possible par la mise en place d'une machine virtuelle Debian sur laquelle est monté un serveur ZABBIX MONITORING, et par les agents Zabbix installés sur les machines à surveiller, et les métriques configurées sur le serveur, que l'agent va inspecter. Un administrateur peut sur une interface graphique analyser les métriques en temps réel et être alerter en cas de problème sur les machines.
- **Une gestion des accès des utilisateurs aux ressources du WEB via un Proxy :**
  Un proxy est configuré de sorte à se placer entre les utilisateurs et le WEB pour filtrer les requêtes, les URL destination, les sites non sécurisés ou proscrits par l'administrateur de l'organisation. La solution ARTICA Proxy est utilisée, un serveur PROXY est mis en place et configuré dans le réseau avec du filtrage d'URL (personnalisé pour l'organisation et par catégories) avec page de blocage Artica.

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

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

Ressources matériels et documentaires utilisées : (voir 'conditions de réalisations')

Ressources logicielles utilisées :

- Logiciel NETGEAR SWITCH DISCOVERY TOOL (1.2.103) ;
- Page WEB d'administration NETGEAR GS108Ev4 ;
- Logiciel BALENA ETCHER (1.18.11) pour la création de clé USB d'installation d'OS ;
- Solution Routeur-Firewall PFSENSE (2.8.1) – basé sur une distribution BSD OS ;
- Administration WEB PFSENSE ;
- Solution d'environnement de virtualisation PROXMOX VE (9.0.1) ;
- Page WEB d'administration PROXMOX VE ;
- PROXMOX BACKUP SERVER ;
- Soliton de sauvegarde des données des machines virtuelles PROXMOX BACKUP SERVER (4.0) ;
- OS Windows Sevrer 2025
- Gestion de ressource réseau Active Directory
- Distribution LINUX Debian 13/12 ;
- Gestion de base de données MariaDB et MySQL ;
- Solution de supervision réseau ZABBIX (7.4.2) ainsi que la version 7.4 de l'agent d'écoute ZABBIX ;
- Page WEB D'administration ZABBIX ;
- Solution Proxy ARTICA (version communautaire) ;
- Page WEB d'administration ARTICA ;
- SNORT IDS (sur pfSense).

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

Modalités d'accès aux productions[3] et à leur documentation[4]

Les différentes ressources de l'infrastructure sont accessibles par le poste administrateur dans le VLAN dédié à L'administration, sur des pages WEB d'administration (voir section 'répertoire identifiants et sessions' du dossier)

La documentation - mise à part le présent dossier – est disponible sur mon site portfolio dans la section :

https://iratnihocine.com

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

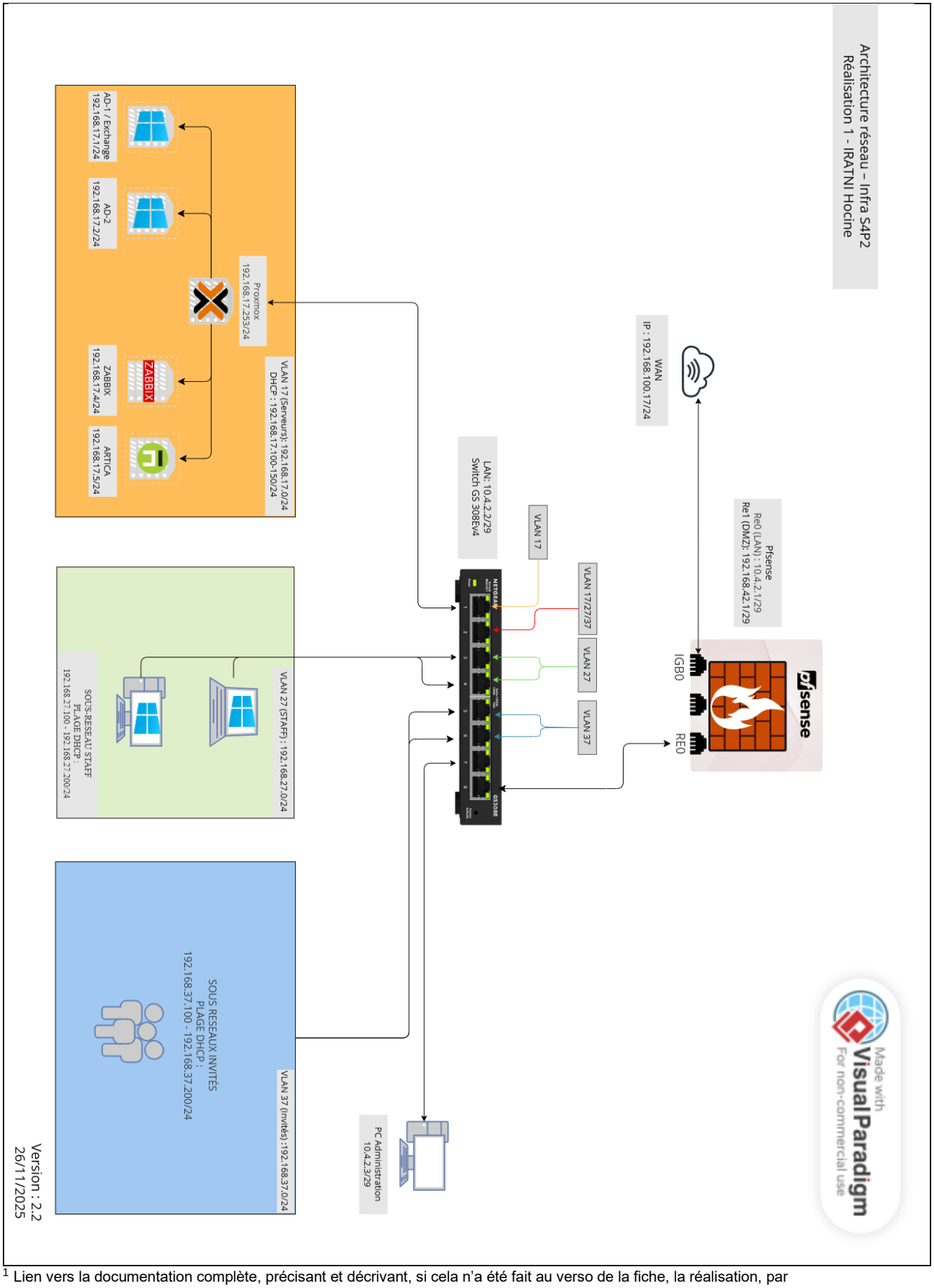
BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle
(verso, éventuellement pages suivantes)

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

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

Schéma de la réalisation :



[1] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

2.1. MISE EN PLACE DU CŒUR DE RÉSEAU

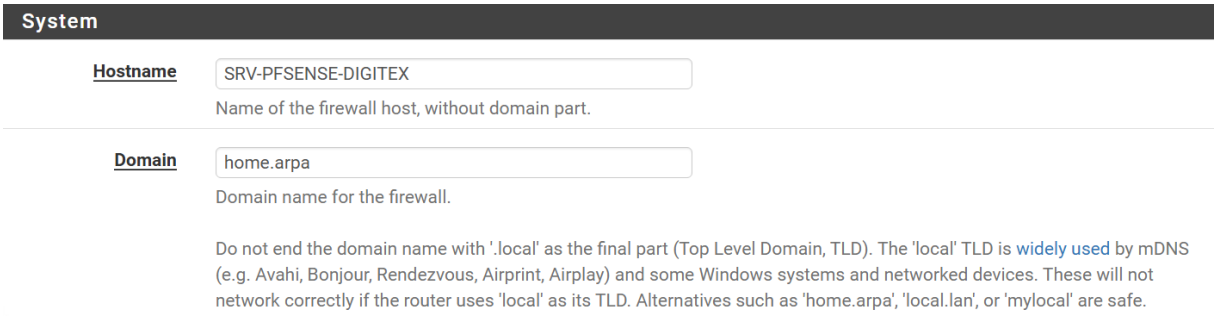
Dans le cadre de l'entreprise fictive **DIGITEX**, l'objectif est de déployer une infrastructure réseau complète, organisée et sécurisée. Le réseau doit permettre aux collaborateurs d'accéder aux différents services informatiques nécessaires à leurs activités (messagerie, partage de fichiers, applications métier...) tout en assurant la disponibilité des ressources essentielles au bon fonctionnement de l'organisation.

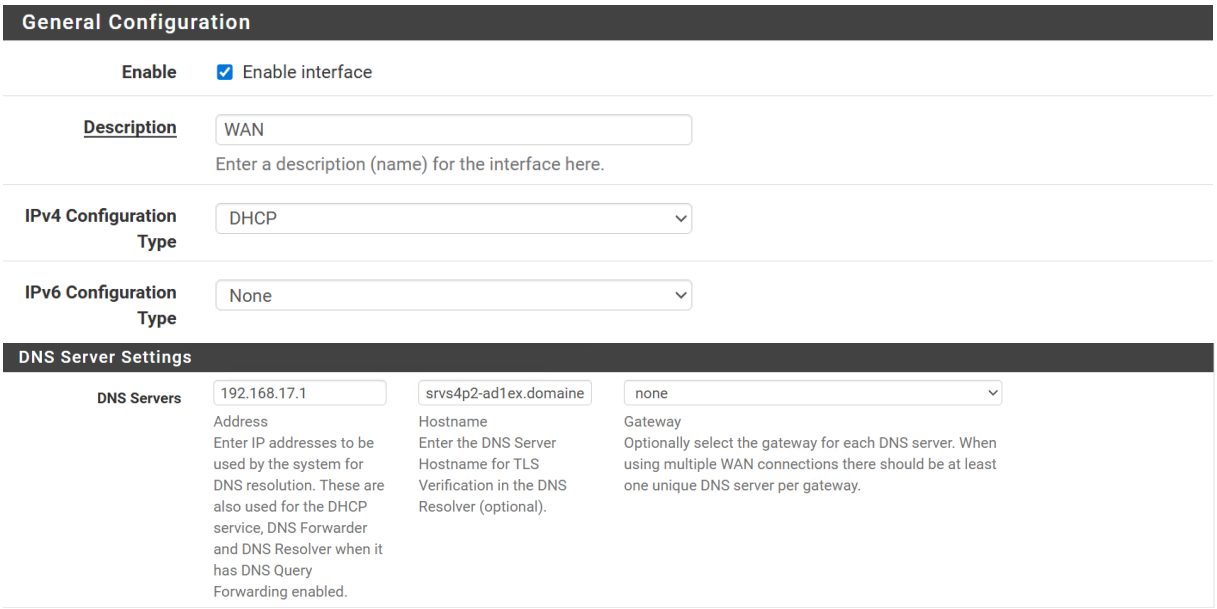
La mise en place inclut également la mise en œuvre de mécanismes de protection contre les menaces internes et externes, ainsi qu'un système de supervision et d'administration centralisée afin de garantir une gestion efficace et fiable du SI.

2.1.2. CONFIGURATIONS GÉNÉRALES PFSENSE

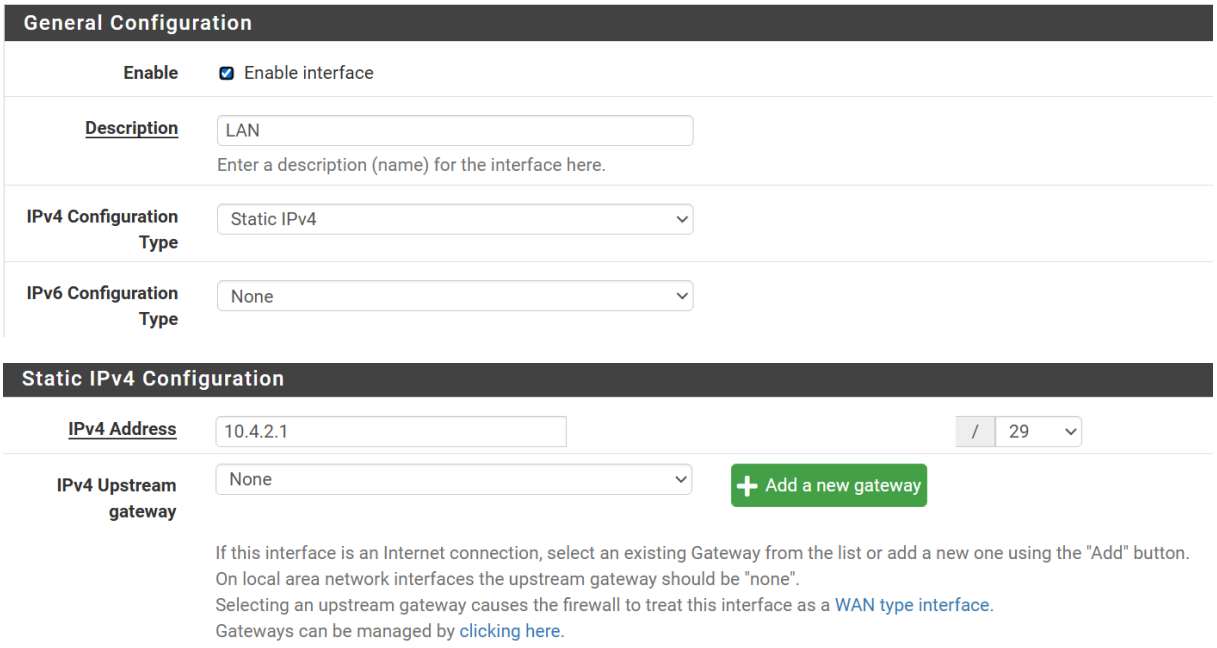
Le pare-feu **pfSense** constitue l'élément central du réseau. Ses configurations de base sont les suivantes :

- L'interface **WAN** est paramétrée pour obtenir automatiquement une adresse IPv4 via DHCP. L'adresse IP est réservée sur le routeur de l'IFC et attribuée en fonction de l'adresse MAC de la carte réseau du serveur pfSense.
- L'interface **LAN** est configurée sur le sous-réseau **10.4.2.0/29**, qui sert de réseau interne pour l'infrastructure de l'organisation

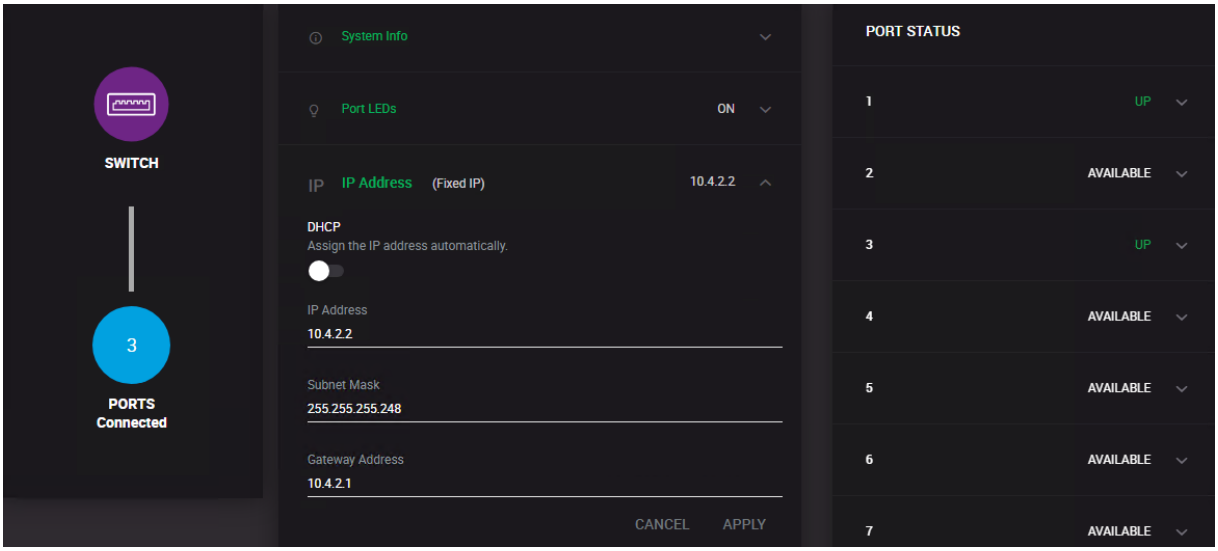




2.1.2. CONFIGURATIONS INTERFACE LAN



2.1.3. CONFIGURATIONS GÉNÉRALES COMMUTATEUR NETGEAR

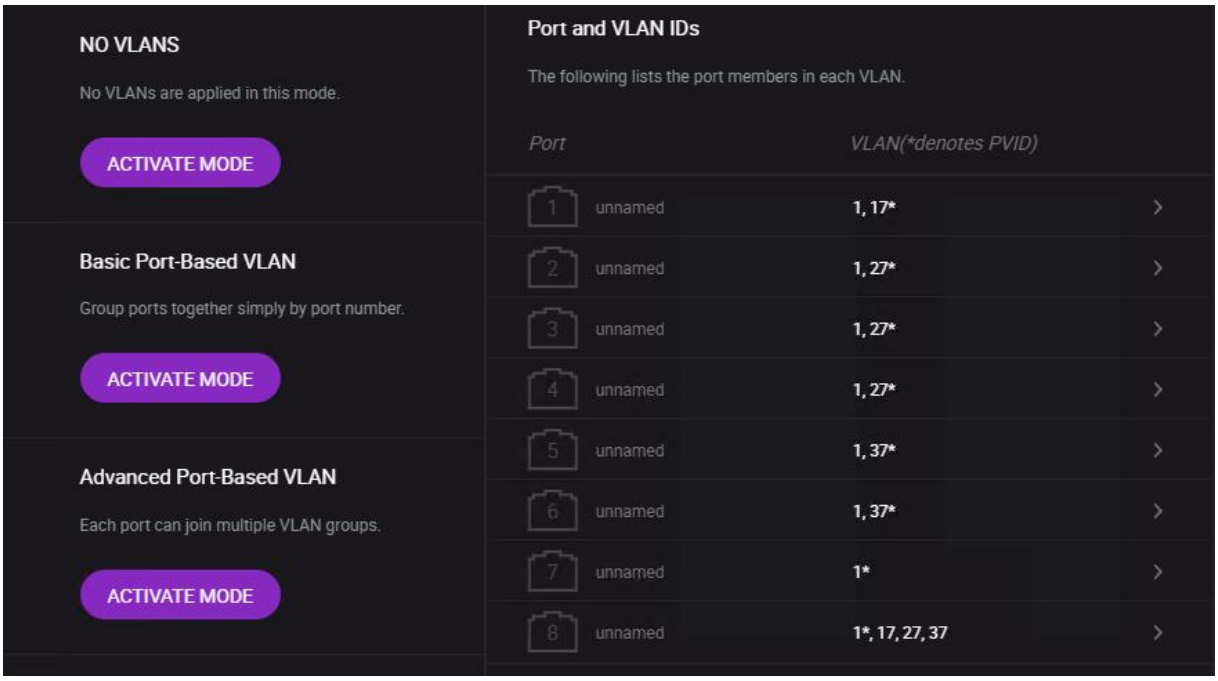


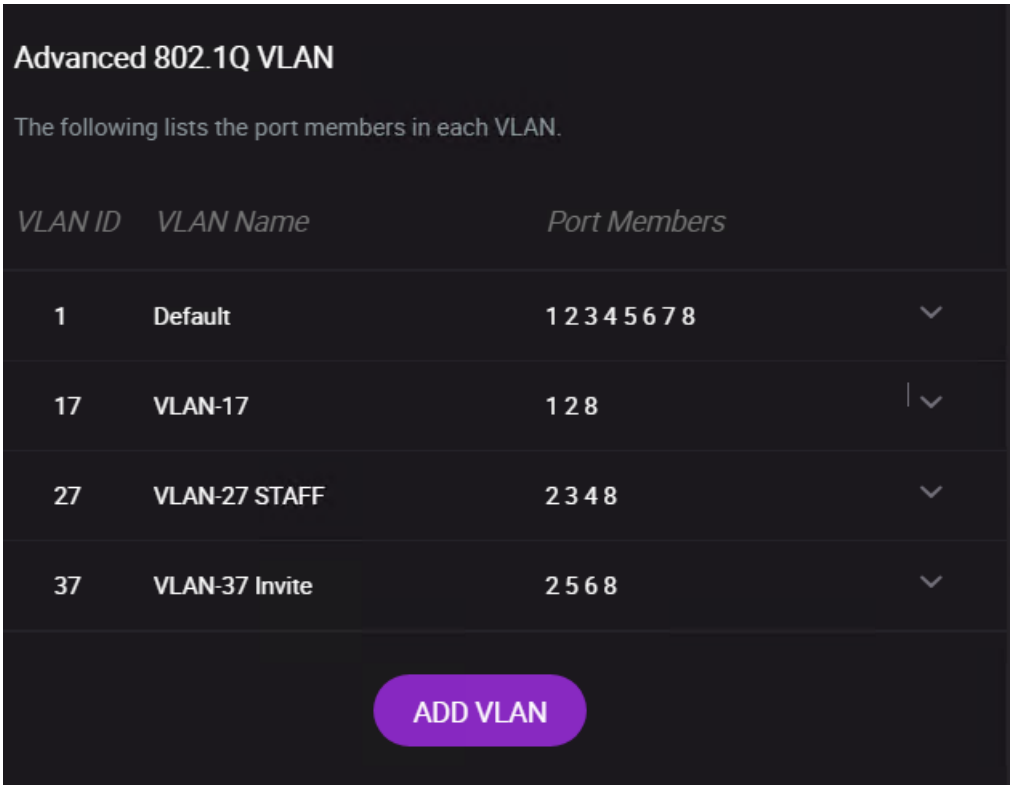
2.1.4. CONFIGURATION VLAN ID / PORTS PVID

Pour répondre aux besoins de l'entreprise **DIGITEX**, l'infrastructure réseau a été segmentée en plusieurs VLAN, chacun jouant un rôle spécifique et des règles de filtrage adaptées :

- **VLAN 17 – Serveurs** : regroupe les serveurs virtualisés sur l'hyperviseur **Proxmox VE**. Ce VLAN assure l'isolation des services critiques tout en permettant leur administration sécurisée.
- **VLAN 27 – Staff** : destiné aux collaborateurs de l'entreprise et à leurs périphériques (postes de travail, ordinateurs portables, imprimantes…).
- **VLAN 37 – Invités** : dédié aux utilisateurs temporaires se connectant via le point d'accès Wi-Fi. L'accès est limité grâce à un **portail captif**, garantissant la sécurité du réseau interne.

Le **poste d'administration** est directement connecté au **port 7 du switch**, qui n'est associé à aucun VLAN. Ce port permet à l'administrateur de gérer l'ensemble du réseau et des applications de manière sécurisée. La sécurité reste assurée par le **pare-feu pfSense**, qui contrôle les flux et protège l'infrastructure contre les menaces internes et externes.


NO VLANS
No VLANs are applied in this mode.
ACTIVATE MODE
Basic Port-Based VLAN
Group ports together simply by port number.
ACTIVATE MODE
Advanced Port-Based VLAN
Each port can join multiple VLAN groups.
ACTIVATE MODE
Port and VLAN IDs
The following lists the port members in each VLAN.
Port
VLAN(*denotes PVID)
1 unnamed 1, 17*
2 unnamed 1, 27*
3 unnamed 1, 27*
4 unnamed 1, 27*
5 unnamed 1, 37*
6 unnamed 1, 37*
7 unnamed 1*
8 unnamed 1*, 17, 27, 37


Advanced 802.1Q VLAN
The following lists the port members in each VLAN.
VLAN ID
VLAN Name
Port Members
1 Default 1 2 3 4 5 6 7 8
17 VLAN-17 1 2 8
27 VLAN-27 STAFF 2 3 4 8
37 VLAN-37 Invite 2 5 6 8
ADD VLAN

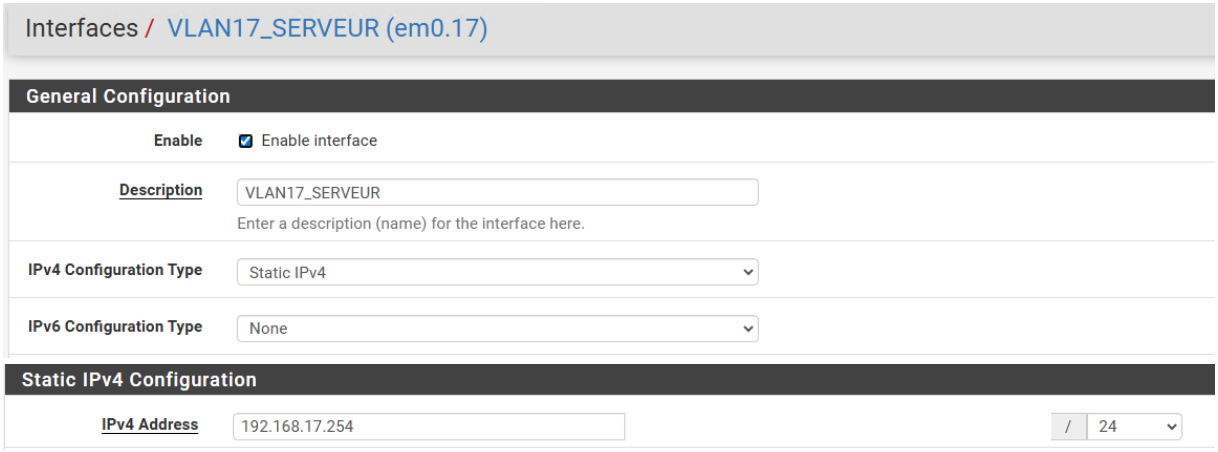
2.1.5 CONFIGURATIONS INTERFACES VLAN SUR LE PFSENSE

Côté routeur (pfSense), la segmentation a été concrétisée par la création de **3 interfaces virtuelles (VLANs)**, rattachées à l'interface physique LAN. Ces interfaces correspondent aux ID de VLAN définis sur le commutateur Netgear.

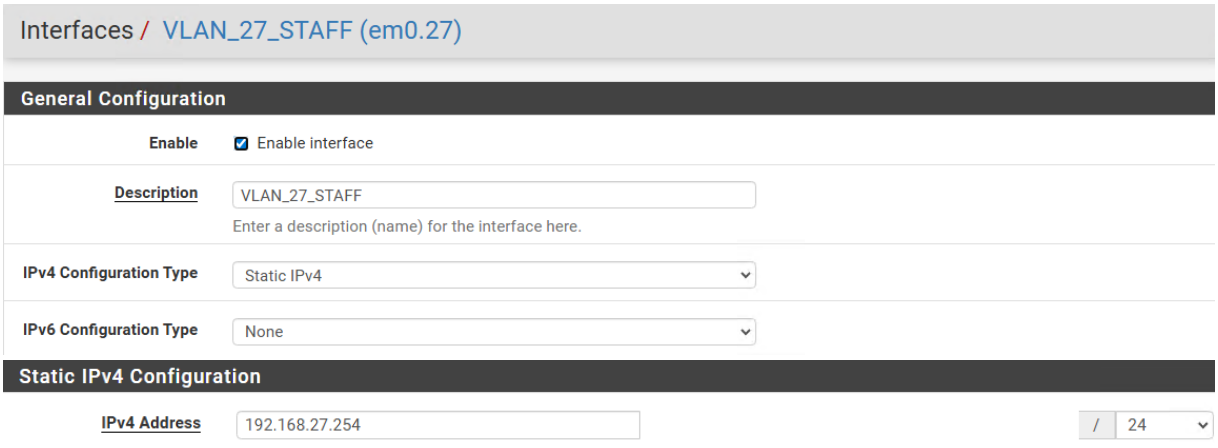
Pour assurer le routage inter-VLAN, chacune de ces interfaces virtuelles a été configurée avec une **adresse IPv4 statique**, servant de passerelle par défaut pour chaque sous-réseau distinct.

VLAN_37_INVITE	↑	1000baseT <full-duplex>	192.168.37.254
VLAN17_SERVEUR	↑	1000baseT <full-duplex>	192.168.17.254
VLAN_27_STAFF	↑	1000baseT <full-duplex>	192.168.27.254

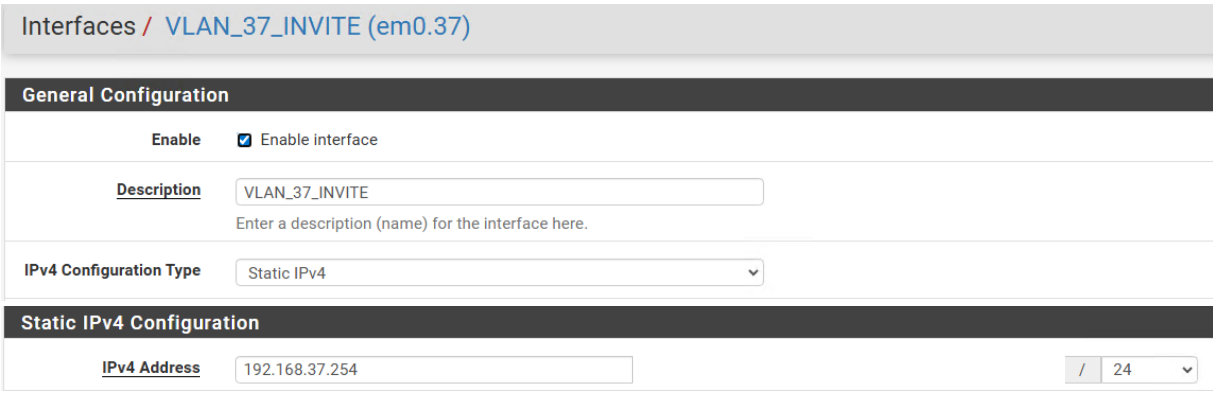
VLAN17 :



VLAN27 :



VLAN37 :



2.1.6. RÈGLES DE FITLRAGE INTER-VLANS

Afin de garantir la sécurité du Système d'Information, les règles de flux inter-VLAN ont été définies selon le principe du moindre privilège :

- **VLAN 17 (Serveurs / Administration) :** Ce réseau héberge les services critiques de l'infrastructure (notamment le Contrôleur de Domaine assurant les rôles DNS et DHCP).
    - **Flux sortants :** Ce VLAN dispose d'une **autorisation totale** pour initier des connexions vers l'ensemble des autres segments du réseau, afin d'assurer l'administration et la maintenance.
    - **Flux entrants :** L'accès à ce VLAN est strictement filtré et limité aux seuls services nécessaires pour les clients.

- **VLAN 37 (Invités / Wi-Fi Invité) :** Ce réseau est considéré comme non fiable et doit être **strictement cloisonné**.
    - **Isolation :** Tout accès vers les réseaux internes (LAN, VLAN 17, VLAN 27) est **bloqué par défaut**.
    - **Exceptions autorisées :** Seuls les protocoles indispensables au fonctionnement de la connectivité client sont autorisés vers les serveurs dédiés : **DNS** (Port 53), **DHCP** (Ports 67) et le **Portails Captif**, et la navigation web
    - **Sécurité critique :** L'accès aux interfaces de gestion des équipements de cœur de réseau (interface web/SSH du pfSense et des commutateurs) est formellement **interdit**.

- **VLAN 27 (Utilisateurs / Production) :** Ce réseau regroupe les postes de travail standards.
    - **Accès :** Les flux sont autorisés uniquement vers les services métiers et transverses nécessaires à l'activité.
    - **Protection du plan d'administration :** À l'instar du réseau Invités, l'accès aux interfaces d'administration des équipements réseau (Gateway, Switchs) est **bloqué** pour prévenir toute tentative de configuration non autorisée.

VLAN17 – SERVEURS :

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	39/38.56 GiB	IPv4 *	*	*	*	*	none			

VLAN27 – STAFF :

Floating | WAN | LAN | DMZ | VLAN_37_INVITE | VLAN17_SERVEUR | VLAN_27_STAFF | OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0/0 B	IPv4 UDP	VLAN_27_STAFF subnets	*	192.168.17.6	10000 - 20000	*	none		ALLOW_RTP_XIVO_VoIP	
☐	✓	0/0 B	IPv4 TCP/UDP	VLAN_27_STAFF subnets	*	192.168.17.6	5060 (SIP)	*	none		ALLOW_SIP_XIVO_VoIP	
☐	✓	0/8.41 MiB	IPv4 TCP	VLAN_27_STAFF subnets	*	192.168.17.3	80 (HTTP)	*	none		ALLOW_WEB_GLPI	
☐	✓	0/2.27 GiB	IPv4 TCP	VLAN_27_STAFF subnets	*	192.168.17.5	3128	*	none		ALLOW_ARTICA_PROXY	
☐	✓	0/0 B	IPv4 TCP	VLAN_27_STAFF subnets	*	192.168.17.5	9025	*	none		ALLOW_ARTICA_ERROR_PAGE	
☐	✗	0/2 KiB	IPv4 *	VLAN_27_STAFF subnets	*	192.168.17.253	*	*	none		BLOCK_CONNECTION_PROXMOX	
☐	✗	0/2 KiB	IPv4 *	VLAN_27_STAFF subnets	*	192.168.17.4	*	*	none		BLOCK_CONNECTION_ZABBIX	
☐	✗	0/0 B	IPv4 *	VLAN_27_STAFF subnets	*	VLAN_37_INVITE subnets	*	*	none		BLOCK_CONNECTION_VLAN37_INVITE	
☐	✗	0/2 KiB	IPv4 TCP	VLAN_27_STAFF subnets	*	10.4.2.2	Netgear_HTTPS_HTTP	*	none		BLOCK_NETGEAR_WEB	
☐	✗	0/0 B	IPv4 TCP/UDP	VLAN_27_STAFF subnets	*	This Firewall (self)	22 (SSH)	*	none		BLOCK_PFSENSE_SSH	

✕	0/3 KiB	IPv4 TCP	VLAN_27_STAFF subnets	*	This Firewall (self)	80 (HTTP)	*	none	BLOCK_PFSENSE_WEB_HTTP	
✕	0/2 KiB	IPv4 TCP/UDP	VLAN_27_STAFF subnets	*	This Firewall (self)	443 (HTTPS)	*	none	BLOCK_PFSENSE_WEB_HTTPS	
✕	0/312 B	IPv4 TCP/UDP	VLAN_27_STAFF subnets	*	Server_Active_Directory	3389 (MS RDP)	*	none	BLOCK_CONNECTION_RDP_AD1-AD2	
✓	4/165.03 MiB	IPv4 *	VLAN_27_STAFF subnets	*	Server_Active_Directory	*	*	none	ALLOW_AD1_AD2	
✓	20/2.65 GiB	IPv4 *	*	*	*	*	*	none		

VLAN37 – INVITÉS :

Floating | WAN | LAN | DMZ | VLAN_37_INVITE | VLAN17_SERVEUR | VLAN_27_STAFF | OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	5/2.61 MiB	IPv4 TCP	VLAN_37_INVITE subnets	*	192.168.17.7	UniFi_Portail_Captif	*	none		ALLOW_PORTAILS_CAPTIF_UNIFI	
✓	0/0 B	IPv4 UDP	VLAN_37_INVITE subnets	*	This Firewall (self)	67	*	none		ALLOW_DHCP_REQUEST	
✕	0/0 B	IPv4 TCP	VLAN_37_INVITE subnets	*	This Firewall (self)	22 (SSH)	*	none		BLOCK_PFSENSE_SSH	
✕	0/0 B	IPv4 TCP	VLAN_37_INVITE subnets	*	This Firewall (self)	80 (HTTP)	*	none		BLOCK_PFSENSE_WEB_HTTP	
✕	0/0 B	IPv4 TCP	VLAN_37_INVITE subnets	*	This Firewall (self)	443 (HTTPS)	*	none		BLOCK_PFSENSE_WEB_HTTPS	
✕	0/0 B	IPv4 TCP	VLAN_37_INVITE subnets	*	10.4.2.2	Netgear_HTTPS_HTTP	*	none		BLOCK_CONNECTION_NETGEAR	
✕	0/0 B	IPv4 *	VLAN_37_INVITE subnets	*	VLAN_27_STAFF subnets	*	*	none		BLOCK_CONNECTION_VLAN27_STAFF	
✕	0/0 B	IPv4 *	VLAN_37_INVITE subnets	*	VLAN17_SERVEUR subnets	*	*	none		BLOCK_CONNECTION_VLAN17_SERVEUR	
✓	0/0 B	IPv4 UDP	VLAN_37_INVITE subnets	*	*	53 (DNS)	*	none		ALLOW_DNS_OVER_INTERNET	
✓	0/27.47 MiB	IPv4 *	*	*	*	*	*	none			

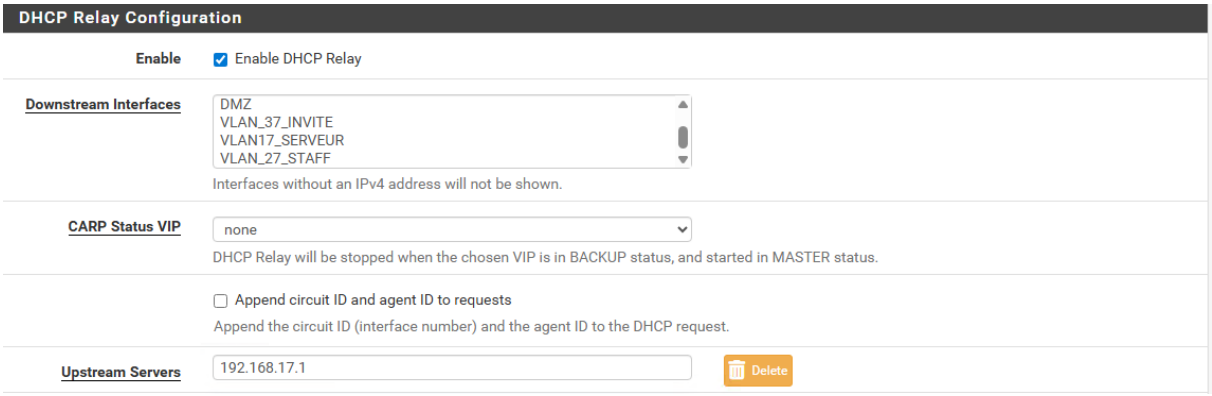
2.1.7. LOGS DE FILTRAGE PARE-FEU

Afin d'assurer une traçabilité complète et une supervision efficace du réseau, la journalisation (logging) a été activée systématiquement sur l'ensemble des règles de filtrage. Cette mesure permet d'analyser les flux en temps réel, de diagnostiquer les incidents et d'affiner la politique de sécurité.

2.1.8. CONFIGURATION RELAIS DHCP

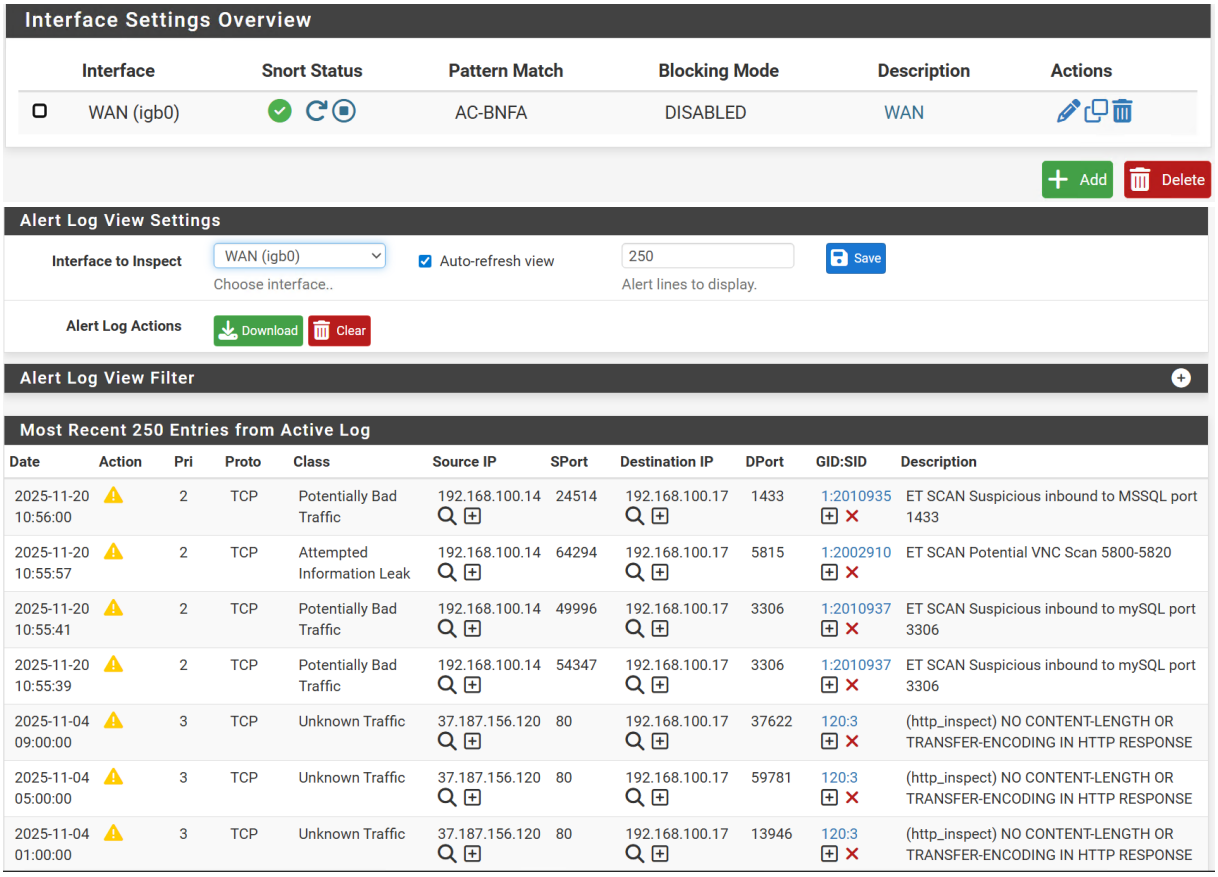
La sécurité est assurée par un filtrage strict et journalisé des flux. Pour centraliser la gestion, la fonction de **Relais DHCP** a été configurée sur les interfaces virtuelles VLAN 17-27-37 : elle redirige les requêtes vers les contrôleurs de domaine (AD1 et AD2),

garantissant l'intégration cohérente des services IP et DNS avec l'annuaire Active Directory.

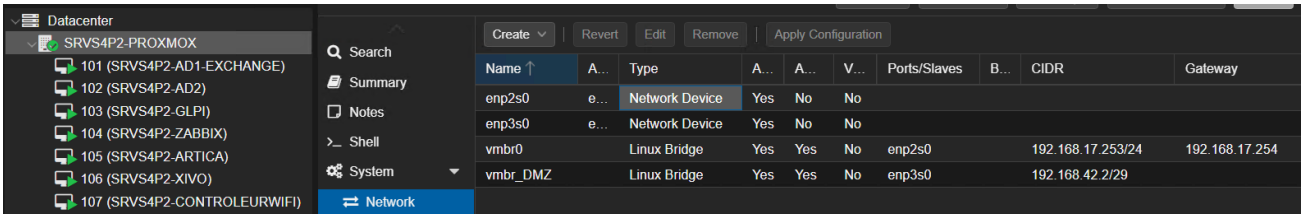


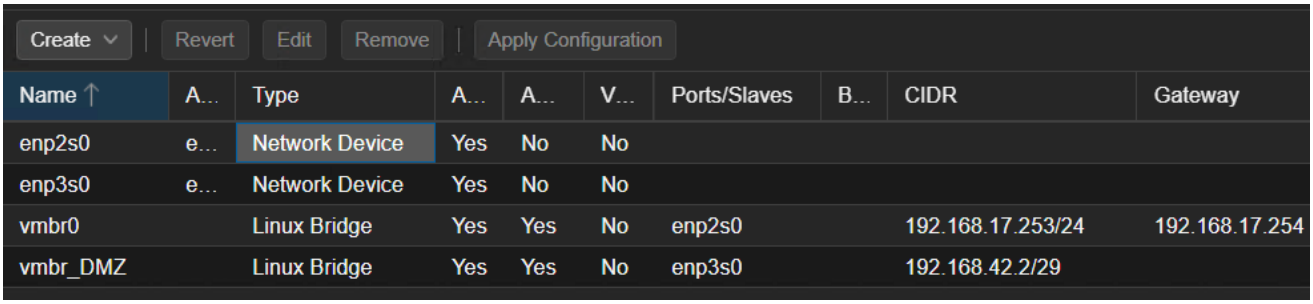
2.1.9. DETECTION/PREVENTION D'INTRUSIONS SNORT :

Nous avons déployé le système de détection et de prévention d'intrusions (IDS/IPS) **Snort** directement sur le pare-feu pfSense. Configuré pour écouter sur l'interface WAN, il analyse les flux en temps réel et génère des alertes lors de la détection d'activités suspectes, en s'appuyant sur les jeux de règles officiels préétablis.



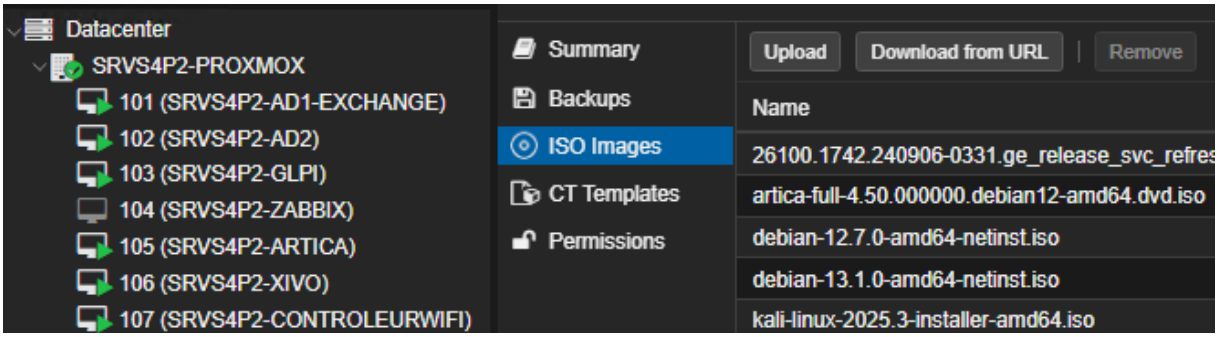
2.2.1 PARAMETRAGE GLOBAL DE L'HYPERVISEUR PROXMOX





2.2.2. GESTION DES RESSOURCES : IMAGES ISO ET MACHINES VIRTUELLES

Nous avons constitué une bibliothèque d'images ISO sur le nœud Proxmox. Ces fichiers sources sont indispensables au déploiement des serveurs virtuels pour l'infrastructure de l'organisation Digitex



Nous présentons ci-après les différentes machines virtuelles, dont la configuration et le rôle seront détaillés individuellement dans les sections suivantes.

2.3. SEVREURS WINDOWS ACTIVE DIRECTORY, CONTROLLEURS DE DOMAINE, SERVICES ET OBJETS AD

Active Directory (AD) constitue le service d'annuaire central de notre infrastructure s4p2. Cette solution nous permet de gérer de manière centralisée l'ensemble des ressources, des utilisateurs et des postes de travail au sein de notre domaine domaines4p2.local. Elle est également essentielle pour le déploiement et l'application des politiques de sécurité (GPO) sur l'ensemble du parc informatique.

Pour garantir la haute disponibilité des services d'authentification, notre architecture s'appuie sur deux contrôleurs de domaine, virtualisés sur notre hyperviseur Proxmox au sein du VLAN 17 :

1. AD-1 (à l'adresse 192.168.17.1/24)

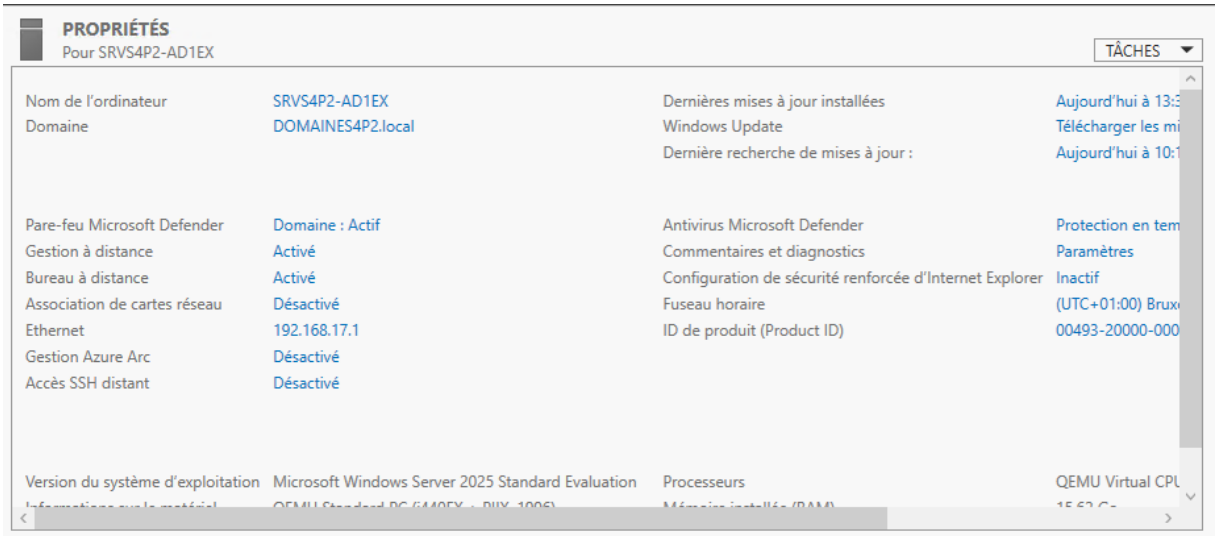
2.AD-2 (à l'adresse 192.168.17.2/24)

Le serveur AD-1 a été configuré en tant que contrôleur de domaine principal pour le domaine. Le serveur AD-2 a ensuite été monté en tant que contrôleur de domaine secondaire.

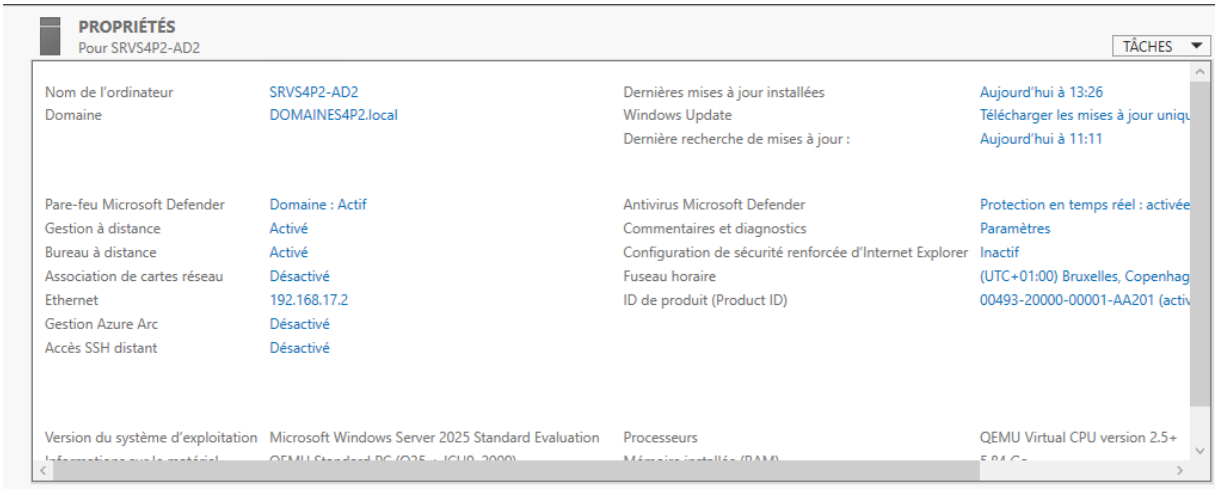
Ce dernier agit comme une réplique, synchronisant automatiquement l'ensemble des données et services de l'annuaire LDAPS depuis AD-1. Ce mécanisme de réplication assure qu'en cas de défaillance du serveur principal, le second contrôleur prendra le relais de manière transparente, garantissant ainsi la continuité des services d'authentification et d'accès aux ressources pour les utilisateurs

2.3.1. CONFIGURATIONS GÉNÉRALES WINDOWS SERVER

CONFIGURATIONS GÉNÉRALES AD 1 :



CONFIGURATIONS GÉNÉRALES AD 2 :

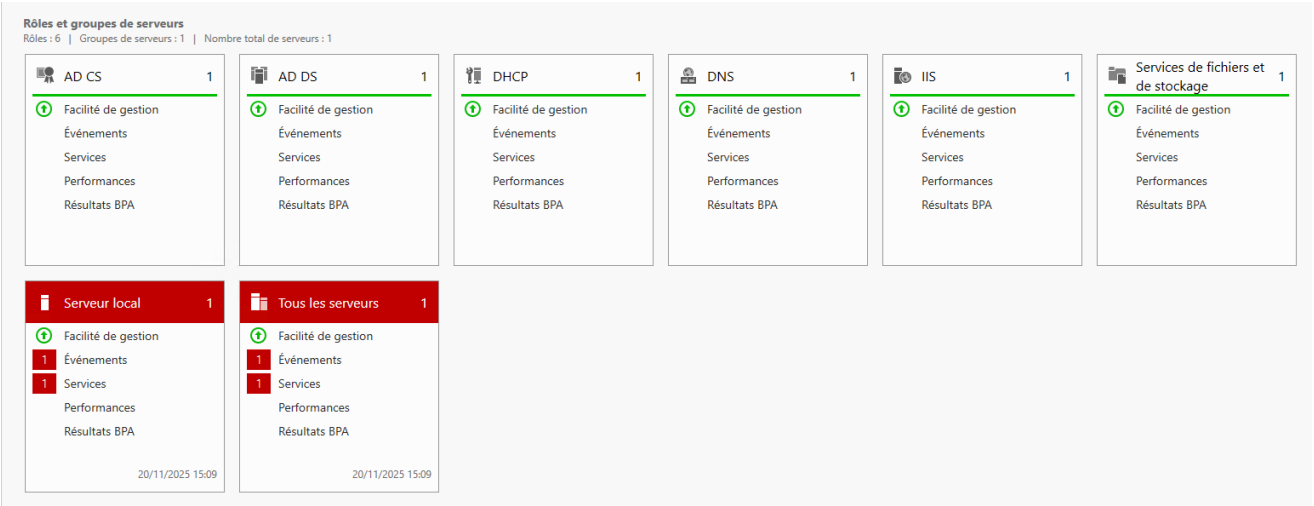


2.3.2. ARCHITECTURE DES SERVICES ET ROLES ACTIVE DIRECTORY

Le serveur **SRVS4P2-AD1EX** a été promu contrôleur de domaine principal via le rôle **AD DS**, actant la création du domaine domaines4p2.local.

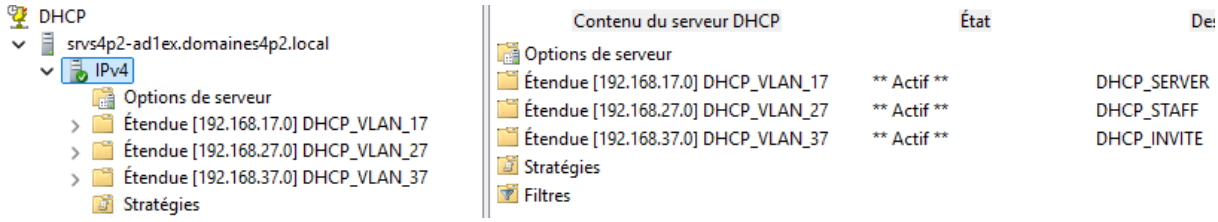
L'ensemble du parc informatique Windows de l'organisation a été joint à ce domaine, en utilisant ce contrôleur comme serveur DNS primaire. Cette centralisation nous permet désormais de gérer les comptes utilisateurs, les groupes de sécurité et d'appliquer des stratégies de groupe (**GPO**) pour standardiser l'environnement de travail des collaborateurs.

Enfin, dans une optique de sécurisation des échanges, nous avons installé le rôle d'Autorité de Certification (**AD CS**). Cette brique essentielle permet de chiffrer les communications de l'annuaire via le protocole **LDAPS** (LDAP over SSL).

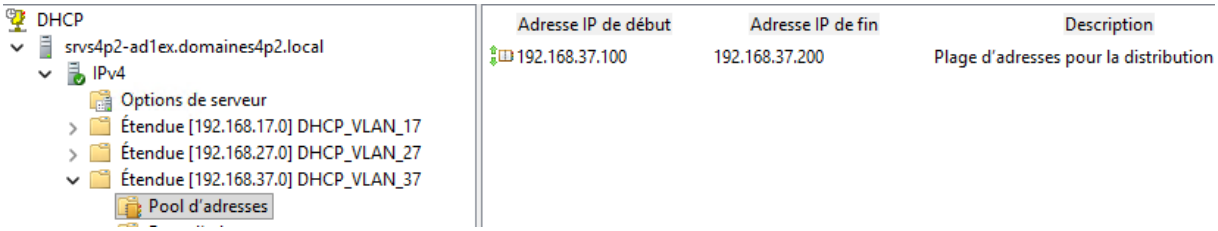


- **DHCP**

En cohérence avec le relais DHCP configuré sur le pfSense, nous avons déployé les rôles DHCP et DNS sur le serveur. La configuration a été établie pour servir les trois VLANs de l'organisation, via la création de trois **étendues** (scopes) d'adresses distinctes.



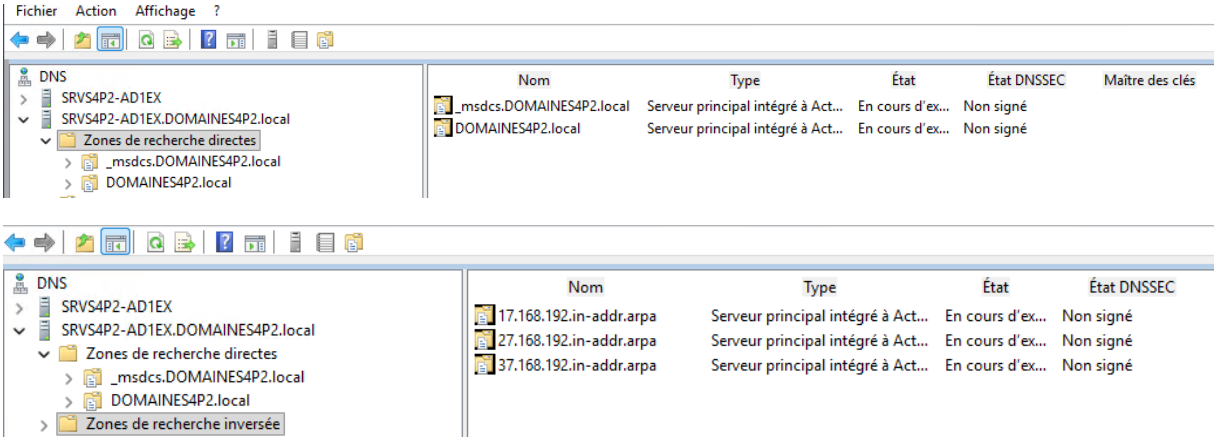
- **Démonstration de l'étendue VLAN 37 :**



- **Configuration des zones DNS et gestion des enregistrements :**

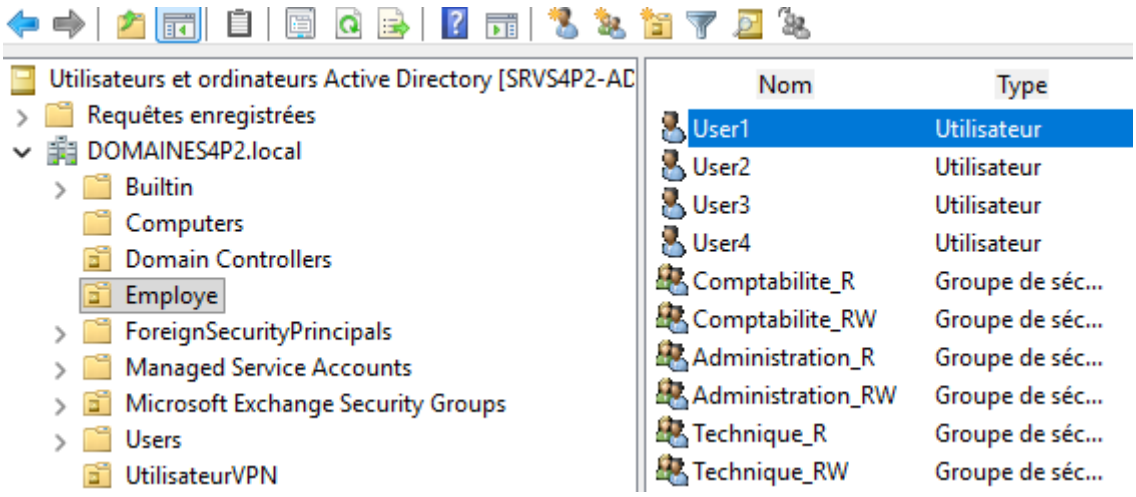
Le service DNS constitue la pierre angulaire du réseau. Au-delà de l'accès à Internet, il est indispensable à la résolution des noms d'hôtes internes, condition *sine qua non* au bon fonctionnement d'Active Directory.

Nous avons ainsi configuré les **zones de recherche directe** pour la résolution Nom vers IP, ainsi que les **zones de recherche inversée** (Reverse Lookup) pour couvrir les deux sous-réseaux de l'organisation DIGITEX.



2.3.3. UNITE D'ORGANISATION, UTILISATEURS ET GROUPES D'UTILISATEURS :

Une Unité d'Organisation (OU) dédiée au personnel a été créée afin de centraliser les comptes utilisateurs et les machines associées. Les utilisateurs y ont été provisionnés avec des identifiants et des mots de passe conformes à la politique de sécurité Active Directory en vigueur. Parallèlement, des groupes de sécurité ont été institués pour rationaliser l'attribution des droits d'accès aux ressources et cibler l'application des stratégies de groupe (GPO)



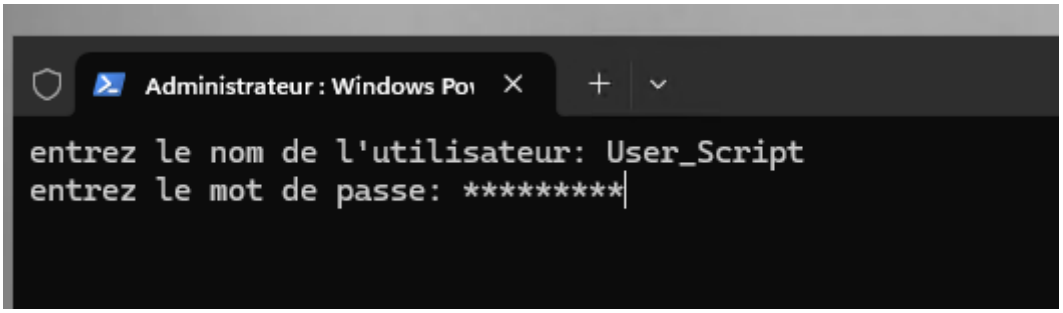
2.3.4 SCRIPT POWERSHELL – CREATION D'UTILISATEURS :

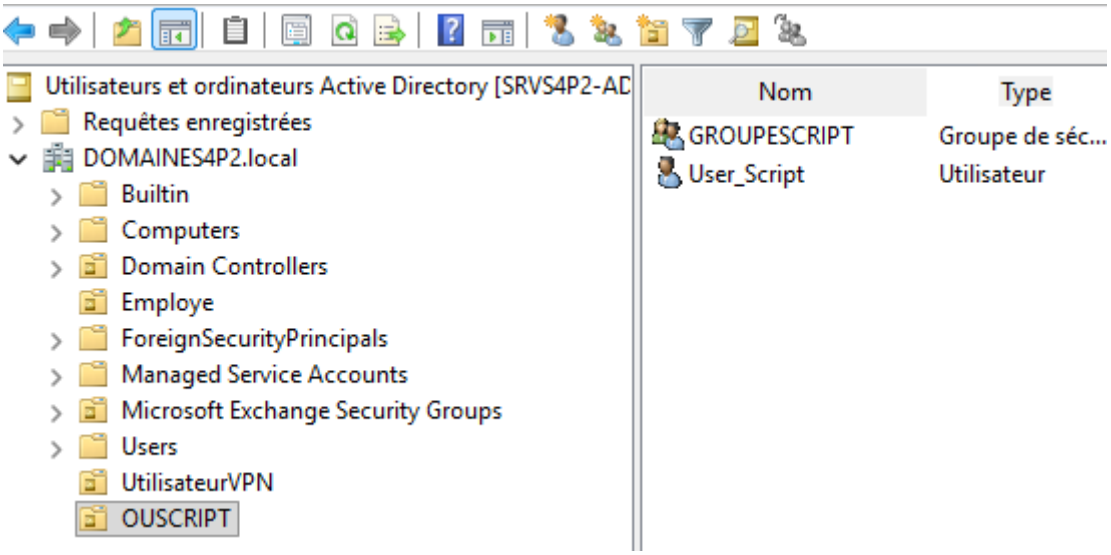
Afin de rationaliser le processus de provisionnement des comptes, un script d'automatisation a été développé. Il permet la création rapide d'utilisateurs directement dans l'Unité d'Organisation cible (actuellement définie sur 'OUSCRIPT' pour l'environnement de test) et leur intégration automatique au groupe de sécurité approprié ('GROUPESCRIPT'). Ce script intègre également la capacité de créer des boîtes aux lettres Exchange, fonctionnalité qui sera détaillée ultérieurement.

Administrateur : Windows PowerShell ISE (x86)

Fichier Modifier Afficher Outils Déboguer Composants additionnels Aide

```powershell
Import-Module ActiveDirectory
# Chargement des commandes Exchange
Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn -ErrorAction SilentlyContinue

$Name = Read-Host "entrez le nom de l'utilisateur"
$Password = Read-Host "entrez le mot de passe" -AsSecureString

# 1. Création de l'utilisateur AD
New-ADUser -Name $Name `
-GivenName "SCRIPT" `
-DisplayName "SCRIPT $Name" `
-Surname $Name `
-SamAccountName $Name `
-UserPrincipalName "$Name@domaines4p2.local" `
-AccountPassword $Password `
-Path "OU=OUSCRIPT,DC=domaines4p2,DC=local" `
-PasswordNeverExpires $true `
-CannotChangePassword $true `
-Enabled $true

# 2. Ajout au groupe de sécurité
Add-ADGroupMember -Identity GROUPESCRIPT -Members $Name
Write-Host "Utilisateur créé, attente de synchronisation..." -ForegroundColor Yellow
Start-Sleep -Seconds 3

# 3. Création de la boîte mail Exchange
Enable-Mailbox -Identity $Name
Write-Host "L'utilisateur $Name et sa boîte mail ont bien été créés avec succées!" -ForegroundColor Green
```





2.3.5. DOSSIER PARTAGES EN RESEAU AVEC DROITS D'ACCÈS

Afin de répondre aux besoins de travail collaboratif, une architecture de fichiers centralisée a été mise en place. Les données sont hébergées sur une partition dédiée du serveur Windows, au sein d'un répertoire racine nommé 'PARTAGE'. L'accès aux différents sous-dossiers est strictement contrôlé via des permissions (NTFS) attribuées selon les droits des collaborateurs.

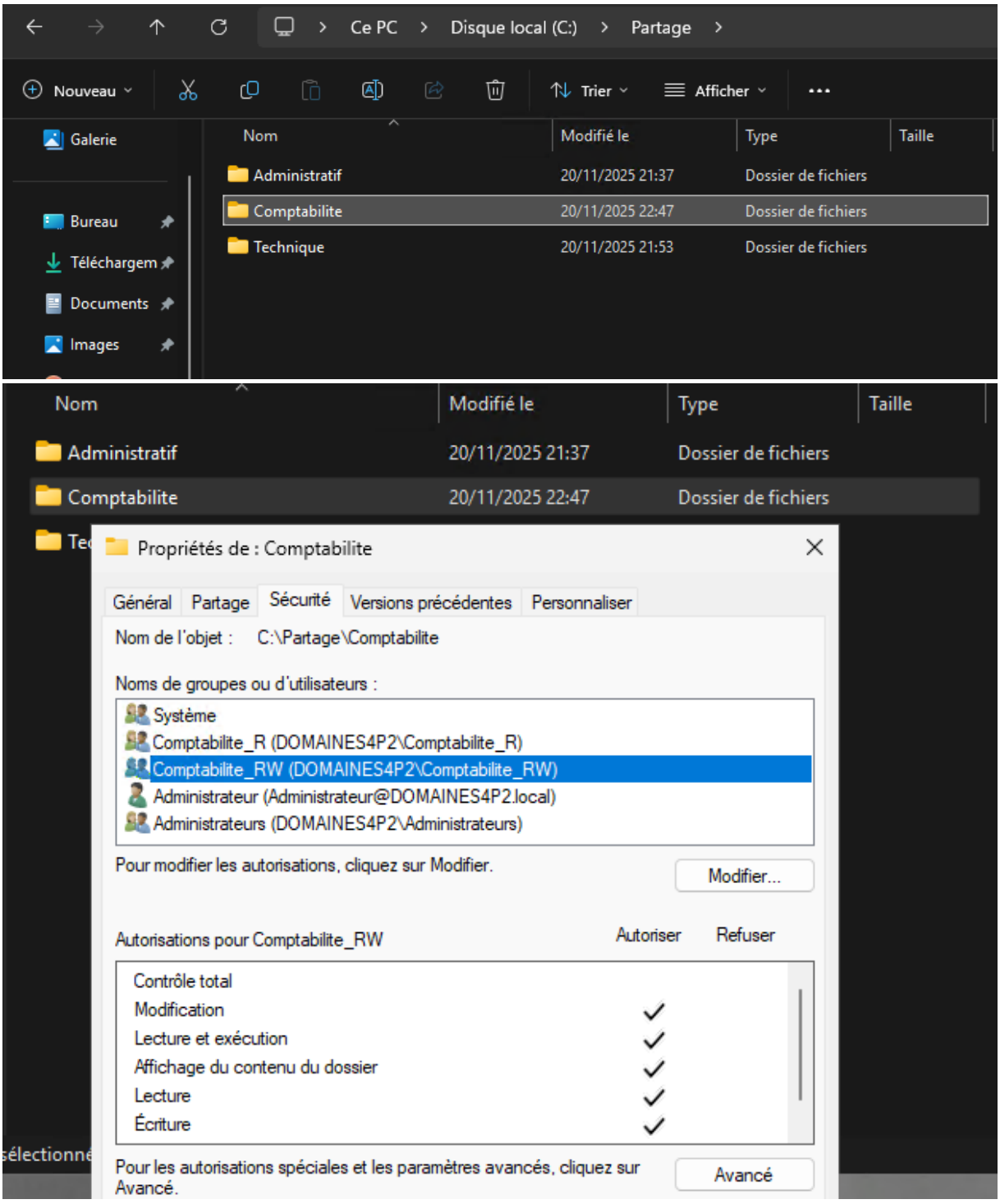
L'architecture de fichiers est organisée par département, avec une gestion fine des espaces privatifs :

- **Dossiers de service :** Des dossiers racines dédiés ('COMPTABILITE' et 'ADMINISTRATIF') ont été créés. Les groupes de sécurité correspondants (“COMPTABILITE_RW” et “ADMINISTRATIF_RW”) y disposent de droits de lecture/écriture (Modification) pour le travail collaboratif.

  Quant au groupe “COMPTABILITE_R” et “ADMINISTRATIF_R” disposent uniquement des droits de lecture pour respectivement les dossier partagé “Comptabilité” et “Administratif”

- **Espaces personnels :** Au sein de chaque dossier de service, des sous-dossiers individuels ont été configurés pour chaque utilisateur (ex: USER 1, USER 2). Sur ces dossiers personnels, seul l'utilisateur propriétaire dispose d'un accès 'Contrôle total', garantissant la confidentialité de ses données.

- **Cloisonnement :** Une stricte ségrégation est appliquée via les permissions NTFS : les membres du groupe Comptabilité n'ont aucun accès au dossier Administratif, et inversement."


Ce PC
Disque local (C:)
Partage
Nouveau
Trier
Afficher
Galerie
Bureau
Téléchargem
Documents
Images
Nom
Modifié le
Type
Taille
Administratif
20/11/2025 21:37
Dossier de fichiers
Comptabilite
20/11/2025 22:47
Dossier de fichiers
Technique
20/11/2025 21:53
Dossier de fichiers
Propriétés de : Comptabilite
Général
Partage
Sécurité
Versions précédentes
Personnaliser
Nom de l'objet : C:\Partage\Comptabilite
Noms de groupes ou d'utilisateurs :
Système
Comptabilite_R (DOMAINES4P2\Comptabilite_R)
Comptabilite_RW (DOMAINES4P2\Comptabilite_RW)
Administrateur (Administrateur@DOMAINES4P2.local)
Administrateurs (DOMAINES4P2\Administrateurs)
Pour modifier les autorisations, cliquez sur Modifier.
Modifier...
Autorisations pour Comptabilite_RW
Autoriser
Refuser
Contrôle total
Modification
Lecture et exécution
Affichage du contenu du dossier
Lecture
Écriture
Pour les autorisations spéciales et les paramètres avancés, cliquez sur Avancé.
Avancé

2.3.6. STRATEGIES ET POLITIQUES DU DOMAINES – GPO :

La gestion centralisée et la sécurisation de l'environnement de travail Windows au sein du domaine DIGITEX reposent sur la mise en œuvre de Stratégies de Groupe (GPO). Ces objets nous permettent de standardiser les configurations des postes, d'appliquer des politiques de sécurité robustes (mots de passe, certificats), de gérer les accès aux fonctionnalités et d'automatiser les tâches d'administration telles que le mappage de lecteurs réseaux ou le déploiement de logiciels.

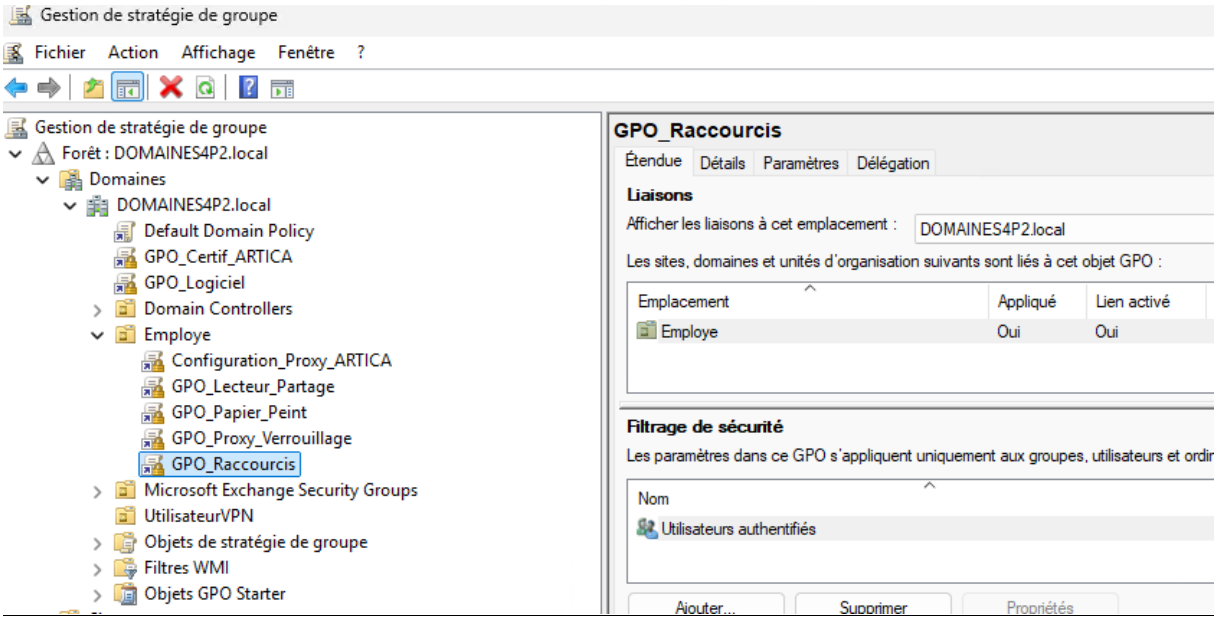
Voici un aperçu des principales stratégies déployées au sein de l'organisation.

GPO APPLIQUÉS AU DOMAINE ENTIER :

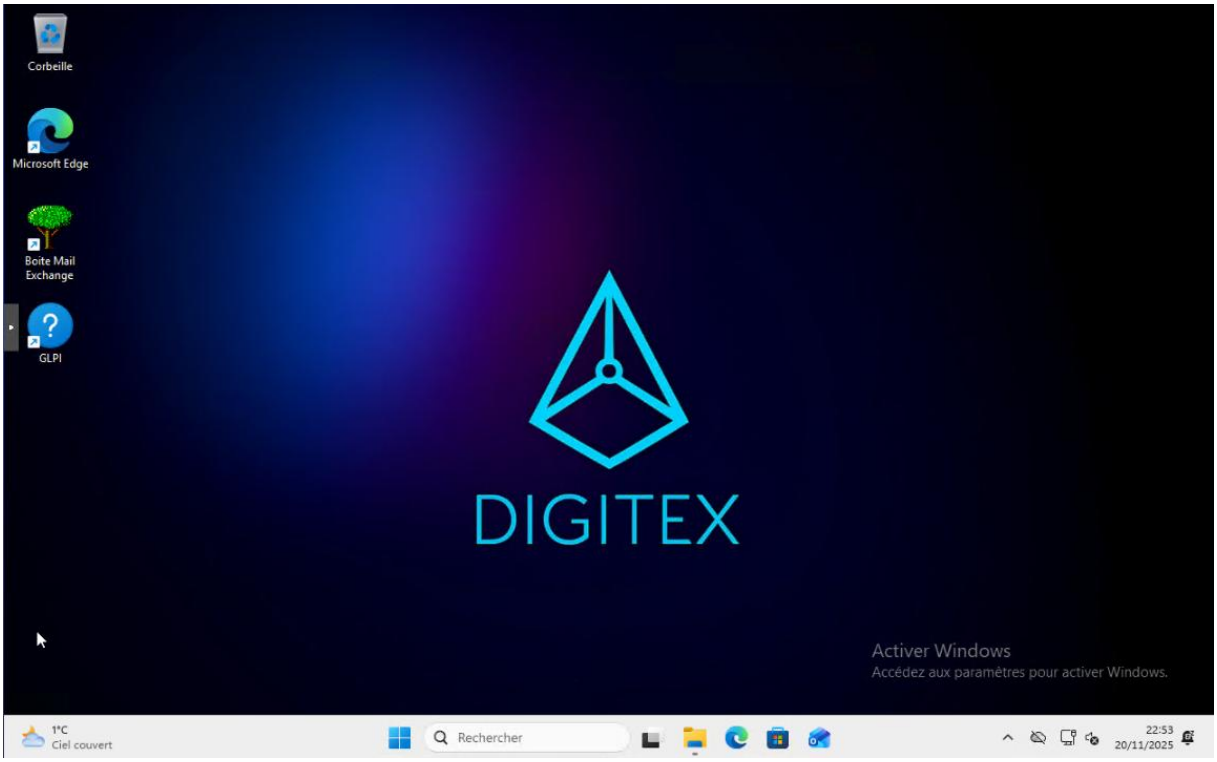
- **Déploiement du navigateur Google Chrome**
- **Logs de connexion des utilisateurs du domaine**
- **Déploiement de certificats (ici Artica Proxy que nous verrons par la suite)**

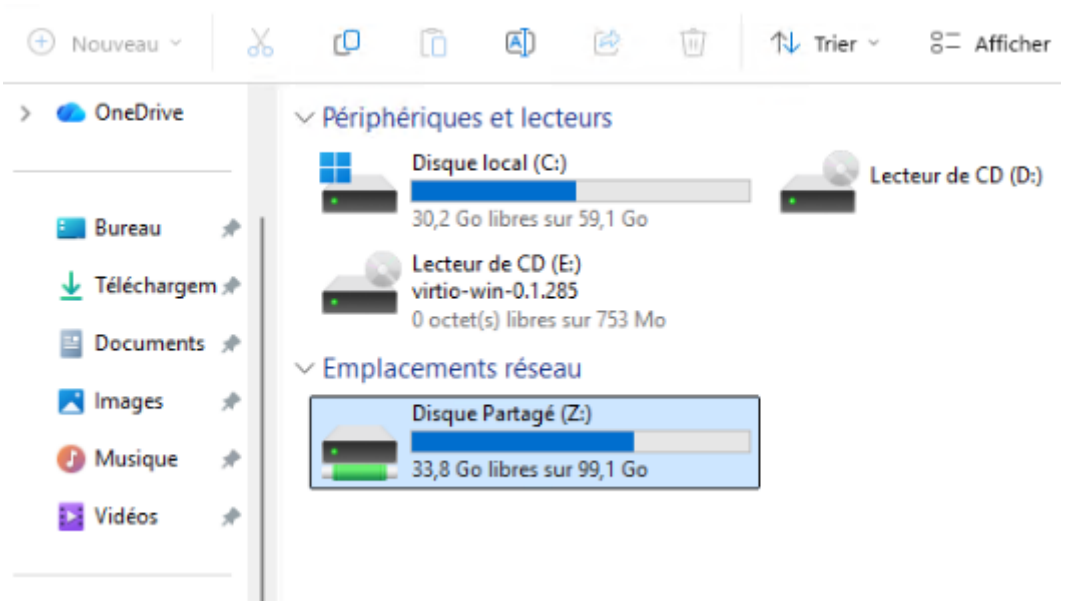
GPO APPLIQUÉS A L'OU « Employé » :

- **Déploiement d'un fond d'écran de l'organisation**
- **Mappage des dossiers partagés en lecteur réseau pour les utilisateurs**
- **Raccourcit WEB des différents services et applications internes**
- **Restriction d'accès aux paramètres et au panneau de configuration**
- **Paramètres PROXY automatiquement déployés sur les postes.**



2.3.7. TEST DES STRATEGIES ET POLITIQUES GPO



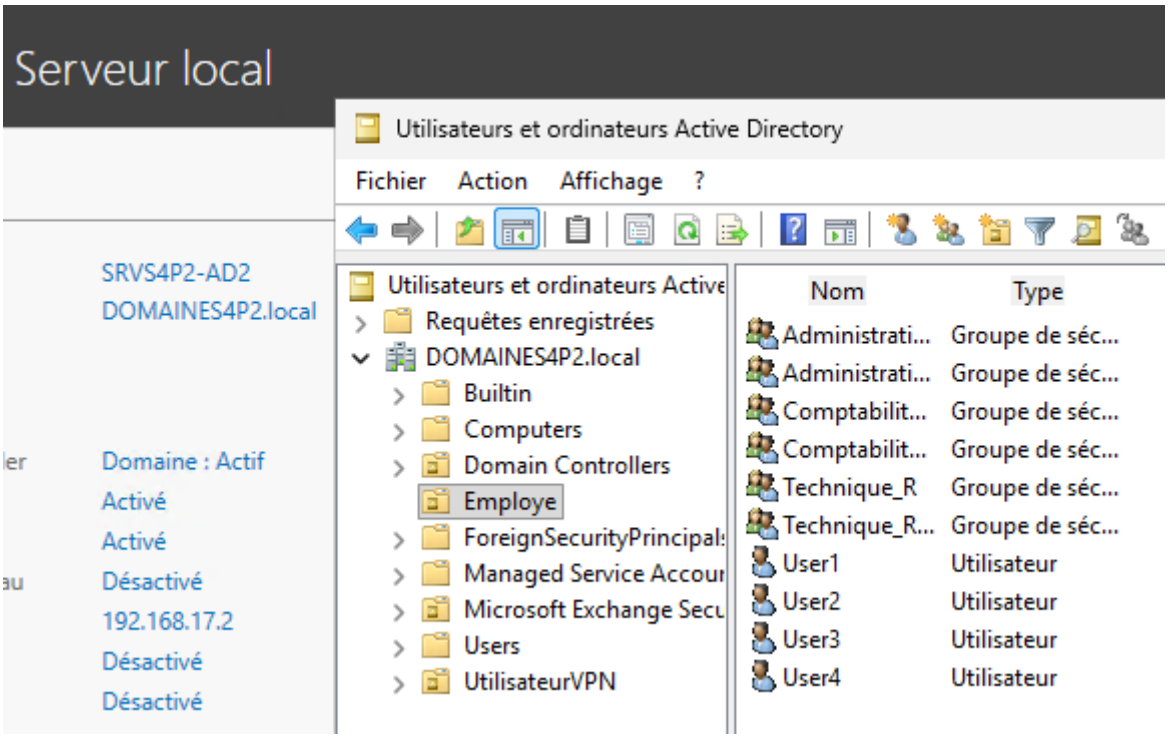


En conclusion, l'infrastructure Active Directory, couplée à la puissance des Stratégies de Groupe (GPO), constitue le levier principal pour une administration centralisée. Elle nous permet de standardiser l'environnement de travail, de sécuriser l'accès aux ressources réseau (comme les espaces partagés) et d'automatiser les configurations Windows. Le périmètre fonctionnel des GPO étant extrêmement vaste, les stratégies implémentées dans ce projet représentent un échantillon clé des capacités de contrôle et de gestion offertes par le domaine.

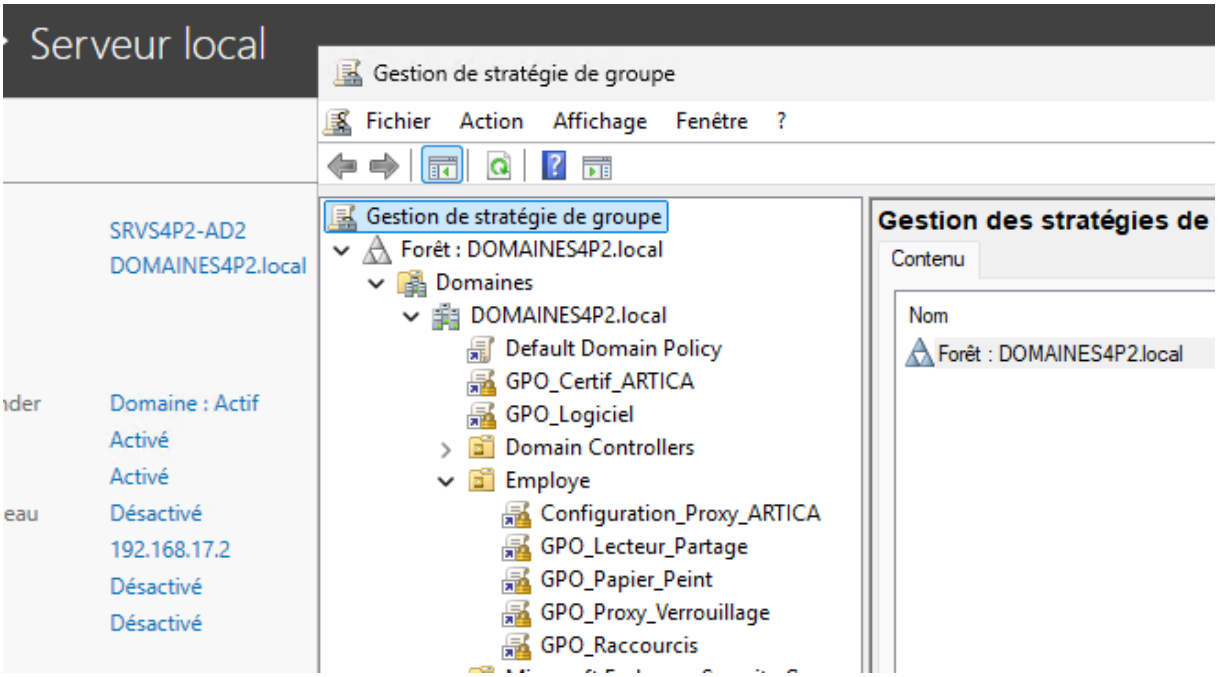
2.3.7. Réplication du Contrôleur de domaines Principal et continuité de service AD :

Pour assurer la haute disponibilité des services critiques, le serveur SRVS4P2-AD2 a été promu contrôleur de domaine additionnel. Il assure une réplication complète de l'annuaire Active Directory (AD DS), des services DNS et de l'ensemble des Stratégies de Groupe (GPO). De plus, un mécanisme de **basculement DHCP (DHCP Failover)** a été configuré entre les deux serveurs. Cette architecture permet non seulement une répartition de la charge des requêtes clients, mais garantit surtout la continuité du service d'adressage IP en cas de défaillance du serveur principal

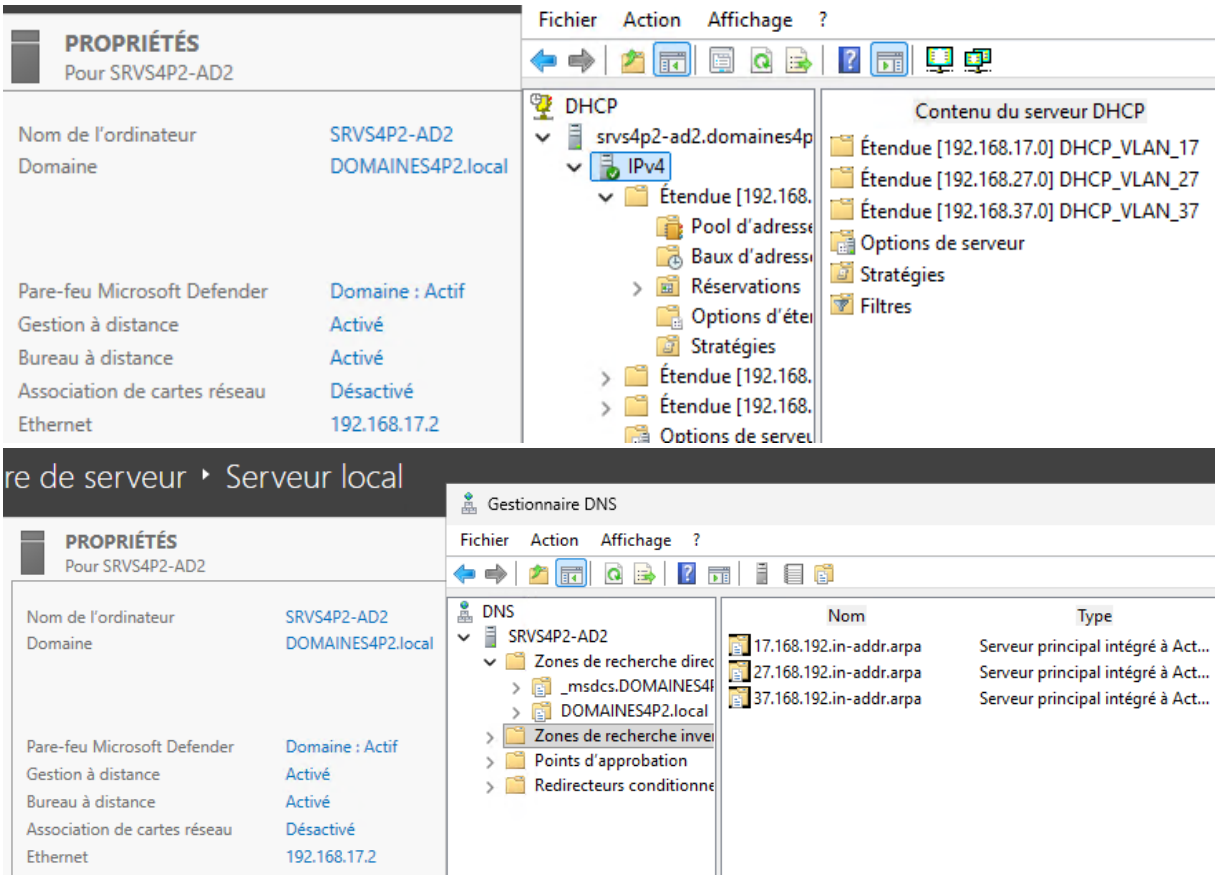
Utilisateurs / Groupes / OU répliqués sur le serveur SRVS4P2-AD2 :



GPO répliqués sur le serveur SRV-AD2 :



Service et étendues DHCP + zones DNS répliqués sur le serveur SRVS4P2-AD2 :



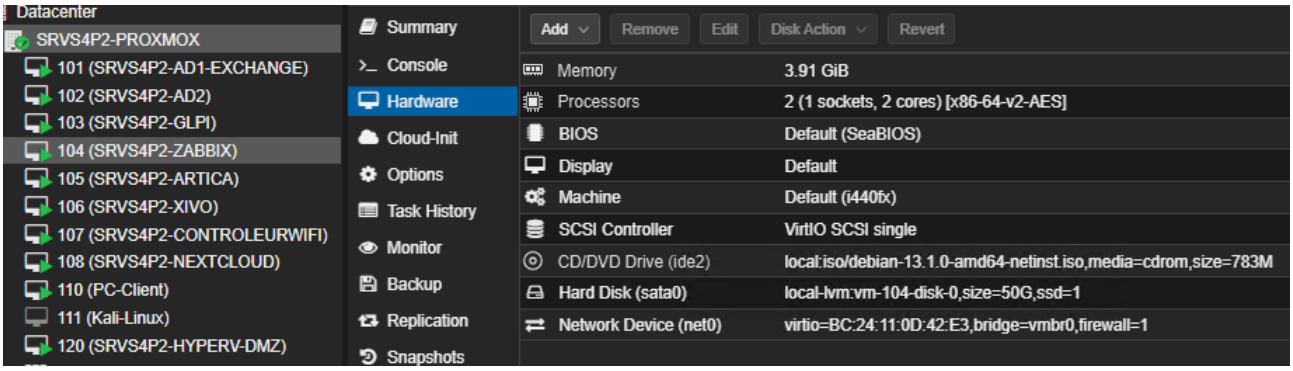
Afin de faciliter la téléadministration des contrôleurs de domaine (AD1 et AD2), le protocole Bureau à distance (RDP) a été activé. L'accès est strictement restreint au compte Administrateur, dont la sécurité est garantie par une politique de mot de passe

robuste. Parallèlement, une sécurisation réseau a été mise en place : les flux RDP vers ces serveurs sont bloqués en provenance des VLAN utilisateurs (27 et 37) et ne sont autorisés que depuis le VLAN17 (Serveurs). Le détail des règles de filtrage correspondantes sera présenté ultérieurement dans ce dossier.

2.4. Supervision Des Machines Du Parc Informatique Avec Zabbix :

Pour assurer la supervision des équipements critiques du Système d'Information, la solution Zabbix a été déployée. Son architecture repose sur des agents installés sur les machines cibles (communiquant via les ports TCP 10050 et 10051), permettant une collecte fine de métriques de performance et d'états (espace disque, mémoire vive, charge CPU, température, etc.). La solution permet également la définition de seuils d'alerte personnalisés. L'ensemble est piloté et visualisé de manière centralisée via une interface Web ergonomique.

2.4.1. Configuration de la VM Debian 13 :

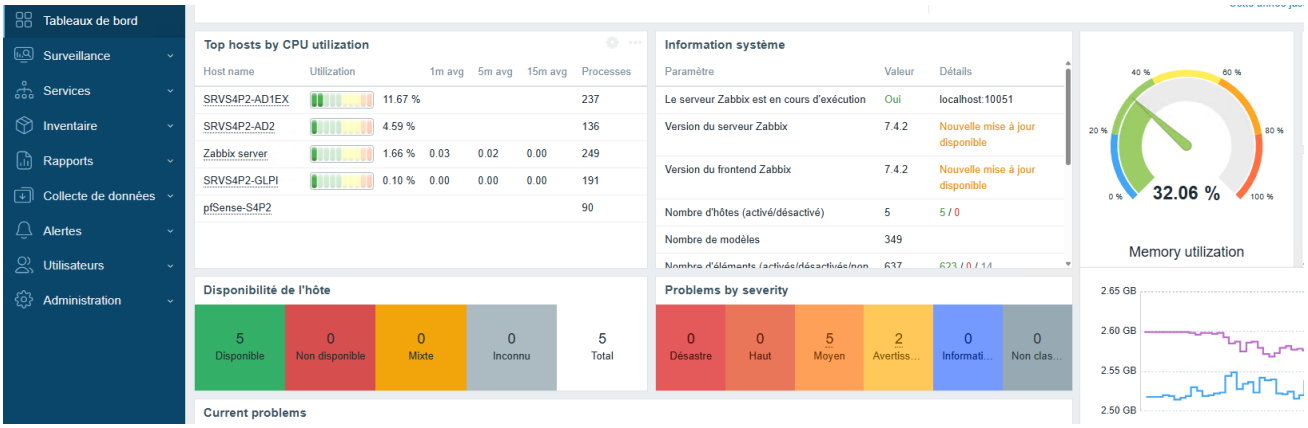


Configuration réseau de la VM :

```
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UP group default qlen 1000
    link/ether bc:24:11:0d:42:e3 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    altname enxbc24110d42e3
    inet 192.168.17.4/24 brd 192.168.17.255 scope global noprefixroute ens
18
       valid_lft forever preferred_lft forever
root@SRVS4P2-ZABBIX:/home/sio#
```

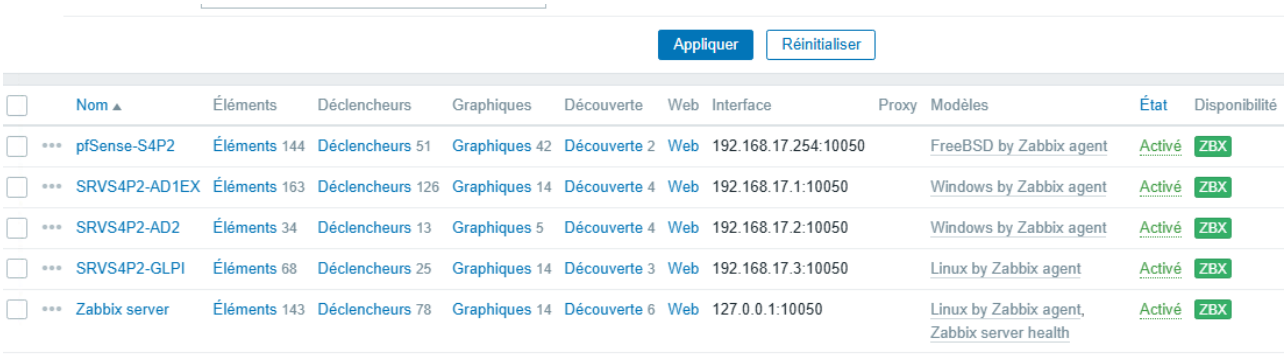
Dans un premier temps, le serveur Web Apache2 a été installé, ainsi que l'ensemble des dépendances techniques requises (PHP, modules de base de données...). Suite à la configuration de ces prérequis, nous avons procédé à l'installation des paquets du serveur Zabbix. L'initialisation et la configuration finale de la solution ont été réalisées via l'interface Web d'administration, accessible à l'adresse :

http://192.168.17.4/zabbix (l'adresse IP du serveur Debian).

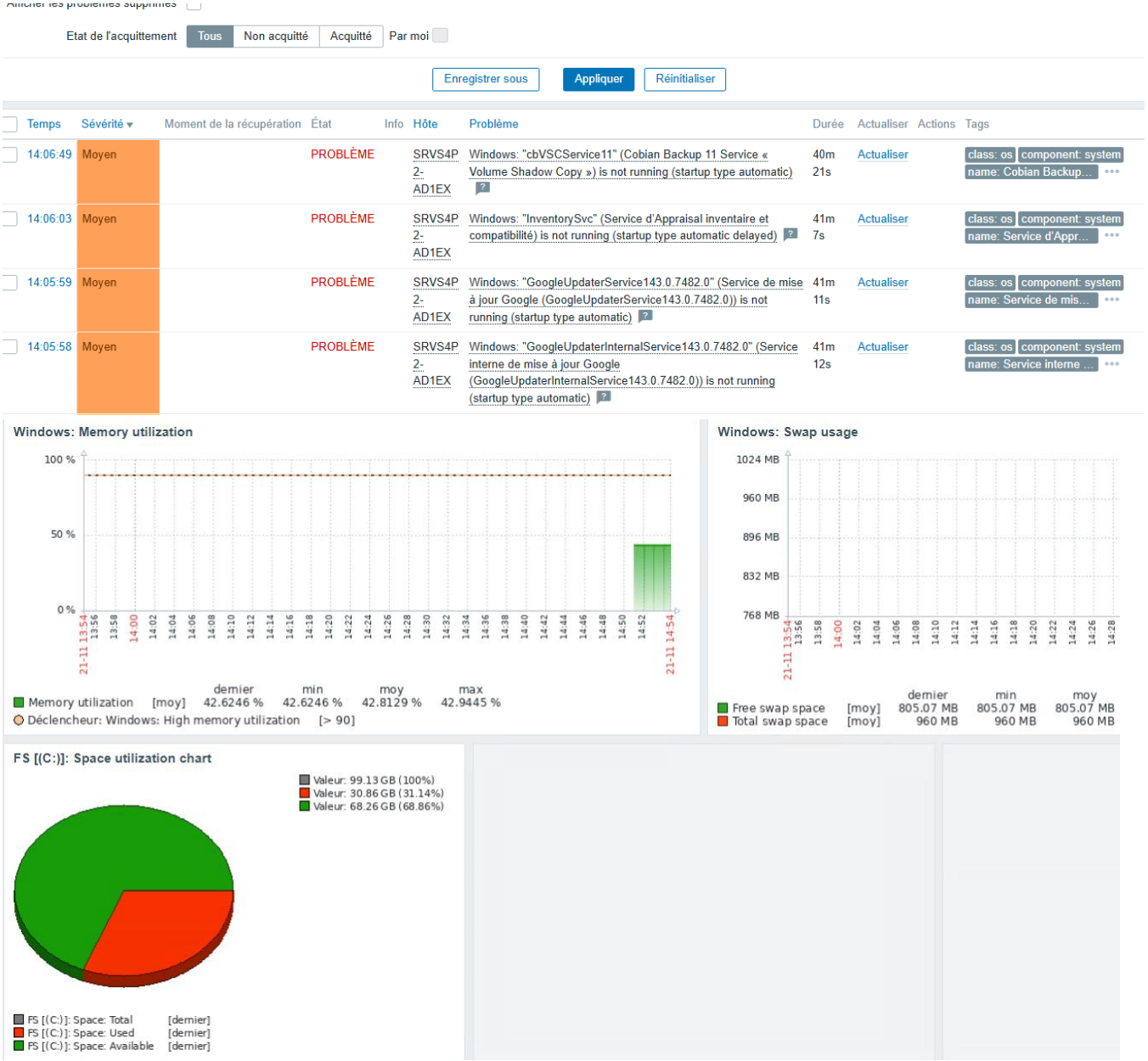


2.4.2. Déploiement des agents et collecte des données :

Cette phase a consisté au déploiement et à la configuration des agents Zabbix sur l'ensemble des serveurs critiques de l'infrastructure. Chaque agent a été paramétré pour autoriser la communication avec le serveur de supervision central. Dans un second temps, nous avons procédé à la déclaration (création) de ces équipements en tant qu'"Hôtes" dans l'interface d'administration Web de Zabbix, permettant ainsi le début de la collecte des données.



Nous avons appliqué des modèles de supervision (templates) prédéfinis pour configurer les données à surveiller et définir les seuils d'alerte correspondants dans l'interface Zabbix



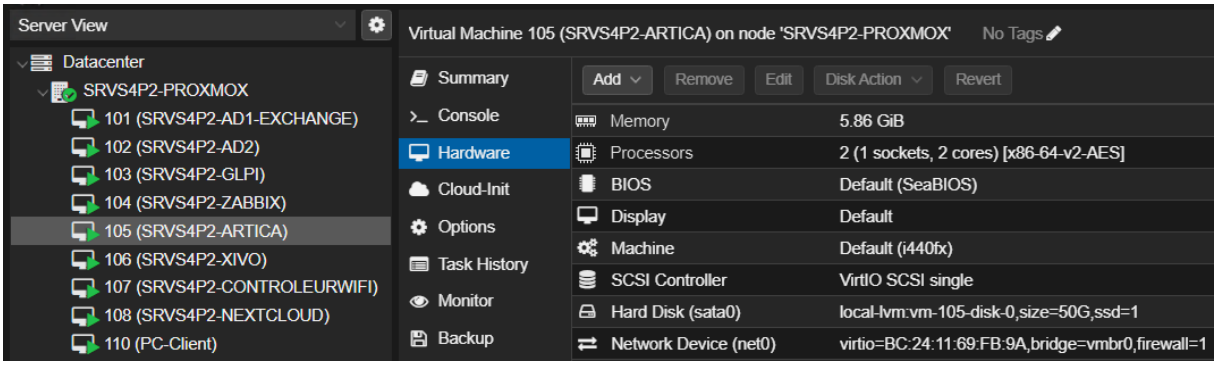
Grâce au déploiement de Zabbix, nous avons désormais la maîtrise totale de la supervision du réseau. La plateforme nous permet de surveiller les hôtes et les métriques de notre choix de manière flexible, et de configurer des alertes précises pour anticiper les incidents (surcharge CPU, saturation disque, panne de service...).

2.5. Mise en œuvre du Proxy Web Artica : Politique de filtrage et page de blocage

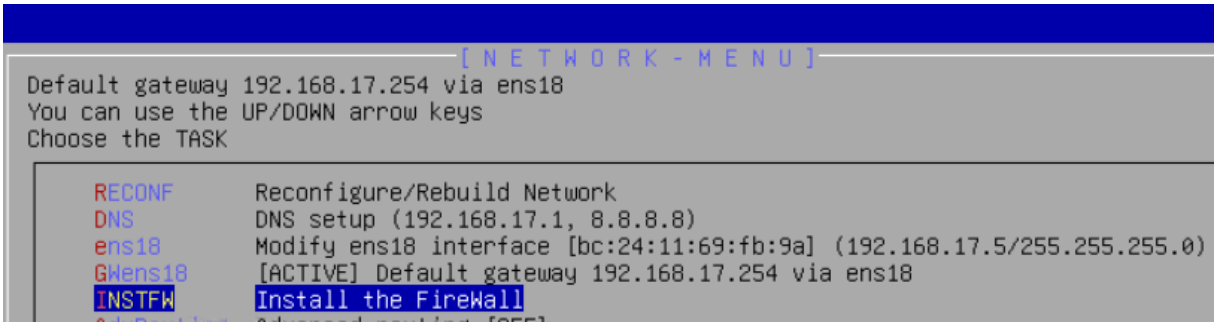
Afin de contrôler et de sécuriser l'accès Internet des utilisateurs du domaine, la mise en place d'une solution de filtrage de contenu (par URLs ou catégories) s'est avérée nécessaire. Le choix s'est porté sur la solution Artica Proxy pour la richesse de ses fonctionnalités. L'architecture retenue est un déploiement en mode **proxy explicite (direct)**, incluant l'**inspection des flux HTTPS** (déchiffrement SSL). Cette fonctionnalité cruciale nécessite l'importation préalable du certificat d'autorité (CA) auto-signé d'Artica sur l'ensemble des postes clients pour valider les connexions sécurisées.

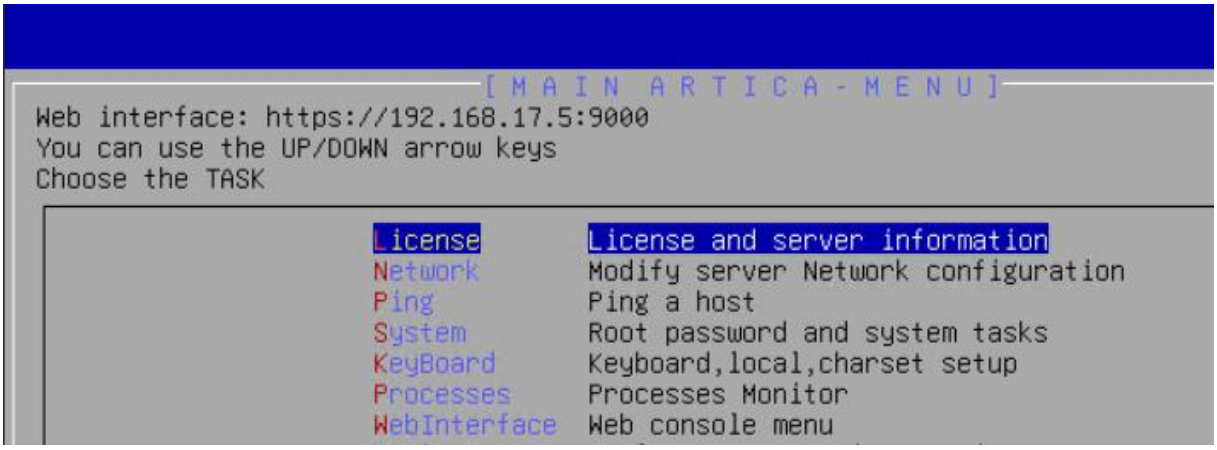
2.5.1 Déploiement de l'Appliance virtuelle Artica sur Debian 12.2 :

Le déploiement du proxy a été réalisé sur une machine virtuelle Proxmox VE, en utilisant l'image ISO fournie par Artica. Cette image fonctionne comme une **Appliance** : il s'agit d'une distribution Debian Linux pré-configurée intégrant nativement la solution Artica. Suite à l'installation et aux configurations réseau de base du système, l'interface Web d'administration du proxy est devenue accessible.

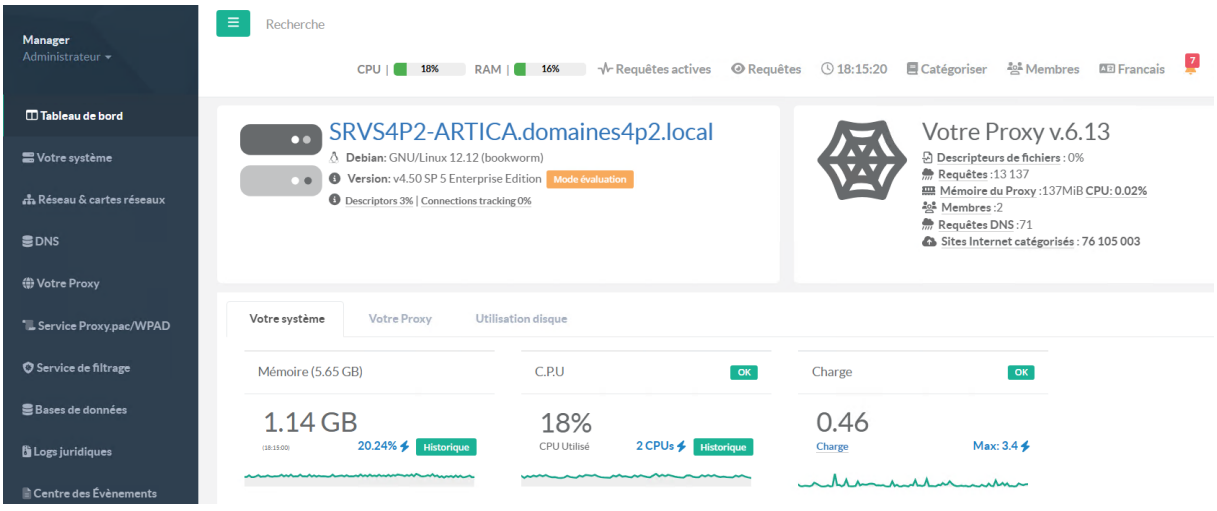


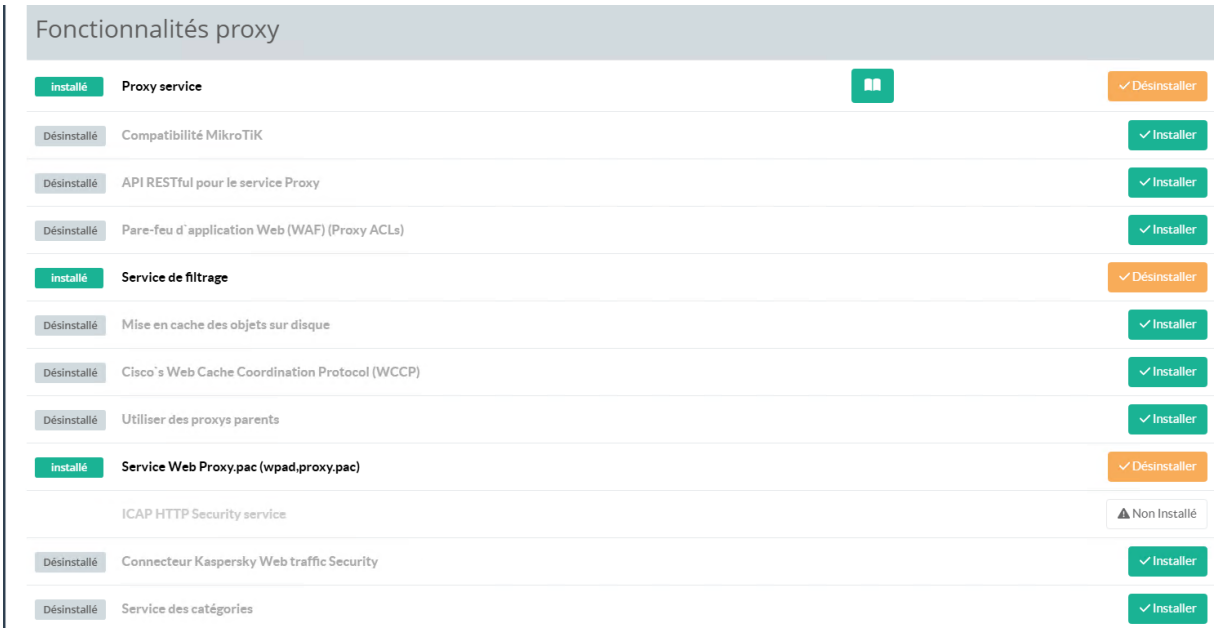
2.5.2. Paramétrage initial de la machine virtuelle (VM)



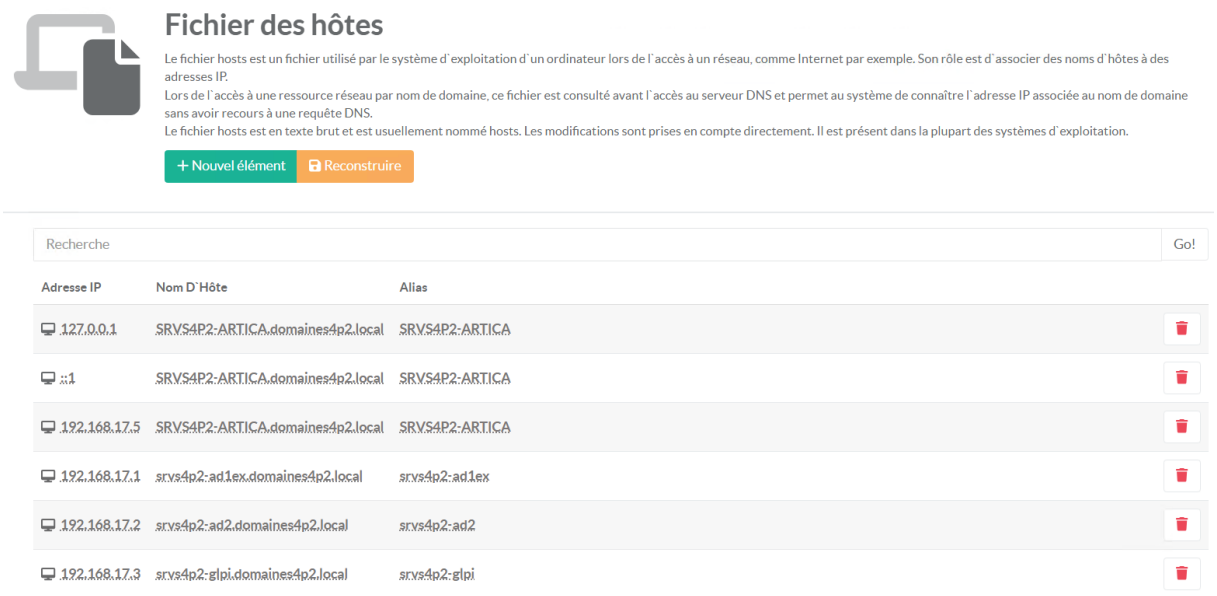


La configuration du proxy Web a été réalisée au travers de l'interface d'administration Web d'Artica (WebUI), accessible à l'adresse https://192.168.17.5:9000. La phase initiale a consisté à déployer l'ensemble des fonctionnalités et modules nécessaires à l'architecture cible.

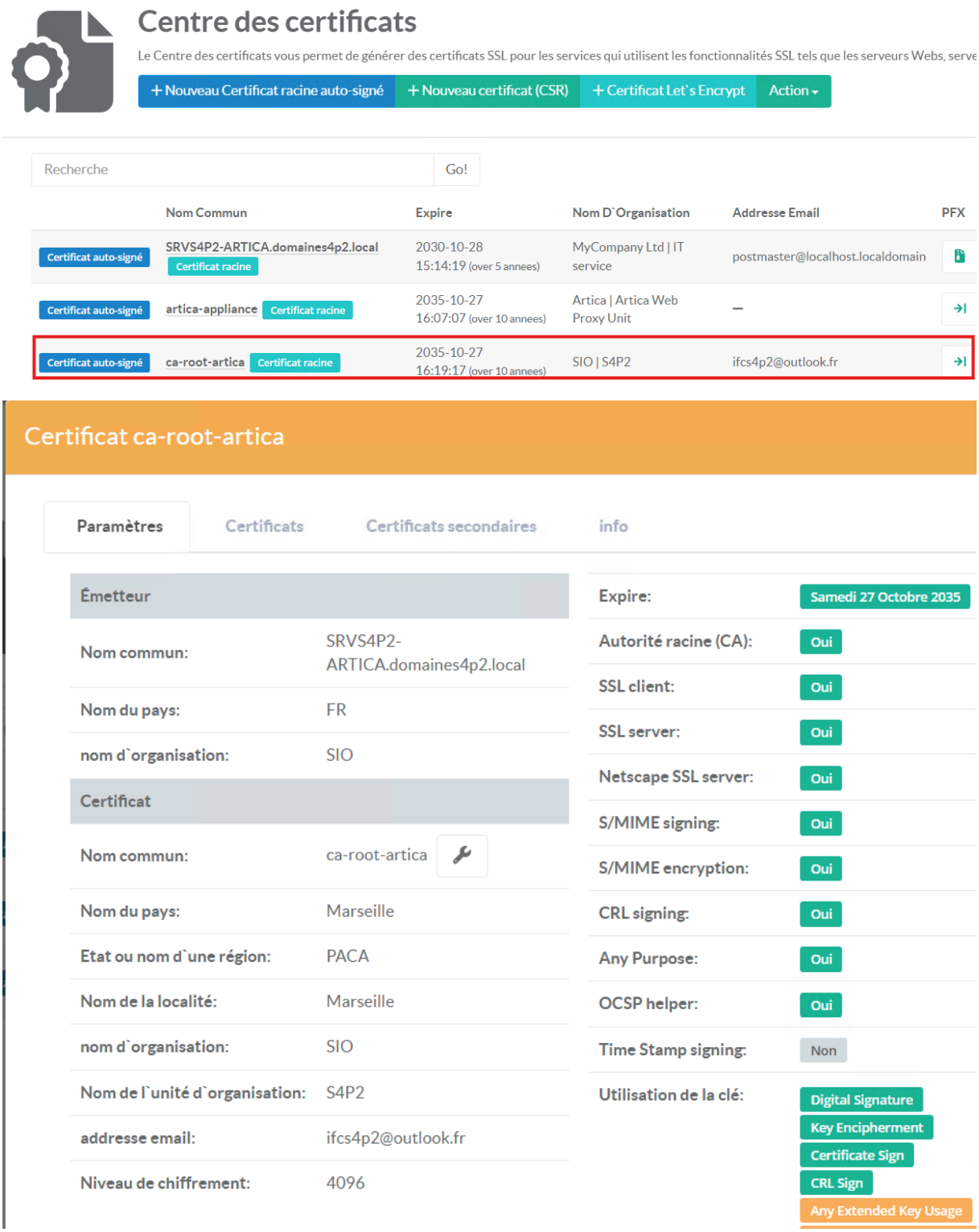




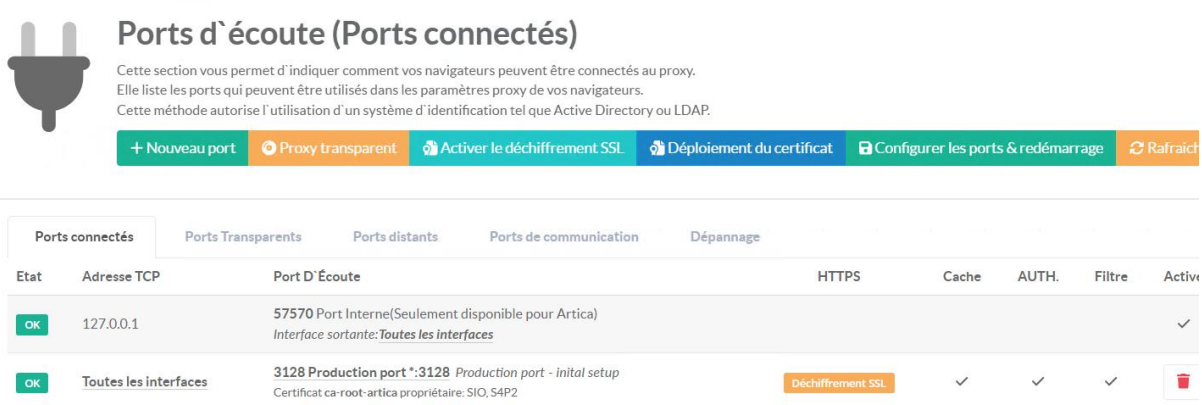
Voici un aperçu des paramètres permettant de bloquer les sites web ciblés avec une redirection vers la page d'erreur personnalisée. Une étape préliminaire cruciale consiste à renseigner le fichier hosts local de la machine. L'ajout des résolutions de noms des serveurs internes est nécessaire pour garantir que le proxy n'intercepte ni ne bloque l'accès aux services du Réseaux interne.



2.5.3. Certificat Auto-Signé SSL :



2.5.4. PORTS D'ECOUTES ARTICA + SERVICE SSL :



2.5.5. Liste de sites bloqués :

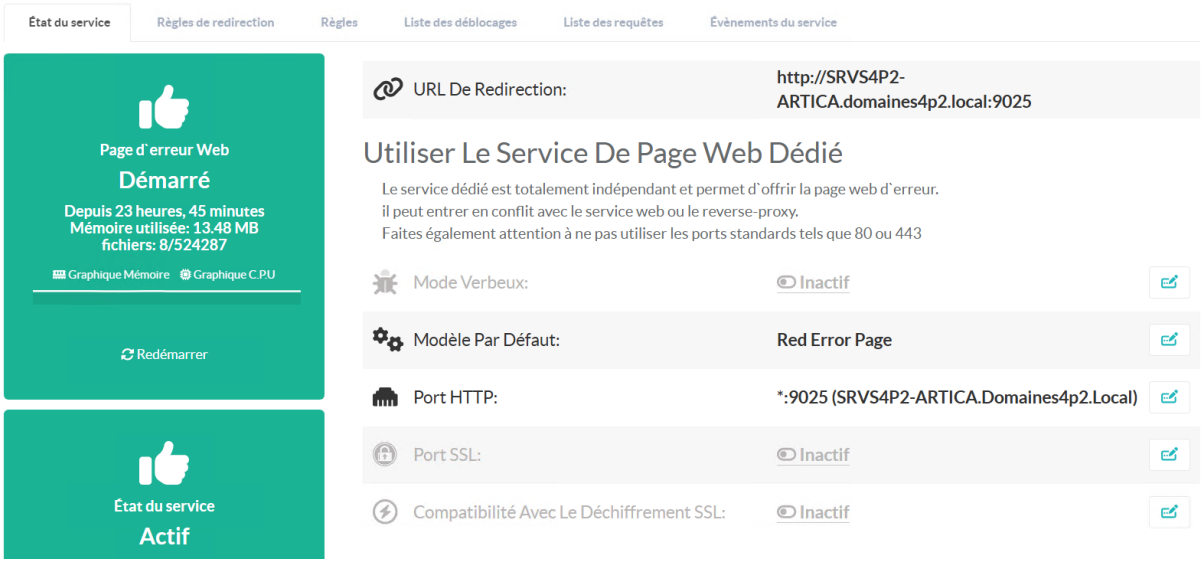
La version d'Artica utilisée ne disposant pas de la licence Enterprise (incluant les bases de données de filtrage dynamiques), la politique de blocage repose sur la définition manuelle de listes noires (blacklists) d'URL ou de domaines

2.5.6. Définition de la politique de filtrage Web :

La stratégie d'accès par défaut a été conservée car elle répond aux exigences actuelles. Elle applique un principe de **filtrage systématique** : tout flux réseau transitant par le proxy, notamment via le port d'écoute standard 3128, est obligatoirement intercepté et analysé par le moteur de filtrage Web d'Artica.

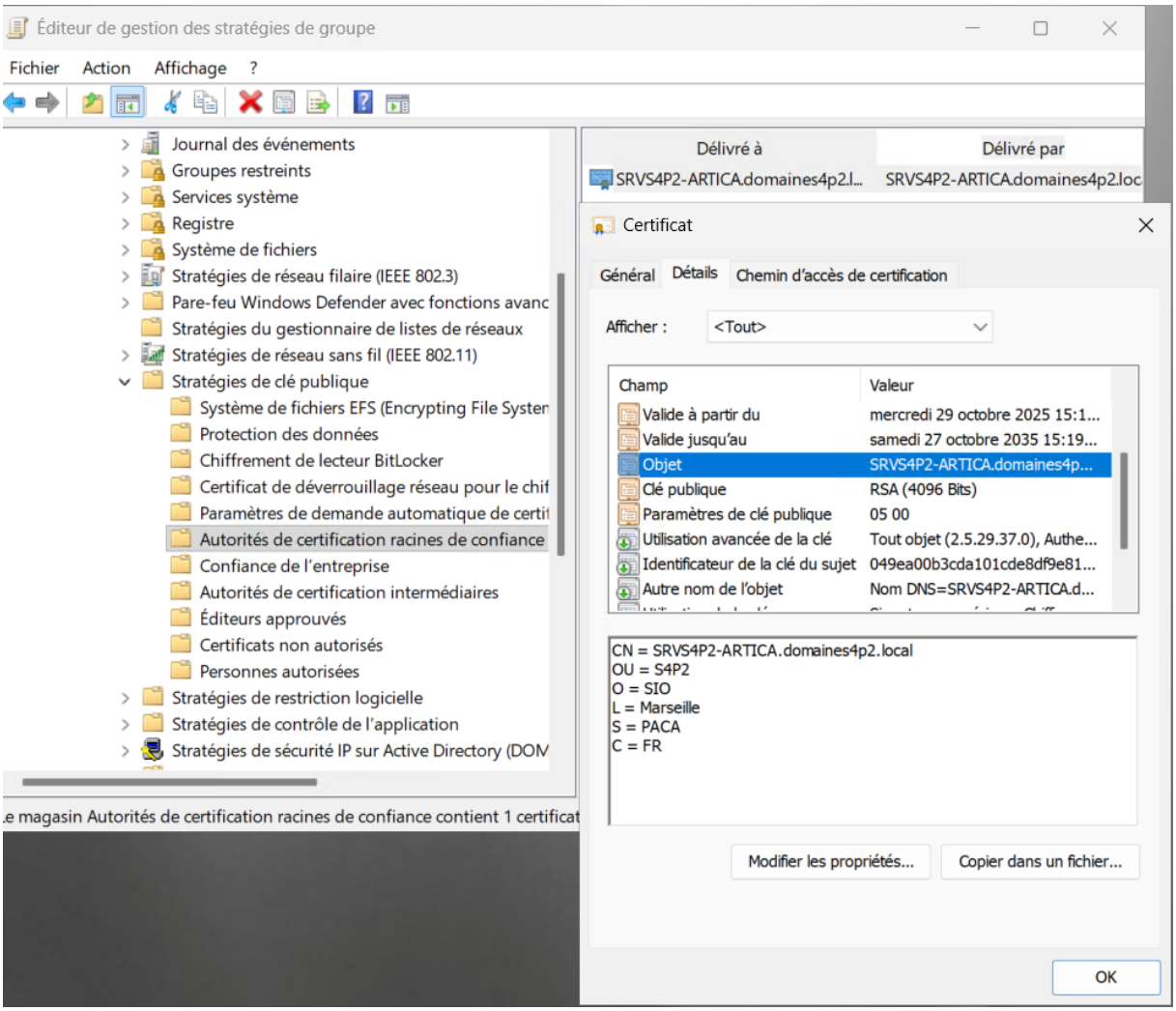
2.5.7. SERVICE PAGE D'ERREUR LOCAL + RÈGLE DE REDIRECTION

Nous avons configuré le proxy pour qu'il intercepte les requêtes Web bloquées et redirige le client vers la page d'erreur interne. Un point crucial de cette configuration est la prise en charge des protocoles HTTPS, en plus du HTTP, pour garantir l'affichage de la notification de blocage en toutes circonstances.

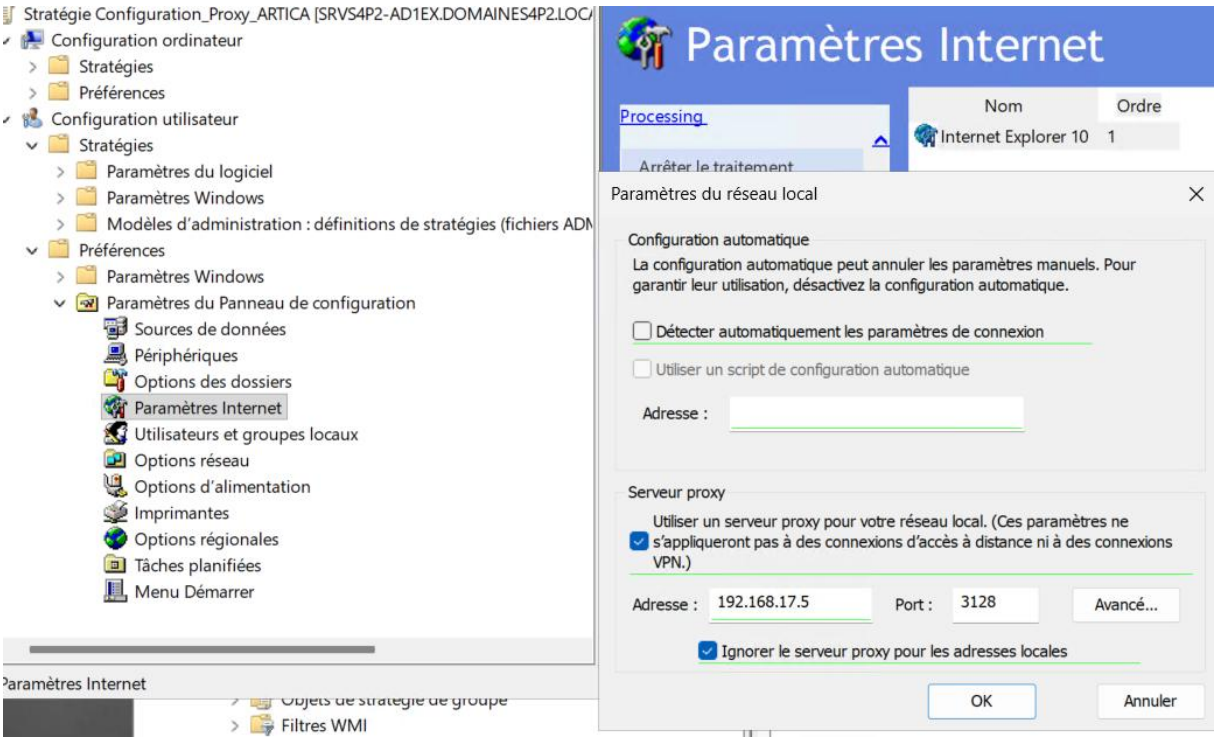


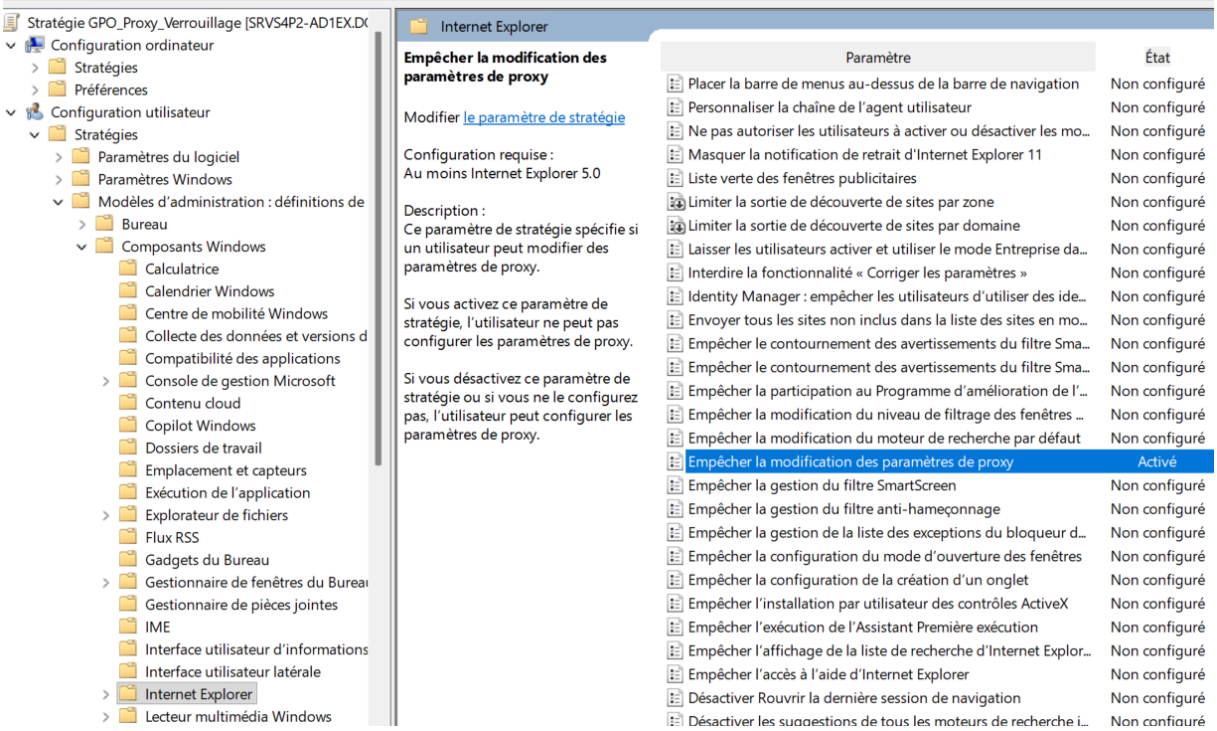
2.5.8. Déploiement du Certificat et Des Paramètres PROXY Avec GPO :

- **Déploiement Du Certificat :**



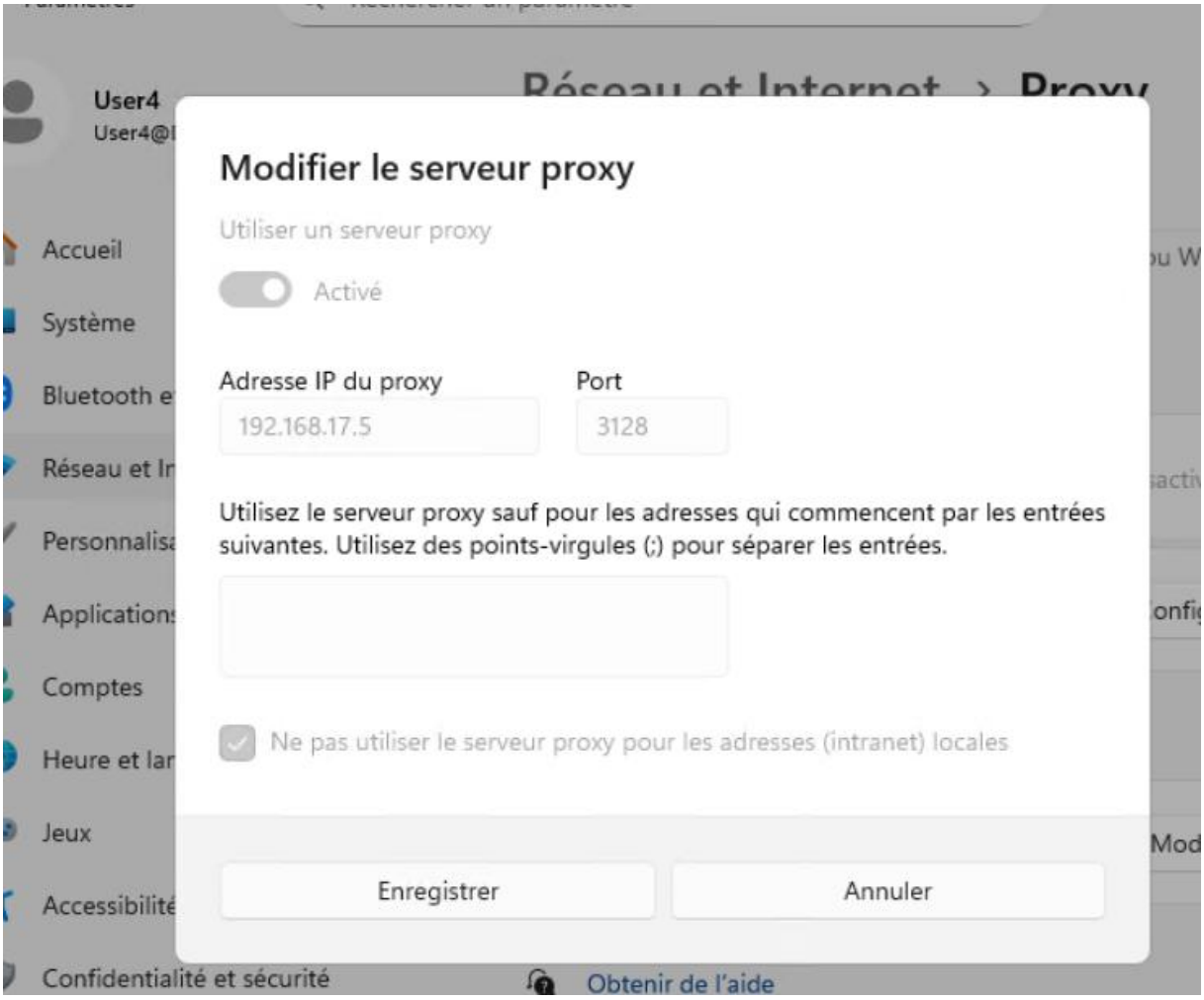
- **Paramètre Proxy :**

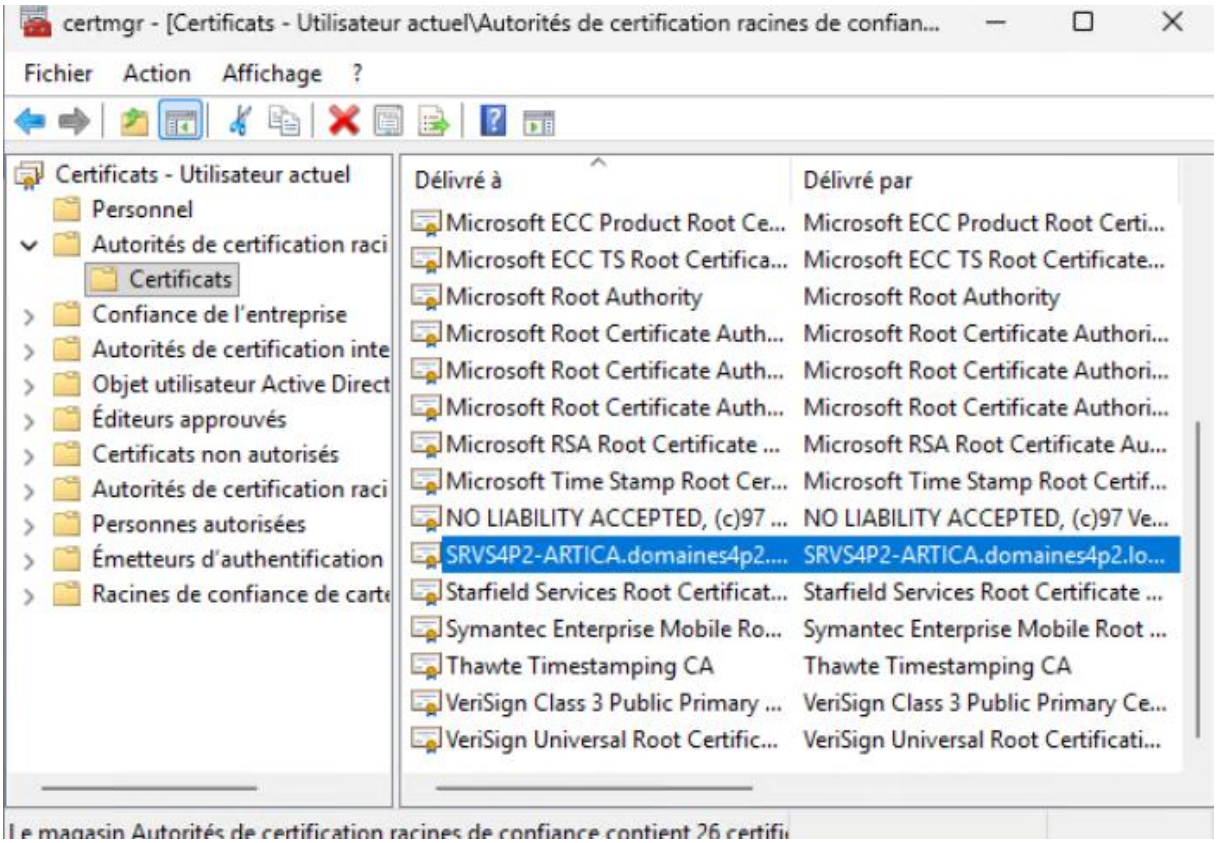




2.5.9 : TEST GPO PROXY :

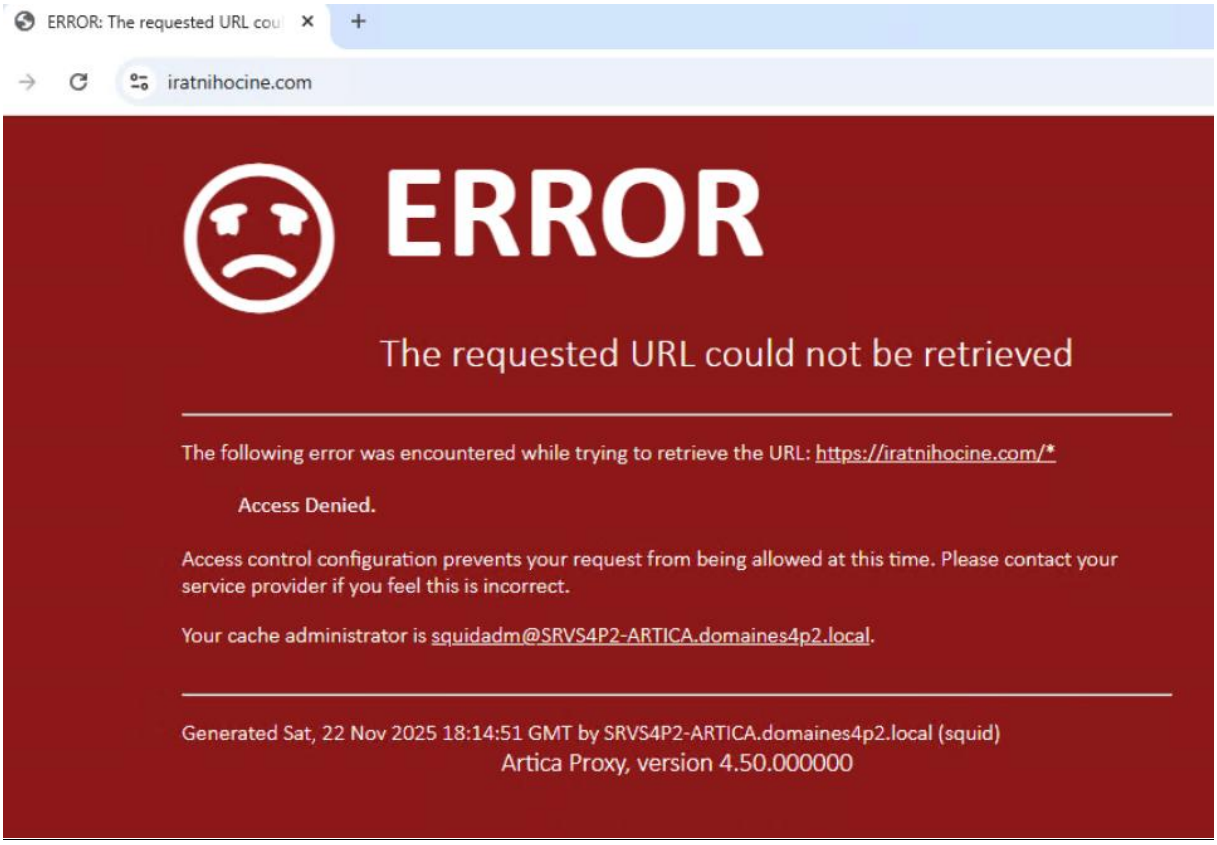
Nous nous sommes connectés à une session du domaine pour contrôler si les paramètres du proxy étaient correctement forcés. Une GPO de sécurité restreignant l'accès au panneau de configuration, nous avons dû la désactiver momentanément pour les besoins du test.

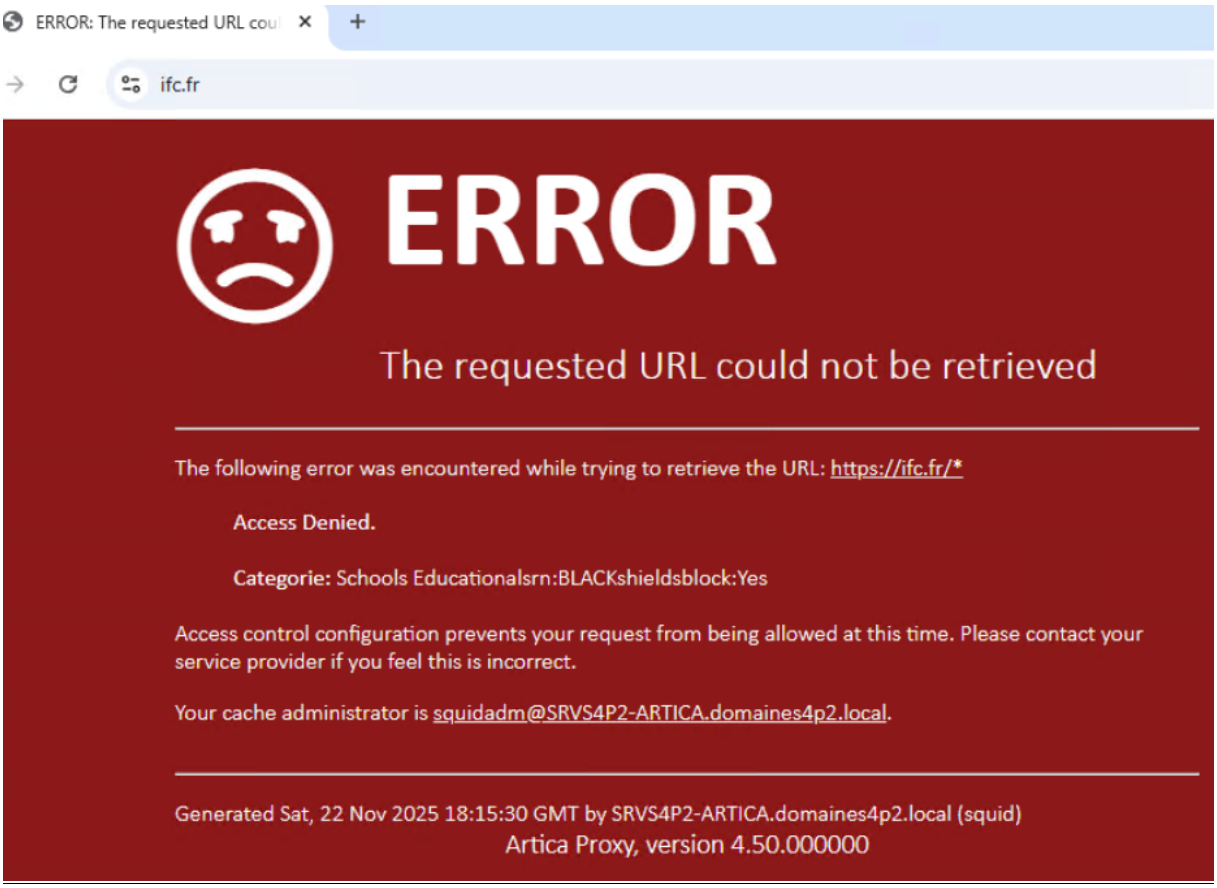




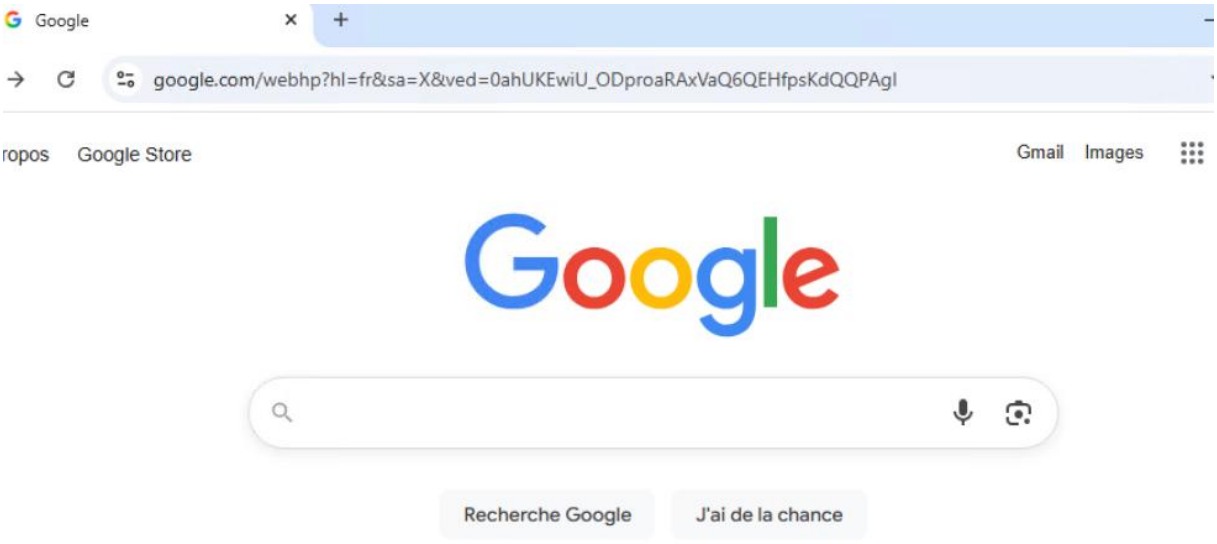
Le certificat a bien été importé dans le magasin de la machine.

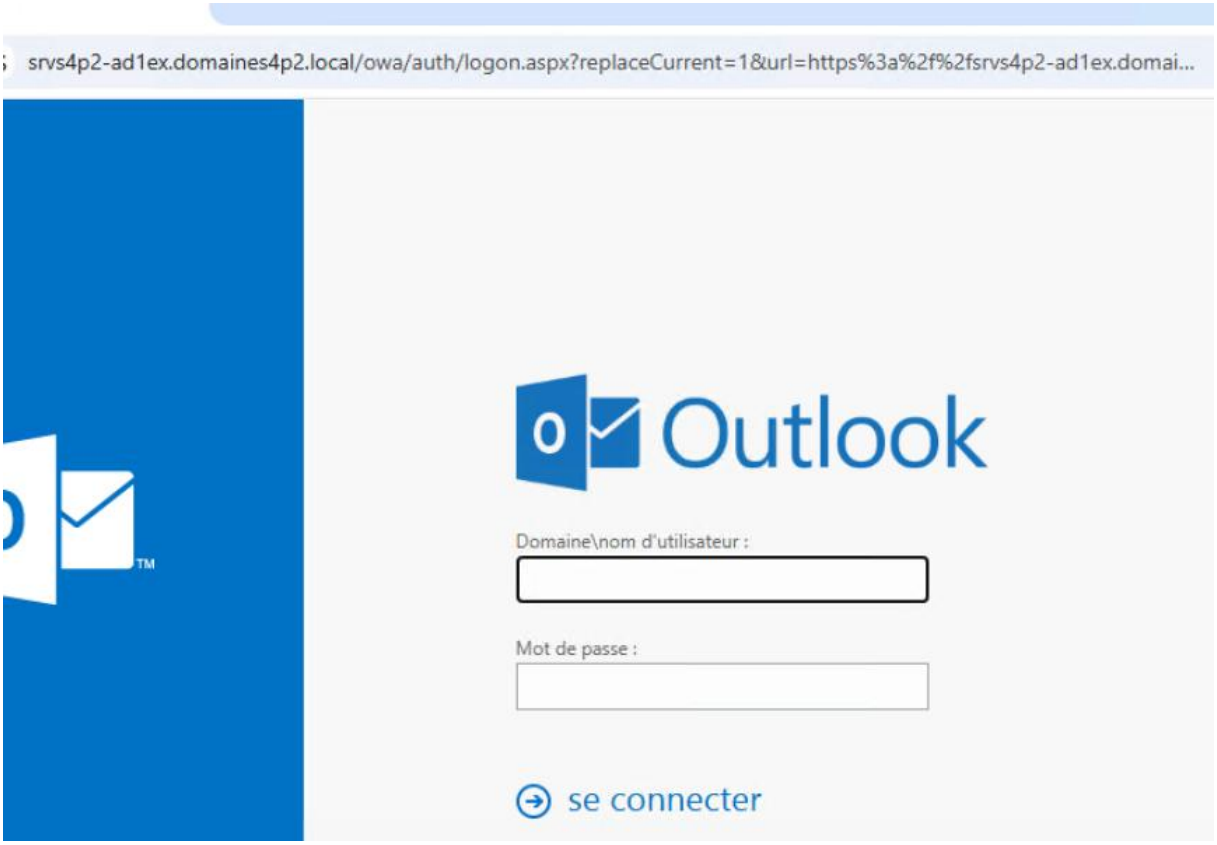
TEST LISTE DE SITES PERSONNELLE :





TEST ACCES AU RESTE DES SITES PERMIS :




srvs4p2-ad1ex.domaines4p2.local/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fsrvs4p2-ad1ex.domai...
Outlook
Domaine\nom d'utilisateur :
Mot de passe :
se connecter

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)

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

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 2**
Nom, prénom : IRATNI Hocine	**N° candidat :**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date : 06** / 06 /2026
Organisation support de la réalisation professionnelle : Organisation fictive « DIGITEX » - Plot « S4P2 » IFC Marseille	
Intitulé de la réalisation professionnelle : Mise en place de services dans le réseau pour répondre aux besoins des utilisateurs du système d'information – Configurer en fonction des besoins des services sur le réseau de niveau physique et logique, assurer leur fonctionnalité, leur disponibilité, ainsi que leur sécurité face aux menaces.	
Période de réalisation : 10/2024 – 05/2026 **Lieu :** Centre de Formation IFC Marseille, Plot S4P2 **Modalité :** ☒ **Seul(e)** ☐ **En équipe**	
Compétences travaillées ☒ Concevoir une solution d'infrastructure réseau ☒ Installer, tester et déployer une solution d'infrastructure réseau ☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau	

Compétences travaillées
☒ Concevoir une solution d'infrastructure réseau
☒ Installer, tester et déployer une solution d'infrastructure réseau
☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[5] (ressources fournies, résultats attendus) :

Ressources fournies :

- Un PC avec clavier et souris USB, utilisé comme base pour construire et configurer l'infrastructure, et pour l'administration de celle-ci ;
- Un PC portable utilisé comme PC Client pour simuler des utilisateurs du SI (Système d'Information) de l'organisation ;
- Un PC avec un disque dur attribué à un serveur PROXMOX VE (environnement de virtualisation utilisé pour héberger et administrer des serveurs virtualisés) ;
- Un espace disque de stockage dédié aux serveurs virtuels PROXMOX sur un serveur de sauvegarde PROXMOX BACKUP ;
- Un PC avec un disque dur attribué à un serveur PFSENSE (routeur/Firewall) possédant 3 cartes réseaux dont une avec deux interface réseaux et donc 4 ports Ethernet ;
- Serveur HYPERV Virtualisé sur Proxmox pour la virtualisation qui sera utilisé pour serveurs accessible de l'extérieur du réseau et mise à disposition de réseaux externes (comme un serveur WEB par exemple) ;
- Trois écrans VGA/HDMI ;
- Une prise Ethernet murale, reliée au réseau WAN de l'établissement IFC Marseille, représentant l'arrivée internet de l'organisation ;
- Des câbles Ethernet RJ45 en nombre suffisant ;
- Un switch NETGEAR GS308Ev4 à 8 ports ;
- Deux multiprises ;
- Des clés USB pour les installations de systèmes d'exploitation
- Un serveur NAS commun aux BTS SIO de l'établissement auquel nous avons accès via des identifiants personnels contenant des ressources indispensables à notre progression (cours, procédures, travaux d'autres étudiants, logiciels, etc.)
- Différentes solutions logicielles et applicatives disponible au téléchargement sur le WEB (voir ressources logicielles utilisées' dans la section 'description des ressources').

Résultats attendus :

- **Un service de déclaration d'incident et demande d'assistances à travers pour centraliser** l'assistance informatique aux utilisateurs :
  Un serveur GLPI (Gestionnaire Libre de Parc Informatique) installé sur une machine virtualisée Debian permet à chaque utilisateur du domaine AD de l'organisation de créer des tickets (déclarer un incident ou demander de l'assistance informatique) sur une session individuelle liée au compte du domaine, et les envoyer à l'administrateur. L'administrateur peut accéder à une session serveur qui centralise les tickets envoyer par les utilisateurs, les classes en fonctions des critères configurés.

- **Un système de messagerie interne dans le domaine AD fonctionnel pour les utilisateurs :**
  Un serveur de messagerie Interne MICROSOFT EXCHANGE est installé et configuré sur le contrôleur de domaine principale, lié au domaine ainsi qu'à l'annuaire AD, il met à disposition des utilisateurs du domaine une boite de messagerie individuelle qui permet d'échanger des mails au sein de l'organisation. L'administrateur peut créer ou supprimer à sa guise des 'boites aux lettres' en fonction des besoins de l'organisation et peut gérer les configurations depuis sa session serveur.

- Un sous-réseau dédié à des invités avec un accès Wi-Fi sécurisé :
  Mise en place d'une borne Wi-Fi sur le réseau LAN de l'organisation dans un VLAN dédié aux utilisateurs passagers du SI devant accéder à des ressources numériques temporairement. Une connexion Sécurisée avec un portail captif et des identifiants transmis dans la confidentialité, un SSID un service DHCP et DNS dédié sur le serveur Windows AD ainsi que des règles de filtrage firewall.

- Un ensemble de règles de filtrage Firewall pour assurer la confidentialité des échanges et la sécurité Des équipements et serveurs sensibles :
  Une configuration de filtrage sur le pare-feu PFSENSE de sorte à garantir que seuls les utilisateurs Légitimes et habilités du réseau puissent accéder aux différentes ressources, machines, serveurs du Réseau. Garantir la sécurité des machines sensibles faces aux menaces extérieurs, garantir le Cloisonnement des sous-réseaux en fonction des départements du SI et des critères de l'organisation.

- Tunnel VPN (Virtual Private Network) sécurisé pour un accès distant aux ressources du réseau local pour les utilisateurs du SI de l'organisation :
  Les utilisateurs du SI étant habilités à accéder à distance (depuis des réseaux externes, en passant par Internet) aux ressources du réseau local de l'organisation disposent d'une connexion VPN chiffrée leur Permettant d'accéder en toute sécurité au réseau et à ses ressources, avec des règles pour garantir des Accès légitimes et autorisés.

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

Description des ressources documentaires, matérielles et logicielles utilisées[6]

Ressources matériels et documentaires utilisées : (voir 'conditions de réalisations')

Ressources logicielles utilisées :

- Page WEB d'administration UniFi OS ;
- Distribution LINUX Debian 13 ;
- Solution GLPI (11.0.0) ;
- Gestion de base de données MariaDB et MySQL ;
- Solution de messagerie Microsoft EXCHANGE 2019 (CU15) ;
- Annuaire LDAPS Active Directory ;
- Page WEB d'administration NETGEAR GS108Ev4 ;
- Administration WEB PFSENSE ;
- Logiciel client OpenVPN (2.6.7) ;

Modalités d'accès aux productions[7] et à leur documentation[8] :

Les différentes ressources de l'infrastructure sont accessibles par le poste administrateur dans le VLAN dédié à l'administration, sur des pages WEB d'administration (voir section 'répertoire identifiants et sessions' du dossier). La documentation - mise à part le présent dossier – est disponible sur mon site portfolio dans la section :

https://iratnihocine.com

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

[7] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[8] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

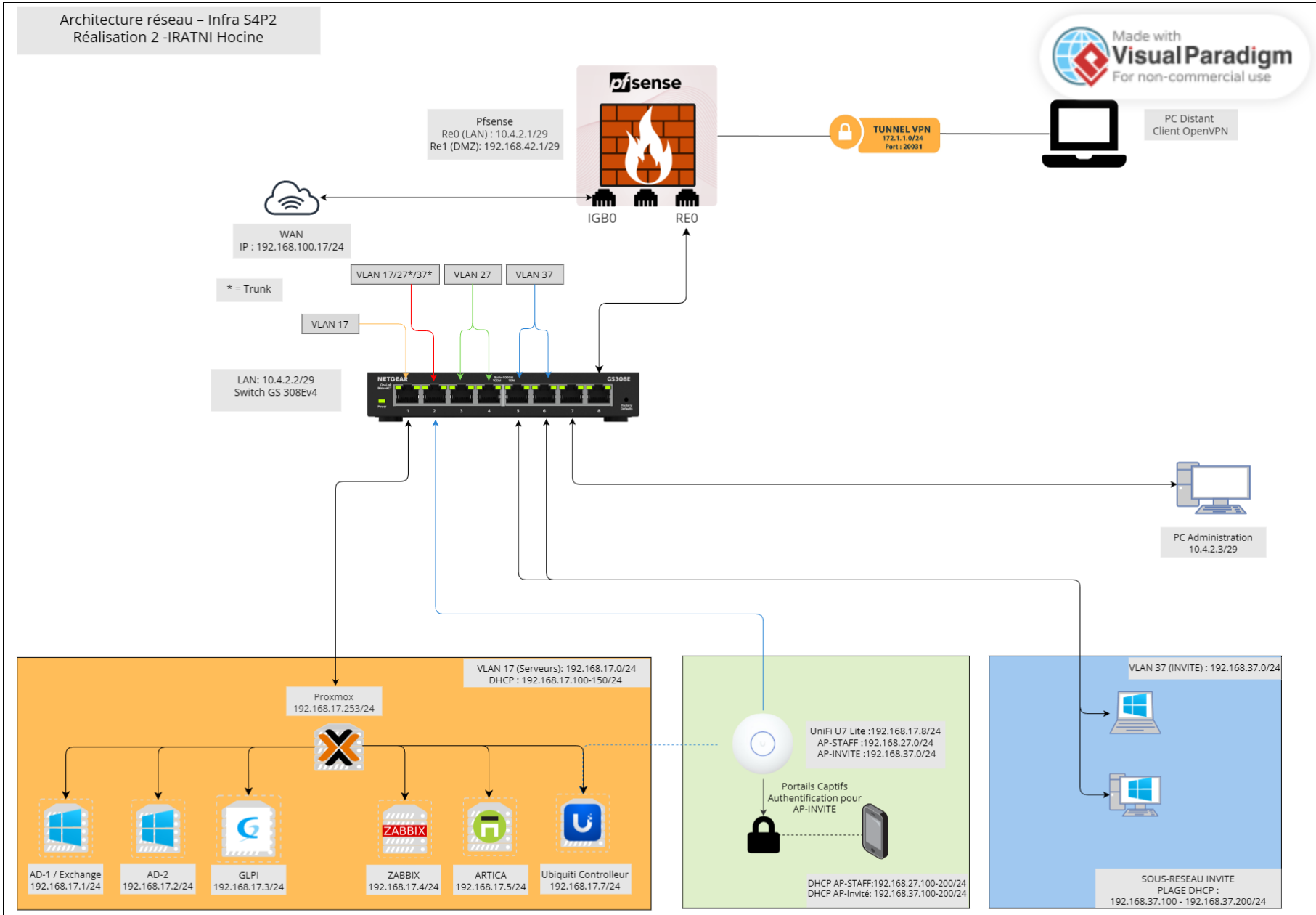
ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

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

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

Schéma de la réalisation :

Architecture réseau – Infra S4P2
Réalisation 2 -IRATNI Hocine

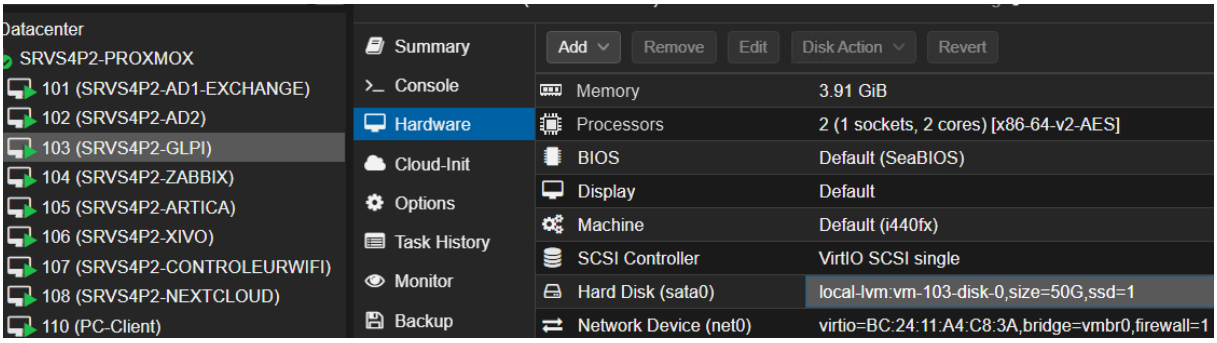


Version : 2.2
26/11/2025

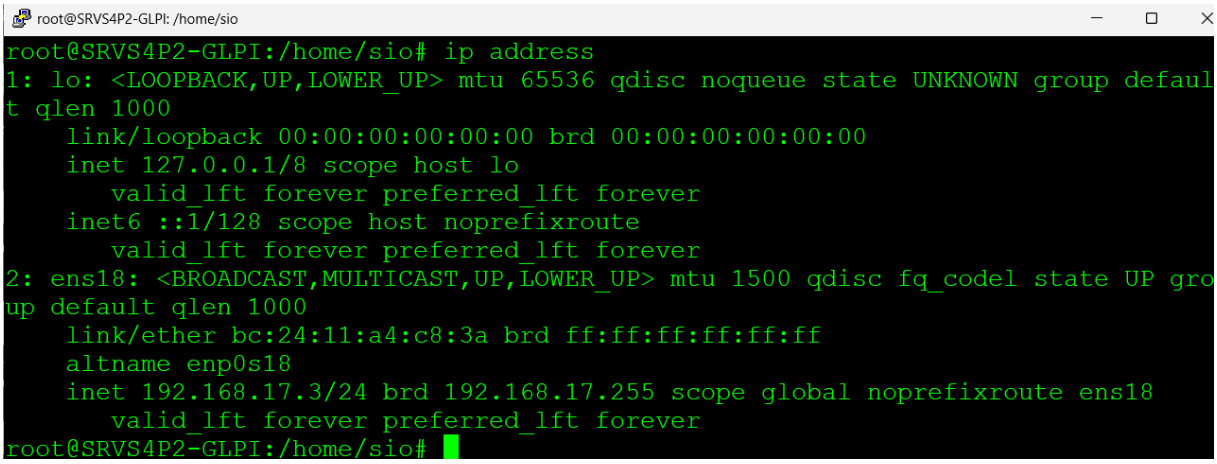
3.1. Solution de gestion de parc et Helpdesk : GLPI (Tickets, Incident et demande d'assistance) :

Afin d'optimiser la prise en charge des demandes d'assistance technique au sein de DIGITEX, nous avons déployé la solution GLPI. Outil de gestion de parc et d'Helpdesk, GLPI a été interconnecté avec l'Active Directory local. Cette intégration permet aux utilisateurs de s'authentifier avec leurs identifiants de domaine habituels pour accéder à leur portail et soumettre des tickets d'incidents, qui sont ensuite centralisés pour traitement par l'administrateur. La solution est hébergée sur une machine virtuelle Ubuntu Server 24.04, déployée sur l'infrastructure Proxmox VE et configurée comme suit :

3.1.1. Machine Virtuelle :



3.1.2. Configurations de la Machine :



MARIADB MYSQL BASE DE DONNEE GLPI :

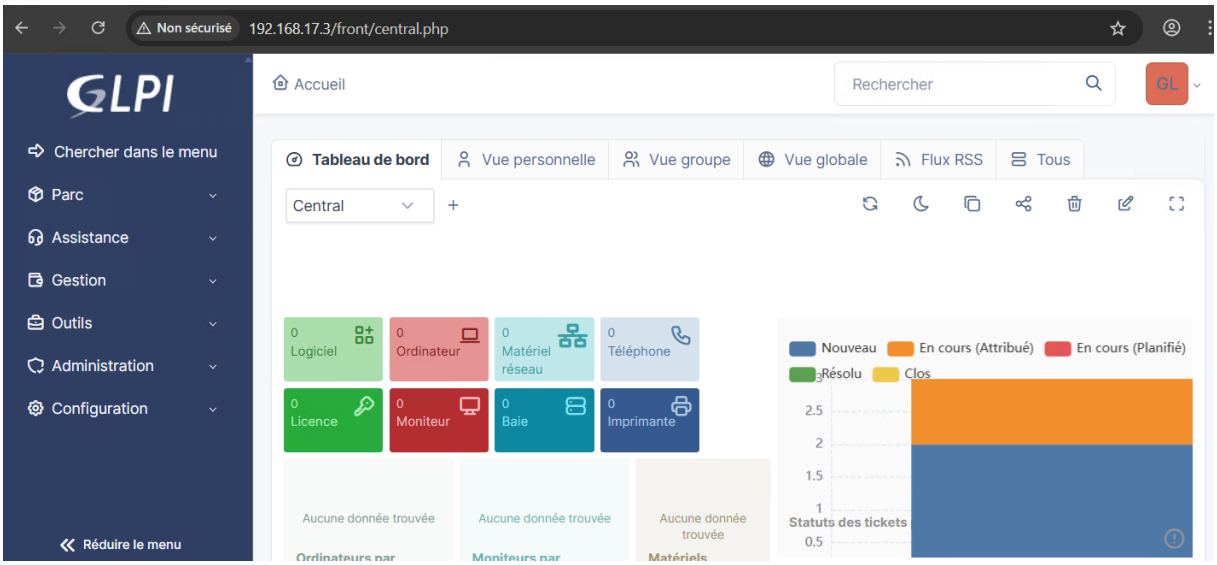
Nous avons créé une base de données MariaDB, comme pour le serveur Zabbix (glpidb avec glpiuser possédant tous les droits.

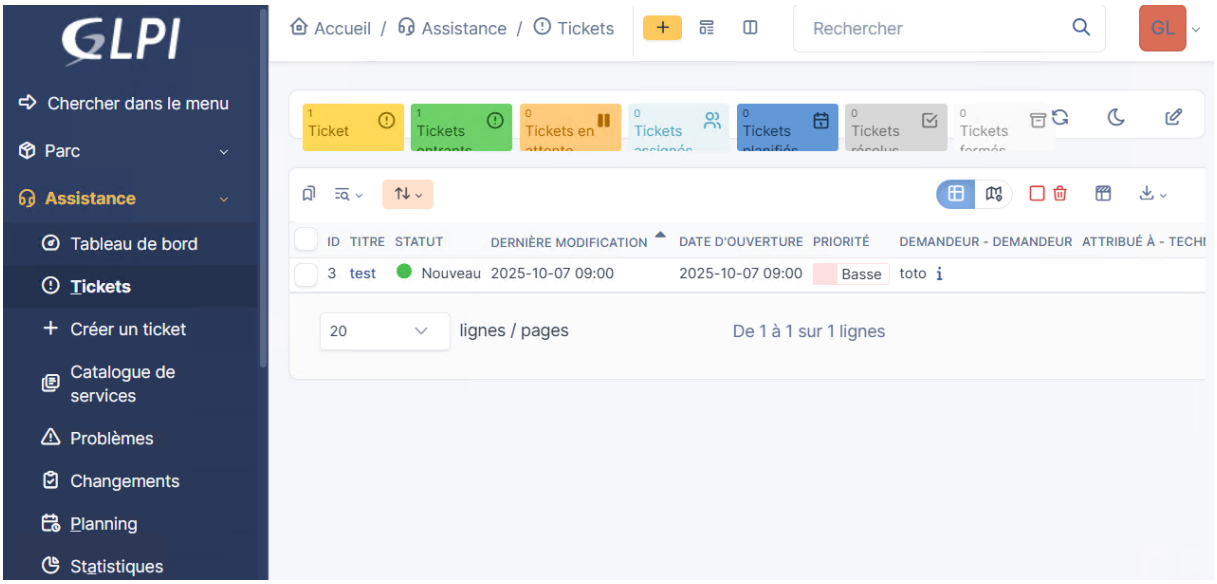
```
root@SRVS4P2-GLPI:/# sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 35
Server version: 10.11.13-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| glpidb             |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0,002 sec)

MariaDB [(none)]>
```

```
MariaDB [(none)]> SELECT user, Host FROM mysql.user;
+-------------+-----------+
| User        | Host      |
+-------------+-----------+
| glpi        | localhost |
| mariadb.sys | localhost |
| mysql       | localhost |
| root        | localhost |
+-------------+-----------+
4 rows in set (0,001 sec)

MariaDB [(none)]>
```

3.1.3. Accès Interface WEB GLPI :

Le déploiement de GLPI a nécessité l'installation préalable des prérequis logiciels, incluant le serveur HTTP Apache. Une fois l'application installée, l'accès à l'interface Web d'administration a été validé localement depuis la machine SRV-GLPI. La première connexion s'effectue via l'URL http://192.168.14.3/glpi, en utilisant le compte administrateur de la base interne locale.

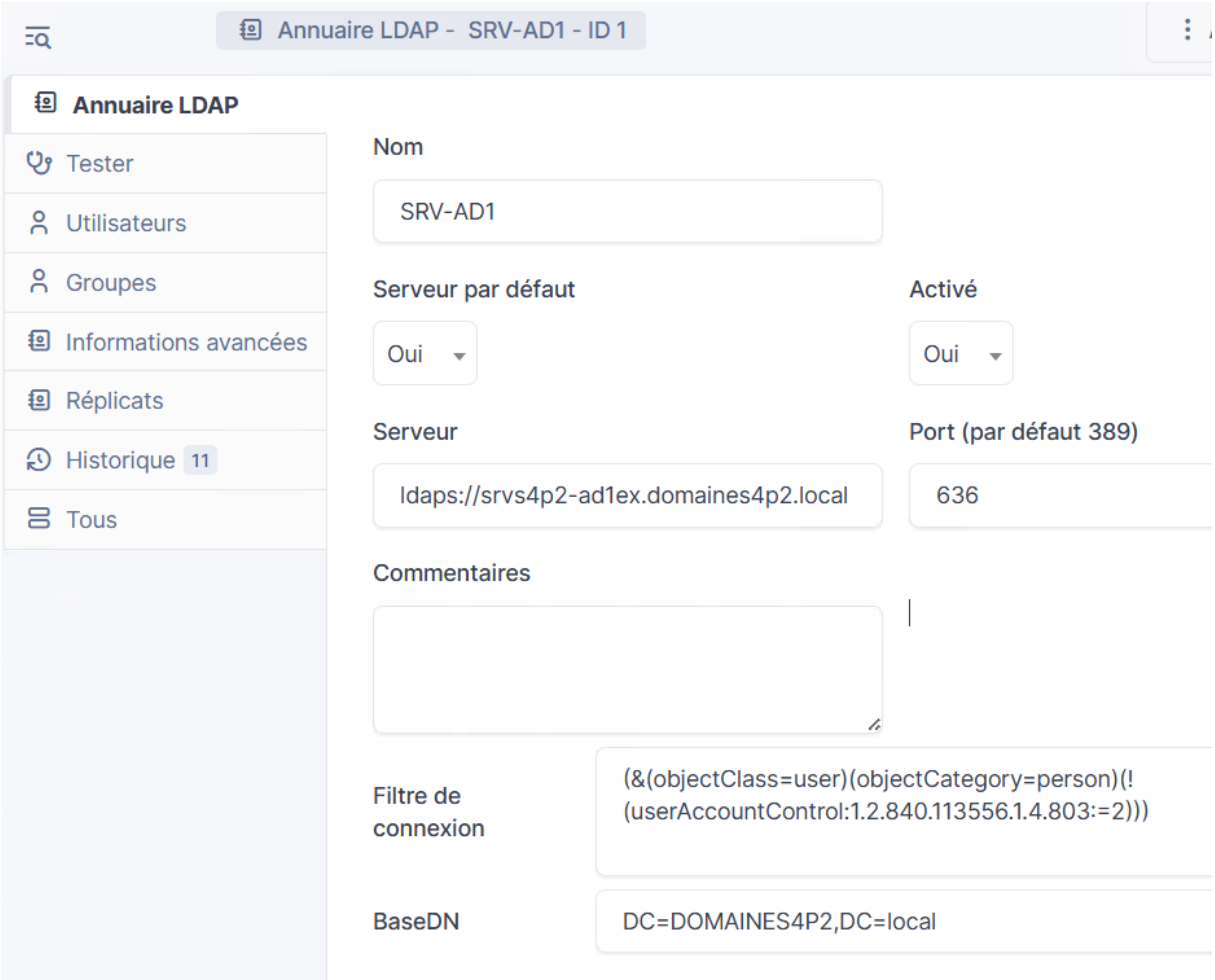


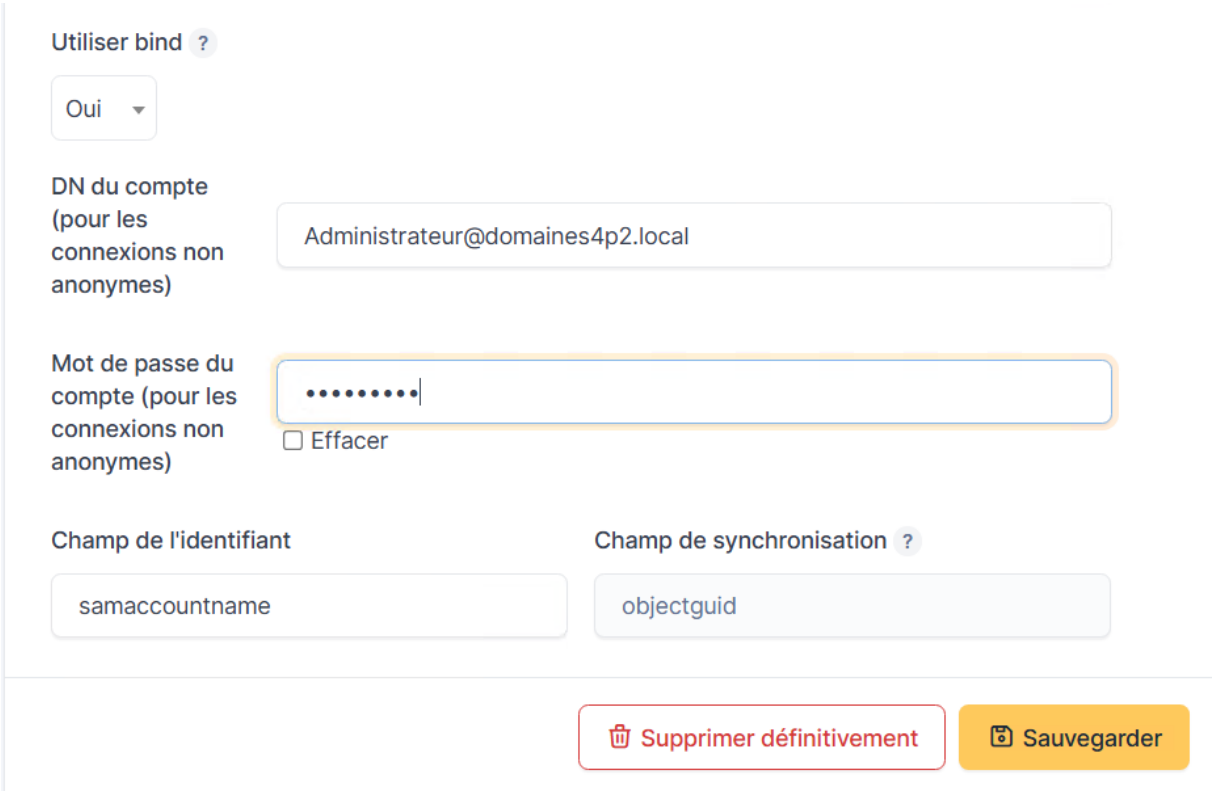


C’est ici que les tickets des utilisateurs du domaine remonteront.

3.1.4. Configuration de la liaison LDAPS avec l'Active Directory

Afin d'automatiser le provisionnement des comptes utilisateurs dans GLPI et de permettre une authentification centralisée via les identifiants du domaine Active Directory, nous avons configuré une liaison d'annuaire sécurisée. Nous avons basculé sur le protocole **LDAPS via le port 636**, garantissant ainsi le **chiffrement** SSL/TLS des échanges d'authentification entre le serveur GLPI et le contrôleur de domaine.





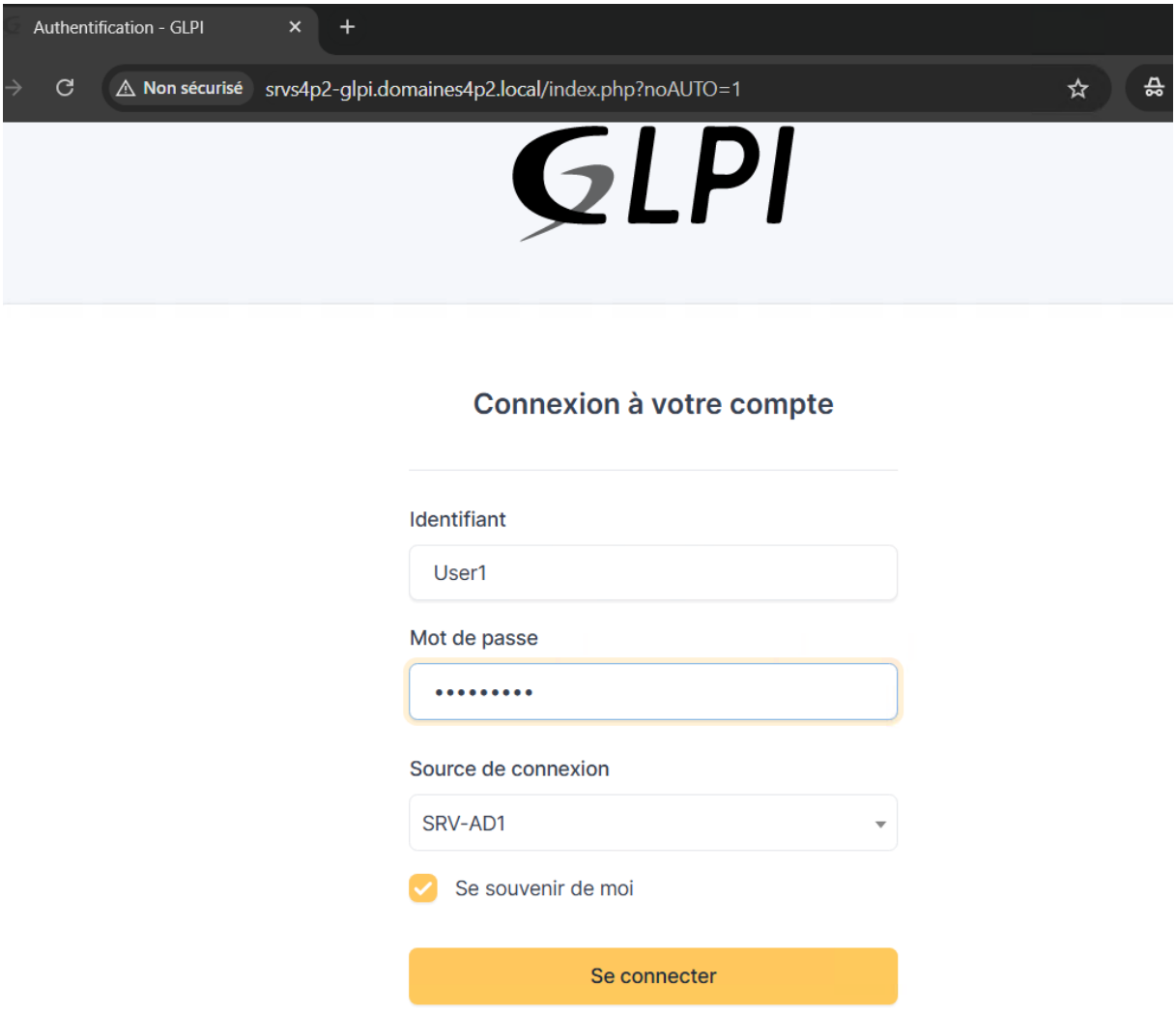
Cette opération a permis de réaliser avec succès l'importation de l'ensemble des comptes utilisateurs ciblés appartenant au domaine Active Directory DOMAINES4P2.local

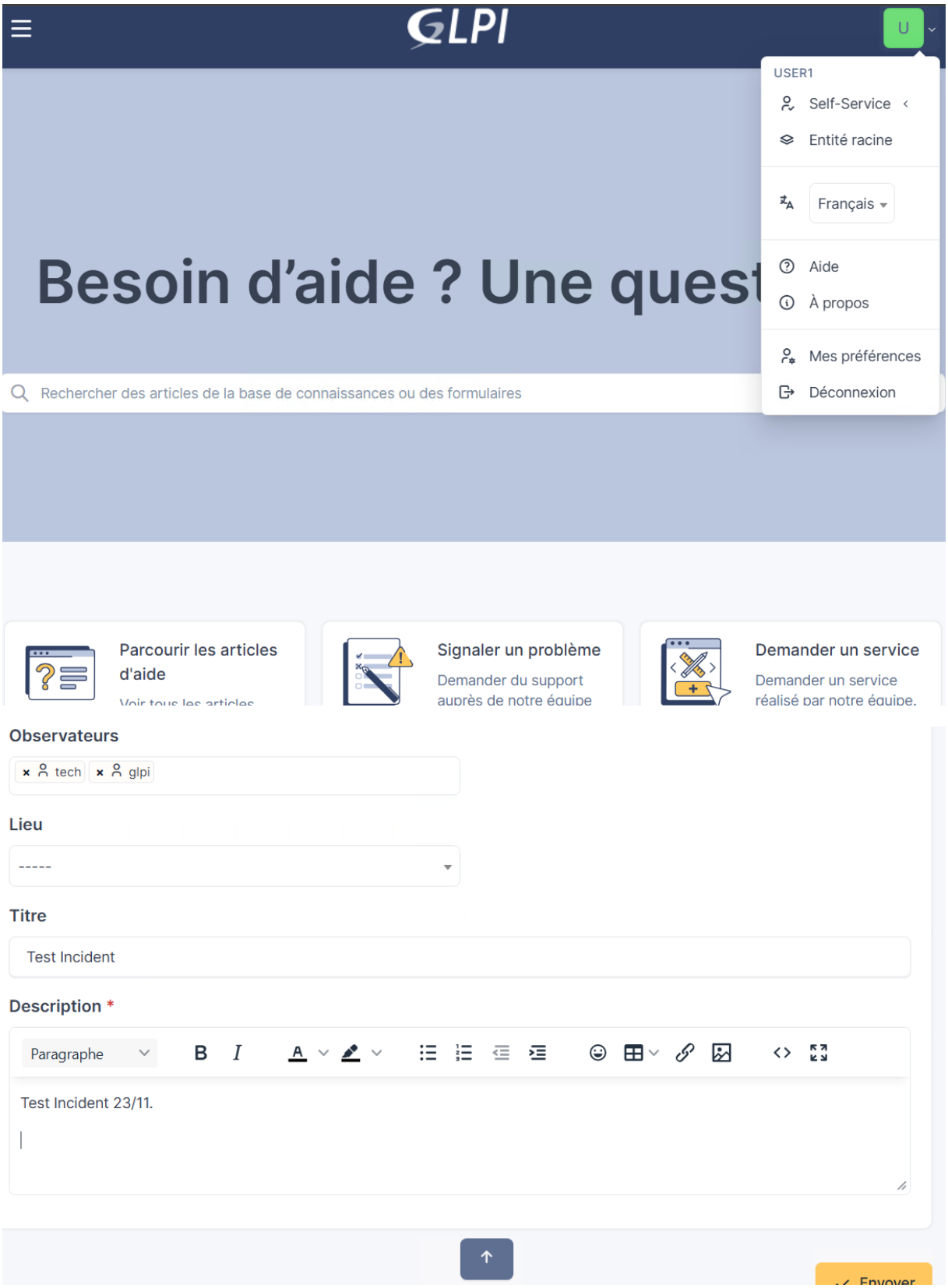
Rechercher Trier

IDENTIFIANT	NOM DE FAMILLE	E-MAILS
GL glpi		
PO post-only		
TE tech		
NO normal		
S glpi-system	Support	
AD Administrateur		Administrateur@domaines4p2.local
U User4		
U User1		
U User2		
U user3		

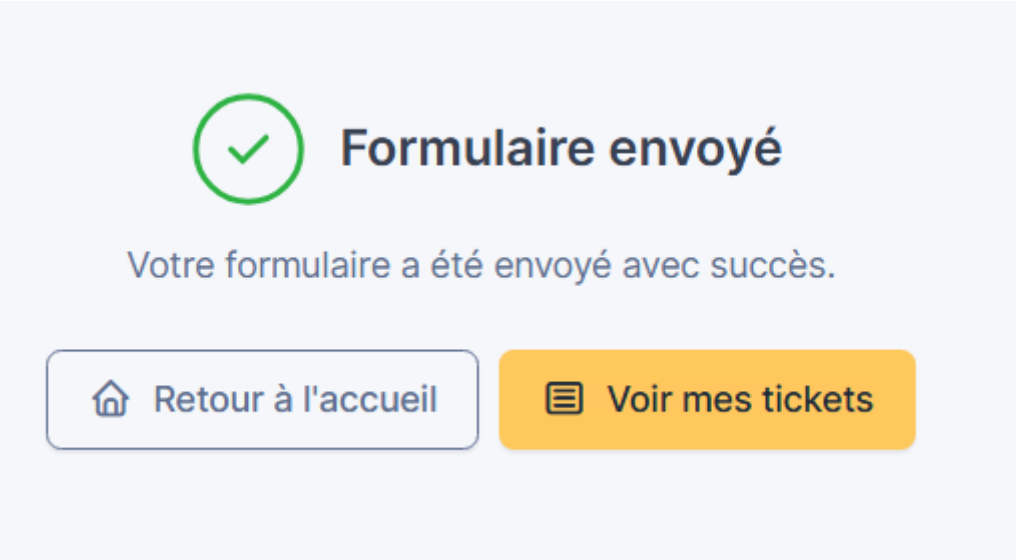
3.1.5. Validation de l'accès utilisateur (« EMPLOYE ») et soumission d'un ticket GLPI.

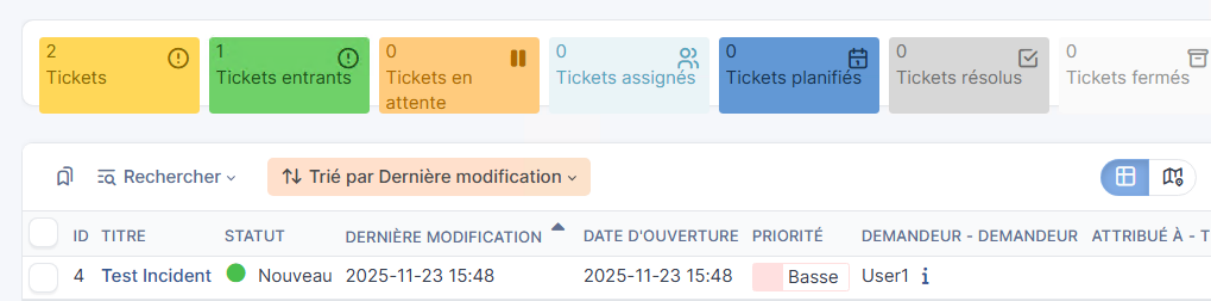
Une phase de validation fonctionnelle est réalisée en utilisant un compte utilisateur standard du domaine (ex : User1). L'accès au portail est initié *via* le raccourci déployé par Stratégie de Groupe (GPO), assurant une expérience utilisateur simplifiée. L'authentification est vérifiée en utilisant les identifiants de session Active Directory habituels. Le test se conclut par la création d'un ticket d'incident pour valider la chaîne complète du service support.




GLPI
U
USER1
Self-Service
Entité racine
Français
Aide
À propos
Mes préférences
Déconnexion
Besoin d'aide ? Une quest
Rechercher des articles de la base de connaissances ou des formulaires
Parcourir les articles d'aide
Signaler un problème
Demander du support auprès de notre équipe
Demander un service
Demander un service réalisé par notre équipe.
Observateurs
tech
glpi
Lieu

Titre
Test Incident
Description *
Paragraphe
Test Incident 23/11.
Envoyer





En conclusion, nous avons déployé avec succès une solution de gestion des incidents et des demandes d'assistance (Helpdesk) pour l'organisation DIGITEX. Les utilisateurs du domaine disposent désormais d'un espace personnalisé pour signaler leurs requêtes à la DSI. Grâce à la centralisation offerte par GLPI, les problématiques techniques du Système d'Information peuvent être gérées de manière organisée et efficiente.

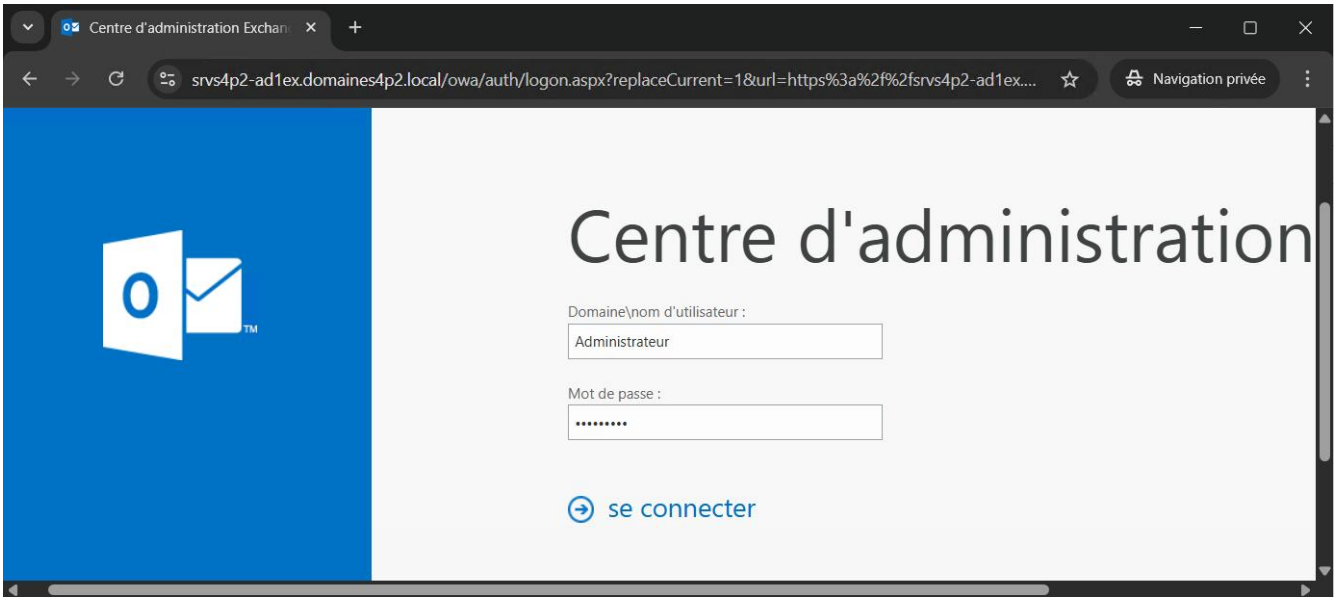
3.2. Messagerie Interne Microsoft EXCHANGE :

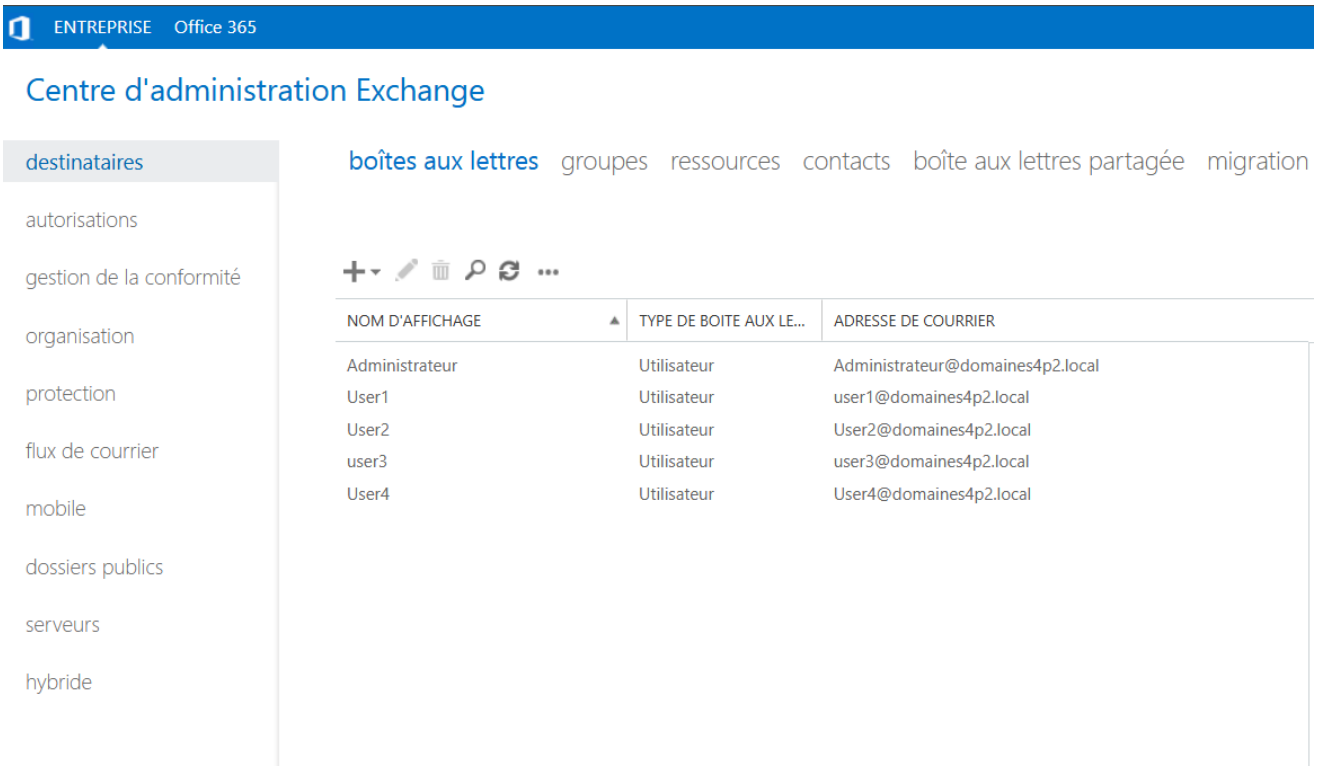
Afin de répondre aux exigences de communication et de collaboration au sein de l'organisation DIGITEX, la mise en œuvre d'une infrastructure de messagerie Microsoft Exchange Server en locale a été décidée. Une intégration native avec l'annuaire Active Directory est implémentée. Elle permet le provisionnement automatique des boîtes aux lettres et l'accès unifié pour les utilisateurs via leurs identifiants de domaine habituels, suivant la même logique que pour le service GLPI.

3.2.2. Interface d'administration Exchange, Import des Utilisateurs :

Suite à l'installation du serveur Exchange, les configurations initiales ont été réalisées via l'interface d'administration Web (Exchange Admin Center) accessible à l'adresse https://srvs4p2-ad1ex.domaines4p2.local/ecp. En utilisant les privilèges d'Administrateur du domaine pour la connexion, nous avons ensuite procédé à l'activation des boîtes aux lettres pour les utilisateurs existants de l'annuaire Active Directory local

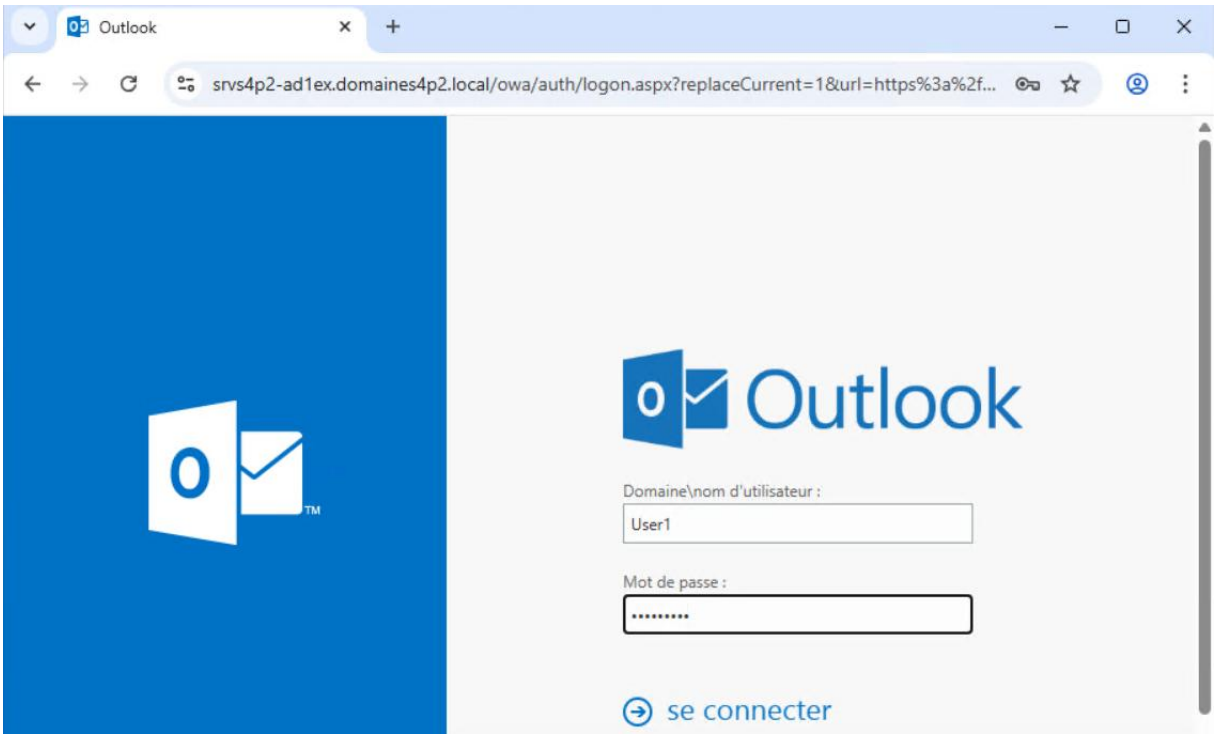
Une boite de messagerie personnelle a été créée pour chaque utilisateur importé.

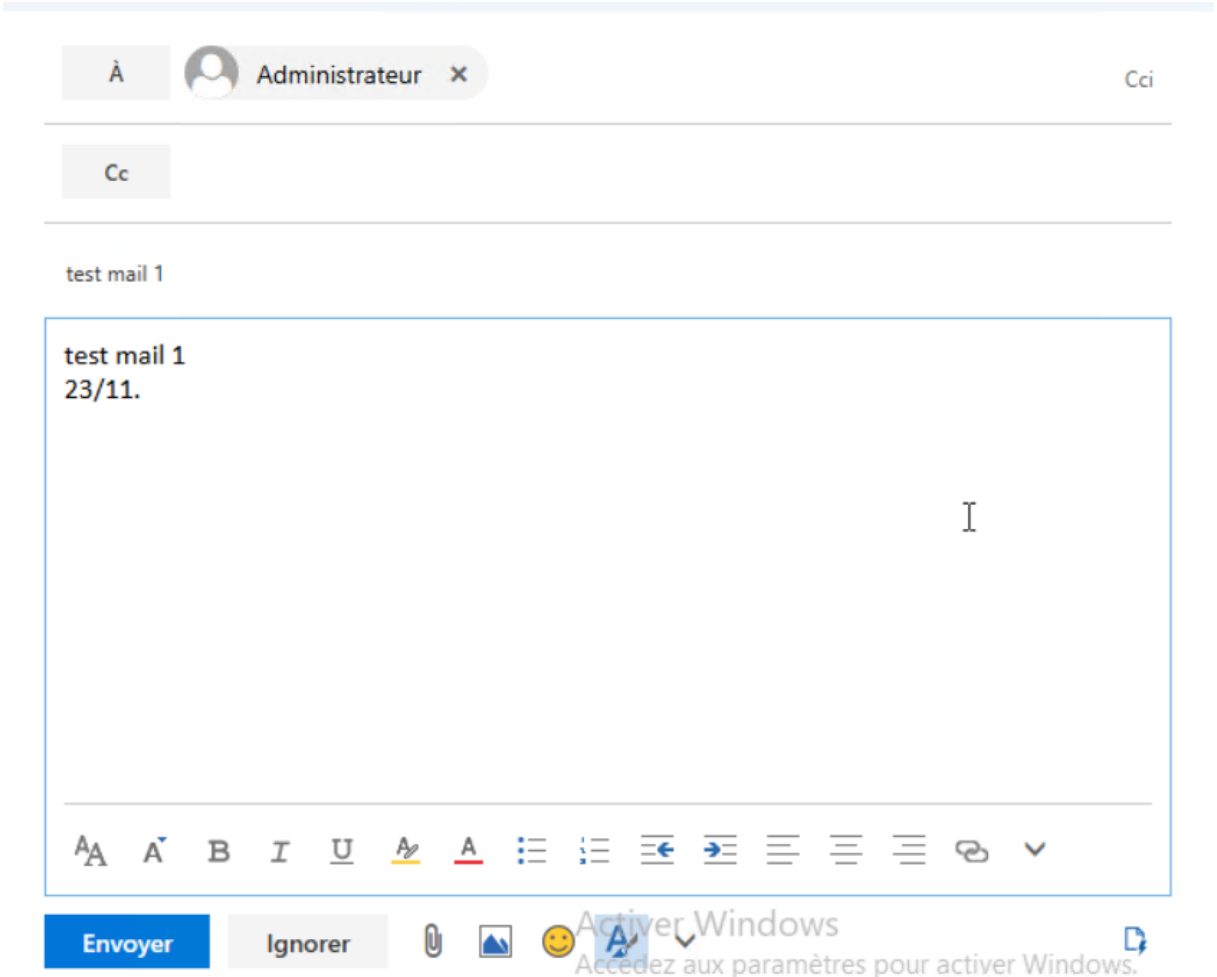


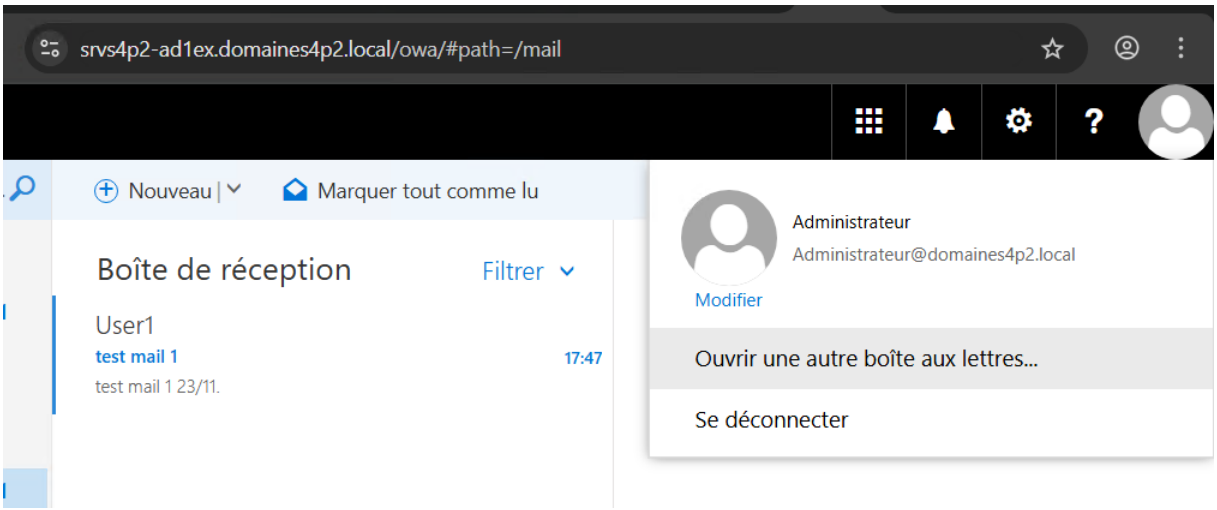


3.2.3. TEST BOITE DE MESSAGERIE UTILISATEUR :

La validation fonctionnelle de la messagerie est réalisée depuis un poste client standard. L'accès à l'interface Outlook Web App (OWA) s'effectue *via* l'URL interne https://srvs4p2-ad1ex.domaines4p2.local/owa , rendue facilement accessible grâce à un raccourci déployé par GPO. Un compte utilisateur test du domaine (ex: User1) est utilisé pour l'authentification. Le bon fonctionnement du service est confirmé par l'envoi et la réception réussis d'un courriel de test vers un autre destinataire interne (ex: le compte Administrateur).


Outlook
srvs4p2-ad1ex.domaines4p2.local/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f...
Outlook
Domaine\nom d'utilisateur :
User1
Mot de passe :
se connecter


À
Administrateur
Cci
Cc
test mail 1
test mail 1
23/11.
Envoyer
Ignorer
Activer Windows
Accédez aux paramètres pour activer Windows.



En conclusion, le déploiement de cette infrastructure Exchange locale répond parfaitement aux exigences de confidentialité des communications internes au domaine Active Directory. Les collaborateurs disposent désormais d'une plateforme centralisée garantissant des échanges de données sécurisés, simplifiés et maîtrisés au sein de l'organisation.

3.2.4. Automatisation du provisionnement des boîtes aux lettres via PowerShell

Le script d'automatisation PowerShell, précédemment présenté pour le déploiement des comptes utilisateurs AD, intègre également un module dédié au provisionnement automatique des boîtes aux lettres Exchange.

3. 3. DÉPLOIEMENT DE L'INFRASTRUCTURE WI-FI MULTI-VLAN (STAFF & INVITÉS)

Afin de répondre aux besoins de mobilité de l'entreprise **Digitex** tout en garantissant la sécurité des données, une architecture Wi-Fi centralisée a été mise en place via une borne **Ubiquiti UniFi U7 Lite** pilotée par un contrôleur sous Debian (192.168.17.7). Cette borne diffuse deux réseaux distincts (SSID), dont les flux sont ségrégués dès la source grâce au marquage **802.1Q**.

1. Réseau Invités (VLAN 37 – 192.168.37.0/24) :

Dédié aux visiteurs, ce réseau offre un accès Internet strictement isolé du réseau de production.

L'authentification est assurée par un **Portail Captif** hébergé sur le contrôleur, imposant la validation des CGU et garantissant la traçabilité légale des connexions.

La sécurité est déléguée au pare-feu **PfSense** qui assure le relais du service DHCP (évitant l'exposition de l'AD interne) et bloque tout accès vers les réseaux locaux (LAN/Serveurs), n'autorisant que le trafic Web vers le WAN.

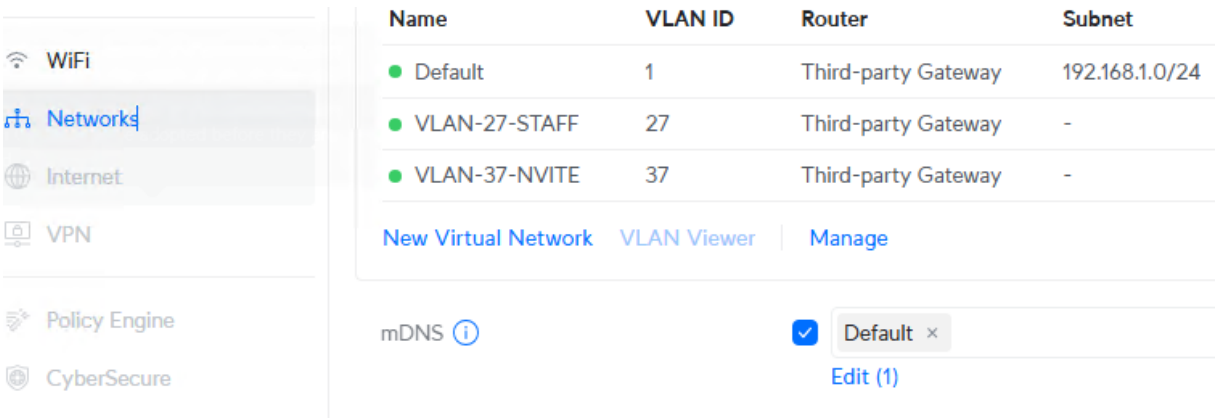
2. Réseau Collaborateurs (VLAN 27 – 192.168.27.0/24) :

Réservé aux employés, ce SSID ("STAFF") permet l'accès aux ressources internes nécessaires à l'activité.

La borne tague les trames sortantes avec l'ID **27**, permettant au commutateur et au routeur de traiter ce flux différemment des invités.

Des règles de pare-feu spécifiques autorisent l'accès aux serveurs de fichiers et imprimantes, tout en maintenant le cloisonnement nécessaire vis-à-vis des zones critiques.

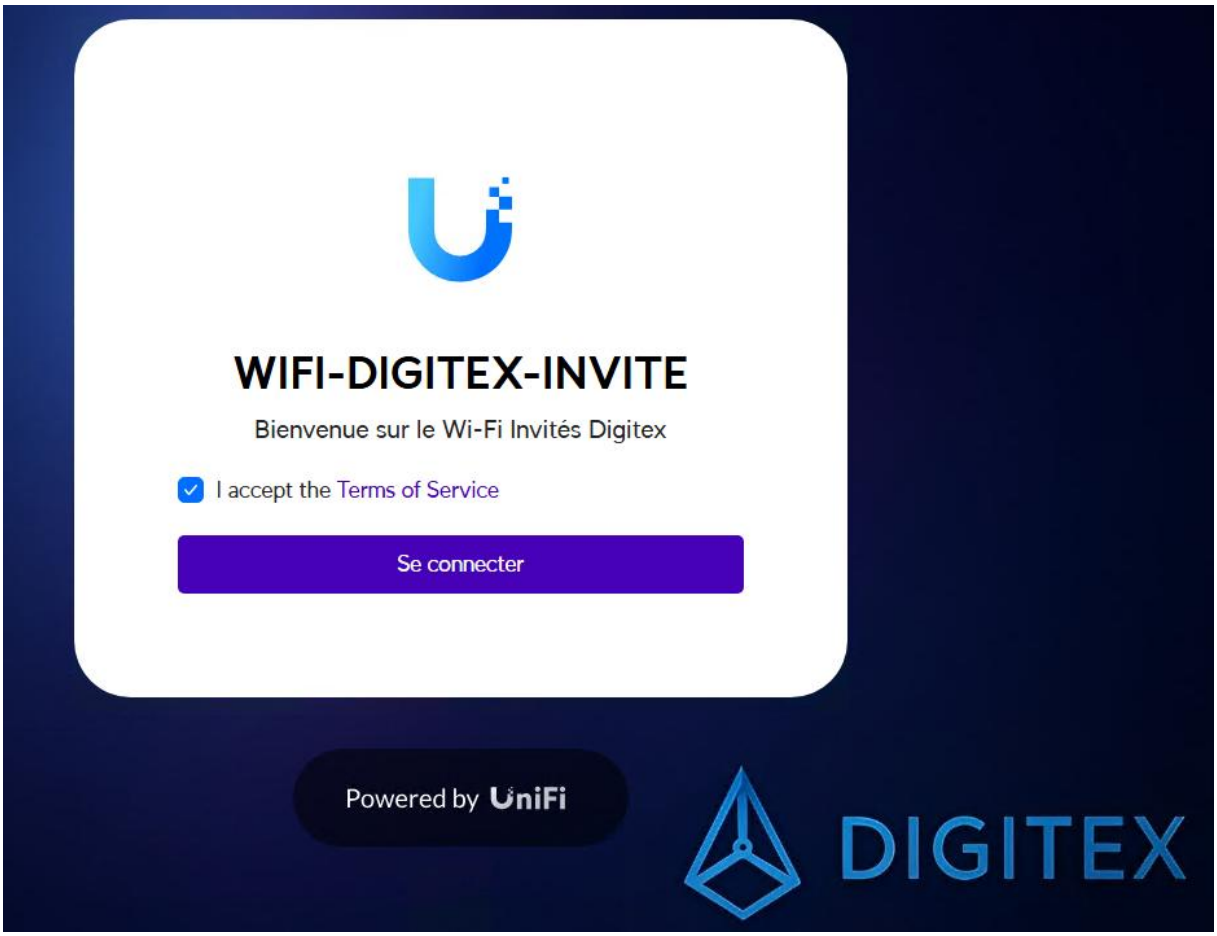
3.3.1. CONFIGURATION GENERALES :



Name	Network	Broadcasting APs	WiFi Band
Wifi-S4P2-STAFF	VLAN-27-STAFF (27)	All APs	2.4 GHz 5 GHz
WIFI-S4P2-INVITE	VLAN-37-NVITE (37)	All APs	2.4 GHz 5 GHz

Create New | Manage

For optimal IoT interoperability, we recommend creating a dedicated network for your 2.4 GHz IoT devices.



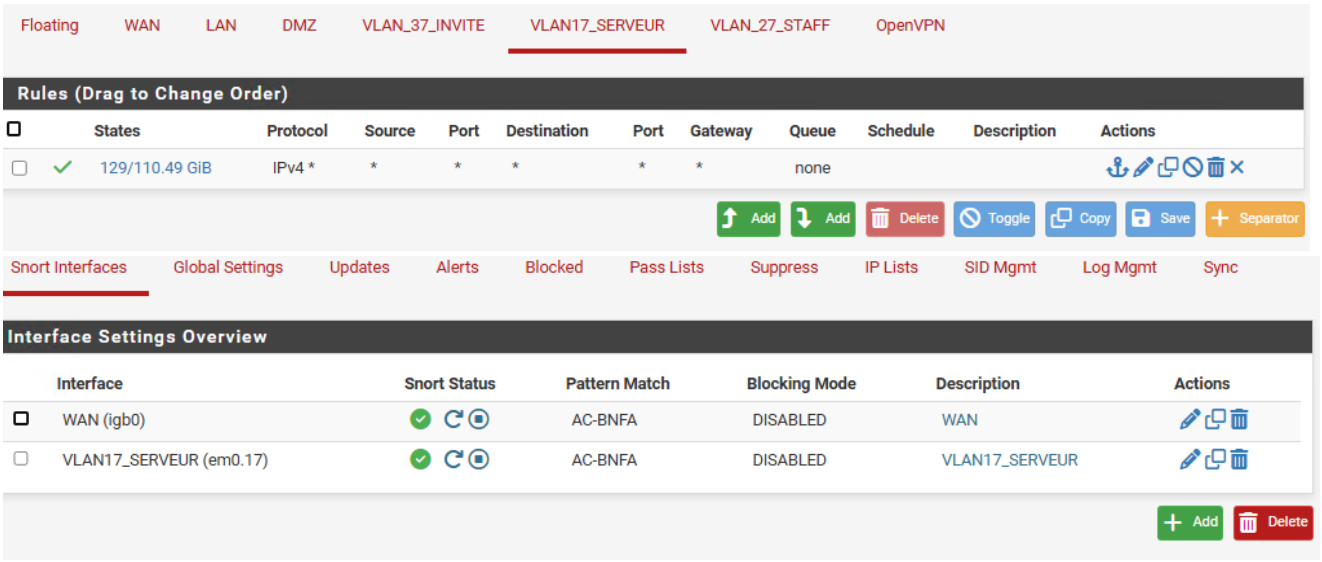
Les invités bénéficient ainsi d'une connectivité Web, sans que cela ne constitue une menace pour l'intégrité des ressources internes de l'entreprise

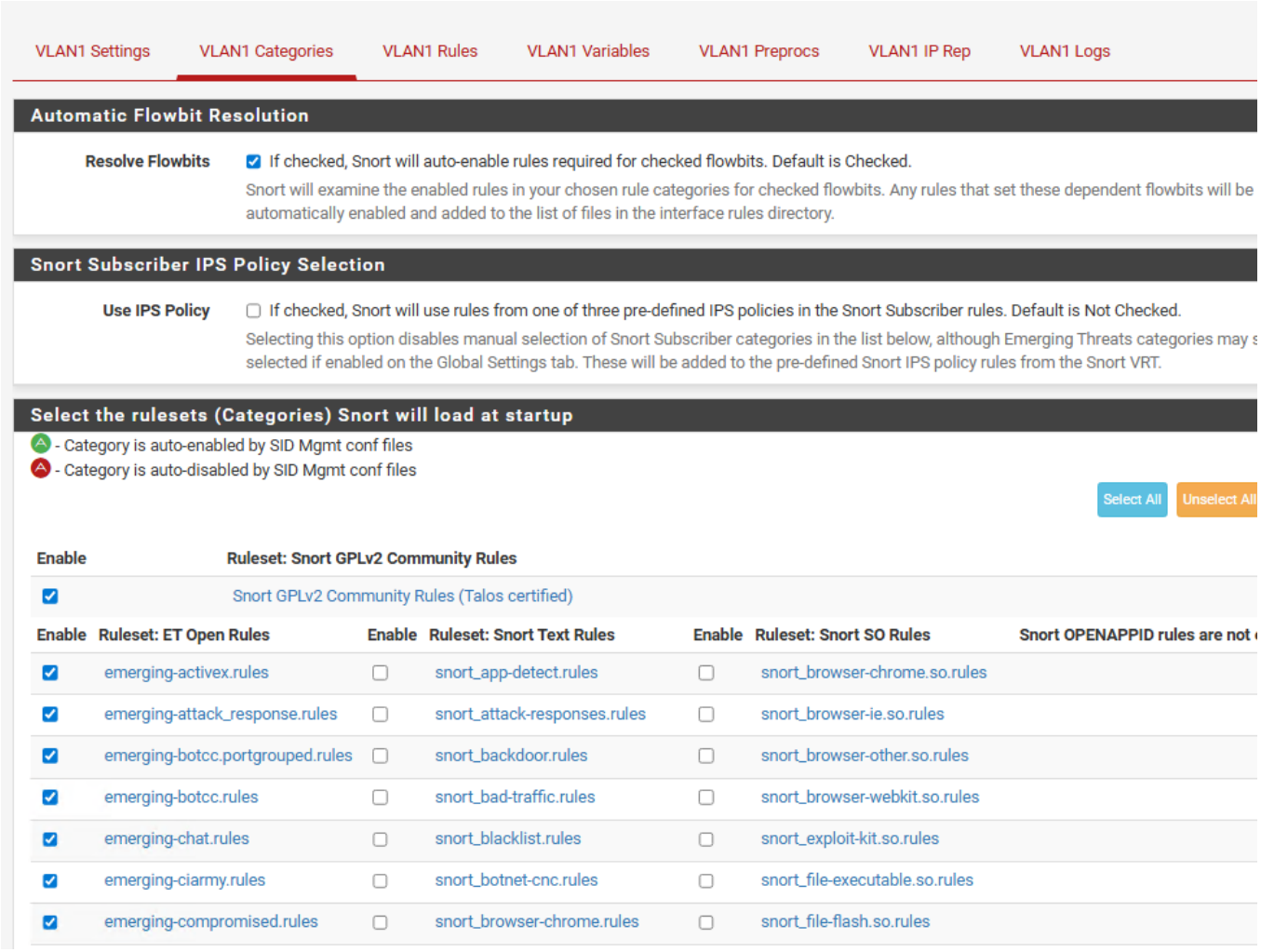
3.4. Sécurisation et cloisonnement réseau via PfSense

L'infrastructure réseau et les services étant désormais opérationnels, la sécurisation des échanges nécessite le déploiement d'une politique de filtrage stricte sur le pare-feu PfSense. Cette étape vise à garantir le cloisonnement logique des différentes zones (VLANs) et à protéger les ressources sensibles en appliquant le principe du moindre privilège. Concrètement, les règles de pare-feu sont configurées pour restreindre les flux réseaux, assurant que seuls les utilisateurs et services dûment habilités puissent accéder aux applications critiques, tout en bloquant systématiquement tout trafic non légitime pour préserver l'intégrité du système d'information.

3.4.1 Règles Interface VLAN-17

Le sous-réseau Serveurs (VLAN 17) est isolé des utilisateurs par des règles de filtrage autorisant uniquement les services nécessaires. Aucune restriction interne n'est appliquée entre les serveurs. Parallèlement, l'activation du module **Snort** assure une surveillance active (IDS) pour détecter les intrusions potentielles.





La surveillance du **VLAN 17** est assurée par l'application des signatures 'Basic' et 'Open Rules'. Les incidents de sécurité (avertissements et alertes critiques) font l'objet d'une **journalisation automatique** via le système de logs de PfSense

Most Recent 250 Entries from Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-11-27 11:20:48	⚠	3	UDP	Misc activity	192.168.17.1	60893	10.0.2.100	47745	1:2033078	ET INFO Session Traversal Utilities for NAT (STUN Binding Request On Non-Standard High Port)
2025-11-27 11:20:48	⚠	3	UDP	Misc activity	192.168.17.1	60893	10.0.2.100	47745	1:2033078	ET INFO Session Traversal Utilities for NAT (STUN Binding Request On Non-Standard High Port)
2025-11-27 11:20:48	⚠	3	UDP	Misc activity	192.168.17.1	60893	10.0.2.100	47745	1:2033078	ET INFO Session Traversal Utilities for NAT (STUN Binding Request On Non-Standard High Port)
2025-11-27 11:20:48	⚠	3	UDP	Misc activity	192.168.17.1	60893	10.0.2.100	47745	1:2033078	ET INFO Session Traversal Utilities for NAT (STUN Binding Request On Non-Standard High Port)

3.4.2. Règles Interface VLAN-27 :

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☐ ✓	0/0 B	IPv4 TCP	VLAN_27_ STAFF subnets	*	192.168.17.3	80 (HTTP)	*	none		ALLOW_WEB_GLPI
☐ ✓	0/0 B	IPv4 TCP	VLAN_27_ STAFF subnets	*	192.168.17.5	3128	*	none		ALLOW_ARTICA_PROXY
☐ ✓	0/0 B	IPv4 TCP	VLAN_27_ STAFF subnets	*	192.168.17.5	9025	*	none		ALLOW_ARTICA_ERROR_PAGE
☐ ✗	0/0 B	IPv4 *	VLAN_27_ STAFF subnets	*	192.168.17.253	*	*	none		BLOCK_CONNECTION_PROXMOX
☐ ✗	0/0 B	IPv4 TCP/UDP	VLAN_27_ STAFF subnets	*	192.168.17.4	80 (HTTP)	*	none		BLOCK_CONNECTION_ZABBIX
☐ ✗	0/0 B	IPv4 *	VLAN_27_ STAFF subnets	*	VLAN_37_INVITE subnets	*	*	none		BLOCK_CONNECTION_VLAN37_INVITE
☐ ✗	0/0 B	IPv4 TCP	VLAN_27_ STAFF subnets	*	10.4.2.2	Netgear_ HTTPS_HTTP	*	none		BLOCK_NETGEAR_WEB
☐ ✗	0/0 B	IPv4 TCP/UDP	VLAN_27_ STAFF subnets	*	This Firewall (self)	22 (SSH)	*	none		BLOCK_PFSENSE_SSH
☐ ✗	0/0 B	IPv4 TCP	VLAN_27_ STAFF subnets	*	This Firewall (self)	80 (HTTP)	*	none		BLOCK_PFSENSE_WEB_HTTP
☐ ✗	0/0 B	IPv4 TCP/UDP	VLAN_27_ STAFF subnets	*	This Firewall (self)	443 (HTTPS)	*	none		BLOCK_PFSENSE_WEB_HTTPS
☐ ✗	0/0 B	IPv4 TCP/UDP	VLAN_27_ STAFF subnets	*	Server_Active_ Directory	3389 (MS RDP)	*	none		BLOCK_CONNECTION_RDP_AD1-AD2
☐ ✓	0/4.08 MiB	IPv4 *	VLAN_27_ STAFF subnets	*	Server_Active_ Directory	*	*	none		ALLOW_AD1_AD2
☐ ✓	14/7.53 GiB	IPv4 *	*	*	*	*	*	none		

3.4.3. RÈGLES INTERFACE VLAN-37 :

Floating WAN LAN DMZ VLAN_37_INVITE VLAN17_SERVEUR VLAN_27_STAFF OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☐ ✓	0/0 B	IPv4 TCP	VLAN_37_ INVITE subnets	*	192.168.17.7	UniFi_Portail_ Captif	*	none		ALLOW_PORTAILS_CAPTIF_UNIFI
☐ ✓	0/0 B	IPv4 UDP	VLAN_37_ INVITE subnets	*	This Firewall (self)	67	*	none		ALLOW_DHCP_REQUEST
☐ ✗	0/0 B	IPv4 TCP	VLAN_37_ INVITE subnets	*	This Firewall (self)	22 (SSH)	*	none		BLOCK_PFSENSE_SSH
☐ ✗	0/0 B	IPv4 TCP	VLAN_37_ INVITE subnets	*	This Firewall (self)	80 (HTTP)	*	none		BLOCK_PFSENSE_WEB_HTTP
☐ ✗	0/0 B	IPv4 TCP	VLAN_37_ INVITE subnets	*	This Firewall (self)	443 (HTTPS)	*	none		BLOCK_PFSENSE_WEB_HTTPS
☐ ✗	0/0 B	IPv4 TCP	VLAN_37_ INVITE subnets	*	10.4.2.2	Netgear_ HTTPS_HTTP	*	none		BLOCK_CONNECTION_NETGEAR
☐ ✗	0/0 B	IPv4 *	VLAN_37_ INVITE subnets	*	VLAN_27_STAFF subnets	*	*	none		BLOCK_CONNECTION_VLAN27_STAFF
☐ ✗	0/0 B	IPv4 *	VLAN_37_ INVITE subnets	*	VLAN17_SERVEUR subnets	*	*	none		BLOCK_CONNECTION_VLAN17_SERVEUR
☐ ✓	0/0 B	IPv4 UDP	VLAN_37_ INVITE subnets	*	*	53 (DNS)	*	none		ALLOW_DNS_OVER_INTERNET
☐ ✓	0/0 B	IPv4 *	*	*	*	*	*	none		

3.5. DÉPLOIEMENT D'UN VPN SÉCURISÉ (OPENVPN)

Afin d'assurer la continuité d'activité en situation de télétravail, une solution de **VPN Client-to-Site** a été déployée sur le pare-feu **PfSense**. Ce tunnel permet aux collaborateurs d'accéder aux ressources du réseau local depuis un réseau externe de manière transparente et sécurisée. L'architecture repose sur le protocole **OpenVPN**, garantissant la confidentialité et l'intégrité des échanges grâce à un chiffrement **SSL/TLS**. La mise en œuvre s'appuie sur une Infrastructure à Clés Publiques complète comprenant :

- La création d'une Autorité de Certification (CA).
- La génération de certificats serveur et utilisateurs.
- La configuration des paramètres de tunnel et de chiffrement.

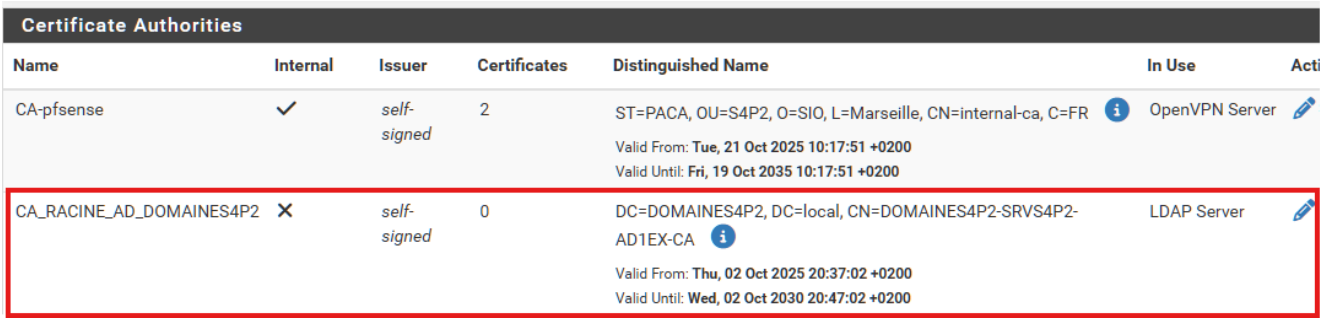
3.6 Sécurisation de l'Authentification (LDAPS)

Afin de simplifier la gestion des comptes et de garantir une sécurité optimale, l'authentification des utilisateurs VPN n'est pas gérée localement sur le pare-feu, mais est déléguée à l'annuaire **Active Directory** de l'entreprise.

Cependant, le protocole LDAP standard transmettant les informations en clair, nous avons configuré une liaison sécurisée **LDAPS** (LDAP over SSL) entre le pare-feu PfSense et le Contrôleur de Domaine.

3.6.1 : Chaîne de confiance (Certificats) :

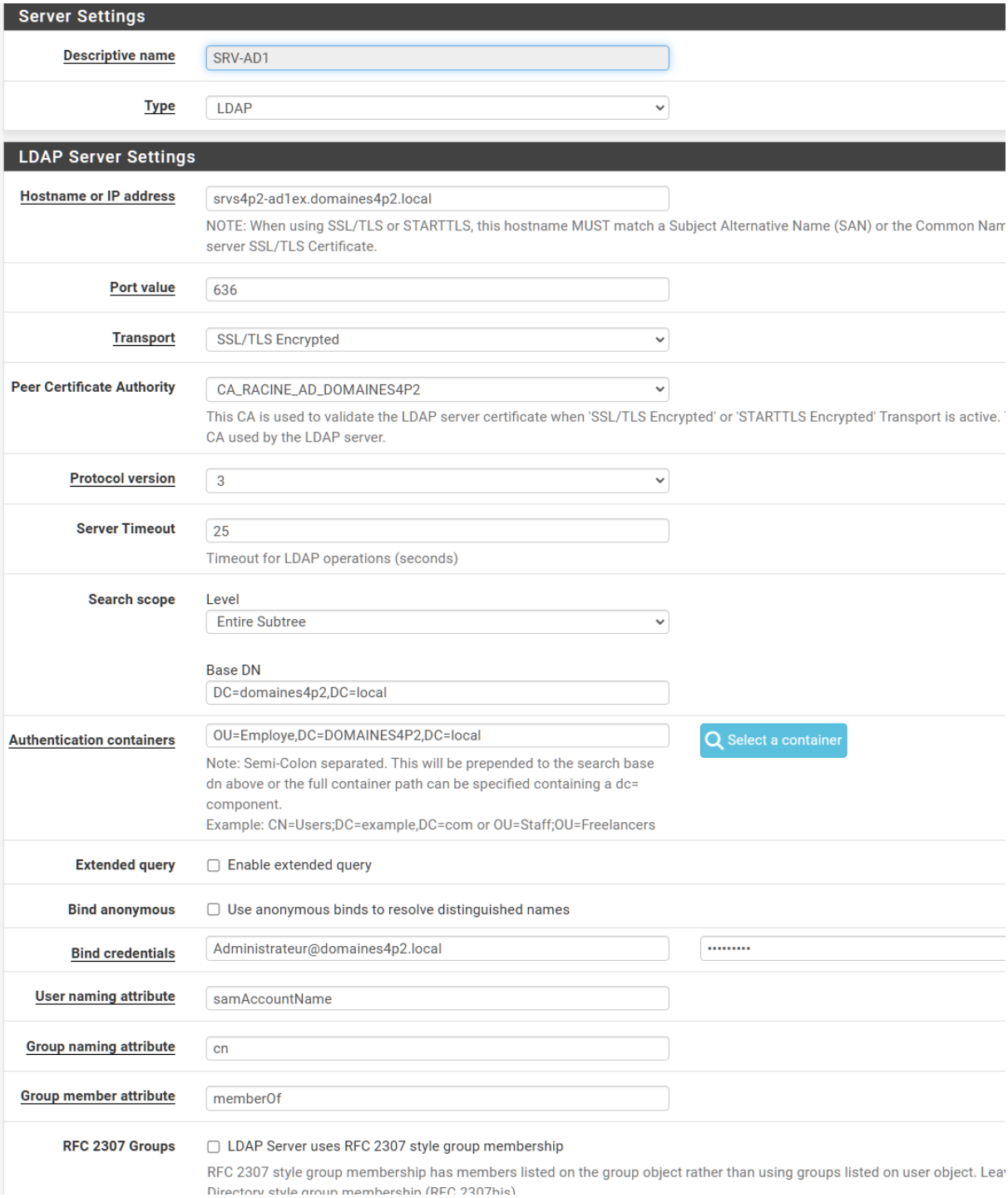
Pour que le chiffrement puisse s'établir, le pare-feu doit faire confiance au serveur Active Directory. Nous avons exporté le certificat de l'Autorité de Certification (CA) Racine depuis le serveur Windows, puis nous l'avons importé dans le gestionnaire de certificats de PfSense.

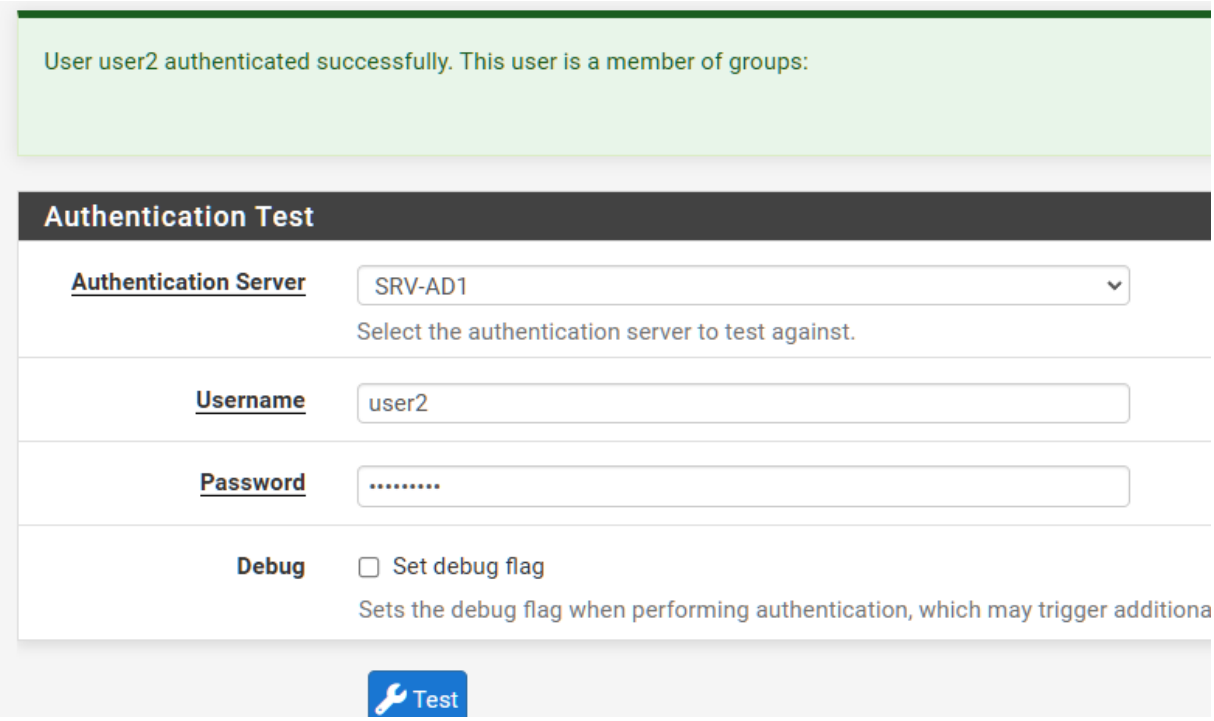


Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Acti
CA-pfsense	✓	*self-signed*	2	ST=PACA, OU=S4P2, O=SIO, L=Marseille, CN=internal-ca, C=FR Valid From: **Tue, 21 Oct 2025 10:17:51 +0200** Valid Until: **Fri, 19 Oct 2035 10:17:51 +0200**	OpenVPN Server	
CA_RACINE_AD_DOMAINES4P2	✗	*self-signed*	0	DC=DOMAINES4P2, DC=local, CN=DOMAINES4P2-SRVS4P2-AD1EX-CA Valid From: **Thu, 02 Oct 2025 20:37:02 +0200** Valid Until: **Wed, 02 Oct 2030 20:47:02 +0200**	LDAP Server	

- Configuration et test liaison LDAPS :





Génération des certificats utilisateurs et Double Authentification

Afin de garantir un niveau de sécurité optimal, le mode **"SSL/TLS + User Auth"** a été retenu. Cette configuration impose la génération d'un **certificat client unique** pour chaque utilisateur de l'Active Directory. Bien que cette étape soit manuelle, elle est essentielle pour assurer une **authentification à double facteur** (2FA) : l'accès au VPN requiert non seulement la validation des identifiants AD (ce que l'utilisateur sait), mais aussi la possession du certificat numérique (ce que l'utilisateur possède), neutralisant ainsi les risques liés au vol de mot de passe.

- Certificat Utilisateur (ex User 2) :

Method : Create an internal Certificate

Descriptive name : Certif_User2

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?,

Internal Certificate

Certificate authority : CA-pfsense

Key type : RSA

2048

The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the ce

Digest Algorithm : sha256

The digest method used when the certificate is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as th
algorithms invalid.

Lifetime (days) : 3650

The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may co

Common Name : user2

The following certificate subject components are optional and may be left blank.

Country Code : FR

State or Province : PACA

Nous avons ensuite créé et configuré le serveur VPN avec son certificat.

OpenVPN Server *Server Certificate* CA: **No** Server: **Yes**	CA-pfsense	ST=PACA, OU=S4P2, O=SIO, L=Marseille, CN=192.168.100.17, C=FR Valid From: **Thu, 30 Oct 2025 13:15:59 +0100** Valid Until: **Sun, 28 Oct 2035 13:15:59 +0100**	OpenVPN Server

VPN / OpenVPN / Servers

Servers | Clients | Client Specific Overrides | Wizards | Client Export

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description
WAN	UDP4 / 20031 (TUN)	172.1.1.0/24	**Mode:** Remote Access (SSL/TLS + User Auth) **Data Ciphers:** AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC **Digest:** SHA256 **D-H Params:** 2048 bits	VPN-S4P2

General Information

Description
VPN-S4P2
A description of this VPN for administrative reference.

Disabled
☐ Disable this server
Set this option to disable this server without removing it from the list.

Unique VPN ID
Server 1 (ovpns1)

Mode Configuration

Server mode
Remote Access (SSL/TLS + User Auth)

Backend for authentication
SRV-AD1
Local Database

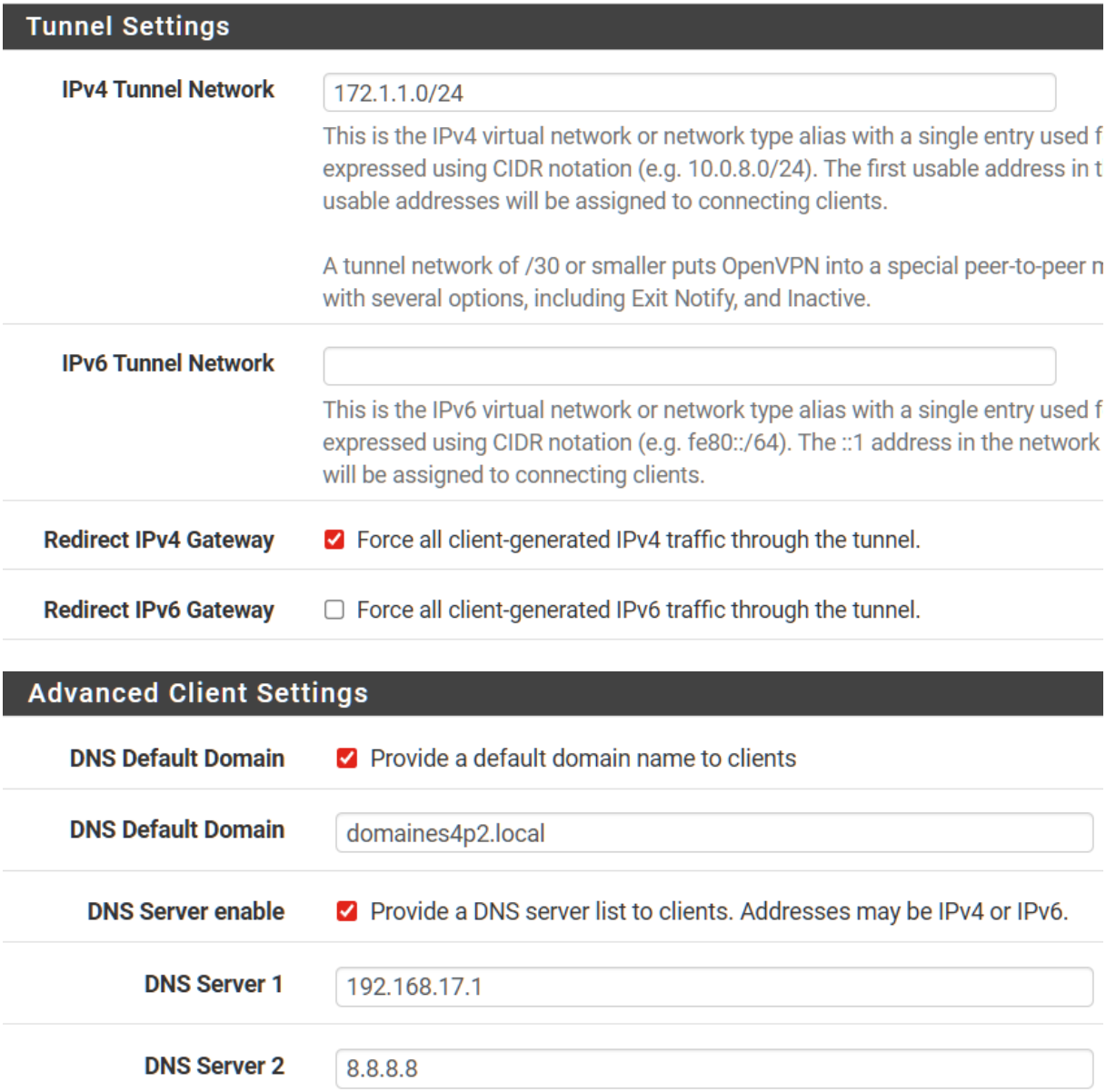
Device mode
tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Endpoint Configuration

Protocol
UDP on IPv4 only

Interface
WAN
The interface or Virtual IP address where OpenVPN will receive client connections.

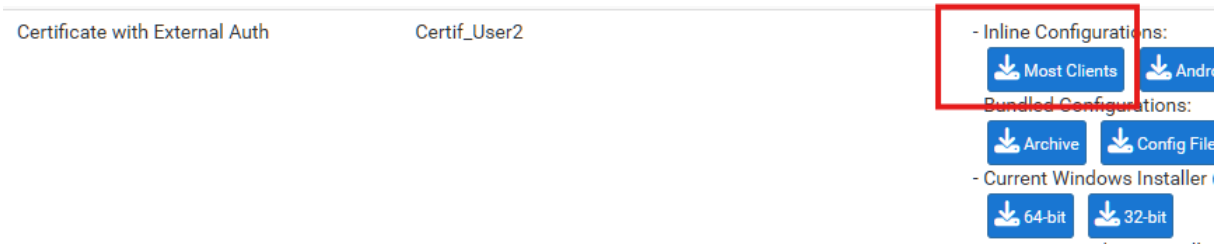
Local port
20031
The port used by OpenVPN to receive client connections.

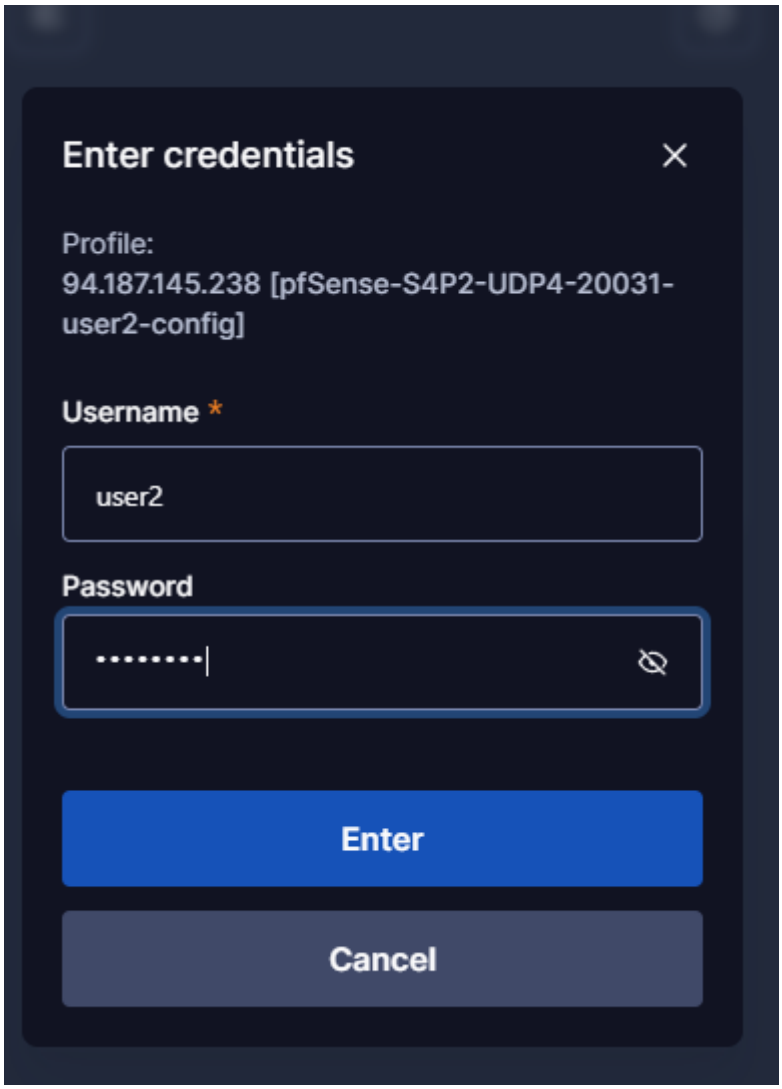


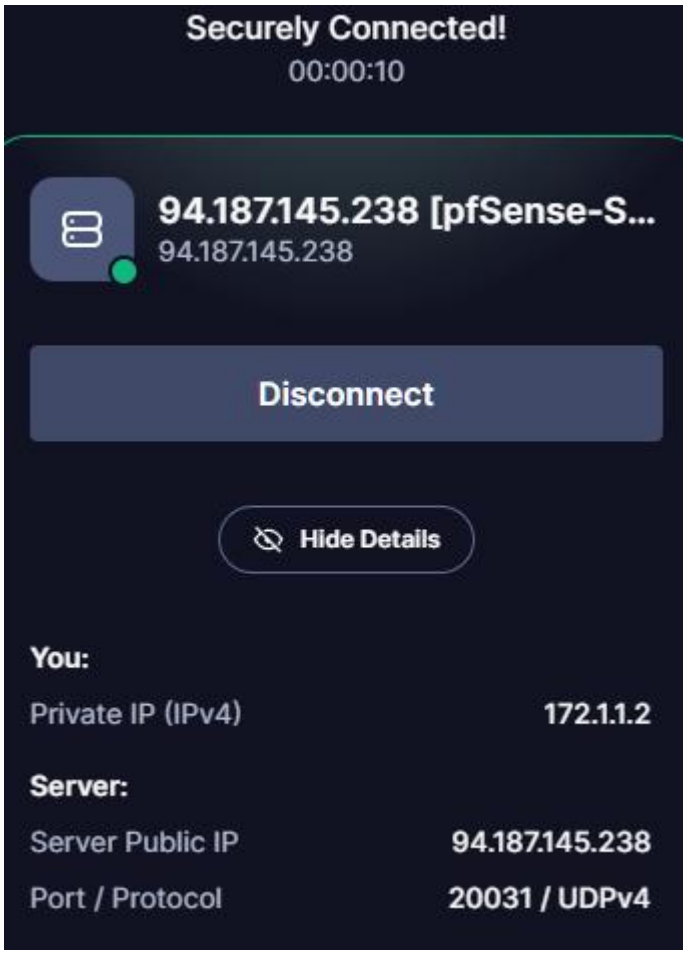
Afin de rendre le service VPN accessible depuis l'extérieur, une règle de traduction d'adresse (NAT/PAT) a été configurée sur le routeur de bordure (Gateway du centre IFC Marseille). Cette règle redirige systématiquement tout le trafic entrant sur l'adresse IP publique via le port **20031** vers l'interface WAN du pare-feu PfSense, qui héberge le serveur OpenVPN.

3.6.2 Déploiement de la Configuration VPN – Client VPN :

Pour le compte **user2**, nous allons télécharger la configuration « **inline** » tout-en-un. Comme le client OpenVPN sera déployé automatiquement par **GPO**, aucune installation manuelle n'est requise, l'utilisateur devra simplement importer ce fichier de configuration pour se connecter.



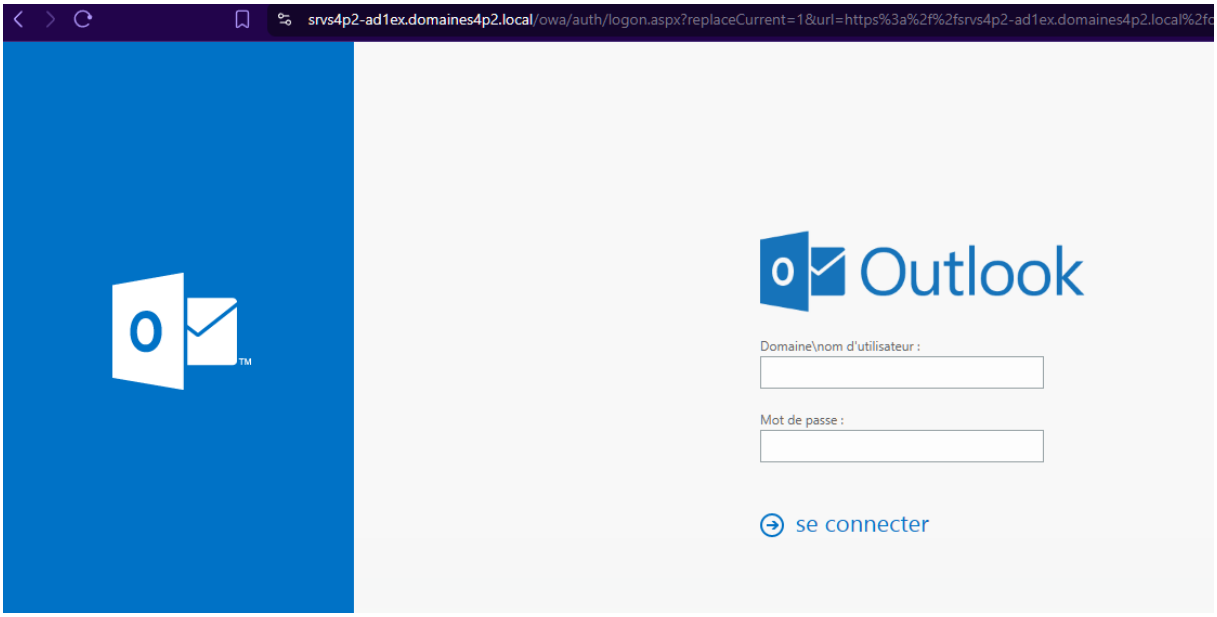


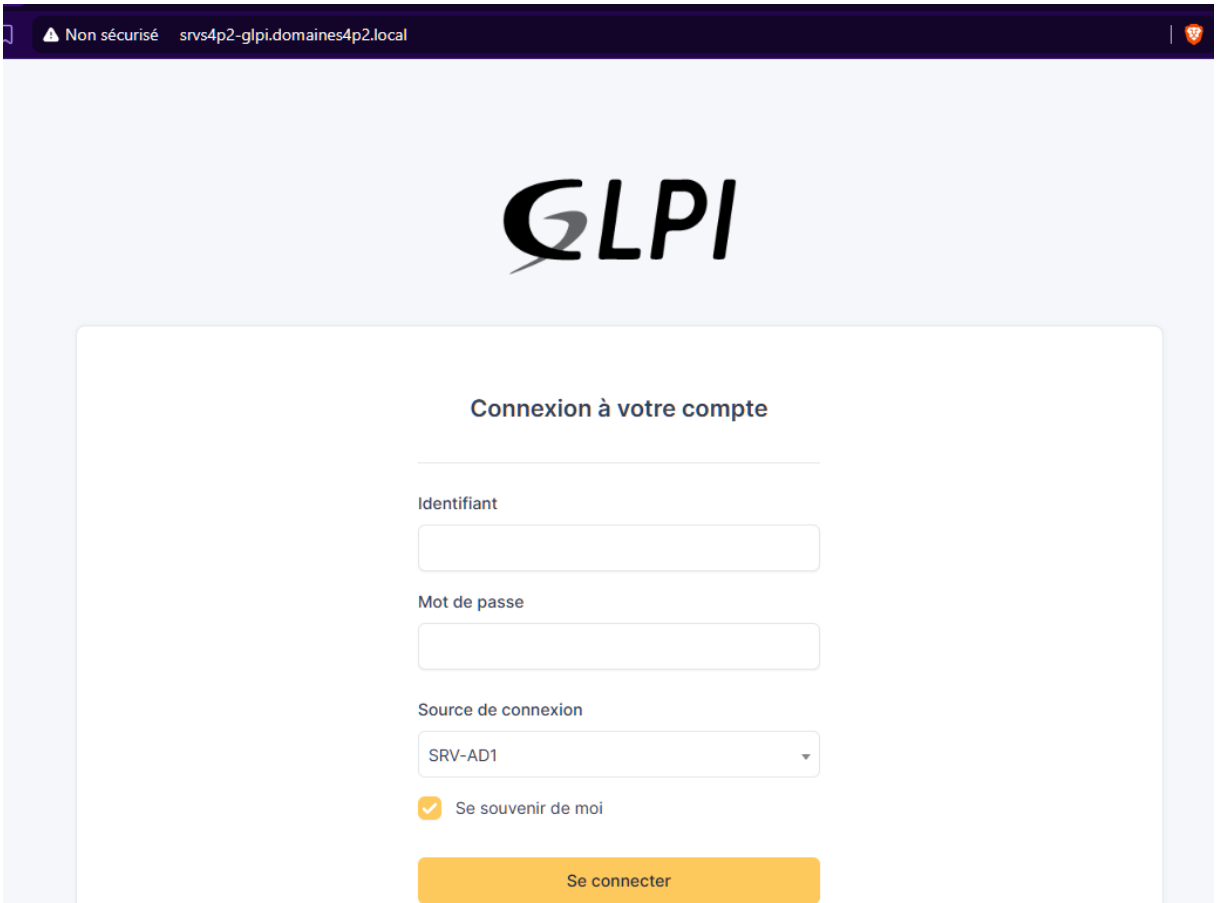


TEST PARAMETTRES DHCP, DNS :

```
Carte inconnue Connexion au réseau local 2 :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : TAP-Windows Adapter V9 for OpenVPN Connect
   Adresse physique . . . . . . . . . . . : 00-FF-AE-F7-C4-B8
   DHCP activé. . . . . . . . . . . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::aa2b:f982:6a6:f9d0%23(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 172.1.1.2(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :
   IAID DHCPv6 . . . . . . . . . . . : 1543569326
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2E-A8-31-42-E8-9C-25-91-37-A9
   Serveurs DNS. . .  . . . . . . . . . : 192.168.17.1
                                 8.8.8.8
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

TEST ACCÈS SERVICES ET RESSOURCES :





6. CONCLUSION

Ce cursus de deux ans en BTS SIO (option SISR) au sein de l'IFC Marseille m'a permis de consolider mes acquis techniques et de développer une expertise concrète en administration réseaux et cybersécurité.

Le projet réalisé pour l'entreprise **Digitex** illustre cette montée en compétences. L'organisation dispose désormais d'une infrastructure robuste, sécurisée et évolutive, répondant aux standards actuels du marché. Au-delà de la simple mise en réseau, l'accent a été mis sur la disponibilité des services, le cloisonnement des flux (VLANs, Pare-feu) et la sécurisation des accès VPN, garantissant ainsi un outil de travail performant pour les utilisateurs.

Cette expérience de déploiement global confirme ma capacité à analyser les besoins d'une entreprise et à y répondre par des solutions techniques adaptées. Je suis désormais opérationnel pour transposer ces compétences dans un environnement professionnel réel.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE 10-A : Outil d'aide à l'appréciation de l'environnement technologique mobilisé par la personne candidate

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

CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE

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

Identification[1]	IFC, CENTRE DE FORMATION 513 AVENUE DU PRADO 13008 MARSEILLE	SISR

1. Environnement commun aux deux options

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

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Un service d'authentification	Service d'authentification Active Directory (AD), Portail Captif Wifi	
Un SGBD	MYSQL, MariaDB	
Un accès sécurisé à internet	Filtrage WEB Artica Proxy, Filtrage communications PFSENSE Firewall	
Un environnement de travail collaboratif	Dossiers partagés serveur Windows AD mappés par GPO	
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (*open source)*	Un serveur ZABBIX basé sur DEBIAN 13 (LINUX), Active Directory sur Windows Serveur 2025	

[1] Nom et adresse du centre d'examen ou identification de la personne candidate individuelle (numéro, nom, prénom)

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E – « Environnement technologique pour la certification » du référentiel

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

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Une solution de sauvegarde	Sauvegardes planifiées des données des serveurs virtualisés (avec PROXMOX VE) sur un serveur PROXMOX PACKUP SERVER	
Des ressources dont l'accès est sécurisé et soumis à habilitation	Dossiers partagés avec gestion des droits d'accès avec Active Directory, Serveur Synology NAS distant avec session attitrées et partage de dossiers dont les droits d'accès sont gérés par un administrateur	
Deux types de terminaux dont un mobile (type *smartphone* ou encore tablette)	Test accès Wi-Fi au réseau depuis un smartphone, Ordinateur portable client, Ordinateur administrateur.	

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

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Gestion des incidents	Serveur GLPI et espaces utilisateur GLPI	
Détection et prévention des intrusions	SNORT sur le Firewall PFSENSE	
Chiffrement	VPN OpenVPN chiffrement SHA-256, connexion SSL-TLS au PFSENSE	
Analyse de trafic	Serveur Proxy ARTICA, Serveur de Supervision ZABBIX, journaux évènements Windows Serveur, LOGS Filtrage Firewall PFSENSE	

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

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E « Environnement technologique pour la certification » du référentiel

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

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

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

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

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Un réseau comportant plusieurs périmètres de sécurité	DMZ pour les serveurs accessibles de l'extérieur, Firewall avec filtrage communications, VLAN Serveur isolé, accès Wi-Fi invité sécuriser via un portail captif, détection d'intrusion PFSENSE, authentifications sessions et services, filtrage WEB avec le proxy ARTICA.	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Serveur de messagerie interne MICROSOFT Exchange	
Un logiciel d'analyse de trames	Wireshark	
Un logiciel de gestion des configurations	Zabbix agent server	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	Accès RDP, accès SSH, accès VPN	
Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	Zabbix Monitoring, PROXMOX (analyse et surveillance de métriques des VM), gestionnaire de serveur AD	
Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	Filtrage WEB http/https et inspection SSL avec ARTICA PROXY, filtrage accès interne et externes aux ressources du réseau local avec PFSENSE Firewall	

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution garantissant la continuité d'un service	Réplique du contrôleur de domaine (services, objets AD, base de données et annuaires machines et utilisateurs), Balancing Zevnet entre deux serveurs WEB (1 et 2) répliqués, Sauvegardes VM PROXMOX et restauration de snapshot, sauvegarde des configurations des équipements réseaux	
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	Réplique du contrôleur de domaine (services, objets AD, base de données et annuaires machines et utilisateurs), Balancing Zevnet entre deux serveurs WEB (1 et 2) répliqués, Sauvegardes VM PROXMOX et restauration de snapshot, sauvegarde des configurations des équipements réseaux	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	Balancing Zevnet entre deux serveurs WEB (1 et 2) répliqués	

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

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution permettant la connexion sécurisée entre deux sites distants	Tunnel chiffré VPN avec logiciel et configurations coté client	
Une solution permettant le déploiement des solutions techniques d'accès	WDS, Active Directory avec les GPO déploiements de logiciels, d'extensions WEB, de configurations, Scripts d'installations serveurs GLPI et ZABBIX (sur distributions linux)	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de *scripting*	Scripts PowerShell création utilisateurs et droits d'accès, Scripts d'installations serveurs GLPI et ZABBIX (sur distributions linux)	
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	SNORT sur PFSENSE Firewall	

9. REMERCIEMENTS

Je tiens en premier lieu à remercier les membres du jury pour l'attention qu'ils porteront à la lecture et à l'évaluation de ce dossier E6, étape décisive de mon parcours académique.

J'adresse mes sincères remerciements à l'équipe pédagogique de l'IFC Marseille, et tout particulièrement à mon professeur d'informatique, Monsieur **Bernard FERNANDEZ**, pour la qualité de son accompagnement et ses conseils précieux tout au long de cette matière.

Je tiens à exprimer toute ma gratitude à mon maître de stage, Monsieur **Nabil ACHOURI**, ainsi qu'à Monsieur **Sofian KOUAY**. Merci pour votre accueil, votre pédagogie et le partage de votre expertise technique, qui ont grandement contribué à mon épanouissement professionnel.

Enfin, une pensée amicale pour mes camarades de promotion, dont l'entraide et la bonne humeur ont rendu cette formation particulièrement enrichissante.