Evan Pellegrino
Hugo Tartrat

CCI VAUCLUSE

Documentation commune Projet ITway

Evan Pellegrino
Hugo Tartrat

CCI VAUCLUSE

1. Présentation de l'entreprise ITWay

1.1. Identité et secteur d'activité

ITWay est une entreprise de services du numérique (ESN) spécialisée dans la fourniture de prestations informatiques à valeur ajoutée. Son cœur de métier s'articule autour de trois domaines complémentaires : l'externalisation de la gestion informatique (infogérance), le développement de solutions logicielles sur mesure et la cybersécurité.

L'entreprise se positionne comme un partenaire de confiance pour ses clients, en leur permettant de se concentrer sur leur cœur de métier tout en bénéficiant d'une infrastructure informatique fiable, performante et sécurisée.

1.2. Historique

Fondée en 2005, ITWay a débuté ses activités en tant que petite société de conseil en informatique. La croissance des besoins numériques de ses clients et la complexification progressive des infrastructures IT ont conduit l'entreprise à élargir significativement son catalogue de services. Elle propose aujourd'hui des prestations d'intégration, de maintenance réseau, de gestion des systèmes d'information et de cybersécurité.

En 2018, ITWay a franchi une étape majeure en ouvrant une antenne régionale à Lille, afin de mieux desservir une clientèle nationale et internationale en pleine expansion.

1.3. Chiffres clés

Date de création	2005
Effectif total	110 collaborateurs
Siège social	Marseille — 80 collaborateurs
Antenne régionale	Lille — 30 collaborateurs
Chiffre d'affaires annuel	15 millions d'euros
Typologie de clients	PME majoritaires, quelques grands comptes, administrations publiques
Secteur	Services informatiques (ESN)

1.4. Organisation et structure

ITWay est organisée autour de deux sites géographiques. Le siège de Marseille concentre l'ensemble des fonctions stratégiques et techniques, tandis que l'antenne de Lille assure une présence opérationnelle dans le nord de la France.

1.4.1. Siège social — Marseille (80 collaborateurs)

Service	Effectif	Mission principale
Département IT	20	Administration des systèmes, des réseaux et de la sécurité
Développement logiciel	15	Conception et maintenance des solutions logicielles
Support technique	15	Assistance utilisateur et résolution d'incidents
Services administratifs	20	RH, finance et direction générale
Commercial	10	Relations clients et développement commercial

1.4.2. Antenne régionale — Lille (30 collaborateurs)

Service	Effectif	Mission principale
Support technique	10	Assistance de proximité pour les clients du nord
Développement logiciel	10	Renforcement de l'équipe de développement
Commercial	10	Prospection et suivi commercial régional

2. Contexte et enjeux du projet

2.1. Une infrastructure en croissance constante

Depuis l'ouverture de l'antenne de Lille en 2018, l'infrastructure d'ITWay s'est complexifiée. La multiplication des services, l'augmentation du nombre d'utilisateurs et la diversification des terminaux (postes fixes, portables, mobiles) ont mis en évidence plusieurs besoins forts en matière d'organisation du système d'information.

L'entreprise souhaite désormais consolider son infrastructure réseau pour répondre à trois impératifs majeurs : renforcer la sécurité, améliorer les temps de réponse et garantir une haute disponibilité des services rendus aux utilisateurs internes comme aux clients.

2.2. Problématique

Comment concevoir et mettre en œuvre une infrastructure réseau multi-sites, sécurisée et hautement disponible, capable d'accompagner la croissance d'ITWay tout en

respectant les exigences en matière de cybersécurité, de continuité d'activité et de qualité de service ?

2.3. Enjeux

Le projet répond à plusieurs enjeux clairement identifiés :

- **Enjeu de sécurité :** protéger les données de l'entreprise et de ses clients face aux menaces internes et externes (segmentation, pare-feu, IDS/IPS, chiffrement, authentification renforcée).
- **Enjeu de disponibilité :** assurer la continuité des services métier grâce à la redondance des composants critiques (contrôleurs de domaine, DNS, DHCP, pare-feu, supervision).
- **Enjeu de performance :** réduire la latence et améliorer la qualité de service via la répartition de charge et l'optimisation du routage inter-sites.
- **Enjeu d'évolutivité :** concevoir une architecture modulaire et virtualisée capable d'absorber la croissance future sans remise en cause structurelle.
- **Enjeu d'exploitabilité :** doter le département IT d'outils de supervision, de gestion d'incidents et de configuration centralisée pour piloter efficacement l'infrastructure au quotidien.

3. Objectifs du projet

Le projet vise à concevoir, déployer et documenter une infrastructure complète répondant aux trois activités métiers du référentiel BTS SIO option SISR :

- Concevoir une solution d'infrastructure réseau ;
- Installer, tester et déployer une solution d'infrastructure réseau ;
- Exploiter, dépanner et superviser une solution d'infrastructure réseau.

3.1. Objectifs techniques

Domaine	Objectif opérationnel
Annuaire & identité	Mettre en place un service d'authentification centralisé (Active Directory) et le redonder entre sites.
Adressage & segmentation	Découper le réseau en VLAN (serveurs, utilisateurs, DMZ, Wi-Fi, management) avec un plan d'adressage cohérent.
Interconnexion	Relier le siège de Marseille à l'antenne de Lille par un VPN site-à-site IPsec.
Sécurité périmétrique	Déployer un pare-feu sur chaque site et exposer les services publics au sein d'une DMZ.
Haute disponibilité	Redonder les services critiques : AD, DNS, DHCP, pare-feu, supervision.
Supervision	Surveiller la disponibilité, la performance et la sécurité via une solution centralisée (Centreon).
Sauvegarde	Mettre en œuvre une politique de sauvegarde régulière des machines virtuelles (Proxmox Backup).
Gestion d'incidents	Déployer un outil de ticketing et de gestion de parc [redacted].
Automatisation	Industrialiser les opérations récurrentes via Ansible/Sémaphore.
Chiffrement	Mettre en place une autorité de certification interne (PKI) et imposer HTTPS sur les services internes.

3.2. Objectifs pédagogiques

Au-delà de la dimension purement technique, ce projet doit permettre à chaque membre de l'équipe de :

- Maîtriser l'ensemble des éléments de l'infrastructure commune (annuaire, DHCP, DNS, GPO, ACL, pare-feu, supervision, sauvegarde, etc.) ;
- Mettre en œuvre deux situations individuelles approfondies couvrant les trois activités du référentiel ;
- Produire une documentation technique exploitable, conforme aux attentes du jury de l'épreuve E5 ;
- Travailler en équipe, communiquer efficacement et tracer les actions menées via les outils du projet (drive d'équipe, [redacted] comptes rendus de réunion).

4. Périmètre du projet

4.1. Périmètre géographique

Le projet couvre l'intégralité de l'infrastructure d'ITWay, répartie sur deux sites distants reliés par une liaison sécurisée :

- **Site de Marseille (siège social) :** héberge l'ensemble des services centraux de l'entreprise (annuaire principal, supervision, [redacted] base de données, proxy, reverse proxy, Nextcloud, etc.). Il dispose d'un routeur Cisco physique faisant office de passerelle Internet et de tête de tunnel VPN.
- **Site de Lille (antenne régionale) :** héberge un contrôleur de domaine secondaire et une instance redondante du pare-feu OPNsense. Le routage et le pare-feu y sont assurés par une solution virtualisée.

Le réseau « WAN » est simulé par le réseau pédagogique [redacted] de la salle de cours. Chaque site dispose d'une adresse IP publique fixe attribuée dans ce plan d'adressage.

5. Contraintes du projet

5.1. Contraintes techniques

- L'infrastructure doit être entièrement virtualisée sur un hyperviseur Proxmox mutualisé ;
- Le site de Marseille doit utiliser un routeur Cisco physique ; le site de Lille un routeur virtualisé (technologie au choix — OPNsense retenu) ;
- L'infrastructure doit comporter au minimum un serveur Windows Server et un serveur GNU/Linux ;
- Tous les services exposant une interface web doivent être chiffrés via HTTPS et certificats émis par la PKI interne ;
- Wireshark doit être déployé sur l'ensemble des postes de l'infrastructures
- L'administration des équipements actifs s'effectue exclusivement en SSH ou RDP, jamais en Telnet.

5.2. Contraintes de sécurité

- Mise en œuvre d'une convention de nommage stricte pour les serveurs, VLAN et postes ;
- Application des règles de défense en profondeur : segmentation, pare-feu, ACL, durcissement des serveurs ;
- Désactivation administrative des ports inutilisés sur les commutateurs ;
- Chiffrement systématique des secrets sur les équipements (service password-encryption sur Cisco) ;
- Toute action sensible (snapshot, modification de GPO, changement d'ACL) doit être précédée d'une sauvegarde et documentée.

5.3. Contraintes organisationnelles

- La documentation technique doit être tenue à jour au fil de l'eau — pas une seule journée d'implémentation sans contribution documentaire ;
- Les modifications impactant l'environnement partagé doivent être communiquées à l'équipe avant intervention ;

Schéma d'infrastructure

Schéma Physique

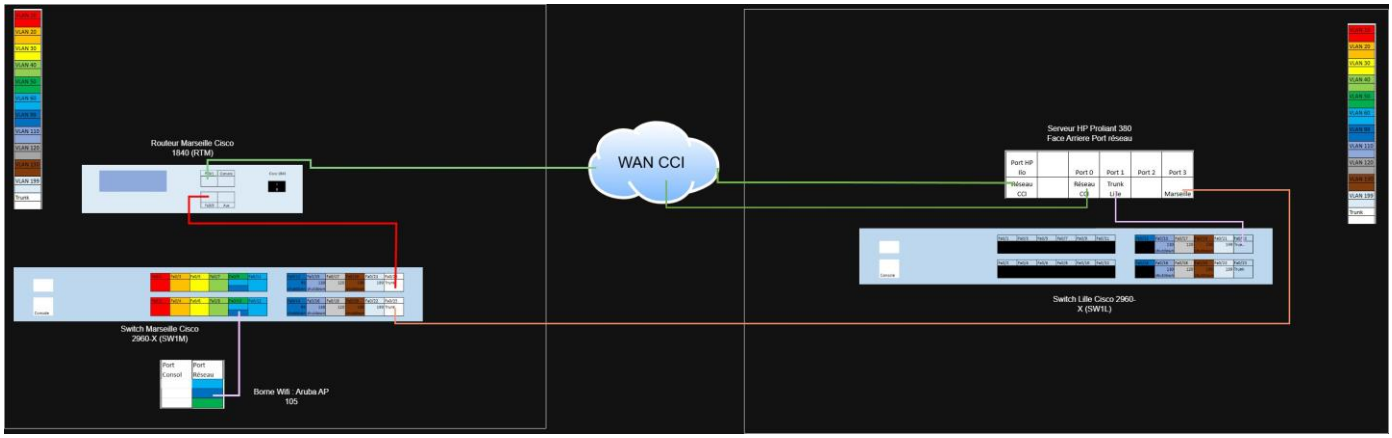
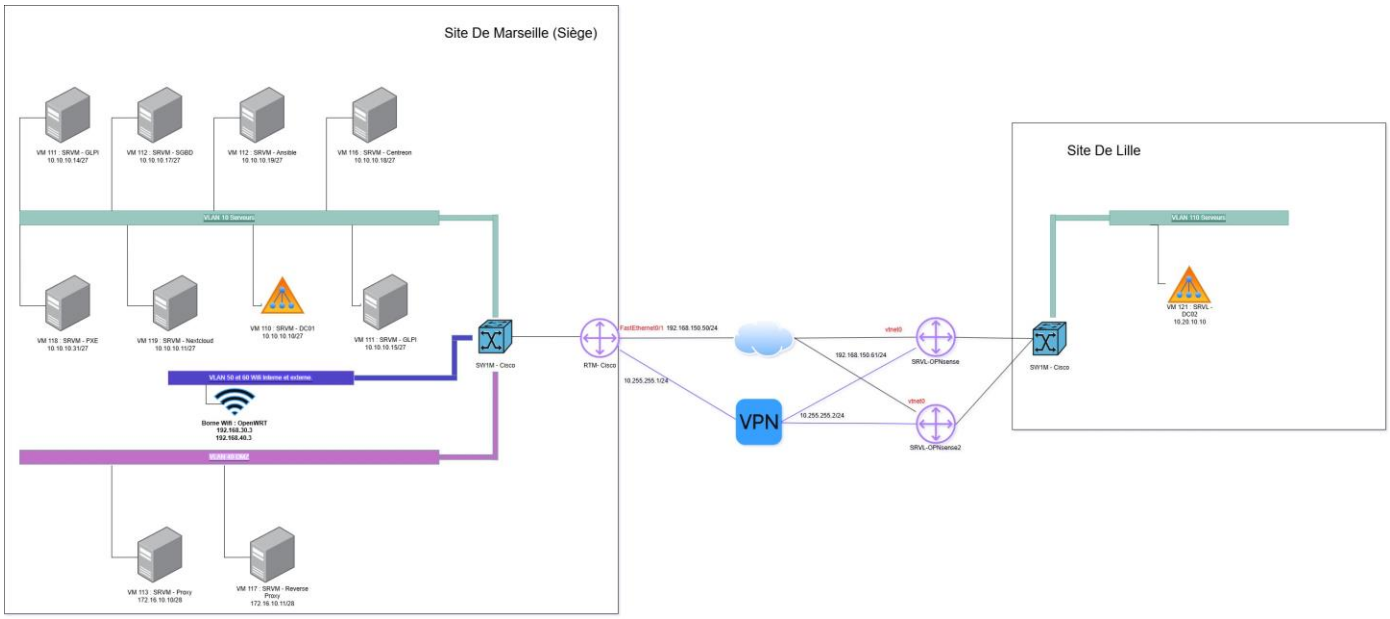


Schéma Logique



Équipements Réseaux - Infrastructure Lille & Marseille

Switch Lille – SW1L-Cisco

Nom	**SW1L-Cisco**
IP Management	[redacted]
VLAN Management	VLNL-MGMT : 199 (Passerelle : [redacted]
Rôles	Commutateur d'accès pour le site de Lille. Segmentation du réseau local et transport des trames.

Rôles & Configuration

Segmentation Réseau (VLANs) : Le commutateur SW1L-Cisco assure l'isolation des flux réseaux pour le site de Lille. Les VLANs ont été configurés de manière à séparer logiquement les serveurs (VLAN 110), les utilisateurs (VLAN 120), la DMZ (VLAN 130) et le management (VLAN 199). Les VLANs de Marseille y sont également déclarés pour permettre une communication inter-sites cohérente si nécessaire.

Configuration des Ports :

- **Ports d'accès (Access) :** Les ports `fa0/1` à `fa0/22` sont assignés de manière statique à leurs VLANs respectifs par paire de ports, garantissant que chaque équipement branché se trouve dans le bon segment réseau.
- **Ports d'interconnexion (Trunk) :** Les ports `fa0/23` et `fa0/24` sont configurés en mode Trunk (agrégation) pour transporter le trafic de multiples VLANs vers le routeur ou d'autres équipements de l'infrastructure.

Sécurité et Administration :

- **Désactivation des ports inutilisés :** Pour des raisons de sécurité (prévention des branchements sauvages), une plage de ports a été administrativement coupée (`shutdown`).
- **Accès distant sécurisé :** L'administration se fait de manière sécurisée via le protocole SSH (version 2) avec un délai d'attente configuré. Les accès non sécurisés (Telnet) sont désactivés.

- **Protection des secrets :** Les mots de passe locaux et le mot de passe d'activation (`enable secret`) sont chiffrés dans le fichier de configuration (`service password-encryption`).

Switch Marseille – SW1M-Cisco

Nom	**SW1M-Cisco**
IP Management	[redacted]
VLAN Management	VLNM-MGMT : 99 (Passerelle : [redacted]
Rôles	Commutateur principal pour le site de Marseille. Segmentation et agrégation.

Rôles & Configuration

Architecture de Niveau 2 :

Tout comme sur le site de Lille, le commutateur de Marseille segmente le trafic local via de multiples VLANs (Serveurs, Admins, Users, DMZ, Wi-Fi interne/externe).

Politique des Ports et Agrégation :

- **Ports d'accès :** Les interfaces Gigabit `gig1/0/1` à `gig1/0/22` distribuent l'accès aux équipements finaux selon leur appartenance aux VLANs définis.
- **Ports Trunk spécifiques :** Le port `gig1/0/9` est un trunk dédié ne laissant passer que les VLANs liés au Wi-Fi et au management (VLANs 50, 60, 99), ce qui limite le domaine de diffusion et augmente la sécurité (probablement connecté à un contrôleur ou une borne Wi-Fi). Les ports `gig1/0/23` et `gig1/0/24` sont les trunks principaux laissant passer l'ensemble du trafic autorisé vers le routeur (RTM-CISCO).
- **Fermeture des ports :** De nombreux ports non utilisés (`gig1/0/10` à `gig1/0/16`, `gig1/0/19-20`) ont été désactivés (`shutdown`) pour durcir la surface d'attaque.

Routeur Marseille – RTM-CISCO

Nom	RTM-CISCO
Interface WAN (Extérieure)	FastEthernet0/1 : [redacted]
Interface LAN (Intérieure)	FastEthernet0/0 (Découpée en sous-interfaces)
Rôles	Routeur de bordure, Passerelle par défaut (Inter-VLAN), Relais DHCP, NAT/PAT, Serveur VPN IPsec.

Rôles & Configuration

Routage Inter-VLAN (Router-on-a-stick) : L'interface LAN physique (`FastEthernet0/0`) est connectée au port Trunk du switch. Elle a été virtuellement découpée en plusieurs sous-interfaces (`Fa0/0.10`, `Fa0/0.20`, etc.). Chaque sous-interface encapsule le trafic avec la norme 802.1Q et porte l'adresse IP de la **passerelle par défaut** de son VLAN correspondant (ex: [redacted] pour le VLAN Serveur 10). Cela permet aux différents réseaux locaux de communiquer entre eux sous le contrôle du routeur.

Agent Relais DHCP (IP Helper) : Afin de centraliser la distribution des adresses IP sur le serveur AD/DHCP (`SRVM-DC01` - [redacted], l'instruction `ip helper-address` [redacted] a été configurée sur l'ensemble des sous-interfaces LAN du routeur. Ainsi, lorsqu'un client fait une requête DHCP en diffusion de type "Broadcast", le routeur intercepte la trame et la transfère directement au serveur DHCP dans le VLAN 10.

NAT / PAT (Translation d'adresses) et Redirection de ports :

- **NAT Overload (PAT) :** Le routeur masque le réseau interne. L'accès à Internet pour les machines locales se fait en translatant leurs adresses IP privées vers l'adresse publique de l'interface WAN [redacted] grâce à une liste de contrôle d'accès (`NAT_OUT_ACL`).

- **Port Forwarding (Static NAT) :** Pour permettre l'administration ou l'utilisation de services depuis l'extérieur, des redirections de ports ont été mises en place. Par exemple :
  - Le port TCP 8889 sur l'IP WAN redirige vers le serveur web du [redacted] 80).
  - Des ports d'administration spécifiques (4444, 6767, 7070) sont ouverts et redirigent vers le port SSH (22) des différents serveurs (Ansible, Proxy, DMZ).
  - Le port TCP 3389 redirige vers le bureau à distance du contrôleur de domaine.

VPN IPsec Site-à-Site (Tunnel S2S) : Pour interconnecter l'infrastructure de Marseille avec celle de Lille de manière totalement sécurisée, un **Tunnel IPsec** a été monté (`Tunnel0` via l'interface WAN vers l'IP distante [redacted].

- **Chiffrement :** Le trafic est chiffré de manière robuste (AES-256) et authentifié par clé pré-partagée (`pre-share`) via ISAKMP et un transform-set IPsec.
- **Routage via le tunnel :** Des routes statiques indiquent au routeur de Marseille que pour joindre les réseaux de Lille (ex: [redacted] ou [redacted], le trafic doit être envoyé au travers du `Tunnel0`. De plus, la règle `NAT_OUT_ACL` empêche explicitement ce trafic inter-sites d'être translaté sur Internet, garantissant qu'il emprunte bien le tunnel VPN sécurisé.

Vlan mis en place dans l'infrastructure

Nom du VLAN	Réseau	Plage d'adresses	Masque de réseau	CIDR
VLNL-SRV	[redacted]	[redacted] -	[redacted]	/27
VLNL-MNGMT	[redacted]	[redacted] -	[redacted]	/28
VLNL-DMZ	[redacted]	[redacted] -	[redacted]	/28

VLNL-Uers	[redacted]	[redacted]-	[redacted]	/26

Politique de nommage du système d'information

Segment du nom	**Signification**	**Codes utilisés dans le projet ITway**
1. TYPE	Identifie la nature physique ou logique de l'équipement.	**SRV** (Serveur) **C** (Poste Client) **SW** (Switch) **RT** (Routeur) **AP** (Point d'accès)
2. LIEU	Identifie le site géographique ou l'agence.	**M** (Marseille) **L** (Lille) *(Ex: C + M = **CM** pour Client Marseille)*
3. SÉPARATEUR	Facilite la lecture entre la localisation et le rôle.	**-** (Tiret du 6)

4. RÔLE	Identifie le service principal hébergé, le département ou l'utilisateur.	**DC** (Contrôleur de domaine) [redacted] (Gestion de parc) **SGBD** (Base de données) **Proxy** (Filtrage web) **Ansible** / **Centreon**

Nom	Décodage (Comment le nom a été construit)
`SRVM-DC01`	**SRV** (Serveur) situé à **M** (Marseille) **-** hébergeant le **DC** (Domain Controller) n°**01**.
`SRVL-DC02`	**SRV** (Serveur) situé à **L** (Lille) **-** hébergeant le **DC** (Domain Controller) n°**02**.
`SRVM-SGBD`	**SRV** (Serveur) situé à **M** (Marseille) **-** hébergeant le service **SGBD** (Base de données).
`SW1M-Cisco`	*Exception nomenclature réseau* : **SW1** (Switch 1) situé à **M** (Marseille) de marque **Cisco**.

Serveur Proxmox

Nom	Prox
Capacité serveur physique	CPU : 40 cœurs RAM : 64Go Stockage : 4.75To répartie en 4 disque virtuel (Backup 1To, DataVM 3,6 To, Local 100Go et Local-lvm 460Go)
IP	[redacted]
Web-access	https:/[redacted]8006/

Rôles	Serveur Physique. Création/Hébergement/Backup des VMs de l'infrastructure.
Backup en Place	Backup hebdomadaire (tous les dimanches à 1h) de toutes les VMs Rétention de 4 backups par VM
Nomenclature	Type + Lieu (-) + Rôle (Ex : Serveur Contrôleur de domaine Numéro 1 situé à Marseille = SRVM-DC01)

VM 110 : Serveur Marseille – Active Directory 01

Nom	SRVM-DC01 (Windows-Server)
Capacité machine	2 Cœurs / 8G RAM / 2 Disques (60Go)
IP	[redacted]
Vlan	VLANSRV 10
Rôles	Active Directory; DNS; DHCP; Radius; Autorité de certifications

Rôles

Active Directory AD DS

Le serveur SRVM-DC01 est la pierre angulaire de l'infrastructure. Il héberge le rôle AD DS (Active Directory Domain Services) dont les missions principales sont :

- Gestion Centralisée de l'Annuaire **:** Il répertorie et organise l'ensemble des objets du réseau (comptes utilisateurs, groupes de sécurité, ordinateurs et serveurs membres).

- Authentification Unique (SSO) : Il centralise la vérification des identités. Une fois connecté au domaine, l'utilisateur accède aux ressources autorisées sans avoir à se réauthentifier systématiquement.

- **Paramétrage des utilisateurs et des ordinateurs (Unités d'Organisation) :** Des unités d'organisation ont été mises en place. Elles servent, entre autres, à donner ou non accès aux utilisateurs aux services de l'infrastructure. L'arborescence sépare géographiquement le parc, puis classe les utilisateurs par départements métiers. Voici le détail de ces unités :

Nom de l'OU	Description et Rôle
Utilisateurs Itway	Unité d'organisation racine qui englobe toute la structure de l'entreprise.
Lille / Marseille	Sous-unités géographiques permettant de séparer les ressources par site physique.
Postes_Travail	Unité dédiée exclusivement au stockage des objets "Ordinateurs" (clients du domaine) pour cibler facilement les déploiements logiciels.
OUs Métiers *(Admin, Commercial, Managagement, Support Techniqu, Developpement L, Departement IT, Services Adminis)*	Sous-unités créées dans chaque site pour classer les collaborateurs par service. Cela facilite la délégation de droits et l'application de stratégies par département.

- Gestion des Groupes de sécurité : Afin de gérer les autorisations de manière centralisée, plusieurs groupes de sécurité ont été mis en place. De plus, un groupe de sécurité « Nextcloud » a été créé afin de restreindre l'accès aux dossiers partagés à certaines personnes uniquement. Voici les groupes documentés :

Nom du groupe	Description des droits accordés
Nextcloud	Restreint l'accès aux dossiers partagés et aux ressources de type Cloud. Seuls les membres de ce groupe peuvent y accéder.
G_Acces_WiFi	Autorise ses membres à s'authentifier sur le réseau Wi-Fi d'entreprise (via le serveur RADIUS/NPS).
G_Centreon_...	Groupes dédiés aux droits d'administration et de lecture pour l'outil de supervision Centreon.

- Service LDAP et Comptes de service : Le serveur expose un annuaire interrogeable via le protocole LDAP (port 389). Le serveur est configuré pour répondre aux requêtes LDAP entrantes, permettant ainsi l'importation automatique des utilisateurs dans l'outil de ticketing [redacted] et l'application de règles de filtrage web nominatives sur le Proxy. Pour que ces services tiers communiquent de façon sécurisée avec l'annuaire, des comptes de service dédiés ont été configurés :

Service tiers	Description de la liaison LDAP et du compte utilisé
Serveur [redacted]	Un compte de service dédié permet au connecteur LDAP d'interroger l'AD pour importer automatiquement les utilisateurs dans la base [redacted] et leur permettre de s'authentifier en SSO.
Serveur Proxy (Artica)	Le proxy utilise un compte de service LDAP pour lire la base des utilisateurs de l'AD, afin d'appliquer des règles de filtrage web basées sur l'identité de l'utilisateur connecté.

- Application des GPO (Stratégies de Groupe) : L'Active Directory assure la diffusion de configurations logicielles (gérées depuis le serveur SRVL-DC02). Une GPO a été mise en place afin de diffuser le logiciel Wireshark à toutes les machines se connectant au domaine. En effet, la GPO a été liée à l'Unité d'Organisation (OU) « Postes_Travail ». De plus chaque poste de travail ajouté à l'organisation se placera dans l'OU "Postes_Travail".

Nom de la GPO	Action réalisée	Application (Liaisons / Cibles)

Wireshark	Déploie et installe automatiquement le logiciel d'analyse réseau Wireshark sur les machines du domaine.	Liée à l'OU **Postes_Travail** (pour cibler les machines) et à l'OU racine **Utilisateurs Itway**.
Default Domain Policy	Gère les règles de sécurité globales du domaine (complexité des mots de passe, etc.).	Liée à la racine du domaine **ITway.local**.

Note de paramétrage : Le serveur est configuré pour répondre aux requêtes LDAP entrantes, permettant ainsi l'importation automatique des utilisateurs dans l'outil de ticketing [redacted] et l'application de règles de filtrage web nominatives sur le Proxy.

DNS

Le rôle DNS (Domain Name System) est installé sur SRVM-DC01 (et redondé sur DC02) pour assurer deux fonctions critiques au sein du réseau :

- Support de l'Active Directory : Ce service est indispensable au fonctionnement de l'AD DS. Il permet aux machines clientes de localiser les contrôleurs de domaine via les enregistrements de service (SRV). Sans DNS, l'authentification des sessions est impossible.

- Résolution de noms (Forward Lookup) : Le DNS permet d'associer des adresses IP à des noms d'hôtes plus simples à retenir (FQDN). Cela facilite l'accès aux services internes sans avoir à manipuler d'adresses IP techniques.

fin de faciliter l'accès aux services internes de l'infrastructure, une zone de recherche directe ITway.local a été créée et configurée. Différents enregistrements DNS ont été déclarés pour assurer la résolution de noms de nos serveurs.

Voici la liste des enregistrements créés dans cette zone :

Nom (Hôte)	Type	Données (Adresse IP)	Description du service cible
srvm-ansible	A	[redacted]	Serveur de gestion centralisée Ansible / Sémaphore
srvm-asterisk	A	[redacted]	Serveur de téléphonie IP
srvm-centreon	A	[redacted]	Serveur de supervision de l'infrastructure
srvm-dc01	A	[redacted]	Contrôleur de domaine principal (Marseille)
srvm [redacted]	A	[redacted]	Serveur de gestion de parc et de ticketing
srvm-nextcloud	A	[redacted]	Serveur de partage de fichiers

srvm-proxy	A	[redacted]	Serveur Proxy pour le filtrage web
SRVL-DC02	A	[redacted]	Contrôleur de domaine secondaire (Lille)
CLL-CLient	A	[redacted]	Poste client (Enregistrement dynamique via DHCP)

DHCP

Le rôle DHCP (Dynamic Host Configuration Protocol) est installé sur SRVM-DC01 pour automatiser la configuration réseau des hôtes de l'infrastructure sur les différents VLANs (découpage FLSM).

En plus de l'attribution classique des adresses IP, le serveur est configuré pour distribuer des paramètres avancés via les options DHCP :

- Distribution Dynamique et Réservations : Le serveur gère l'adressage de la majorité des machines. Les serveurs, bien qu'en IP fixe, possèdent des réservations DHCP basées sur leurs adresses MAC pour centraliser la gestion du plan d'adressage.
  Voici le plan d'adressage des IPs sur le serveur DHCP :

Nom du VLAN	Réseau	Plage d'adresses	Masque de réseau	CIDR
VLANSRV	[redacted]	[redacted] -	[redacted]	/27

VLANmanagement	[redacted]	[redacted]	[redacted]	/28
VLANAdmin	[redacted]	[redacted]	[redacted]	/26
VLANUsers	[redacted]	[redacted]	[redacted]	/25
WIFIint	[redacted]	[redacted]	[redacted]	/26
WIFIext	[redacted]	[redacted]	[redacted]	/26

- Déploiement via FOG Project (Boot PXE) : Pour permettre le démarrage sur le réseau, le DHCP intègre les options nécessaires (Options 66 et 67) pointant vers la VM FOG Project. Cela permet de capturer ou de déployer des images système sur les machines du parc dès leur allumage.

- Gestion Multi-VLAN : Le serveur distribue les adresses sur l'ensemble des segments réseaux grâce à l'utilisation d'agents relais configurés sur l'équipement de niveau 3.

Note technique : Le plan d'adressage a été conçu de façon à optimiser chaque VLAN via le découpage FLSM, garantissant qu'aucune adresse IP disponible ne soit laissée de côté dans les étendues configurées.

Autorité de certifications

Le rôle d'Autorité de Certification (AD CS - Active Directory Certificate Services) est déployé sur SRVM-DC01 pour garantir la sécurité, l'intégrité et la confidentialité des échanges au sein de l'infrastructure informatique.

- Délivrance et Gestion des Certificats : Ce service centralise la création, la distribution, le renouvellement et la révocation des certificats numériques pour les utilisateurs, les ordinateurs et les services du domaine.

- Sécurisation des Communications (Chiffrement) : Il permet la mise en place de protocoles sécurisés (comme le HTTPS/SSL) pour les services web internes. Cela garantit que les données transitant sur le réseau ne peuvent pas être interceptées en clair.

- Support à l'Authentification Forte : L'autorité de certification est un prérequis indispensable pour la mise en place de méthodes d'authentification réseau avancées (comme le 802.1X couplé au RADIUS), permettant aux machines de prouver leur identité de manière cryptographique.

Afin de garantir la confiance au sein du domaine `ITway.local`, une Autorité de Certification d'entreprise a été configurée. Voici ses caractéristiques techniques :

Paramètre	**Valeur configurée**
Nom de l'autorité (Common Name)	ITway-SRVM-DC01-CA
Type de CA	Autorité de certification d'entreprise
Date d'émission	09/03/2026
Date d'expiration	09/03/2031 (Validité de 5 ans)

Notre CA a généré plusieurs certificats essentiels au fonctionnement sécurisé de l'infrastructure :

Nom du demandeur (Cible)	Modèle de certificat utilisé	Service sécurisé (Usage)
ITWAY\SRVM-DC01$	Contrôleur de domaine	Sécurisation LDAPS et RADIUS
ITWAY\SRVL-AD2$	Contrôleur de domaine	Réplication et annuaire sécurisé
ITWAY [redacted]	Serveur Web	Accès HTTPS sécurisé

Radius

Le rôle RADIUS (implémenté via le service NPS - Network Policy Server sous Windows Server) est configuré sur SRVM-DC01 pour centraliser et durcir le contrôle d'accès au réseau sans fil (Wi-Fi) de l'entreprise.

- Authentification Centralisée (802.1X): Le serveur RADIUS agit comme un pont de sécurité entre les points d'accès Wi-Fi et l'Active Directory. L'authentification s'appuie sur le protocole sécurisé Microsoft : PEAP (Protected EAP), permettant aux collaborateurs d'utiliser directement leurs identifiants de session Windows.
- Contrôle d'Accès par Groupe de sécurité: Les autorisations ne sont pas globales. Une stratégie réseau (Network Policy) a été spécifiquement créée dans le NPS pour n'autoriser la connexion au Wi-Fi Interne qu'aux utilisateurs membres du groupe de sécurité Active Directory dédié : G_Acces_WiFi. Si un utilisateur n'est pas dans ce groupe, ou si son compte AD est désactivé, l'accès réseau lui est instantanément refusé.

- Clients RADIUS (Déclaration des bornes): Pour des raisons de sécurité, le serveur NPS n'accepte de traiter que les requêtes provenant d'équipements réseaux explicitement déclarés. Les bornes Wi-Fi (ex: l'équipement avec l'IP [redacted] sont configurées en tant que "Clients RADIUS", avec un Secret Partagé complexe servant à chiffrer les échanges entre la borne et le serveur SRVM-DC01.

Point d'accès Wi-Fi Marseille – OpenWrt

Nom	**AP-OpenWrt (Marseille)**
IP Management	[redacted]
VLAN	VLANAdmin (Management) / WIFlint (Interne) / WIFlext (Externe)
SSID diffusés	**1.** (Corporate / 802.1x) **2.**(Visiteurs / WPA2-PSK)
Interface / OS	LuCI / Linux OpenWrt

Rôles & Configuration

L'infrastructure sans fil repose sur un équipement sous OpenWrt. La configuration a été pensée de manière à séparer strictement les flux des collaborateurs et ceux des visiteurs pour garantir la sécurité du réseau local et de l'Active Directory.

- Réseau Wi-Fi Interne (Corporate) : Ce SSID est réservé exclusivement aux collaborateurs de l'entreprise.
    - Sécurité WPA2-EAP (Entreprise) : Contrairement à un réseau domestique, il n'y a pas de clé de sécurité partagée. La borne agit comme un relais d'authentification (pass-through). Elle transmet les identifiants saisis par les utilisateurs vers le serveur RADIUS (SRVM-DC01 : [redacted] sur le port standard 1812.
    - Accès réseau : Une fois authentifiés par l'Active Directory, les clients de ce réseau reçoivent une adresse IP via le DHCP (VLAN WIFlint) et ont un accès légitime aux ressources de l'entreprise (Serveurs de fichiers, [redacted] Intranet).
    - Note technique OpenWrt: Par défaut, l'OS OpenWrt intègre un gestionnaire Wi-Fi allégé (wpad-basic) qui ne prend pas en charge l'authentification 802.1X. Pour activer le protocole WPA2-EAP, le paquet de base a été désinstallé et remplacé par le paquet complet wpad-openssl depuis le gestionnaire de logiciels.
- Réseau Wi-Fi Externe (Invités / Guest) : Ce SSID est un réseau de courtoisie destiné aux visiteurs, prestataires ou smartphones personnels. Il est considéré comme une zone non sécurisée (Zero Trust).
    - Sécurité WPA2-PSK : Ce réseau utilise une simple clé de sécurité partagée, modifiable régulièrement.

- Isolation stricte (Pare-feu): Ce réseau n'a aucun accès à l'infrastructure LAN de l'entreprise. Les règles de pare-feu bloquent toute communication vers les autres VLANs. Seul l'accès à Internet est autorisé sur une plage IP distincte (VLAN WIFIext).
- Client Isolation : Cette option est activée sur la borne pour empêcher les appareils des invités de communiquer entre eux sur le réseau sans fil, limitant ainsi drastiquement les risques de propagation de malwares ou d'attaques latérales.

VM121 : Serveur Lille – Active Directory 02

Nom	SRVL-DC02 (Windows-Server)
Capacité machine	2 Cœurs / 4G RAM / 1 Disque (32Go)
IP	[redacted]
Vlan	VLNL-SRV 110
Rôles	Active Directory; DNS; DHCP

Rôles

AD DS

Le serveur SRVL-DC02 comprend le rôle AD DS. En effet, celui-ci assure la redondance du SRVM-DC01 en cas de panne. La configuration est donc une copie conforme de la configuration AD DS de SRVM-DC01 et se met à jour à chaque modification sur l'un comme sur l'autre.

- Concernant les GPO, la seule différence entre les deux serveurs se situe à ce niveau. En effet, le fichier .msi de l'application Wireshark se trouve dans un dossier partagé, accessible par tous les utilisateurs du domaine, sur son disque C: (chemin d'accès : \\SRL-DC02\GPO).
  C'est donc sur ce deuxième serveur que nous avons mis en place les GPO. Nous avons estimé que le premier serveur AD avait une importance trop critique en raison des nombreux rôles qu'il assure déjà. Nous avons donc privilégié le second serveur pour la gestion des stratégies de groupe.

- DHCP : Le serveur assure aussi l'attribution dynamique des adresses pour le réseau de Lille. En effet, un rôle DHCP a été mis en place afin de distribuer des adresses IP aux différents VLAN de l'agence. Voici sa configuration :
-

VM 111 : Serveur Marseille – [redacted]

Nom	SRVM [redacted] (Linux - Débian13)
Capacité machine	2 Cœurs / 4G RAM / 1 Disque (30Go)
IP	[redacted]
Vlan	VLNM-SRV : 10
Rôles	Service [redacted]

Rôles

[redacted]

Le serveur SRVM [redacted] est une machine virtuelle sous Debian 13 hébergeant le service [redacted] Celui-ci est accessible via l'adresse suivante : https://srvm [redacted] ITway.local.

L'objectif de ce service est d'assurer la gestion des tickets pour le département informatique. Le service est lié à l'Active Directory (SRVM-DC01) grâce à un connecteur LDAP, ce qui permet à tout utilisateur du domaine de se connecter avec ses identifiants Windows pour soumettre un ticket.

Paramétrage du connecteur LDAP

Afin d'établir cette communication de façon sécurisée, un compte de service dédié a été configuré pour interroger l'annuaire. Voici les paramètres techniques de la liaison LDAP configurés dans [redacted] :

Paramètre [redacted]	**Valeur configurée**	**Description**
Serveur (Hôte)	[redacted]	Adresse IP du contrôleur de domaine

		(SRVM-DC01)
Port	389	Port LDAP standard
Base DN	*DC=ITway,DC=local*	Chemin de base pour la recherche des utilisateurs
[redacted] **DN (Compte de service)**	*CN* [redacted] *CN=Users,DC=ITway,DC=local*	Identifiant du compte de service autorisé à lire l'AD
Filtre de connexion	`(&(objectClass=user)(objectCategory=person))`	Filtre permettant de ne remonter que les vrais comptes utilisateurs

La base de données de [redacted] est hébergée sur le Machine Virtuel SGBD [redacted] sur la base faite pour : base : [redacted] User : [redacted] de la VM

De plus le serveur [redacted] est redonder. En effet un deuxième serveur [redacted] a été mis en place afin de répondre à la demande de répartition des charges. De ce fait la base de données est utiliser sur 2 serveurs et pour les fichiers locaux le dossier /var/www [redacted] files/ est ouvert afin que la deuxième VM puisse y accéder et chargé les fichiers des tickets depuis cette machine et afin qu'il n'y ait pas de bug pour un utilisateur étant connecter sur le [redacted] .

VM 112 : Serveur Marseille – SGBD

Nom	SRVM-SGBD (Linux - Débian13)
Capacité machine	2 Cœurs / 2G RAM / 1 Disque (100Go)
IP	[redacted]
Vlan	VLNM-SRV : 10
Rôles	Base de données Mariadb

Rôles

Base de données

Le serveur SRVM-SGBD est une machine virtuelle sous Linux Debian 13 hébergeant le service MariaDB, qui permet de mettre en place des bases de données pour d'autres services de l'infrastructure. En effet, celui-ci héberge la majorité des bases de données de l'infrastructure ; ce service est donc important.

L'objectif a été de centraliser les bases de données : au lieu d'héberger les bases directement sur chaque machine, nous avons créé une machine virtuelle dédiée uniquement à ce rôle. Cela nous permet de tout centraliser, mais aussi d'éviter de perdre toutes les données d'un service en cas de panne. Si une machine virtuelle tombe en panne, il suffit de restaurer une sauvegarde pour que le service retrouve sa base de données intacte sur le serveur SGBD.

Base de données	Utilisateur
Next cloud	[redacted]
sémaphore	[redacted]
[redacted]	[redacted]

VM 113 : Serveur Marseille – Proxy

Nom	SRVM-Proxy (Linux - Débian12)
Capacité machine	2 Cœurs / 2G RAM / 1 Disque (42Go)
IP	[redacted]
Vlan	VLNM-DMZ : 40
Rôles	Serveur Proxy

Rôles

Serveur Proxy

Le serveur Proxy de Marseille est un serveur Artica. Nous avons choisi Artica car il s'agit d'un proxy français ; nous l'avons privilégié afin de le mettre en avant par rapport à d'autres solutions plus répandues mais étrangères. Son rôle est de protéger les clients lors de leur navigation web. En effet, le proxy a été paramétré pour s'appliquer automatiquement sur la machine du client lors de l'attribution de l'adresse IP via le serveur DHCP.

De plus, nous avons activé le blocage de sites en récupérant une liste de domaines reconnus comme malveillants en ligne pour l'injecter dans le serveur proxy. Lorsqu'un utilisateur tentera de s'y connecter, une page d'alerte rouge s'affichera, indiquant que la connexion n'est pas sécurisée et qu'elle est bloquée. Par ailleurs, les sites de type pornographique, les IA et autres catégories similaires ont également été bloqués. Pour ces derniers, un message d'erreur signalant que la connexion est bloquée s'affichera lors du chargement.

VM 115 : Serveur Marseille – Ansible

Nom	SRVM-Proxy (Linux - Débian13)
Capacité machine	4 Cœurs / 2G RAM / 1 Disque (90Go)
IP	[redacted]
Vlan	VLNM-SRV : 10
Rôles	Ansible, Sémaphore

Rôles

Ansible

Le serveur Ansible de Marseille permet une gestion centralisée de tous les serveurs de l'infrastructure. En effet, ce service permet de se connecter et d'envoyer des commandes à un groupe de serveurs de façon automatisée. Nous pouvons programmer des tâches via une connexion SSH pour les serveurs Linux et via une connexion PowerShell (WinRM) pour les serveurs Windows.

Actuellement, nous avons créé des tâches planifiées afin de mettre à jour, de façon hebdomadaire, l'ensemble des serveurs. Pour les serveurs Windows, les mises à jour sont injectées le mercredi (jour de sortie des correctifs) : le script met à jour le système puis redémarre la machine si nécessaire. De la même manière, les serveurs Linux sont mis à jour tous les samedis à 5h du matin, avec un redémarrage automatique si l'état du système l'exige.

Sémaphore

Sémaphore est, quant à lui, une interface graphique permettant de simplifier le paramétrage et la gestion d'Ansible. En effet, Ansible n'est pas forcément évident à appréhender, et Sémaphore nous a permis de mieux comprendre son utilisation.

Il permet de créer des tâches complexes de façon plus intuitive. En cas de problème lors de l'exécution, nous disposons d'une remontée visuelle, ce qui facilite grandement le débogage par rapport à une interface en ligne de commande.

VM 116 : Serveur Marseille – Centreon

Nom	SRVM-Centreon (Linux - Débian12)
Capacité machine	2 Cœurs / 4G RAM / 1 Disque (60Go)
IP	[redacted]
Vlan	VLNM-SRV : 10
Rôles	Centreon

Rôles

Centreon

Le serveur Centreon de Marseille héberge le service Centreon, qui permet d'avoir une visualisation des services en cours de fonctionnement sur l'infrastructure.

En effet, Centreon est connecté via le protocole SNMP aux autres serveurs de l'infrastructure et remonte des informations importantes comme leur état de charge, leur état de fonctionnement, et bien plus. Nous pouvons donc voir de façon rapide s'il y a des problèmes, tels que des services hors ligne. De plus, le tableau de bord (Dashboard) récapitulatif permet une prise d'information immédiate.

On accède a l'interface de Centreon via son FQDN svrm-centreon.itway.local

Centreon a besoin d'une base de données pour fonctionner, laquelle est hébergée sur le serveur SGBD [redacted]. Sa base de données est nommée centreon_storage et seul l'utilisateur [redacted] y a accès.

Tableau récapitulatif des services surveillés.

Serveur	CPU	Usage	Mémoire	Réponse au ping	Swap
SRVL-AD02	X		X	X	X
SRVM-AD01	X		X	X	X
SRVM-Ansible		X	X	X	X
SRVM-OPNsense	X	X	X	X	X
SRVM-SGBD		X	X	X	X
SRVM [redacted]		X	X	X	X

SRVM-Astérisk		X	X	X	X

VM 117 : Serveur Marseille – Reverse Proxy

Nom	SRVM-ReverseProxy (Linux - Débian12)
Capacité machine	2 Cœurs / 2G RAM / 1 Disque (40Go)
IP	[redacted]
Vlan	VLNM-DMZ : 40
Rôles	Reverse Proxy

Rôle

Reverse Proxy

Pour compléter notre installation, nous avons mis en place un serveur appelé Reverse Proxy, qui utilise le logiciel Caddy. Nous avons choisi cet outil car il est moderne et moins habituel que les solutions classiques, ce qui nous a permis d'apprendre à manipuler un nouveau logiciel.

Concrètement, Caddy agit comme un aiguilleur ou une réception à l'entrée de notre réseau. Voici ses rôles principaux :

- Une porte d'entrée unique : Au lieu de se connecter directement à chaque serveur, l'utilisateur passe par Caddy. C'est lui qui reçoit les demandes et les renvoie vers le bon service (comme Centreon) de manière fluide.
- Simplicité et efficacité : Caddy est réputé pour être très facile à paramétrer. Cela nous permet de mettre en place des connexions sécurisées rapidement et sans erreur. La configuration se fait via le fichier de configuration caddy se trouvant sur notre machine dans /etc/caddy/Caddyfile. Et nous créons les redirections de la manière suivante :
  Ex[redacted]:
  srvm[redacted]itway.local {
  tls /etc/ssl/caddy/proxy.crt /etc/ssl/caddy/proxy.key
  reverse_proxy https://srvm[redacted]itway.local
  }

- Sécurité renforcée : En restant "devant" nos autres serveurs, il les protège en ne montrant qu'une seule façade à l'utilisateur. Il s'occupe aussi de sécuriser la connexion pour que les informations échangées restent confidentielles.

De plus une configuration de répartition des charges a été mis en place sur ce serveur afin que lorsque 2 client différent se connecte au [redacted] (srvm [redacted] itway.local) le reverse proxy redirige soit sur le premier serveur soit sur le deuxième afin qu'aucun des deux ne soit surchargé.

En résumé, Caddy nous sert de guide sécurisé pour accéder à nos outils, tout en simplifiant la gestion de l'infrastructure au quotidien.

Nous l’avons mis en place pour les services suivant :

Nom du service
[redacted]
Centreon
Nexctloud
Astérisk

VM 118 : Serveur PXE Marseille – FogProject

Nom	SRVM-PXE (Linux - Débian12)
Capacité machine	2 Cœurs / 2G RAM / 1 Disque (40Go)
IP	[redacted]
Vlan	VLNM-SRV : 10
Rôles	PXE / FogProject

Rôle

PXE

Pour gérer notre parc informatique, nous utilisons un serveur PXE (Preboot eXecution Environment) via la solution FOG Project. Cet outil est essentiel pour automatiser l'installation des ordinateurs.

Au lieu d'utiliser une clé USB ou un CD sur chaque machine, FOG nous permet de tout faire à travers le réseau. Voici comment il simplifie notre travail :

- Installation à distance : Lorsqu'on allume un nouvel ordinateur, il se connecte directement au serveur FOG via le réseau pour récupérer son système d'exploitation (Windows ou Linux). On appelle cela le "boot PXE".
- Gain de temps (Clonage) : FOG permet de créer une "image" (une copie parfaite) d'un ordinateur déjà configuré et de la distribuer sur plusieurs autres machines en même temps. C'est un gain de temps énorme pour préparer une salle entière, par exemple.

En conclusion, la solution FOG Project constitue notre outil de gestion de parc pour le provisionnement des machines. Ce serveur PXE rend l'infrastructure plus agile en permettant une réinstallation rapide et uniforme des systèmes à travers le réseau.

VM 119 : Serveur Marseille – Nexctloud

Nom	SRVM-Nexctloud (Linux - Débian12)
Capacité machine	2 Cœurs / 2G RAM / 1 Disque (32Go)
IP	[redacted]
Vlan	VLNM-SRV : 10
Rôles	Gestionnaire de fichiers / Nextcloud

Rôle

Gestionnaire de fichiers

Le serveur de fichiers de Marseille héberge le service Nextcloud, qui nous permet de centraliser et de sécuriser la gestion de nos données. Contrairement à un simple dossier partagé, Nextcloud offre une interface moderne accessible aussi bien en interne qu'à distance.

Voici les rôles principaux de ce service dans notre infrastructure :

- Stockage et Partage : Il permet aux utilisateurs de stocker leurs documents de manière sécurisée grâce à des restrictions mise en place par service et de les partager facilement entre collaborateurs via des liens ou des dossiers communs, tout en gardant un contrôle strict sur les droits d'accès afin qu'aucun utilisateur n'est accès à des données non nécessaires a sont travaille.
- Synchronisation en temps réel : Grâce aux clients Nextcloud installés sur les postes de travail, les fichiers sont synchronisés automatiquement. Cela garantit que les utilisateurs travaillent toujours sur la version la plus récente de leurs documents.
- Alternative Souveraine : Le choix de Nextcloud nous permet de garder la pleine maîtrise de nos données (auto-hébergement), offrant une alternative sécurisée aux solutions de stockage cloud grand public.

En résumé, Nextcloud constitue notre plateforme collaborative de gestion de fichiers. Ce service garantit la disponibilité et l'intégrité des données des utilisateurs, tout en facilitant le travail d'équipe grâce à des outils de partage centralisés.

VM 120 : Serveur Lille – OpenSense

Nom	SRVL-OPNsense
Capacité machine	2 Cœurs / 2G RAM / 1 Disque (20Go)
IP Publique	[redacted]
Rôles	Firewall

Rôle

OPNsense

Le serveur de Lille sous **OPNsense** occupe une place centrale dans l'architecture de l'agence. Il remplit le rôle de pare-feu (Firewall) et de routeur, agissant comme le point de passage obligatoire pour tout le trafic réseau.

Voici ses missions principales au sein de l'infrastructure :

- **Segmentation et Interfaces Virtuelles :** Pour assurer le cloisonnement du réseau, OPNsense gère plusieurs **interfaces virtuelles** associées à chaque **VLAN**. Chaque VLAN dispose ainsi de sa propre interface sur le firewall, lui servant de passerelle par défaut (Gateway). Cette segmentation permet d'isoler les flux (par exemple, séparer le réseau des serveurs de celui des postes clients) afin de limiter les risques en cas d'intrusion.
- **Filtrage et Sécurité :** Grâce à la mise en place de règles de pare-feu précises par interface, il contrôle strictement les autorisations de communication entre les différents VLANs. Seuls les flux nécessaires au fonctionnement des services sont autorisés (politique du moindre privilège).
- **Routage et NAT :** En tant que passerelle, il assure le routage entre les sous-réseaux internes et l'accès vers l'extérieur via la translation d'adresses (NAT).

Haute disponibilité et Redondance

Afin de garantir une continuité de service maximale, ce serveur est **redondé** par un second équipement, **Lille OPNsense 2**. Cette configuration en cluster permet d'assurer une **haute disponibilité** : en cas de défaillance matérielle du premier serveur, le second prend automatiquement le relais pour maintenir l'accès aux interfaces et au routage.

Configuration des Interfaces

Le tableau ci-dessous détaille l'adressage IP configuré sur chaque interface du firewall, correspondant aux différentes passerelles de l'agence :

Voici un tableau récapitulatif des interfaces virtuel mise en place sur la machine, les VLAN qu'elle diffuse ainsi que leur adresse IPs.

Interface	Vlan	IP
WAN	-	[redacted]
LAN	-	-
VLAN110	110	[redacted]
VLAN120	120	[redacted]
VLAN130	130	[redacted]
VLAN199	199	[redacted]
IPSEC	-	[redacted]
Redondance	-	[redacted]

VM 123 : Serveur Lille – OpenSense2

Nom	SRVL-OPNsense2
Capacité machine	4 Cœurs / 4G RAM / 1 Disque (40Go)
IP Publique	[redacted]
Rôles	Firewall

Rôles

Opensense 2

Le serveur Lille OPNsense 2 assure la redondance du premier serveur Lille OPNsense (VM 120) afin de garantir une continuité de service optimale pour l'agence. Une liaison dédiée a été configurée entre les deux machines pour permettre un basculement automatique en cas de défaillance de l'un des nœuds. Ce mécanisme repose sur le partage d'une adresse IP publique unique, configurée via des adresses IP virtuelles (VIP) dans la rubrique "Virtual IP" des interfaces.

Dans cette architecture, l'adresse IP publique est détenue par le routeur actif, qui la relaie instantanément au second en cas de panne. Un système de supervision mutuelle évalue en permanence l'état de santé et la réactivité des deux équipements pour déterminer lequel doit gérer le trafic. Actuellement, le serveur OPNsense 2 dispose de ressources plus importantes et assure donc le rôle de nœud actif. Pour maintenir une politique de sécurité cohérente, l'option "High Availability" a été activée dans les paramètres système, permettant ainsi de synchroniser automatiquement l'intégralité de la configuration du premier serveur vers le second. Cette configuration garantit que les règles de filtrage et les accès restent identiques, quel que soit le serveur en fonction.

VM 125 : Serveur Marseille – [redacted]

Nom	SRVM [redacted] (Linux - Débian12)
Capacité machine	4 Cœurs / 4G RAM / 1 Disque (60Go)
IP	[redacted]
Vlan	VLNM-SRV : 10
Rôles	[redacted] – Outils de ticketing

Rôle

[redacted]

Afin de garantir la continuité du service [redacted] et de répondre à l'exigence de répartition des charges du référentiel, une seconde VM **SRVM** [redacted] a été déployée sous Debian 13, à l'identique du serveur principal SRVM [redacted] Les deux instances [redacted] travaillent en parallèle et se partagent la charge des requêtes utilisateurs.

Pour que les deux serveurs fonctionnent de manière cohérente, trois éléments ont été mutualisés :

Élément partagé	Localisation	Rôle
Base de données	SRVM-SGBD [redacted] – base « [redacted] »	Stockage unique des tickets, utilisateurs et configuration [redacted]
Dossier /var/www [redacted] files/	Exporté en NFS depuis SRVM [redacted] et monté sur SRVM [redacted]	Stockage commun des pièces jointes et fichiers applicatifs
Sessions utilisateurs	Gérées via sticky sessions au niveau de Caddy	Maintien de la connexion d'un utilisateur sur le même backend

Le serveur Caddy déjà en place a été reconfiguré pour assurer la répartition de charge entre les deux instances [redacted] L'accès se fait toujours via l'URL unique `https://srvm-[redacted]ITway.local`, Caddy se chargeant de distribuer les requêtes vers SRVM [redacted] ou SRVM [redacted] selon la politique définie.

Paramètre Caddy	Valeur configurée	Description
Backends	SRVM [redacted] , SRVM-[redacted]	Serveurs cibles de la répartition
Politique de répartition	cookie (sticky session)	Maintient l'utilisateur sur le même backend pendant sa session
Health check	Vérification HTTP toutes les 10 secondes	Détecte automatiquement un backend indisponible
Bascule	Automatique	En cas de panne d'un [redacted] tout le trafic est redirigé vers l'autre

Cette mise en œuvre permet à la fois la **répartition de charge** (les deux serveurs traitent les requêtes en parallèle) et la **haute disponibilité** (en cas de panne d'un [redacted] le service reste accessible via le second). L'utilisateur final n'est pas impacté par une éventuelle indisponibilité d'un des serveurs et continue d'utiliser la même URL d'accès.

VM 109 : Serveur Marseille - ELK

Nom	SRVM-ELK (Linux - Débian12)
Capacité machine	4 Cœurs / 8G RAM / 1 Disque (60Go)
IP	[redacted]
Vlan	VLNM-SRV : 10
Rôles	Cenralisation des logs

Rôle

Centralisation des logs

Le serveur ELK héberge la solution [redacted] Stack, qui nous permet de centraliser les journaux d'événements de l'ensemble de notre infrastructure. Contrairement à une gestion des logs machine par machine, cette solution offre une interface unifiée accessible depuis n'importe quel poste de l'infrastructure.

Voici les rôles principaux de ce service dans notre infrastructure :

- **Collecte centralisée des journaux :** L'agent Filebeat est déployé sur l'ensemble des serveurs de l'infrastructure. Il collecte automatiquement les journaux système et applicatifs sur certaine machine de l'infrastructure (SRVM-DC01, SRVM-ReverseProxy, SRVM PXE, SRVM-Nextcloud) (logs d'authentification, logs applicatifs, logs système…) et les transmet en temps réel vers [redacted] earch qui les indexe et les stocke de manière structurée.
- **Visualisation et analyse :** Grâce à l'interface Kibana, les [redacted] disposent de tableaux de bord dynamiques offrant une vue d'ensemble de l'activité de l'infrastructure. Les données sont représentées sous forme de graphiques et de chronologies, facilitant l'identification de tendances et d'anomalies sur l'ensemble du parc.
- **Gestion du cycle de vie des données :** Une politique de rétention a été mise en place afin de conserver les données pendant 7 jours, garantissant ainsi un équilibre entre la disponibilité des informations et l'occupation des ressources de stockage.

En résumé, la solution [redacted] Stack constitue notre plateforme centrale de supervision des journaux d'événements. Elle garantit la traçabilité des actions sur l'ensemble de l'infrastructure et facilite le travail des [redacted] grâce à une interface de consultation unifiée et en temps réel.

Annexe 10

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 E5 - 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]		**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 : Active Directory (Contrôleur de domaine principal) Hôte : SRVM-DC01 IP : [redacted] User : [redacted] MDP : [redacted] Accès : RDP	
Un SGBD	**Service :** Serveur de base de données (ex: MariaDB/PostgreSQL) **Hôte :** SRVM-SGBD **IP :** [redacted]	

	User : [redacted] **MDP :** [redacted] **Accès :** SSH	
Un accès sécurisé à internet	**Service :** Pare-feu / Routeur **Hôte :** SRVL-OPNsense **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** Interface Web (HTTPS) et SSH **Service :** Routeur 1840 Cisco **Hôte :** RTM **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** SSH	
Un environnement de travail collaboratif	**Service :** Nextcloud **Hôte :** SRVM-Nextcloud **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** Interface Web (HTTPS) (https://srvm-nextcloud.itway.local/) et Console Vm	
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (*open source)*	**Service :** Windows Server et Linux (Debian/Ubuntu) **Hôtes :** SRVM-DC01 (Windows) & SRVM [redacted] (Linux) **IP :** [redacted] / [redacted] **User :** [redacted] / [redacted] **MDP :** [redacted] / [redacted]	

	Accès : RDP / SSH	

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

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

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Une solution de sauvegarde	Backup proxmox , backup tous les dimanche, rétention de 3backup par vm	
Des ressources dont l'accès est sécurisé et soumis à habilitation	**Service :** Nextcloud **Hôte :** SRVM-Nextcloud **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès** : Page web (HTTPS)	
Deux types de terminaux dont un mobile (type *smartphone* ou encore tablette)	**Service :** Borne WIFI OpenWRT **Hôtes :** Borne WIFI Aruba AP 105 **IP :** [redacted] / [redacted] **User :** [redacted] **MDP :** [redacted] **Accès** : Page web (HTTPS)	

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	**Service :** [redacted] (Gestion de parc et Helpdesk) **Hôte :** SRVM [redacted] **IP :** [redacted] **User :** [redacted] / [redacted] **MDP :** [redacted] **Accès :** Interface Web (HTTPS) et SSH	
Détection et prévention des intrusions	**Service :** IDS/IPS intégré **Hôte :** SRVL-OPNsense **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** Interface Web (HTTPS)	
Chiffrement	HTTPS Service : Autorité de certification (Contrôleur de domaine principal) Hôte : SRVM-DC01 IP : [redacted] User : [redacted] MDP : [redacted] Accès : RDP	
Analyse de trafic	**Service :** Wireshark **Mis en place sur tout les client du domaine via GPO sur les controleurs de domaines.** HTTPS Service : Autorité de certification (Contrôleur de domaine principal) Hôte : SRVM-DC01 IP : [redacted] User : [redacted]	

	MDP : [redacted] Accès : RDP	

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 E5 - 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	Mise en place de VLAN sur les équipements réseau (RTM, SW1L,SW1M, OPNsense)	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Service : Active Directory (Contrôleur de domaine principal) Hôte : SRVM-DC01 IP : [redacted] User : [redacted] MDP : [redacted] Accès : RDP	

Un logiciel d'analyse de trames	**Service :** Wireshark **Mis en place sur tout les client du domaine via GPO sur les controleurs de domaines.** HTTPS Service : Controleur de domaine (Contrôleur de domaine principal) Hôte : SRVM-DC01 IP : [redacted] User : [redacted] MDP : [redacted] Accès : RDP	
Un logiciel de gestion des configurations	**Service :** Ansible (Automatisation) **Hôte :** SRVM-Ansible **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** SSH et Interface Web (Semaphore)	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	SSH mis sur toute les machines. **Service :** Pare-feu / Routeur **Hôte :** SRVL-OPNsense **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** Interface Web (HTTPS) et SSH **Service :** Routeur 1840 Cisco **Hôte :** RTM **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** SSH	

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	**Service :** Centreon **Hôte :** SRVM-Centreon **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** Interface Web (HTTPS) et Console VM	
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)	**Service :** Proxy SSH **Hôte :** SRVM-Proxy **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** SSH	
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	Redondance OPNsense (Routeur Lille) **Service :** Pare-feu / Routeur **Hôte :** SRVL-OPNsense **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** Interface Web (HTTPS) et SSH **Service :** Pare-feu / Routeur **Hôte :** SRVL-OPNsense2 **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** Interface Web (HTTPS) et SSH	

Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	**Service :** Contrôleur de domaine de secours (Réplication AD) Hôte : SRVM-DC01 IP : [redacted] User : [redacted] MDP : [redacted] Accès : RDP Service : Controleur de domaine (Contrôleur de domaine principal) Hôte : SRVM-DC03 IP : [redacted] User : [redacted] MDP : [redacted] Accès : RDP	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	Répartition des charges sur Reverse Proxy Caddy sur 2 serveur [redacted] **Service :** ReverseProxy Hôte : SRVM-ReverseProxy IP : [redacted] User : [redacted] MDP : [redacted] Accès : SSH	

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	VPN Ipsec Entre RTM et OPNsense Lille **Service :** Pare-feu / Routeur **Hôte :** SRVL-OPNsense	

	IP : [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** Interface Web (HTTPS) et SSH **Service :** Routeur 1840 Cisco **Hôte :** RTM **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** SSH	
Une solution permettant le déploiement des solutions techniques d'accès	**Service :** Fog Project **Hôte :** SRVM-PXE **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** SSH / Acces Web (http:/[redacted]fog/management/index.php)	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de *scripting*	**Service :** Ansible (Automatisation) **Hôte :** SRVM-Ansible **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** SSH et Interface Web (Semaphore)	
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	**Service :** ELK **Hôte :** SRVM-ELK **IP :** [redacted] **User :** [redacted] **MDP :** [redacted] **Accès :** SSH et Interface Web (Kibana)	

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2024**

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 : PELLEGRINO Evan	**N° candidat :2048594120**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☐	**Date :** 29 / 04 /2026

Organisation support de la réalisation professionnelle
ITway (entreprise fictive - environnement de laboratoire)

Intitulé de la réalisation professionnelle
Mise en place d'une infrastructure de téléphonie IP avec FreePBX / Asterisk en environnement virtualisé Proxmox.

Période de réalisation : 1er mars 2026 au 30 Mars 2026 **Lieu :** Avignon
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)
Contexte : L'entreprise fictive ITway dispose de plusieurs services (IT, Accueil, Administration, Technique, Commercial) et nécessite une solution de téléphonie IP interne complète. Aucun trunk SIP physique n'est disponible : la situation est réalisée en environnement de simulation.
Résultats attendus :
- Création de 8 postes SIP (chan_pjsip) couvrant tous les services de l'entreprise
- Mise en place d'un IVR (menu vocal) avec redirections vers les files d'attente de chaque service
- Configuration de files d'attente avec stratégies différenciées (ringall pour l'accueil, linear pour le commercial)
- Messageries vocales individuelles et partagées, blocage des appels surtaxés, sécurisation via Fail2Ban

Description des ressources documentaires, matérielles et logicielles utilisées[2]
Ressources matérielles :
- Serveur Proxmox VE (hyperviseur) | Machine virtuelle FreePBX : 3,7 Go RAM, disque 49+ Go, réseau bridge vmbr0 | Poste client Windows avec MicroSIP

Ressources :
- FreePBX [redacted] (interface web de gestion) | Asterisk 22.8.2 (moteur de téléphonie SIP) | MicroSIP (softphone est) | Fail2Ban (sécurité) | Linux (OS de la VM)

Ressources documentaires :
- Documentation officielle FreePBX (wiki.freepbx.org) | Forums communautaires FreePBX (community.freepbx.org) | Documentation Asterisk (wiki.asterisk.org)

[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.

[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]

Interface FreePBX : http://srvm-asterisk.itway.local/ - Login : [redacted] - MDP : [redacted]

SSH [redacted] - Login : [redacted] - MDP : [redacted]

Documentation technique : Disponible dans le dossier de projet.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2024**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle

(verso, éventuellement pages suivantes)

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

[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.

[4] 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.

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

1. Présentation de la réalisation

Dans le cadre de cette situation professionnelle personnelle, j'ai deployé et configuré une infrastructure complète de téléphonie IP basée sur FreePBX 17 / Asterisk 22.8.2, hébergée sur une machine virtuelle Proxmox. L'objectif était de simuler l'infrastructure téléphonique d'une entreprise fictive (ITway) sans trunk SIP physique.

2. Plan de numérotation mis en place

100 : ITDep (IT) | 200 : Accueil1 / 201 : Accueil2 | 300 : Admin | 400 : Technique | 500 : Commercial1 / 501 : Commercial2 | 999 : Test (simulation) | 6201 : VM_Accueil (VM partagée) | 6501 : VM_Admin (VM partagée Commercial)

3. Configuration des files d'attente (Queues)

Queue 6000 (Accueil) : stratégie ringall - 200 et 201 sonnent simultanément. Queue 6400 (Admin) : stratégie ringall - poste 300. Queue 6500 (Commercial) : stratégie linear - 500 sonne en premier puis 501. Les queues utilisent le protocole chan_pjsip et des agents statiques (Local/[num]@from-queue).

4. IVR (Serveur Vocal Interactif) - ivr-1

Touche 1 : redirection directe poste 100 (ITDep) | Touche 2 : Queue 6400 (Admin) | Touche 3 : redirection directe poste 400 (Technique) | Touche 4 : Queue 6500 (Commercial) | Touche 5 : Queue 6000 (Accueil). En l'absence de trunk SIP, une Misc Application (numéro 7000) permet de simuler l'accès à l'IVR depuis un poste interne.

5. Messageries vocales et sécurité

VM individuelles : boites 100 (ITDep), 300 (Admin), 400 (Technique). VM partagées : boite 6201 (VM_Accueil pour 200+201), boite 6501 (VM_Admin pour 500+501). Consultation via *97. Blocage appels surtaxés (0800, 09XX, international) via route sortante sans trunk. Sécurisation par Fail2Ban (8 jails actives dont pbx-gui, asterisk-iptables, recidive).

6. Incidents rencontrés et résolutions

Incident 1 : Bannissement IP répétitif par Fail2Ban (jail recidive) suite à des tentatives de connexion UCP échouées → Débannissement via fail2ban-client + ajout en whitelist (ignoreip). Incident 2 : WebRTC UCP non fonctionnel (Node.js absent) → Utilisation de MicroSIP comme softphone de test. Ces incidents ont été diagnostiqués via la console Proxmox, les logs Asterisk et la CLI (pjsip show endpoints, asterisk -rvvvv).

7. Tests et validation

Tests réalisés depuis le poste 999 (MicroSIP) : appels internes directs entre postes, accès IVR via 7000, validation des stratégies de sonnerie (ringall / linear), test des redirections IVR, vérification du blocage des appels surtaxés. Validation via CDR (Reports > Journaux d'appels) et Asterisk CLI en mode debug (asterisk -rvvvv).

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS

Option SISR - Solutions d'Infrastructure, Systemes et Reseaux

SITUATION PROFESSIONNELLE

Mise en place d'une infrastructure de telephonie IP

avec FreePBX / Asterisk 22 en environnement virtualise Proxmox

Annee scolaire : 2024 - 2025

Infrastructure reseau - Telephonie IP - VoIP

1. Contexte et objectifs de la situation

1.1 Cadre de la situation

Dans le cadre de ma formation BTS SIO option SISR, j'ai realise une situation professionnelle personnelle portant sur la mise en place d'une infrastructure de telephonie IP complete. Cette situation s'inscrit dans un contexte d'entreprise fictive (ITway) disposant de plusieurs services et necessitant une solution de communication interne performante.

J'ai choisi de mettre en oeuvre FreePBX, un IPBX open source base sur Asterisk 22, deploye en tant que machine virtuelle sur un hyperviseur Proxmox VE. Ce choix me permet d'acquerir de nouvelles competences techniques tout en comparant cette solution avec Yeastar, outil que je maitrise deja dans le cadre de mes activites professionnelles.

1.2 Objectifs techniques

- Deployer et configurer FreePBX sur une machine virtuelle Proxmox
- Creer et gerer des postes SIP chan_pjsip pour chaque service de l'entreprise
- Mettre en place un IVR (Serveur Vocal Interactif) pour les appels entrants
- Configurer des files d'attente avec des strategies de sonnerie differenciees
- Implementer des messageries vocales individuelles et partagees
- Bloquer les appels vers les numeros surtaxes et internationaux
- Simuler et tester l'ensemble de la configuration sans trunk SIP physique

1.3 Comparaison avec l'existant (FreePBX vs Yeastar)

Concept telephonie	Yeastar S-Series	FreePBX (interface FR)
Poste SIP	Extension	Poste (Connectivite > Postes)
Trunk SIP	Trunk	Trunk
Menu vocal entrant	IVR	IVR (Applications > IVR)
File d'attente	Queue	Queues (Applications > Queues)
Sonnerie simultanee	Ring Group - Ring All	Queue - strategie ringall
Sonnerie sequentielle	Ring Group - Sequential	Queue - strategie linear
Blocage appels sortants	Outbound Restriction	Routes Sortantes sans trunk
Message audio IVR	Custom Prompts	Admin > System Recordings
Appels entrants	Inbound Route	Routes Entrantes
Softphone integre	Linkus (natif)	UCP + WebRTC (config avancee)
Protection brute force	Blacklist integree	Fail2Ban (automatique)

Concept telephonie	Yeastar S-Series	FreePBX (interface FR)
IVR numero composable	Oui (numero direct)	Non (Misc Application requise)

2. Environnement technique

2.1 Infrastructure de virtualisation

Composant	Configuration	Remarque
Hyperviseur	Proxmox VE	Environnement de laboratoire
OS VM	Linux (base FreePBX)	Distribution officielle FreePBX
Version FreePBX	[redacted]	Interface web de gestion
Version Asterisk	22.8.2	Moteur de telephonie SIP
RAM allouee	3.7 Go	Minimum recommande : 2 Go
Espace disque disponible	> 49 Go libres	Logs Asterisk = consommateur important
Reseau	Bridge vmbr0	Acces LAN direct
Adresse IP	[redacted]	Fixe sur le reseau local
FQDN	srvm-asterisk.itway.local	Resolu par DNS interne
Protocole SIP	chan_pjsip (UDP port 5060)	Protocole SIP moderne recommande

2.2 Outils utilises

Outil	Role	Equivalent Yeastar
FreePBX 17	Interface web de gestion IPBX	Interface web Yeastar S-Series
Asterisk 22.8.2	Moteur de telephonie	Moteur integre Yeastar
MicroSIP (Windows)	Softphone de test	Application Linkus
Fail2Ban	Protection anti-brute force	Blacklist integree Yeastar
chan_pjsip	Stack SIP moderne	SIP transparent Yeastar
Proxmox VE	Hyperviseur de virtualisation	Serveur physique dedié

3. Plan de numerotation reel

Voici le plan de numerotation tel qu'il a ete mis en place sur le serveur FreePBX, extrait directement de la configuration Asterisk (pjsip.endpoint.conf et queues_additional.conf) :

Numero	Nom configure	CallerID	Type	Service
100	ITDep	ITDep <100>	Poste SIP + VM individuelle	IT
200	Accueil1	Accueil1 <200>	Poste SIP	Accueil
201	Accueil2	Accueil2 <201>	Poste SIP	Accueil
300	Admin	Admin <300>	Poste SIP + VM individuelle	Administration
400	Technique	Technique <400>	Poste SIP + VM individuelle	Technique
500	Commercial1	Commercial1 <500>	Poste SIP	Commercial
501	Commercial2	Commercial2 <501>	Poste SIP	Commercial
999	test	test <999>	Poste SIP - Simulation	Test
6201	VM_Accueil	VM_Accueil <6201>	Poste virtuel - VM partagee	Accueil
6501	VM_Admin	VM_Admin <6501>	Poste virtuel - VM partagee	Commercial
6000	Queue Accueil	-	File d'attente ringall	Accueil
6400	Queue Admin	-	File d'attente ringall	Administration
6500	Queue Commercial	-	File d'attente linear	Commercial
7000	ITway test	-	Misc Application -> IVR	Simulation

4. Creation et configuration des postes SIP

4.1 Protocole utilise : chan_pjsip

Tous les postes ont ete crees avec le protocole chan_pjsip, visible dans la configuration Asterisk generee (pjsip.endpoint.conf). Les parametres communs a tous les postes sont :

Parametre pjsip	Valeur	Signification
type	endpoint	Definition d'un point de terminaison SIP
context	from-internal	Contexte dialplan des appels internes
allow	ulaw,alaw,gsm,g726,g722	Codecs audio autorises
dtmf_mode	rfc4733	Mode de transmission des tonalites DTMF
language	fr	Langue des messages systeme
rtp_timeout	30	Timeout RTP en secondes
direct_media	yes	RTP direct entre endpoints si possible
force_rport	yes	Force le port source pour NAT
rewrite_contact	yes	Reecrit le contact pour NAT

4.2 Point particulier : deux mots de passe distincts

Une difference notable avec Yeastar est la coexistence de deux mots de passe independants par poste :

- Le Secret SIP (champ 'Secret') : utilise par le client SIP (MicroSIP, telephone IP) pour s'enregistrer sur Asterisk via pjsip
- Le Password For New User : utilise exclusivement pour se connecter a l'interface web UCP (User Control Panel)

Sur Yeastar, Linkus utilise un systeme d'authentification unifie. Sur FreePBX, ces deux acces sont completement independants, ce qui peut preter a confusion lors de la premiere configuration.

5. Configuration du Serveur Vocal Interactif (IVR)

5.1 Message d'accueil

Chemin : Admin > System Recordings

Le message d'accueil IVR est stocke dans la bibliotheque System Recordings de FreePBX. Contrairement a Yeastar ou les prompts sont dans 'PBX > Custom Prompts', FreePBX separe clairement la bibliotheque audio (System Recordings) de sa destination (IVR).

5.2 Configuration reelle de l'IVR (ivr-1 / IVR_Principal)

L'analyse du fichier extensions_additional.conf revele la configuration reelle de l'IVR :

Touche	Destination configuree	Type	Cible
1	from-did-direct, 100	Appel direct poste	ITDep (100)
2	ext-queues, 6400	File d'attente	Queue Admin (300 - Admin)
3	from-did-direct, 400	Appel direct poste	Technique (400)
4	ext-queues, 6500	File d'attente	Queue Commercial (500+501)
5	ext-queues, 6000	File d'attente	Queue Accueil (200+201)
i (invalide)	Retour IVR	Boucle max 3x	Message erreur + retour

Note : Les touches 1 et 3 redirigent directement vers les postes sans passer par une file d'attente, car IT et Technique ne disposent que d'un seul poste chacun. Les touches 2, 4 et 5 utilisent les queues pour les services multi-postes ou necessitant une file.

5.3 Point specifique : l'IVR n'a pas de numero direct

Contrairement a Yeastar ou l'IVR possede son propre numero composable, sur FreePBX l'IVR est une destination et ne peut pas etre appele directement depuis un poste interne. Ce point est resolu par la Misc Application (voir section 7.2).

6. Configuration des files d'attente (Queues)

Configuration extraite de queues_additional.conf :

6.1 Queue Accueil (6000) - Sonnerie simultanee

Parametre	Valeur configuree
Numero de queue	6000
Strategie	ringall - tous les agents sonnent simultanement
Timeout par agent	15 secondes
Agent 1	Local/200@from-queue - Accueil1
Agent 2	Local/201@from-queue - Accueil2
Acces IVR	Touche 5

6.2 Queue Admin (6400) - Poste unique

Parametre	Valeur configuree
Numero de queue	6400
Strategie	ringall
Timeout par agent	15 secondes
Agent	Local/300@from-queue - Admin
Acces IVR	Touche 2

6.3 Queue Commercial (6500) - Sonnerie sequentielle

Parametre	Valeur configuree
Numero de queue	6500
Strategie	linear - Commercial1 sonne en premier, puis Commercial2
Timeout par agent	15 secondes
Agent 1	Local/500@from-queue - Commercial1
Agent 2	Local/501@from-queue - Commercial2
Acces IVR	Touche 4

6.4 Strategies de sonnerie

Strategie	Comportement	Utilise pour	Equivalent Yeastar
ringall	Tous les agents sonnent simultanement	Accueil (6000), Admin (6400)	Ring All
linear	Sonne dans l'ordre de la liste	Commercial (6500)	Sequential

7. Configuration des routes

7.1 Route entrante

Chemin : Connectivite > Routes Entrantes

La route entrante est configuree avec DID = ANY pour attraper tous les appels entrants et les rediriger vers l'IVR_Principal (ivr-1). En l'absence de trunk SIP physique, elle sert de base pour la simulation.

Parametre	Valeur	Remarque
Description	Entrant_Simulation	Route de simulation sans trunk
DID Number	ANY (vide)	Attrape tous les appels entrants
CallerID Number	ANY (vide)	Pas de filtre sur l'appelant
Set Destination	IVR > IVR_Principal (ivr-1)	Redirige vers le menu vocal

7.2 Misc Application - Point d'entree IVR (numero 7000)

Chemin : Applications > Misc Applications

Extrait de extensions_additional.conf :

Parametre	Valeur configuree
Numero (Feature Code)	7000
Nom	ITway test
Destination	Goto(ivr-1,s,1) - IVR_Principal
Contexte dialplan	app-miscapps

En composant le 7000 depuis n'importe quel poste interne, l'appelant arrive directement sur l'IVR_Principal, simulant ainsi un appel entrant externe. Cette solution compense l'absence de numero direct sur les IVR FreePBX, comportement different de Yeastar.

7.3 Route sortante - Blocage des appels surtaxes

Chemin : Connectivite > Routes Sortantes

Une route sortante sans trunk assigne est creee en priorite haute. Tout appel correspondant aux patterns est automatiquement rejete par Asterisk.

Pattern bloque	Type de numero concerne
0800XXXXXXX	Numeros verts et surtaxes 0800
0900XXXXXXX	Numeros surtaxes 0900
08XXXXXXXXX	Ensemble des numeros 08XX
+XXXXXXXXXXX	Internationaux format E.164 (+)
00XXXXXXXXXX	Internationaux format 00

Principe : en l'absence de trunk sur cette route, FreePBX rejette l'appel automatiquement. C'est l'equivalent fonctionnel du 'Deny' dans les restrictions sortantes Yeastar, mais implemente via la logique de priorite des routes sortantes Asterisk.

8. Configuration des messageries vocales

Configuration extraite de voicemail.conf (contexte [default]) :

8.1 Messageries vocales individuelles

Boite voicemail	Nom configure	Code PIN	Poste associe	Service
100	ITDep	[redacted]	100	IT
300	Admin	[redacted]	300	Administration
400	Technique	[redacted]	400	Technique

Ces messageries sont activees directement sur le poste via l'onglet 'Boite vocale'. En cas d'absence de reponse, l'appel est redirige vers la boite vocale personnelle du poste.

8.2 Messageries vocales partagees

Pour les services multi-postes, des postes virtuels dedies uniquement a la messagerie ont ete crees. Ces postes ne sont pas associes a un client SIP reel :

Boite voicemail	Nom configure	Code PIN	Service concerne	Agents
6201	VM_Accueil	[redacted]	Accueil telephonique	200 (Accueil1), 201 (Accueil2)
6501	VM_Commercial	[redacted]	Commercial	500 (Commercial1), 501 (Commercial2)

La consultation de la messagerie partagee s'effectue depuis n'importe quel poste en composant *97, puis en saisissant le numero de la boite et le code PIN.

9. Securite et gestion des incidents

9.1 Systeme Fail2Ban

FreePBX installe automatiquement Fail2Ban. Les jails actives sur ce serveur sont :

Jail active	Ce qu'elle surveille	Consequence
pbx-gui	Tentatives connexion interface web FreePBX	Ban IP apres echecs
asterisk-iptables	Tentatives enregistrement SIP echouees	Ban IP au niveau iptables
sshd	Tentatives connexion SSH	Ban IP SSH
apache-badbots	Requetes HTTP de bots malveillants	Ban IP HTTP
apache-tcpwrapper	Connexions TCP suspectes Apache	Ban via TCP wrappers
recidive	IPs bannies dans plusieurs jails	Ban long terme (heures)
vsftpd-iptables	Tentatives FTP	Ban IP FTP

9.2 Incident rencontre : bannissement IP repetitif

Au cours du projet, deux coupures totales d'acces au serveur (interface web FreePBX + SSH simultanement inaccessibles) ont ete constatees apres des tentatives de connexion UCP echouees.

Diagnostic et resolution depuis la console Proxmox :

- Identification des jails : fail2ban-client status
- Confirmation du bannissement dans pbx-gui et recidive
- Debannissement : fail2ban-client set pbx-gui unbanip [IP] et idem pour recidive
- Prevention : ajout de ignoreip = [redacted] [IP] dans /etc/fail2ban/jail.local
- Ajout du reseau LAN en zone Trusted dans Admin > Firewall > Networks

La jail 'recidive' est particulierement restrictive : elle ban pour plusieurs heures toute IP ayant ete bannie dans plusieurs autres jails, expliquant pourquoi meme le SSH devenait inaccessible simultanement.

10. Procedures de test et validation

10.1 Outil de test : MicroSIP

En raison de la complexite de configuration du module WebRTC/UCP (absence de Node.js, necessite d'un certificat SSL valide et d'une configuration WSS), MicroSIP a ete utilise comme softphone de test.

Champ MicroSIP	Valeur	Remarque
Serveur SIP	[redacted]	IP du serveur FreePBX
Nom d'utilisateur	999	Numero du poste (pas le nom affiche)
Domaine	[redacted]	IP recommandee plutot que FQDN
Login	999	Identifiant SIP
Mot de passe	Secret SIP du poste	Champ 'Secret' dans FreePBX (pas le mdp UCP)
Transport	UDP	Port 5060

Statut confirme dans Asterisk CLI (pjsip show endpoints) : 'Not in use' = poste enregistre et disponible.

10.2 Plan de tests

Test	Action depuis 999	Resultat attendu
Appel interne IT	Composer 100	ITDep (100) sonne
Appel interne Admin	Composer 300	Admin (300) sonne
Acces IVR simulation	Composer 7000	Message d'accueil IVR se declenche
IVR touche 1 - IT	Appuyer 1	Redirection directe vers poste 100
IVR touche 2 - Admin	Appuyer 2	Queue 6400 - Admin (300) sonne
IVR touche 3 - Technique	Appuyer 3	Redirection directe vers poste 400
IVR touche 4 - Commercial	Appuyer 4	Queue 6500 - 500 sonne, puis 501
IVR touche 5 - Accueil	Appuyer 5	Queue 6000 - 200 ET 201 sonnent
Failover messagerie	Ne pas repondre	Bascule sur voicemail
Blocage surtaxe	Composer 0800XXXXXX	Appel rejete (pas de trunk)
Consulter VM partagee	Composer *97 > 6201	Acces boite VM_Accueil

10.3 Verification via les CDR

Chemin : Reports > Journaux d'appels (Call Detail Records)

Les CDR permettent de valider chaque appel avec : poste source, destination, statut (ANSWERED / NO ANSWER / BUSY / CANCEL), duree et horodatage. Ils constituent les preuves documentaires des tests effectues pour le dossier BTS.

10.4 Verification via Asterisk CLI

Commande CLI	Utilisation
pjsip show endpoints	Etat de tous les postes (Not in use / Unavailable)
asterisk -rvvvv	Mode debug temps reel - suivi du routage d'un appel
core show channels	Appels en cours
queue show	Etat des agents dans les files d'attente
fail2ban-client status	Etat des jails et IPs bannies

11. Bilan et retour d'experience

11.1 Competences acquises

- Deploiement d'un IPBX open source (FreePBX/Asterisk 22) sur infrastructure virtualisee Proxmox
- Configuration complete d'une infrastructure VoIP : postes chan_pjsip, IVR, queues, routes, voicemail
- Lecture et interpretation des fichiers de configuration Asterisk (pjsip.endpoint.conf, queues_additional.conf, extensions_additional.conf, voicemail.conf)
- Diagnostic et resolution d'incidents systeme : Fail2Ban, analyse de logs Asterisk en CLI
- Analyse comparative approfondie entre FreePBX et Yeastar S-Series
- Mise en place d'une solution de simulation sans trunk SIP (Misc Application)

11.2 Difficultes rencontrees et solutions

Difficulte	Cause identifiee	Solution apportee
VM inaccessible (x2)	Bannissement IP par Fail2Ban (jail recidive)	Debannissement CLI + whitelist /etc/fail2ban/jail.local
WebRTC UCP non fonctionnel	Node.js absent, config WSS complexe	Utilisation MicroSIP comme softphone de test
Confusion mots de passe	Secret SIP != Password For New User	Documentation et identification des deux champs
IVR sans numero direct	Logique FreePBX differente de Yeastar	Misc Application numero 7000 -> IVR
Login UCP echoue	Login = numero poste, pas nom affiche	Utilisation du numero (999) comme identifiant
Perte acces SSH + web	jail recidive (multi-ban)	Console Proxmox + debannissement manuel

11.3 Comparaison finale FreePBX vs Yeastar

Critere	FreePBX / Asterisk	Yeastar S-Series
Prise en main	Complexe (Linux + SIP requis)	Intuitive et guidee
Flexibilite	Tres elevee (tout configurable)	Limitee aux options proposees
Visibilite config	Fichiers .conf lisibles (Asterisk)	Config opaque (interface uniquement)
Softphone integre	UCP WebRTC (config difficile)	Linkus (integre nativement)
Protection securite	Fail2Ban explicite et configurable	Blacklist integree discrete

Critere	FreePBX / Asterisk	Yeastar S-Series
IVR avec numero	Non (Misc Application necessaire)	Oui (numero direct integre)
Cout	Gratuit (open source)	Licence payante
Valeur pedagogique	Tres elevee	Moyenne (solution connue)
Usage professionnel	Tres repandu (PME, operateurs)	Repandu PME/ETI

11.4 Conclusion

Ce projet m'a permis d'acquerir une maitrise concrete de FreePBX/Asterisk, solution de telephonie IP open source tres repandue en milieu professionnel. La comparaison permanente avec Yeastar m'a aide a comprendre les mecanismes sous-jacents de la telephonie IP de maniere plus profonde, en depassant la simple utilisation d'une interface graphique.

La lecture directe des fichiers de configuration Asterisk (pjsip.endpoint.conf, queues_additional.conf, extensions_additional.conf, voicemail.conf) a permis de comprendre comment FreePBX traduit les configurations graphiques en directives Asterisk, competence directement applicable en environnement professionnel.

Les incidents rencontres (bannissement Fail2Ban, problemes WebRTC, gestion des logs) constituent des situations reelles que tout technicien SISR rencontrera en production. L'infrastructure deployee - 10 postes, 3 queues actives, 1 IVR a 5 options, messageries vocales individuelles et partagees, blocage des appels surtaxes, securite Fail2Ban - constitue une solution complete et fonctionnelle demontrant les competences attendues en fin de BTS SIO option SISR.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

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

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

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 2**
Nom, prénom : PELLEGRINO Evan	**N° candidat :2048594120**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** 29 / 04 /2026

Organisation support de la réalisation professionnelle

Établissement scolaire – Projet de fin de BTS SIO option SISR. Infrastructur[redacted] us Proxmox, composée de plusieurs serveurs Debian 12 interconnectés en réseau local [redacted].

Intitulé de la réalisation professionnelle

[redacted] place d'une soluti[redacted] lyse de trafic réseau et de supervision de l'infrastructure à l'aide de la suite [redacted] Stack (Packetbeat, [redacted] earch, Kibana).

Période de réalisation : 1er mars 2026 au 30 Mars 2026 **Lieu :** Avignon

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 : Infrastructure virtuelle Proxmox, serveurs Debian 12, accès [redacted] sur toutes les VMs, accès internet pour le téléchargement des paquets [redacted]
Résultats attendus : Déploiement d'une solution fonctionnelle de capture et d'analyse du trafic réseau en temps réel sur l'ensemble de l'infrastructure, avec visualisation dans Kibana, mise en place de règles d'alerting et activation du module SIEM de détection de menaces.

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

Ressources matériel[redacted] erveur Proxmox hébergeant 3 VMs [redacted] RVM-ELK (4 vCPU, 8 Go RAM, 60 Go disque), SRVM [redacted] SRVM-ReverseProxy. Réseau l[redacted]
Ressources logiciell[redacted] bian GNU/Linux 12 (Bookworm), [redacted] .14, Kibana 8.19.14, Packetbeat 8.19.14.
Ressources documentaires : Documentation officielle [redacted] (docs [redacted] co), documentation Packetbeat 8.x, référentiel BTS SIO.

1

2

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

Interface Kibana : http:/ 5601 – Identifiant : – Mot de passe :

SSH - Login : - MDP :

Documentation technique : Disponible dans le dossier de projet.

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

1. Contexte et objectifs

Dans le cadre du projet de fin de BTS SIO option SISR, cette réalisation professionnelle constitue la partie individuelle du projet. L'objectif est de mettre en place une solution complète d'analyse du trafic réseau et de supervision de l'infrastructure à l'aide de la suite Stack, afin de permettre une surveillance en temps réel des échanges réseau entre les différents serveurs de l'infrastructure.

2. Architecture mise en place

L'infrastructure repose sur 3 machines virtuelles Debian 12 hébergées sous Proxmox, interconnectées sur le réseau :

- SRVM-ELK : serveur central hébergeant earch 8.19.14 et Kibana 8.19.14. C'est le cœur de la solution, il stocke toutes les données et expose l'interface graphique de supervision.
- SRVM et SRVM-ReverseProxy : serveurs applicatifs sur lesquels Packetbeat est déployé pour capturer le trafic réseau local et l'envoyer vers earch.

3. Réalisations effectuées

Installation et configuration d earch et Kibana sur SRVM-ELK. Déploiement de Packetbeat sur les 3 VMs avec configuration du fichier packetbeat.yml (connexion HTTPS sécurisée via certificat TLS, fingerprint SHA-256). Chargement des dashboards officiels Packetbeat dans Kibana. Configuration d'une politique de rétention des données (7 jours) via Index Lifecycle Management. Création de 3 règles d'alerting personnalisées (détection d'erreurs HTTP, volume DNS anormal, scan de ports). Activation du module Security SIEM avec installation de règles de détection préconstruites orientées supervision réseau.

4. Protocoles capturés et dashboards

Packetbeat capture les protocoles suivants : DNS (port 53), HTTP (ports 80, 8080), TLS/HTTPS (port 443), ICMP, DHCPv4 et les flux réseau (Flows). Les dashboards Kibana utilisés sont : Packetbeat Overview ECS (vue globale), Packetbeat DNS Overview ECS, Packetbeat HTTP ECS, Packetbeat Flows ECS et Packetbeat DNS Tunneling ECS.

5. Compétences mobilisées

Installation et configuration d'éléments d'infrastructure earch, Kibana, Packetbeat). Administration de services sur Debian 12 (systemctl, configuration de fichiers YAML). Gestion des indicateurs et fichiers d'activité (dashboards, règles d'alerting). Supervision d'une solution d'infrastructure réseau via SIEM. Rédaction de la documentation technique associée.

[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.

[4] 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

Option SISR - Solutions d'Infrastructure, Systèmes et Réseaux

SITUATION PROFESSIONNELLE

Mise en place d'une solution d'analyse de trafic réseau

et de supervision de l'infrastructure avec la suite [redacted] Stack

Année scolaire : 2025 - 2026

Supervision réseau - Analyse de trafic - SIEM

1. Contexte et objectifs de la situation

1.1 Cadre de la situation

Dans le cadre de ma formation BTS SIO option SISR, j'ai réalisé une situation professionnelle personnelle portant sur la mise en place d'une solution complète d'analyse de trafic réseau et de supervision de l'infrastructure. Cette situation s'inscrit en complément du projet commun mené avec mon binôme, et constitue ma partie individuelle du dossier.

J'ai choisi de mettre en œuvre la suite [redacted] Stack [redacted] earch, Kibana et Packetbeat), une solution open source largement utilisée en e emen ssionnel pour la supervision réseau et la détection d'incidents de sécurité. Cette solution m'a permis d'acquérir des compétences directement transposables en milieu professionnel, dans un domaine en forte demande (SOC, supervision, cybersécurité).

1.2 Objectifs techniques

- Déployer [redacted] earch et Kibana sur une machine virtuelle Debian 12
- Installer et configurer Packetbeat sur plusieurs serveurs de l'infrastructure
- Centraliser les données de capture réseau dans [redacted] earch
- Sécuriser la communication entre les agents et le serveur via TLS
- Mettre en place des dashboards de visualisation dans Kibana
- Configurer une politique de rétention des données via ILM
- Créer des règles d'alerting personnalisées pour la détection d'anomalies
- Activer le module [redacted] Security (SIEM) avec règles de détection préconstruites

1.3 Présentation de la suite [redacted] Stack

La suite [redacted] Stack se compose de plusieurs briques logicielles complémentaires qui forment ensembl lution complète de collecte, stockage, visualisation et analyse des données :

Composant	Rôle	Position dans l'architecture
[redacted] earch	Base de données NoSQL et moteur de recherche distribué	Stockage central des données
Kibana	Interface graphique web de visualisation et d'administration	Front-end utilisateur
Packetbeat	Agent léger de capture du trafic réseau	Déployé sur chaque machine à superviser
[redacted] Security (SIEM)	Module de détection automatique de menaces	Intégré à Kibana

2. Environnement technique

2.1 Infrastructure de virtualisation

Composant	Configuration	Remarque
Hyperviseur	Proxmox VE	Environnement de laboratoire
OS des VMs	Debian GNU/Linux 12 (Bookworm)	Distribution stable et légère

Composant	Configuration	Remarque
VM serveur ELK	4 vCPU, 8 Go RAM, 60 Go disque	SRVM-ELK - [redacted]
VM [redacted]	2 vCPU, 4 Go RAM	SRVM [redacted] - agent Packetbeat
VM Reverse Proxy	2 vCPU, 4 Go RAM	SRVM-ReverseProxy - agent Packetbeat
Réseau	Bridge vmbr0	Réseau local [redacted]

2.2 Versions logicielles déployées

Logiciel	Version	Rôle
[redacted] earch	8.19.14	Stockage et indexation des données
Kibana	8.19.14	Interface graphique de visualisation
Packetbeat	8.19.14	Capture et envoi du trafic réseau
OpenSSL	3.0.x	Génération du certificat TLS pour HTTPS

2.3 Ports réseau utilisés

Port	Protocole	Usage
9200	HTTPS	API REST [redacted] earch
5601	HTTP	Interface web Kibana
9300	TCP	Communication inter-nœuds [redacted] earch

3. Architecture de la solution

3.1 Schéma logique de la solution

La solution repose sur une architecture centralisée où chaque machine de l'infrastructure héberge un agent Packetbeat. Cet agent capture l [redacted] nt le trafic réseau passant par sa carte réseau et l'envoie en temps réel vers le serveur central [redacted] earch via une connexion HTTPS sécurisée. L'utilisateur consulte ensuite l'ensemble des donn [redacted] 'interface web Kibana.

3.2 Flux de données

Le cheminement d'un événement réseau capturé est le suivant :

- Packetbeat intercepte un paquet réseau sur la VM (DNS, HTTP, TLS, ICMP, etc.)
- Il décode le protocole applicatif et extrait les métadonnées pertinentes
- Les données sont sérialisées au format JSON et envoyées en HTTPS vers [redacted] earch
- [redacted] earch valide le certificat TLS via le fingerprint CA configuré
- L'événement est indexé dans un index packetbeat-8.19.x-YYYY.MM.DD
- Kibana interroge [redacted] earch et affiche les données dans les dashboards

3.3 Avantages de cette architecture

Avantage	Description
Centralisation	Toutes les données réseau de l'infrastructure sont consultables depuis une seule interface
Scalabilité	Possibilité d'ajouter de nouvelles VMs en y déployant simplement un agent Packetbeat
Sécurité	Communication chiffrée TLS entre agents et serveur central
Faible empreinte	Packetbeat est un agent léger (Go), peu gourmand en CPU et RAM
Open source	Solution gratuite, bien documentée et largement adoptée en entreprise

4. Installation et configuration d [redacted] earch et Kibana

4.1 Ajout du dépôt officiel [redacted]

[redacted] fournit un dépôt APT officiel pour Debian/Ubuntu. La clé GPG est importée pour authentifier uets installés.

Étape	Commande
Importer la clé GPG	wget -qO - https://a [redacted] co/GPG-KEY [redacted] earch | gpg --dearmor -o /usr/share/keyrings [redacted] keyring.gpg
Ajouter le dépôt	echo "deb [signed-by=...] https [redacted] cts [redacted] co/packages/8.x/apt stable main" > /etc/apt/sources.list.d [redacted] 8.x
Mettre à jour APT	apt-get update

4.2 Installation des paquets

Les paquets [redacted] earch et Kibana sont installés sur la VM SRVM-ELK uniquement, qui constitue le serveur cent a solution.

Paquet	Commande
[redacted] earch	apt-get install [redacted] earch
Kibana	apt-get install kibana

À l'installation d [redacted] earch 8.x, la sécurit st activée automatiquement. Un certificat auto-signé est généré TTP layer dans /etc [redacted] earch/certs/http_ca.crt, ainsi qu'un mot de passe pour l'utilisateur [redacted] affiché en sortie de .

4.3 Démarrage et activation des services

Service	Commande de démarrage	Activation au boot
[redacted] earch	systemctl start [redacted] earch	systemctl enable [redacted] earch
Kibana	systemctl start kibana	systemctl enable kibana

4.4 Récupération du fingerprint TLS

Pour permettre aux agents Packetbeat de faire confiance au certificat auto-signé d [redacted] earch, le fingerprint SHA-256 du certificat CA doit être récupéré et utilisé dans la configuratio ents.

Commande utilisée :

openssl x509 -fingerprint -sha256 -noout -in /etc [redacted] earch/certs/http_ca.crt | awk -F= '{print $2}' | sed 's/://g'

Cette commande retourne le fingerprint sous forme d'une chaîne hexadécimale de 64 caractères, sans séparateurs, directement utilisable dans le fichier packetbeat.yml.

4.5 Configuration de la clé de chiffrement Kibana

Pour utiliser la fonctionnalité d'alerting, Kibana nécessite une clé de chiffrement de minimum 32 caractères dans son fichier de configuration.

Ajout dans /etc/kibana/kibana.yml :

xpack.encryptedSavedObjects.encryptionKey: [redacted]

5. Déploiement de Packetbeat sur les machines

5.1 Stratégie de déploiement

Packetbeat est déployé sur les 3 VMs de l'infrastructure (SRVM-ELK, SRVM [redacted] SRVM-ReverseProxy) afin de capturer le trafi [redacted] u de chacune. Chaque agent envoie ses don [redacted] ers le serveur central SRVM-ELK qui héberge [redacted] earch.

5.2 Installation de l'agent

L'installation se fait via le dépôt APT précédemment configuré. La commande est identique sur les 3 VMs.

apt-get install packetbeat

5.3 Fichier de configuration packetbeat.yml

Le fichier /etc/packetbeat/packetbeat.yml a été modifié sur chaque VM. Trois sections principales ont été éditées :

Interface réseau écoutée :

packetbeat.interfaces:

device: any

Sortie vers [redacted] earch :

output [redacted] earch:

hosts: ["https:/ [redacted] 9200"]

username: [redacted]

password: "[mot_de_passe]"

ssl.ca_trusted_fingerprint: "[fingerprint_64_caracteres]"

Connexion à Kibana :

setup.kibana:

host: [redacted] 5601"

5.4 Protocoles capturés

Packetbeat est capable de décoder de nombreux protocoles applicatifs en analysant le trafic réseau brut. Les protocoles activés dans la configuration de ce projet sont :

Protocole	Port(s)	Usage
DNS	53	Requêtes de résolution de noms
HTTP	80, 8080	Trafic web non chiffré
TLS	443, 8443	Connexions HTTPS chiffrées (handshake)
ICMP	-	Ping et messages de contrôle
DHCPv4	67, 68	Attribution d'adresses IP
Flows	tous	Métadonnées de flux entre machines

5.5 Initialisation des dashboards

Une fois la configuration terminée, la commande suivante a été exécutée sur SRVM-ELK pour charger automatiquement les dashboards officiels Packetbeat dans Kibana :

packetbeat setup -e

Cette commande a cha [redacted] de 10 dashboards préconstruits, les pipelines d'ingestion ainsi que les templates d'index dans [redacted] earch.

6. Configuration des dashboards et visualisations

6.1 Création du Data View

Avant d'exploiter les données dans Kibana, un Data View 'packetbe [redacted] été créé via Stack Management > Data Views. Ce pattern correspond à tous les index [redacted] earch dont le nom commence par 'packetbeat-' (créés quotidiennement par les agents).

6.2 Dashboards officiels exploités

Dashboard	Contenu
Packetbeat Overview ECS	Vue globale du trafic réseau (volume, top protocoles, top hôtes)
Packetbeat DNS Overview ECS	Statistiques sur les requêtes DNS, top domaines interrogés
Packetbeat HTTP ECS	Codes de réponse HTTP, temps de réponse, top URLs
Packetbeat Flows ECS	Flux réseau entre machines, volumes échangés
Packetbeat TLS ECS	Connexions chiffrées, versions TLS négociées, certificats
Packetbeat DNS Tunneling ECS	Détection d'anomalies DNS (exfiltration de données)

6.3 Visualisations clés pour la démonstration

Lors de la présentation au jury, les visualisations suivantes seront mises en avant car elles démontrent concrètement l'apport de la solution :

- Carte de répartition du trafic par hostname (SRVM-ELK / SRVM [redacted] / SRVM-ReverseProxy)
- Top 10 des domaines DNS interrogés depuis l'infrastructure
- Distribution des codes de réponse HTTP (2xx / 3xx / 4xx / 5xx)

- Évolution temporelle du volume de trafic capturé

7. Mise en place de l'alerting

7.1 Principe et utilité

La fonctionnalité Rules de Kibana permet de définir des conditions qui, lorsqu'elles sont remplies, déclenchent une alerte. Cela transforme la solution d'un simple outil de visualisation passive en un système de supervision active.

7.2 Règles personnalisées créées

[redacted]gles d'alerting ont été configurées via Stack Management > Rules. Chaque règle est de type [redacted]earch query' avec un langage KQL et est liée à un dashboard pour faciliter l'investigation.

Règle 1 - Détection d'erreurs HTTP

Paramètre	Valeur
Data view	packetbeat-*
Requête KQL	network.protocol: http and not (http.response.status_code >= 200 and http.response.status_code < 300)
Seuil	Plus de 2 occurrences en 2 minutes
Fréquence de vérification	Toutes les 2 minutes
Dashboard lié	Packetbeat HTTP ECS

Règle 2 - Volume DNS anormal

Paramètre	Valeur
Data view	packetbeat-*
Requête KQL	network.protocol: dns
Seuil	Plus de 100 occurrences en 1 minute
Fréquence de vérification	Toutes les minutes
Dashboard lié	Packetbeat DNS Overview ECS

Règle 3 - Scan de ports potentiel

Paramètre	Valeur
Data view	packetbeat-*
Requête KQL	event.dataset: flow and network.direction: outbound
Seuil	Plus de 50 occurrences en 1 minute
Fréquence de vérification	Toutes les minutes
Dashboard lié	Packetbeat Flows ECS

7.3 Limitation de la licence Basic

La licence gratuite Basic d[redacted]ne permet pas l'utilisation de connecteurs avancés (email, Slack, webhooks). Les actions di[redacted]es sont limitées à 'Cases' et 'Observability AI Assistant'. Dans un

contexte de production, une licence Platinum permettrait l'envoi automatique de notifications par email.

8. Activation du module SIEM [redacted] Security)

8.1 Présentation du module

[redacted] Security est un module intégré à Kibana qui combine SIEM (Security Information and Event [redacted] ement), XDR (Extended Detection and Response) et endpoint security. Il transforme la solution d'une supervision réseau passive en une plateforme active de détection de menaces.

8.2 Activation et installation des règles préconstruites

Le module est accessible via le menu Security de Kibana. Plus de 1600 règles de détection préconstruites sont disponibles, classées par tags. Pour ce projet, les règles correspondant aux tags suivants ont été installées :

- Data Source: Network Packet Capture - règles spécifiques aux données Packetbeat
- Data Source: Network Traffic - règles génériques de trafic réseau
- Use Case: Network Security Monitoring - règles de monitoring sécurité réseau

8.3 Règles pertinentes pour l'infrastructure

Sur les règles installées, les suivantes ont déjà détecté des correspondances dans les données capturées :

Règle	Description	Sévérité
Potential Network Sweep Detected	Détection de balayage réseau (recensement d'hôtes)	Low
Potential SYN-Based Port Scan Detected	Détection de scan de ports basé sur SYN	Low
Potential Network Scan Detected	Détection de scan réseau générique	Low
Initial Access via File Upload Followed by GET Request	Détection d'upload suivi d'accès web (potentiel webshell)	Medium
Potential Webshell Deployed via Apache Struts	Détection de webshell via vulnérabilité Apache Struts	High

9. Politique de rétention des données (ILM)

9.1 Problématique

[redacted] nnées capturées par Packetbeat peuvent rapidement saturer l'espace disque du serveur [redacted] earch. Sur un disque de 60 Go, sans politique de rétention, le serveur deviendrait inutilisable [redacted] lques semaines. Une politique de gestion automatique du cycle de vie des index a donc été mise en place.

9.2 Configuration de la policy 'packetbeat'

La gestion s'effectue via Stack Management > Index Lifecycle Policies. La policy par défaut 'packetbeat' a été modifiée pour mieux correspondre aux contraintes du projet.

Paramètre	Valeur par défaut	Valeur configurée
Maximum age (Hot phase)	30 jours	7 jours
Maximum primary shard size	50 Go	40 Go
Use recommended defaults	Activé	Désactivé

9.3 Phases du cycle de vie d'un index

Phase	Description
Hot	Données récentes, fréquemment consultées, stockage rapide
Warm	Données moins consultées, stockage moins rapide
Cold	Données rarement consultées, stockage économique
Delete	Suppression automatique des anciennes données

10. Procédures de test et validation

10.1 Vérification de la remontée des données

La validation du déploiement est réalisée en consultant l'interface Kibana via Analytics > Discover. Le Data View 'packetbeat-*' affiche en temps réel les événements capturés par les 3 agents.

10.2 Plan de tests

Test	Action	Résultat attendu
Connectivité agents	curl -k https:/ [redacted] 9200 depuis chaque VM	Réponse HTTP 401 (auth requise)
Statut services	systemctl status packetbeat	Active (running)
Indexation	curl _cat/indices?v sur [redacted] earch	Présence d'index packetbeat-8.19.x-*
Réception multi-agents	Filtre agent.hostname dans Discover	3 hostnames distincts visibles
Capture DNS	nslookup google.com depuis une VM	Événement DNS visible dans dashboard
Capture HTTP	curl http://example.com depuis une VM	Événement HTTP visible dans dashboard
Déclenchement règle	Génération de trafic anormal	Alerte visible dans Stack Management > Rules

10.3 Commandes utiles de diagnostic

Commande	Utilité
systemctl status packetbeat	Vérifier que l'agent tourne sur une VM
journalctl -u packetbeat -n 20	Consulter les derniers logs de l'agent
journalctl -u packetbeat -f	Suivre les logs en temps réel

Commande	Utilité
curl -k -u [redacted] [mdp] https://l t:9200/_cat/indices?v	Lister les index présents dans [redacted] earch
packetbeat test config	Valider la syntaxe du fichier packetbeat.yml
packetbeat test output	Tester la connectivité avec [redacted] earch

11. Bilan et retour d'expérience

11.1 Compétences acquises

- Déploiement complet de la suite [redacted] Stack [redacted] earch, Kibana, Packetbeat) en environnement Debian
- Configuration de la sécurité TLS via certificat auto-signé et fingerprint SHA-256
- Administration multi-machines avec déploiement d'agents légers sur plusieurs serveurs
- Création et exploitation de dashboards Kibana pour la visualisation de données
- Configuration de règles d'alerting basées sur le langage KQL
- Mise en œuvre d'une politique de rétention des données via Index Lifecycle Management
- Activation et configuration du module SIEM [redacted] Security pour la détection de menaces
- Diagnostic et résolution d'erreurs de configuration via les logs systemd

11.2 Difficultés rencontrées et solutions

Difficulté	Cause identifiée	Solution apportée
Erreur de connexion HTTPS	Confusion entre HTTP et HTTPS dans hosts	Ajout du préfixe https:// dans la config
Erreur fingerprint TLS	Espaces parasites lors du copier-coller	Utilisation de la commande openssl avec sed pour nettoyer
Clé de chiffrement absente	xpack.encryptedSavedObjects manquant	Ajout de la clé dans kibana.yml + redémarrage
Connecteurs d'action limités	Licence Basic restreinte	Liaison aux dashboards en alternative
Configuration YAML dupliquée	Doublon dans packetbeat.interfaces	Commenter la ligne dupliquée
Charge système élevée	Capture sur 'any' interface	Acceptable car infrastructure de test

11.3 Apport pour ma formation BTS SIO SISR

Ce projet m'a permis de découvrir une solution professionnelle complète de supervision réseau, dans un d [redacted] en très forte demande sur le marché de l'emploi (cybersécurité, SOC, supervision). La suite [redacted] Stack est utilisée par de nombreuses grandes entreprises et organismes (Cisco Talos, Oak Ridg [redacted] al Laboratory, NASA), ce qui en fait une compétence directement valorisable.

Au-delà de la simple configuration, j'ai dû comprendre les mécanismes sous-jacents : pourquoi un certificat TLS, à quoi sert un fingerprint, comment fonctionnent les index et les data views, comment les règles d'alerting s'appuient sur des requêtes structurées. Cette compréhension en profondeur correspond exactement à ce qui est attendu d'un technicien SISR en entreprise.

11.4 Perspectives d'évolution

Plusieurs pistes d'enrichissement ont été identifiées et pourraient faire l'objet de développements ultérieurs :

- Déploiement de Filebeat pour la centralisation des logs système (en complément de Packetbeat)
- Configuration d'un reverse proxy Nginx avec certificat valide pour exposer Kibana en HTTPS
- Mise en place de Logstash pour le traitement et l'enrichissement avancé des données
- Création d'utilisateurs et de rôles [redacted] earch pour une gestion fine des accès
- Sauvegarde régulière des données via la fonctionnalité Snapshot and Restore

11.5 Conclusion

Ce projet m'a permis de déployer une solution complète et fonctionnelle de supervision et d'analyse de trafic réseau sur une infrastructure de 3 machines virtuelles. Au-delà de l'aspect purement technique, il m'a confronté à des problématiques co [redacted] de certificats, dimensionnement du stockage, choix des règles de détection) que tout [redacted] système et réseau rencontre en environnement professionnel.

La solution déployée est opérationnelle, sécurisée par TLS, dotée de dashboards de visualisation, de règles d'alerting personnalisées et d'un module de détection de menaces. Elle constitue une base solide qui pourrait être étendue à un parc plus import [redacted] s modification majeure de l'architecture, démontrant ainsi les qualités de scalabilité de la suite [redacted] Stack.