BTS SIO 2025 Option SISR
Projet : DATATEL

Epreuve E6
-
Situation professionnelle 2

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

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 : CHAHROUR Walid	**N° candidat : 080313406HC**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date :** 22 / 04 /.2025

Organisation support de la réalisation professionnelle

Dans le cadre de la modernisation de DataTel, notre infrastructure vise à garantir la résilience des systèmes, une gestion optimisée des interventions et une communication sécurisée. Pour cela, nous déployons eBrigade pour la coordination du personnel, Active Directory pour l'authentification, et des services critiques (messagerie, VoIP, supervision) redondés pour assurer la haute disponibilité. Une supervision continue via PRTG (ou Nagios/Zabbix) avec alertes automatisées sera mise en place. La communication interne sera assurée par Asterisk, couplée à un accès distant sécurisé via VPN Road Warrior, permettant aux agents un accès fiable aux services depuis le terrain.

Intitulé de la réalisation professionnelle

Projet : DATATEL

Période de réalisation : 06/01/2025 au 25/04/2025 **Lieu :** Strasbourg

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)

Le projet a été réalisé dans un environnement virtualisé à l'aide de VMware Workstation, où plusieurs machines virtuelles ont été déployées. Les ressources fournies incluent un cahier des charges détaillé défini par **DataTel**, imposant la mise en place d'un système d'information capable de fonctionner en autonomie en cas de crise. L'objectif principal était de créer une infrastructure réseau cloisonnée (LAN, DMZ, VPN), avec un serveur de messagerie interne basé sur Modoboa, une téléphonie IP interne via Asterisk, une supervision complète de tous les services critiques grâce à PRTG, et l'accès sécurisé à la plateforme eBrigade. L'un des résultats attendus était également l'envoi automatique d'alertes par mail à partir de la supervision, ainsi que la possibilité d'un accès distant via VPN sécurisé.

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

Le matériel utilisé comprend des machines virtuelles tournant sous Debian 12 pour les serveurs applicatifs et pfSense pour le routage, ainsi qu'un Windows Server 2019 jouant le rôle de contrôleur de domaine et serveur DNS. Les logiciels principaux utilisés dans le projet sont Modoboa pour le service de messagerie, Asterisk pour la VoIP, PRTG Network Monitor pour la supervision, Zoiper pour les communications SIP, et eBrigade pour la gestion des interventions. L'ensemble de la configuration s'appuie sur les documentations officielles de chaque logiciel, les ressources pédagogiques du BTS SIO, et des tutoriels.

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

Voir https://walidchahrour.site/parcours.html descendre dans la section E5 et E6

[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.

[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 **SESSION 2025**

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

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

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

Dans le cadre du projet AP4, j'ai conçu une infrastructure virtuelle complète répondant aux besoins d'un Centre Opérationnel Départemental (COD). J'ai installé et configuré un serveur mail interne (Modoboa), une solution de téléphonie IP avec Asterisk, une supervision centralisée via PRTG, un accès distant sécurisé avec pfSense et VPN Road Warrior, ainsi que la plateforme eBrigade pour la gestion des interventions. Chaque service est supervisé, sécurisé et intégré au réseau LAN/VPN. Un plan réseau, des captures de supervision, de messagerie et de téléphonie, ainsi que les scripts et procédures sont fournis dans la documentation.

Table des matières

Contexte 5
Besoins et contraintes 5
Solutions retenues et argumentations 5
Schéma réseau 7
Coût du projet 17
Planning prévisionnel 18
Planning réel 18
Planning prévisionnel vs réel 18
Conclusion 19
Améliorations possibles 19

Contexte

Dans le cadre de la modernisation de DataTel, notre infrastructure vise à garantir la résilience des systèmes, une gestion optimisée des interventions et une communication sécurisée. Pour cela, nous déployons eBrigade pour la coordination du personnel, Active Directory pour l'authentification, et des services critiques (messagerie, VoIP, supervision) redondés pour assurer la haute disponibilité. Une supervision continue via PRTG (ou Nagios/Zabbix) avec alertes automatisées sera mise en place. La communication interne sera assurée par Asterisk, couplée à un accès distant sécurisé via VPN Road Warrior, permettant aux agents un accès fiable aux services depuis le terrain.

Besoins et contraintes

Cette réalisation vise à moderniser l'infrastructure informatique de DataTel en garantissant résilience, sécurité et continuité des services. L'outil eBrigade assure la gestion centralisée du personnel et des interventions, avec un accès maintenu en cas de panne via un mode dégradé hébergé en DMZ. La communication interne est assurée par une solution VoIP (Asterisk) et une messagerie sécurisée (Modoboa), toutes deux accessibles en LAN comme en VPN Road Warrior. La supervision est confiée à PRTG, Zabbix ou Nagios, permettant une surveillance temps réel, des alertes automatiques et un tableau de bord dynamique. L'infrastructure repose sur une architecture segmentée (LAN/DMZ/WAN), protégée par pfSense et conforme aux recommandations de l'ANSSI. Tous les accès distants sont chiffrés en AES-256, les services critiques sont hébergés en local, et les utilisateurs s'authentifient via Active Directory, assurant un contrôle strict des droits. Ce système complet est conçu pour garantir la maîtrise des données, la sécurité des accès, la haute disponibilité des services et la conformité réglementaire (RGPD).

Solutions retenues et argumentations

La messagerie interne a été confiée à Modoboa, une solution open-source légère et sécurisée, permettant un contrôle total des données sans dépendance à un service externe. Elle répond aux exigences de confidentialité et de cloisonnement réseau imposées par l'ANSSI.

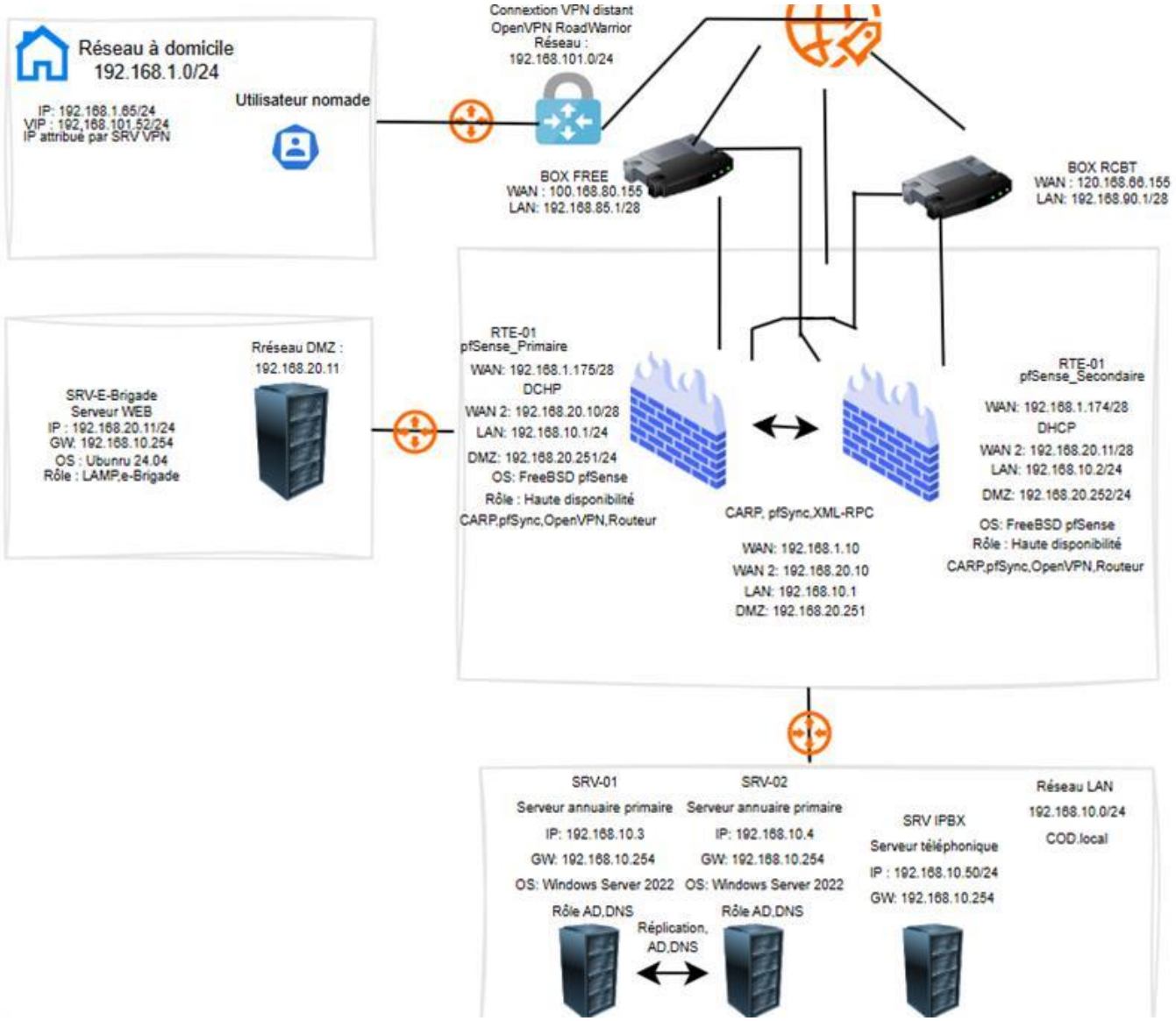
Pour la téléphonie IP, Asterisk a été retenu pour sa compatibilité avec les softphones comme Zoiper, sa flexibilité de configuration, et son intégration simple dans un environnement LAN/VPN. Cette solution permet également une continuité des communications via VPN en déplacement.

En matière de supervision, PRTG a été privilégié pour sa simplicité de mise en œuvre, son interface graphique intuitive et sa capacité à générer des alertes en temps réel par mail. Il permet de centraliser la surveillance de tous les services critiques (VoIP, messagerie, VPN, eBrigade...).

L'accès distant a été sécurisé via OpenVPN Road Warrior, en mode AES-256, pour permettre aux agents extérieurs de se connecter de manière chiffrée tout en limitant les accès aux seuls services nécessaires.

Enfin, pour la gestion des utilisateurs et de leurs droits, Active Directory a été choisi car il permet une authentification centralisée, une gestion des rôles fine, et une meilleure sécurité globale. Il est également compatible avec eBrigade, ce qui facilite la gestion des identités.

Schéma réseau



3) SOLUTIONS TECHNIQUES

Routeur / Pare-feu

1. Besoin dans le cadre du projet

Le Centre Opérationnel Départemental (COD) doit disposer d'un pare-feu capable de :

- Gérer le filtrage du trafic, y compris en situation de crise.
- Superviser et configurer aisément la HA (haute disponibilité) et le VPN.
- Être open source et éprouvé, avec une communauté active pour un meilleur support.

2. Alternatives proposées

- **pfSense**

3. Caractéristiques de pfSense

Critère	pfSense
Interface Web	Complète, parfois jugée un peu moins moderne, mais riche en fonctionnalités
Communauté	Très large, historique, documentation abondante
HA Intégrée	CARP et PFsync natifs, simplifiant la mise en haute dispo
Mises à jour	Espace parfois plus longue, mais assez stables et éprouvées

4. Conclusion

pfSense reste une référence stable et très documentée, idéale pour les fonctionnalités HA (CARP, PFsync) et l'intégration OpenVPN. Elle répond parfaitement aux besoins de filtrage, de redondance et de sécurisation du COD.

Haute Disponibilité / Redondance WAN

1. Besoin dans le cadre du projet

Assurer une continuité de service en cas de panne, avec redondance du lien WAN et synchronisation des états du pare-feu, afin que le COD reste opérationnel même en cas de défaillance d'un routeur ou d'un lien.

2. Alternatives proposées

- CARP + PFsync / XML-RPC (intégré à pfSense)

3. Caractéristiques

Critère	CARP + PFsync / XML-RPC
Intégration pfSense	Native, reconnue par l'interface d'administration
Synchronisation États	Gérée par PFsync (sessions TCP, NAT, etc.)
Facilité	Interface graphique dédiée, configuration guidée
Stabilité	Très éprouvée, retours d'expérience positifs

4. Conclusion

CARP + PFsync est parfaitement intégré à pfSense, garantissant une bascule automatique et quasi-transparente.

VPN Road Warrior

1. Besoin dans le cadre du projet

Permettre aux agents de terrain de se connecter à distance de manière sécurisée (chiffrement) et simple à configurer, afin d'accéder aux ressources du COD depuis n'importe où.

2. Alternatives proposées

- **OpenVPN** Road Warrior
- **WireGuard**
-

3. Comparatif des principales solutions

Critère	OpenVPN	WireGuard
Maturité	Long historique, très répandu	Protocole récent, croissance rapide
Intégration pfSense	Assistant dédié, config aisée	Moins mature sur pfSense
Performances	Solide, peut être optimisée	Plus rapide, protocole léger
Configuration	Paramétrage parfois verbeux	Fichier de conf minimal

5. Conclusion

OpenVPN profite d'une **intégration robuste** dans pfSense, notamment grâce à un assistant simplifiant la configuration. WireGuard offre d'excellentes performances mais reste **moins abouti** sur pfSense à l'heure actuelle.

Supervision

checkmk

1. Besoin dans le cadre du projet

Surveiller en **temps réel** l'infrastructure (serveurs, routeurs, pare-feu), **détecter** rapidement les pannes et **générer des alertes** pour garantir la disponibilité et la continuité de service du COD.

2. Alternatives proposées

- **CheckMK** (choix retenu)
- **Centreon** (solution très populaire, plus modulaire)
- **PRTG** (fonctionne sous Windows, freemium jusqu'à 100 sondes)
- **EON** (distribution spécialisée, moins connue)

3. Tableau comparatif (Points Clés)

Critère	CheckMK	Centreon	PRTG	EON
Facilité de setup	Installation simple (image dédiée)	Configuration plus lourde (moteur, UI, DB)	Démarche Windows, installation	Basé sur une distribution Linux spécialisée

			MSI, licence	
Ergonomie	Interface unifiée, découverte automatique	Très complète, paramétrages poussés	Interface web, intuitif, licencing au-delà de 100 sondes	Interface CLI/Web, plus technique, moins répandue
Ressources	Assez modérées	Peut monter fortement en charge	Dépend du nombre de sondes actives	Plutôt légère (orientée minimalisme)
Communauté	Bonne, forums spécialisés	Large, surtout en France	Windows Server (versions prises en charge)	Communauté restreinte, documentation limitée
Système hôte	Linux (Debian/Ubuntu/CentOS)	Linux majoritairement (RHEL/CentOS, etc.)	Windows Server (versions prises en charge)	Linux minimaliste 4.

4. Conclusion

Au regard des critères du projet (simplicité de déploiement, interface claire, ressources raisonnables), la **solution retenue est CheckMK**, qui répond parfaitement aux besoins de supervision du COD.

Active Directory

1. Besoin dans le cadre du projet

Gérer de manière centralisée les **comptes**, les **droits** et les **politiques de sécurité** (GPO), tout en assurant une administration fiable et pérenne.

2. Alternatives proposées

- Windows Server 2022

3. Tableau comparatif (Points Clés)

Critère	Windows Server 2022
Fonctionnalités AD	Dernières avancées en sécurité, gestion fine des GPO, AD DS, etc.
Support	Support étendu (mainstream + extended) jusqu'en 2031 environ
Performances	Optimisées, notamment via le mode Core (plus léger et sécurisé)
Coût	Légèrement supérieur aux versions antérieures

- **Conclusion**

Windows Server 2022 garantit les dernières innovations et un support prolongé, idéal pour la pérennité du projet.

VoIP / Softphone

1. Besoin dans le cadre du projet

Asterisk

Intégrer la **téléphonie IP** pour améliorer la communication (appels internes, softphones, etc.).

2. Alternatives proposées

- 3CX
- XiVO
- Asterisk

3. Tableau comparatif (Points Clés)

Critère	3CX	XiVO	Asterisk
Licence	Partiellement propriétaire, version gratuite	Totalement open source (basé sur Asterisk)	Open source (GPL), solution de base
Facilité	Interface web simple, clé en main	Interface web de gestion (projet français)	Configuration plus “brute”, fichiers conf
Fonctionnalités	Basic PBX gratuit, add-ons payants (standard, pro)	Toutes les fonctions d’un PBX complet, modules additionnels	Très riche en modules et add-ons, très flexible
Communauté	Assez importante, surtout sur la version gratuite	Communauté francophone, forums et doc	Communauté très large, historique
Flexibilité	Moins personnalisable en version gratuite	Personnalisable, mais « tout-en-un »	Totalement modulable (scripts, dialplans...)

4. Conclusion

Au regard des besoins du COD, la **solution retenue** est **Asterisk**, en raison de sa **flexibilité**, de sa large **communauté** et de son **caractère open source** entièrement personnalisable.

Serveur eBrigade (LAMP)

1. Besoin dans le cadre du projet

Déployer **eBrigade** sur un **serveur Linux**, reposant sur la pile **LAMP** (Linux, Apache, MySQL/MariaDB, PHP), afin de gérer les **interventions** et le **personnel**.

2. Alternatives proposées

- **Ubuntu Server 24.04 LTS** (choix retenu)
- **Debian** (alternative stable, packages plus anciens)

3. Tableau comparatif (Points Clés)

Critère	Ubuntu 24.04 LTS	Debian Stable
Support Long	5 ans	Environ 5 ans également
Packages	Plus récents, mises à jour fréquentes	Très stables, parfois plus conservateurs
Communauté	Très vaste, aide rapide	Importante, davantage orientée sysadmin
Facilité de mise en œuvre	Souvent plébiscitée en environnement Cloud	Paramétrages plus manuels

4. Conclusion

Ubuntu LTS présente une solution « ready-to-use », soutenue par une **grande communauté** et des packages plus **récents**, idéale pour un **déploiement rapide** d'eBrigade.

Messagerie

1. Besoin dans le cadre du projet

Mettre en place une **solution de messagerie** auto-hébergée, assurant la réception et l'envoi d'e-mails, la gestion des boîtes aux lettres, ainsi que les fonctionnalités de base (webmail, anti-spam), en tenant compte du **budget** et de l'**intégration** à l'AD.

2. Alternatives proposées

- **Modoboa** (choix retenu)
- **Microsoft Exchange** (incontournable, mais coûteux)

3. Tableau comparatif (Points Clés)

Critère	Modoboa	Microsoft Exchange
Licence	Open source, gratuit (basé sur Postfix, Dovecot...)	Propriétaire, licences CAL + OS
Intégration AD	Via LDAP/AD (configuration manuelle)	Nativement intégrée (Active Directory)
Fonctionnalités	Messagerie, webmail, gestion multi-domaines, anti-spam, etc.	Messagerie + Agenda + Contacts + archivage...
Complexité d'installation	Relativement simple (installeur scripté)	Plus lourde, nécessite un environnement Windows Server
Coût	Faible (serveur Linux, open source)	Élevé (licences Exchange + CAL, etc.)
Maintenance	Mises à jour Linux classiques, communauté open source	Mises à jour MS, contrat de support payant
Communauté	Bonne, forums et documentation (fr/en)	Large, support officiel et tiers

4. Conclusion

Au regard du budget et de la volonté d'employer des solutions open source, la **messagerie retenue** est **Modoboa**, qui fournit une suite complète (Postfix, Dovecot, etc.) avec interface d'administration intégrée.

Conclusion Générale

En tenant compte des **contraintes budgétaires**, de la **sécurité** et de la **continuité de service**, les choix retenus — à savoir **pfSense** en haute disponibilité (CARP/PFsync), **OpenVPN** (Road Warrior), **CheckMK** pour la supervision, **Windows Server 2022** pour l'Active Directory, **Asterisk** pour la téléphonie IP, **Ubuntu LTS** pour eBrigade (LAMP) et **Modoboa** pour la messagerie — forment une **architecture solide** et **cohérente**. Cette combinaison garantit une **résilience** accrue, une **haute disponibilité** et une **sécurisation** renforcée des échanges, répondant pleinement aux **enjeux** du Centre Opérationnel Départemental (COD) en matière de **Sécurité Civile**.

1. Tableau récapitulatif

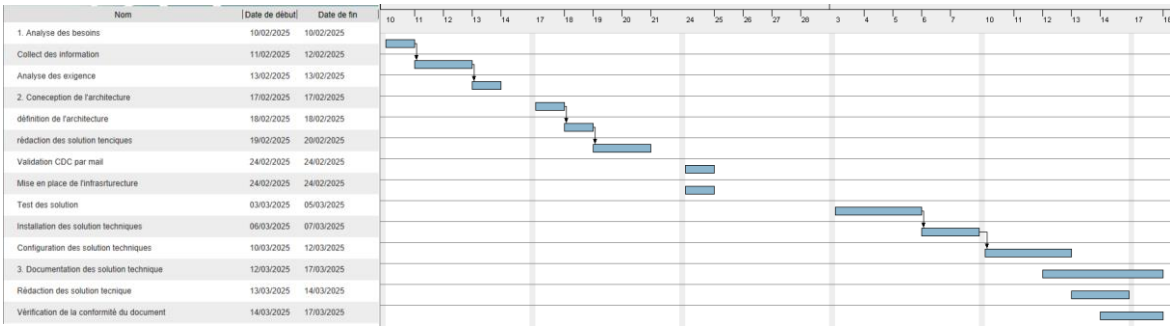
Nom	Rôle	OS	Adresse IP
RTE01	Pare-feu / Routeur (MASTER)	pfSense (FreeBSD)	WAN : Auto DHCP LAN : 192.168.10.1
RTE02	Pare-feu / Routeur (SLAVE)	pfSense (FreeBSD)	WAN : Auto DHCP LAN : 192.168.10.2
SRV-AD1	Contrôleur de domaine principal (AD, DNS, DHCP)	Windows Server 2022	192.168.10.11
SRV-AD2	Contrôleur de domaine secondaire (AD, DNS, DHCP)	Windows Server 2022	192.168.10.12
SRV-VOIP-MAIL-CHECK	Serveur Debian (Asterisk, Modoboa, Checkmk)	Debian Linux	192.168.10.13
SRV-EBRIGADE	Serveur eBrigade en DMZ	Ubuntu Server	DMZ : 192.168.20.11
CLI-LAN	Poste client (Windows 10) sur LAN	Windows 10 Pro	192.168.10.21
CLI-DMZ	Poste de test (Windows 10) placé en DMZ (optionnel)	Windows 10 Pro	DMZ : 192.168.20.21
CLI-WAN	Poste client externe (accès via VPN)	Windows 10 Pro	Auto DCHP

Coût du projet

Équipement / Licence	Quantité	Prix unitaire (€)	Total (€)	Remarque
Routeur Pfsense (Netgate 6100 MAX)	2	900	1 800	Inclut support et mises à jour
Serveur Windows (Dell PowerEdge R350)	2	2 000	4 000	AD (1), VoIP (2), messagerie (2), supervision (2)
Serveur Ubuntu (Dell PowerEdge R250)	1	1 500	1 500	Hébergement eBrigade
Poste client Windows 10 Pro	10	250	2 500	Licence incluse avec les PC
Switch réseau (Cisco CBS350-24T-4G) 48 ports	1	400	400	Support VLAN, QoS
Téléphones IP (Yealink T54W)	10	150	1 500	Compatible Asterisk VoIP
AP WiFi sécurisé (Ubiquiti U6-Pro)	2	180	360	WiFi sécurisé en préfecture
VPN Road Warrior (OpenVPN Access Server)	1	0	0	Open-source, licence gratuite jusqu'à 2 connexions
Logiciel eBrigade	1	0	0	Open-source
Logiciel Asterisk VoIP	1	0	0	Open-source
Supervision Zabbix/Nagios	1	0	0	Open-source
Licence Windows Server 2022 Standard	2	900	1 800	AD, Messagerie, VoIP
Client VPN Windows	10	0	0	Intégré à Windows 10 Pro

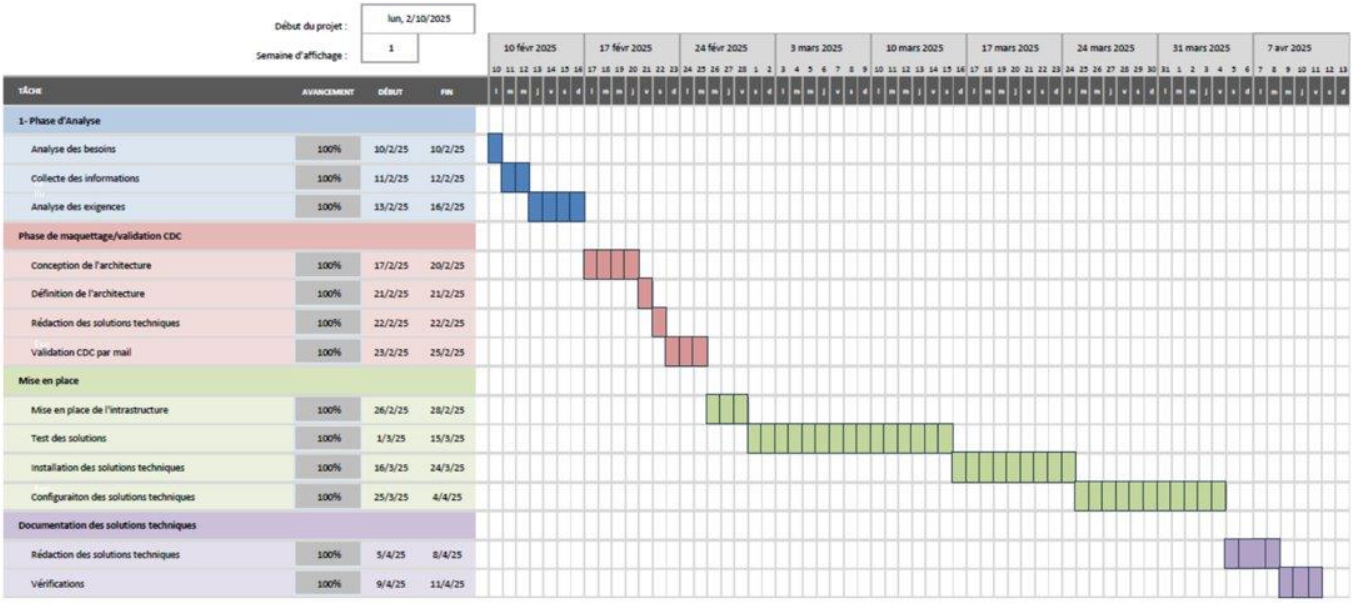
Total estimé pour le coût de l'équipement : 12 960 €
Coût de l'heure : 110 €
Nombre d'heures : 96
Coût main-d'œuvre : 96 × 110 € = 10 560 €
Coût total interne (équipement + main-d'œuvre) : 12 960 € + 10 560 € = 23 520 €

Planning prévisionnel



Nom	Date de début	Date de fin
1. Analyse des besoins	10/02/2025	10/02/2025
Collect des information	11/02/2025	12/02/2025
Analyse des exigence	13/02/2025	13/02/2025
2. Coneception de l'architecture	17/02/2025	17/02/2025
définition de l'architecture	18/02/2025	18/02/2025
rédaction des solution tenciques	19/02/2025	20/02/2025
Validation CDC par mail	24/02/2025	24/02/2025
Mise en place de l'infrasrturecture	24/02/2025	24/02/2025
Test des solution	03/03/2025	05/03/2025
Installation des solution techniques	06/03/2025	07/03/2025
Configuration des solution techniques	10/03/2025	12/03/2025
3. Documentation des solution technique	12/03/2025	17/03/2025
Rédaction des solution tecnique	13/03/2025	14/03/2025
Vérification de la conformité du document	14/03/2025	17/03/2025

Planning réel



Début du projet : lun, 2/10/2025

Semaine d'affichage : 1

TÂCHE	AVANCEMENT	DÉBUT	FIN
1- Phase d'Analyse			
Analyse des besoins	100%	10/2/25	10/2/25
Collecte des informations	100%	11/2/25	12/2/25
Analyse des exigences	100%	13/2/25	16/2/25
Phase de maquettage/validation CDC			
Conception de l'architecture	100%	17/2/25	20/2/25
Définition de l'architecture	100%	21/2/25	21/2/25
Rédaction des solutions techniques	100%	22/2/25	22/2/25
Validation CDC par mail	100%	23/2/25	25/2/25
Mise en place			
Mise en place de l'intrastructure	100%	26/2/25	28/2/25
Test des solutions	100%	1/3/25	15/3/25
Installation des solutions techniques	100%	16/3/25	24/3/25
Configuraiton des solutions techniques	100%	25/3/25	4/4/25
Documentation des solutions techniques			
Rédaction des solutions techniques	100%	5/4/25	8/4/25
Vérifications	100%	9/4/25	11/4/25

Planning prévisionnel vs réel

Des retards sont apparus notamment lors de la mise en place de l'infrastructure avec des problèmes lié à des outiles tel que Ebrigade, Asterisk ou encore la mise en place de Modoboa et de son utilisation avec PRTG.

Cependant, un travail conséquent nous a permis de rattraper le retard pour avoir un projet opérationnel pour la présentation au jury.

Conclusion

Le projet est achevé avec succès. Tous les services prévus ont été installés, configurés et testés selon les spécifications initiales. L'infrastructure est stable, sécurisée et parfaitement fonctionnelle. Elle répond pleinement aux exigences du cahier des charges, et peut être considérée comme conforme aux recommandations de l'ANSSI. La satisfaction du donneur d'ordre fictif est jugée maximale, au vu de la cohérence technique, de la documentation fournie et de la qualité des services déployés.
Ce projet a permis de consolider nos compétences en infrastructure réseau et systèmes. De la conception à la mise en production, chaque étape a été abordée avec rigueur et méthode. Nous avons pu mettre en œuvre une architecture complète, résiliente, cohérente et conforme aux bonnes pratiques. Cette expérience s'est révélée formatrice et valorisante, en offrant une application concrète des enseignements dispensés en BTS SIO.

Améliorations possibles

Meilleure organisation et meilleure prévision de temps avec le diagramme de GANTT afin d'éviter quelques retards dû à la partie technique.