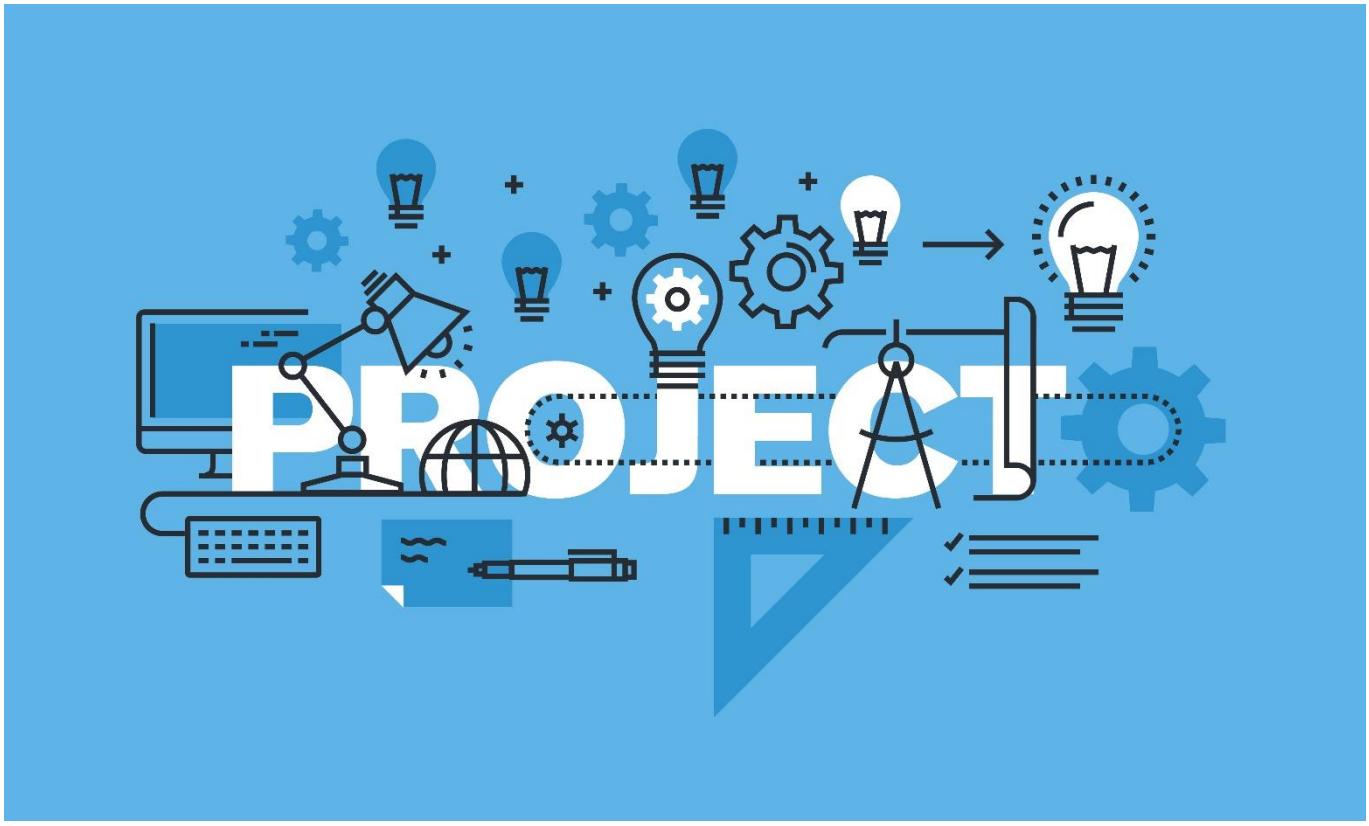
Projet sécurité civile : Assurer le fonctionnement permanent et optimum des Centres Opérationnels Départementaux et mettre en œuvre une connexion distante

-

SIO 2023 Option SISR



Epreuve E5

-

Situation professionnelle 2

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2023**

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

ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (recto)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE

N° réalisation : 2

Nom, prénom : Koehler Erwann

N° candidat : 01948562258

Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒ **Date :** 14 / 04 /2023

Organisation support de la réalisation professionnelle

Les Centre Opérationnel Départemental est un service de la préfecture. Ce dernier doit améliorer la résilience informatique en cas de crise, optimiser son système d'information ainsi que l'accessibilité sécurisée de son système d'information à l'extérieur. Le projet consiste à proposer une solution technique et commerciale ainsi qu'une maquette sous la forme d'un environnement virtuel qui répondent à ce besoin.

Intitulé de la réalisation professionnelle

Assurer le fonctionnement permanent et optimum des Centres Opérationnels Départementaux et mettre en œuvre une connexion distante

Période de réalisation : 02/01/2023 au 30/03/2023 **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)

Ressources fournies :

Un cahier des charges, comprenant le contexte, les besoins et les contraintes

Résultats attendus :

- Mise en œuvre d'une haute disponibilité de routeurs et liaison Internet redondée (2 routeurs / 2 accès Internet)
- Mise en œuvre de 2 serveurs Active Directory (Principal et Secondaire)
- Mise en œuvre d'1 serveur de téléphonie IpBX et déploiement d'un client softphone
- Mise en œuvre d'1 serveur de messagerie et déploiement d'un client de messagerie -> Utilisation des comptes de l'AD
- Mise en œuvre d'1 serveur de supervision et de monitoring
  - Supervision de la disponibilité des routeurs et serveurs
  - Monitoring et historique des indisponibilités des routeurs et serveurs
  - Alerte par mail aux administrateurs en cas de panne
- Mise en œuvre d'une solution de VPN RW (Road Warrior)-> Utilisation des comptes de l'Active Directory
- Mise en œuvre d'une DMZ pour accéder au Serveur WEB E-Brigade

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

Documentations :

Le cahier des charges

Logiciels :

Windows Server 2019, Windows10 Pro, pfSense, Ubuntu Server 22.04, CheckMK, Asterisk, Hmail, eBrigade

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

https://www.erwann-koehler.fr/pages/ressources.html

[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 2022

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

ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

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

Table des matières

Contexte

Le service interministériel départemental des systèmes d'information et de communication (SIDSIC) est placé sous l'autorité du secrétaire général de la préfecture, est chargé de missions opérationnelles de supervision et de maintenance de réseaux informatiques et télécoms gouvernementaux. Le projet prend place au sein de ce service (SIDSIC). Il doit permette aux Préfectures d'améliorer leur résilience informatique en cas de crise, d'optimiser son système d'information ainsi que l'accessibilité sécurisée de son système d'information à l'extérieur.

Le projet consiste en la réalisation d'une proposition technique et commerciale ainsi que la mise en œuvre d'un maquettage sous environnement virtuel de l'ensemble des besoins exprimés ci-dessous.

Besoins et contraintes

Les besoins sont :

1. Mise en œuvre d'une haute disponibilité de routeurs et liaison Internet redondée (2 routeurs / 2 accès Internet)
2. Mise en œuvre de 2 serveurs Active Directory (Principal et Secondaire)
3. Mise en œuvre d'1 serveur de téléphonie IpBX et déploiement d'un client softphone
4. Mise en œuvre d'1 serveur de messagerie et déploiement d'un client de messagerie -> Utilisation des comptes de l'Active Directory
5. Mise en œuvre d'1 serveur de supervision et de monitoring
    a. Supervision de la disponibilité des routeurs et serveurs
    b. Monitoring et historique des indisponibilités des routeurs et serveurs
    c. Alerte par mail aux administrateurs en cas de panne
6. Mise en œuvre d'une solution de VPN RW (Road Warrior) -> Utilisation des comptes de l'Active Directory
   Lorsque la connexion VPN est établie, l'accès aux ressources et outils est possible sinon non (Téléphonie, Messagerie...)
7. Mise en œuvre d'une DMZ pour accéder au Serveur WEB E-Brigade (Avec règles de pare-feu adaptés)

Les contraintes sont :

- Finir le projet avant le 25/04/2023
- Le projet doit être à moindre coût
- Une authentification à l'AD préalable sera nécessaire pour l'accès au contenu des données

Solutions retenues et argumentations

La solution retenue pour les besoins n°1,6 et 7 est **pfSense 2.6.0**. C'est un système d'exploitation open source basé sur FreeBSD qui répond parfaitement aux besoins de routage / firewall. Il prend également en charge le protocole OpenVPN, qui sera le protocole utilisé pour ce projet.

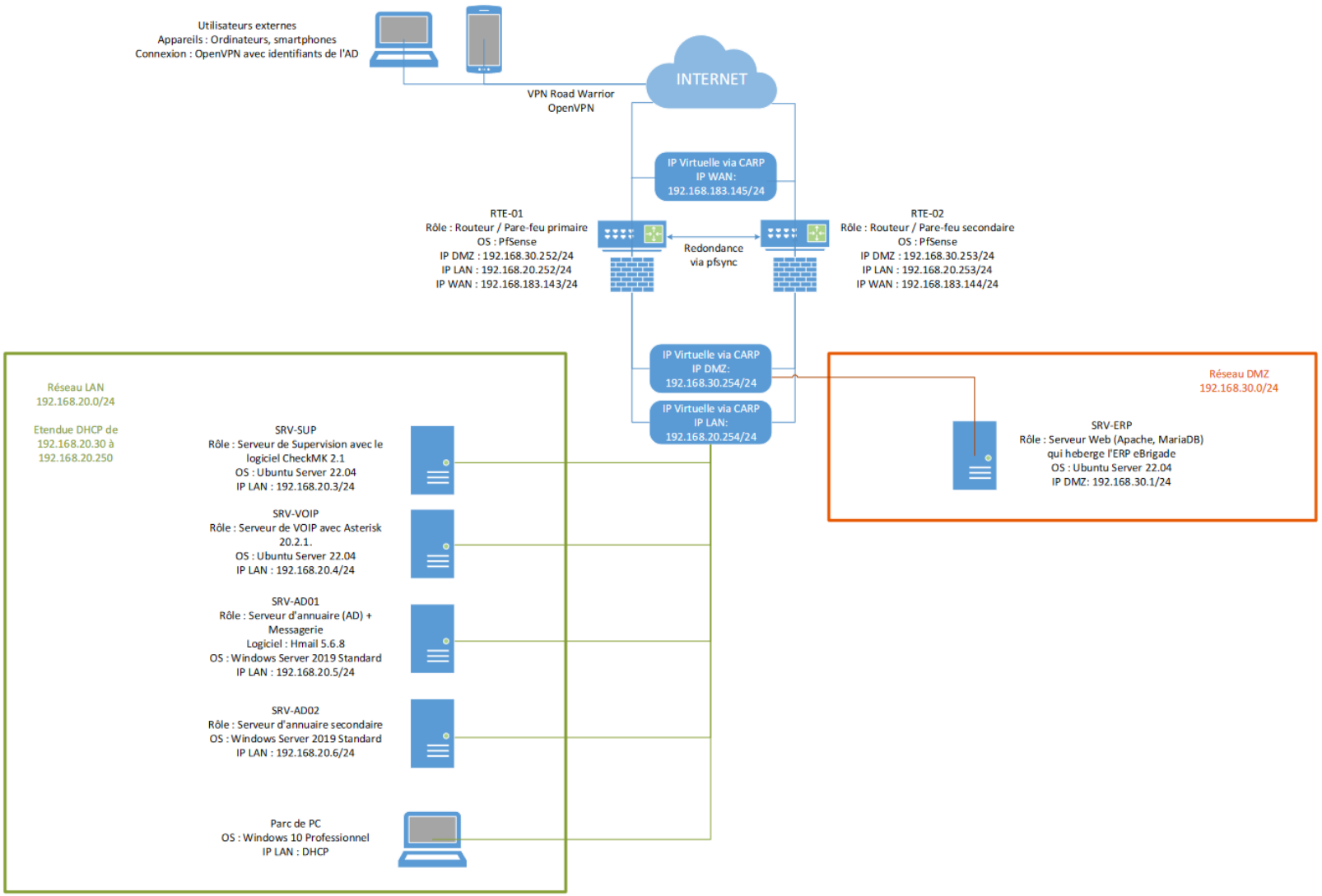
La solution retenue pour le besoin n°2 est 2 **serveurs Windows 2019 Standard**. Ce choix est nécessaire, car un active directory doit être mis en place lors de ce projet. Seul Windows fournit ce service.

La solution retenue pour le besoin n°3 est le logiciel **Asterisk LTS (20.2.1)** sur un serveur Ubuntu Server 22.04.
Ce logiciel possède une grande communauté et donc un accès à de nombreuses ressources.
Il est gratuit, et possède une prise en main facile. Cela est un gain de temps pour les techniciens qui seront en charge de l'exploiter, donc un gain d'argent pour l'organisme.

La solution retenue pour le besoin n°4 est le logiciel **Hmail 5.6.8**, installé sur un des serveurs Windows.
C'est un logiciel gratuit, fonctionnant sous Windows. Comme nous possédons déjà 2 serveurs Windows cela n'entrainera pas de cout supplémentaire.
Il est facile à prendre en main. Cela est un gain de temps pour les techniciens qui seront en charge de l'exploiter, et donc un gain d'argent pour l'organisme.
Il permet l'utilisation des comptes de l'active Directory. Ainsi chaque utilisateur de l'AD pourra se connecter à son client de messagerie grâce à ses identifiants AD.

La solution retenue pour le besoin n°5 est le logiciel **CheckMK 2.1**, installé sur un serveur Ubuntu Server 22.04 pour sa prise en main et son interface faciles, et le fait qu'il possède une version RAW (open source et gratuite).
Ce logiciel permet de superviser de nombreux appareils via un agent à installer (notamment Linux et Windows), ou via le protocole SNMP. Ainsi tous les équipements de notre infrastructure pourront être supervisés.
CheckMK analysent de nombreux services, et les catégorisent en 3 sortes : OK, WARN et CRIT.
CheckMK regarde également la disponibilité en réseau de l'équipement. Et si un équipement n'est plus accessible, sont état est déclaré DOWN et non plus UP.
Ces dernières informations peuvent être envoyés par mail.
Toutefois, CheckMK n'intègre pas de relais SMTP. Il faut installer un service mail et le configurer en tant que serveur relais SMTP qui renvoie tous les mails vers un serveur SMTP, donc notre serveur de messagerie. Cela ne pose pas de soucis quant au choix de cette solution. Nous allons simplement rajouter et configurer la solution Postfix sur notre serveur de supervision pour qu'il réalise cela.

Schéma réseau



Nos 2 routeurs possèdent une liaison WAN différentes. Ainsi l'accès à internet est en haute disponibilité.

Des adresses IP virtuelles sont crées pour les interfaces LAN, WAN et DMZ. Nos 2 routeurs utilisent ces adresses IP virtuelles. Cela est utile pour que les ordinateurs et les serveurs puissent avoir accès de manière transparente aux 2 routeurs, et ainsi utiliser le second en cas de panne du 1er sans. Cela assure la haute disponibilité de l'accès à internet et au VPN.

Nos 2 serveurs Windows fournissent les services d'annuaire (AD), DNS et DHCP de manière redondée.

Avec ces différentes fonctionnalités, notre architecture est hautement disponible et donc la disponibilité est optimale, ce qui répond aux besoins du projet.

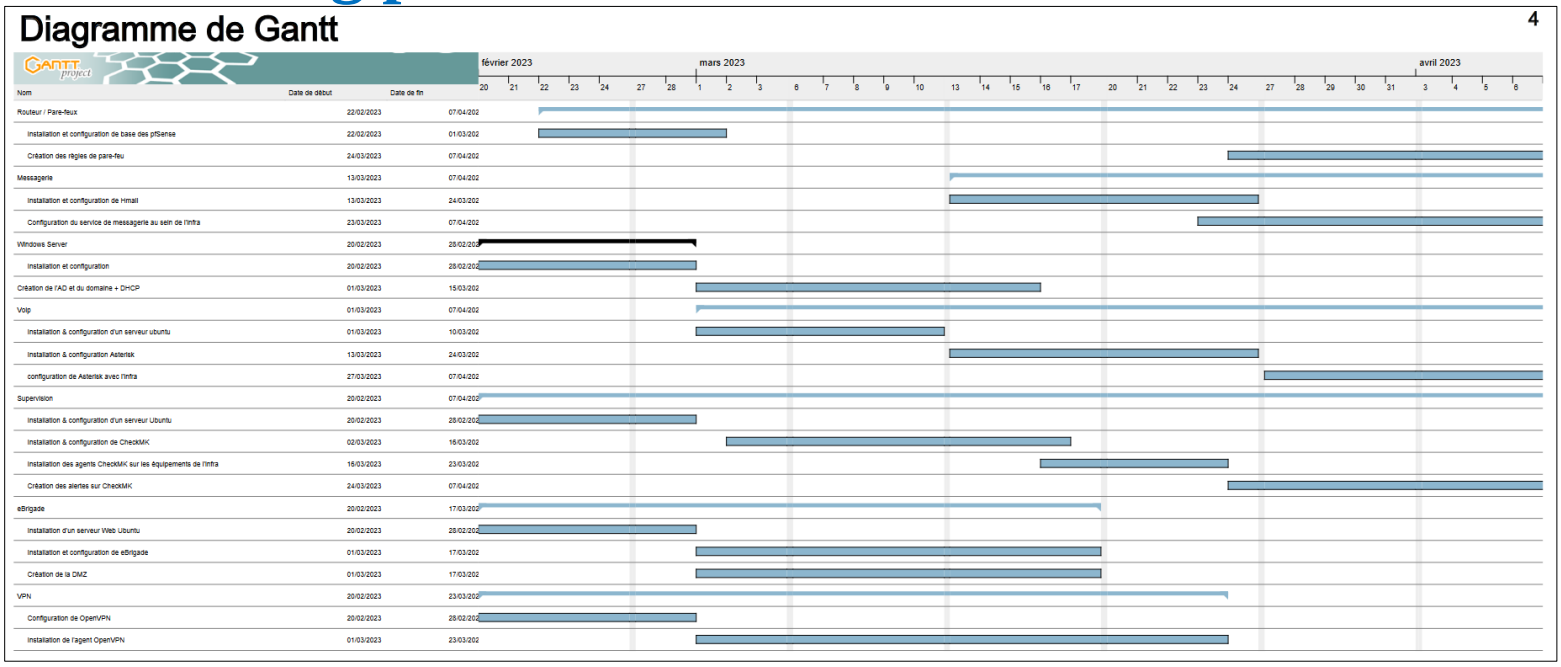
Coût du projet

	Quantité	Prix unité	Prix
Licence Windows Serveur 2019 Standard	2	1946 €	3892 €
CAL Utilisateurs	10	50 €	500 €
Licence OpenVPN pour 10 utilisateurs	1	595 €	595 €
Serveurs de virtualisation : Smart Selection PowerEdge R7515 Rack Server	2	3351,80 €	6703,60 €
Mains d'oeuvre	48h	50 €	2 400 €
Total HT			14 090, 60 €
TVA			2 818,12 €
TOTAL TTC			**16 908,72 €**

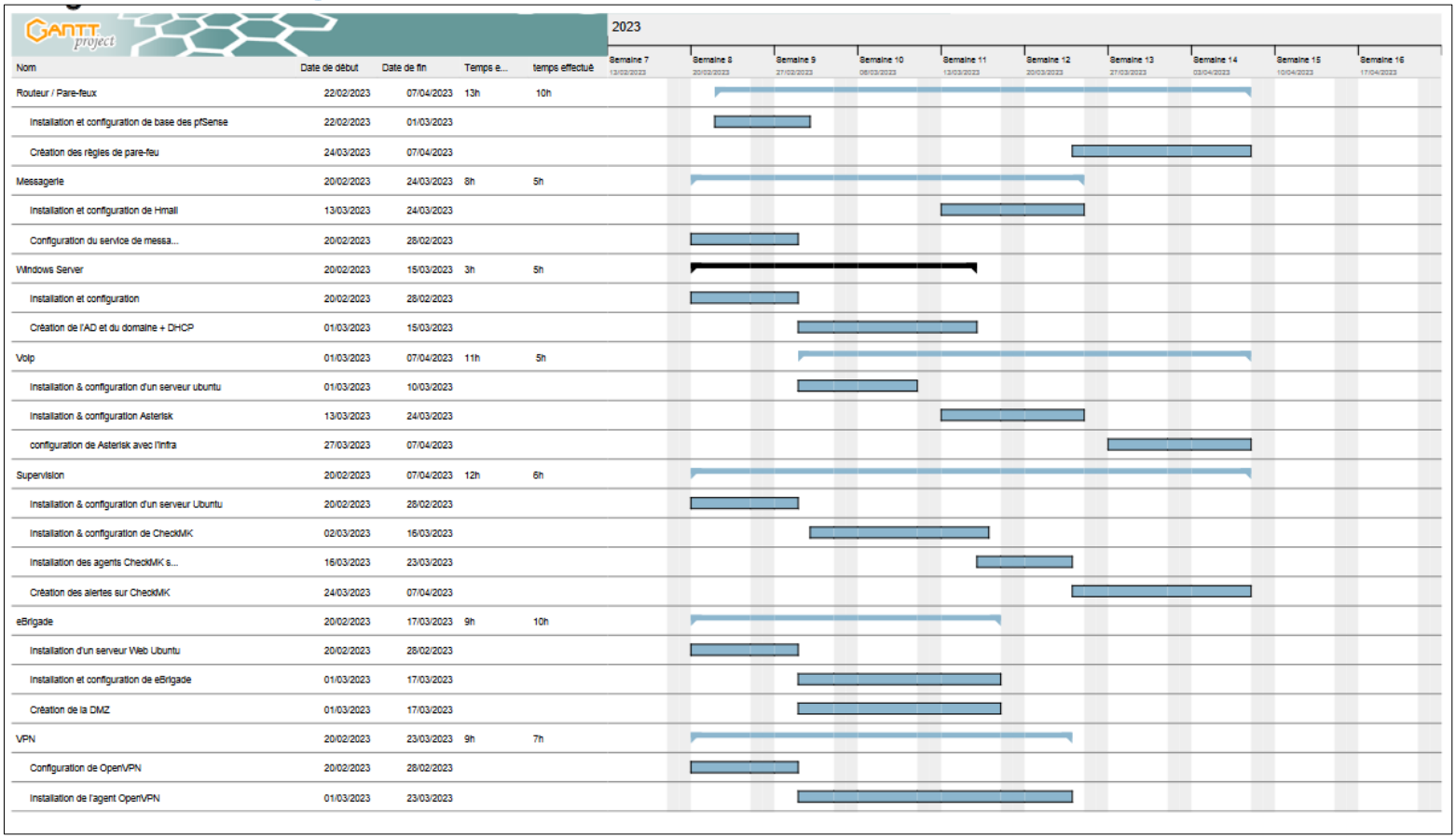
Le projet doit être à moindre coût. Mis à part les solutions imposés (Windows Serveur et OpenVPN), nous avons donc opté pour des solutions gratuites et open sources.

Nos 2 hyperviseurs sont 2 Proxmox VE 7.4 en Cluster.
Les logiciels utilisés sont également des logiciels gratuits (Asterisk, CheckMK, Hmail). Il existe une version payante, qui permet d'avoir plus de fonctionnalités et accès à un meilleur support. Cela n'est pas nécessaire dans notre cas.

Planning prévisionnel



Planning réel



Nom	Date de début	Date de fin	Temps e...	temps effectué
Routeur / Pare-feux	22/02/2023	07/04/2023	13h	10h
Installation et configuration de base des pfSense	22/02/2023	01/03/2023		
Création des règles de pare-feu	24/03/2023	07/04/2023		
Messagerie	20/02/2023	24/03/2023	8h	5h
Installation et configuration de Hmail	13/03/2023	24/03/2023		
Configuration du service de messa...	20/02/2023	28/02/2023		
Windows Server	20/02/2023	15/03/2023	3h	5h
Installation et configuration	20/02/2023	28/02/2023		
Création de l'AD et du domaine + DHCP	01/03/2023	15/03/2023		
Voip	01/03/2023	07/04/2023	11h	5h
Installation & configuration d'un serveur ubuntu	01/03/2023	10/03/2023		
Installation & configuration Asterisk	13/03/2023	24/03/2023		
configuration de Asterisk avec l'infra	27/03/2023	07/04/2023		
Supervision	20/02/2023	07/04/2023	12h	6h
Installation & configuration d'un serveur Ubuntu	20/02/2023	28/02/2023		
Installation & configuration de CheckMK	02/03/2023	16/03/2023		
Installation des agents CheckMK s...	16/03/2023	23/03/2023		
Création des alertes sur CheckMK	24/03/2023	07/04/2023		
eBrigade	20/02/2023	17/03/2023	9h	10h
Installation d'un serveur Web Ubuntu	20/02/2023	28/02/2023		
Installation et configuration de eBrigade	01/03/2023	17/03/2023		
Création de la DMZ	01/03/2023	17/03/2023		
VPN	20/02/2023	23/03/2023	9h	7h
Configuration de OpenVPN	20/02/2023	28/02/2023		
Installation de l'agent OpenVPN	01/03/2023	23/03/2023		

Planning prévisionnel vs réel

Tâches

Nom	Date de début	Date de fin	Temps estimé	temps effectué
Routeur / Pare-feux	22/02/2023	07/04/2023	13h	10h
Installation et configuration de base des pfSense	22/02/2023	01/03/2023		
Création des règles de pare-feu	24/03/2023	07/04/2023		
Messagerie	20/02/2023	24/03/2023	8h	5h
Installation et configuration de Hmail	13/03/2023	24/03/2023		
Configuration du service de messagerie au sein de l'infra	20/02/2023	28/02/2023		
Windows Server	20/02/2023	15/03/2023	3h	5h
Installation et configuration	20/02/2023	28/02/2023		
Création de l'AD et du domaine + DHCP	01/03/2023	15/03/2023		
Voip	01/03/2023	07/04/2023	11h	5h
Installation & configuration d'un serveur ubuntu	01/03/2023	10/03/2023		
Installation & configuration Asterisk	13/03/2023	24/03/2023		
configuration de Asterisk avec l'infra	27/03/2023	07/04/2023		
Supervision	20/02/2023	07/04/2023	12h	6h
Installation & configuration d'un serveur Ubuntu	20/02/2023	28/02/2023		
Installation & configuration de CheckMK	02/03/2023	16/03/2023		
Installation des agents CheckMK sur les équipements de l'infra	16/03/2023	23/03/2023		
Création des alertes sur CheckMK	24/03/2023	07/04/2023		
eBrigade	20/02/2023	17/03/2023	9h	10h
Installation d'un serveur Web Ubuntu	20/02/2023	28/02/2023		
Installation et configuration de eBrigade	01/03/2023	17/03/2023		
Création de la DMZ	01/03/2023	17/03/2023		
VPN	20/02/2023	23/03/2023	9h	7h

Total heures estimées : 65h
Total heures effectuées : 48h

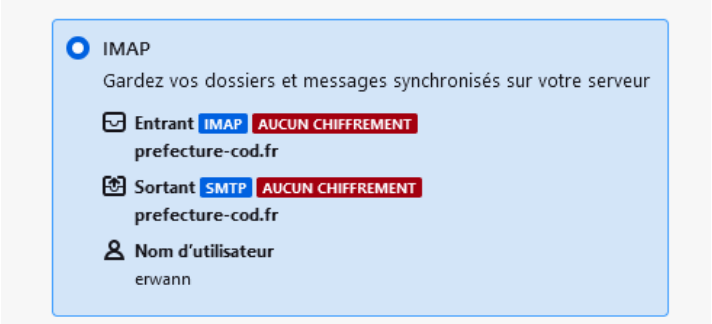
On remarque que la charge de travail a été surestimé de 17h. Cela s'explique surtout pour les lots VOIP et SUPERVISION, qui ont pris 6h de moins que prévu. La prise en main de ces logiciels a été plus rapide que prévu.

Conclusion

Le projet a été mené à bien. La charge de travail a été surestimé de 17h. Le budget et les délais ont été respectés.
Le projet répond à tous les besoins du client.

Améliorations possibles

Une amélioration possible est de sécuriser le flux de messagerie et de VOIP.
Concernant la messagerie, on pourrait chiffrer les flux entrants et sortants, qui ne sont pas chiffrés actuellement :



Concernant la VOIP, on pourrait utiliser le protocole SIP via e port 5061 et non plus via le 5060. Le port 5061 est sa version sécurisée (SIP-TLS).

Afin d'accroitre la sécurité de l'architecture, on pourrait ajouter un IDS/IPS dans l'infrastructure. Cela peut être intéressant car notre firewall pfSense analyse seulement les entêtes des trames. Le contenu des paquets n'est pas analysé, et un hacker pourrait « camoufler » son attaque. L'IDS / IPS analysent les comportements suspects, et permet donc de compléter la sécurité du pare-feu.