

PROJET KGAMBIT

**Sécurisation et supervision d'un système
d'information hautement disponible**

SIO 2023 – Option SISR



Épreuve 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 : RAKOTOZAFY Winness		N° candidat : 02243995935
Épreuve ponctuelle <input type="checkbox"/>	Contrôle en cours de formation <input checked="" type="checkbox"/>	Date : 26 / 04 / 2023
Organisation support de la réalisation professionnelle Cette situation professionnelle consiste à mettre en place une infrastructure composée d'une zone LAN pour les serveurs locaux permettant de faire fonctionner le SI et répondre aux besoins, et d'une zone DMZ pour héberger un serveur web qui sera accessible depuis Internet. Compte tenu du fait que le SI comprend des utilisateurs nomades, ce projet intègre l'implémentation d'un VPN RoadWarrior pour un accès distant sécurisé des ressources internes de l'entreprise.		
Intitulé de la réalisation professionnelle Projet KGAMBIT		
Période de réalisation : 06/01/2023 au 25/04/2023 Lieu : Strasbourg Modalité : <input type="checkbox"/> Seul(e) <input checked="" type="checkbox"/> En équipe		
Compétences travaillées <input checked="" type="checkbox"/> Concevoir une solution d'infrastructure réseau <input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau <input checked="" type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau		
Conditions de réalisation¹ (ressources fournies, résultats attendus) - Des pare-feux en très haute disponibilité avec redondance d'accès Internet - Un serveur d'annuaire secondaire redondé au serveur d'annuaire existant, avec redondance DNS et DHCP - Un serveur de messagerie avec authentification centralisé - Une solution de téléphonie IP - Un serveur web isolé du réseau interne mais accessible depuis Internet et réseau local qui héberge l'application de secours - Une solution de supervision pour superviser tout le parc informatique - Un accès distant sécurisé pour les utilisateurs itinérants		
Description des ressources documentaires, matérielles et logicielles utilisées² - 2 pare-feux sous pfSense FreeBSD - 2 serveurs AD, DNS, DHCP et RADIUS sous Windows Server 2019 - 1 serveur e-brigade avec LAMP (Linux Debian 11, Apache, MariaDB, Php) - 1 serveur IPBX sous Asterisk (Linux Debian 11) - 1 serveur de supervision avec Zabbix (Linux Debian 11) - 1 serveur de messagerie avec Postfix/Dovecot (Linux Debian 11) - 1 serveur VPN RoadWarrior avec OpenVPN sous pfSense FreeBSD		
Modalités d'accès aux productions³ et à leur documentation⁴ Les documentations de présentations et technique du projet sont accessibles depuis la section E4-E5 de mon portfolio via le lien suivant : https://www.winness-rakotozafy.fr		

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

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
(verso, éventuellement pages suivantes)**

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

Table des matières

Contexte	4
Besoins et objectifs	4
Solutions retenues et argumentations	5
Redondance WAN et Internet : pfSense CARP, pfSync, XML-RPC	5
Serveur d'annuaire redondés : Microsoft Active Directory	5
Serveur IPBX : Asterisk	6
Client sofphone : Linphone	6
Serveur de messagerie : Postfix & Dovecot	7
Serveur de supervision : ZABBIX	8
Serveur VPN RoadWarrior : OpenVPN	8
Application e-brigade : Serveur LAMP	9
Tableau de synthèse des solutions	10
Schéma réseau	12
Tableau d'adressage complet	13
Tableau des flux	13
Coût du projet	15
Planning prévisionnel	16
Planning réel	16
Planning prévisionnel vs réel	16
Conclusion	17
Améliorations possibles	18
Chiffrements de communication sur tous les flux type SSL/TLS	18
Accès webmail à la messagerie	18
Serveur de centralisation de logs	18
Solution de sauvegarde	18

Contexte

La sécurité des systèmes d'information est actuellement un sujet à ne pas prendre à la légère depuis l'émergence des nouvelles technologies, et l'intégration du numérique dans le mode de fonctionnement des entreprises.

L'entreprise KGAMBIT, soucieux de la sécurité de son SI, souhaite mettre en place des dispositifs de sécurité afin de séparer ses ressources accessibles depuis le réseau extérieur et son réseau interne.

Aussi, elle souhaite rendre hautement disponible l'accès Internet de ses utilisateurs pour pouvoir collaborer de manière continue avec ses collaborateurs. Par suite de la popularisation du télétravail, la mise en place d'un accès distant sécurisé des utilisateurs nomades sera également implémentée.

Pour s'assurer du maintien des opérations, un système de monitoring sera mis en place pour surveiller l'état du réseau et des équipements de tout le système d'information de KGAMBIT.

Besoins et objectifs

Les **besoins du projet** exprimés par suite de l'étude du cahier des charges sont :

- Redondance des routeurs et liens WAN (2 routeurs, 2 accès Internet, pour la simulation 1 seul accès Internet est autorisé)
- Accès aux ressources du serveur e-Brigade en LAN et DMZ
- Messagerie électronique fonctionnelle uniquement en LAN/VPN RoadWarrior
- Serveur VoIP et logiciels de téléphonie IP uniquement en LAN/VPN RoadWarrior
- Les postes de travail sur Windows 10 Pro x64
- Mise en place d'un annuaire Active Directory couplé à l'annuaire existant
- Connexion distante chiffrée et sécurisé avec authentification unique

Ainsi, pour répondre aux besoins exprimés, les **objectifs du projet** sont :

- Proposition de solutions techniques et logicielles à moindre coût ;
- Mise en œuvre d'une haute disponibilité des routeurs et liaison Internet redondée ;
- Mise en œuvre de deux serveurs Active Directory redondés ;
- Mise en œuvre d'un serveur de téléphonie IPBX et déploiement du client softphone
- Mise en œuvre d'un serveur de messagerie et déploiement client de messagerie accessible par les comptes Active Directory
- Mise en œuvre d'un serveur de supervision
- Mise en œuvre d'une solution de VPN RoadWarrior : authentification comptes Active Directory
- Mise en œuvre d'une DMZ pour l'hébergement du serveur web E-Brigade
- Mise en place des politiques de pare-feu spécifiques et sécurisées en suivant les recommandations de l'ANSSI

Solutions retenues et argumentations

Dans l'élaboration de ce projet, afin de satisfaire les besoins exprimés par l'entreprise, et atteindre les objectifs fixés du projet, ci-dessous les **solutions retenues** avec leurs avantages et inconvénients.

Redondance WAN et Internet : pfSense CARP, pfSync, XML-RPC

Comme solution de routeur et pare-feu au sein du réseau, nous recommandons l'utilisation de **PfSense**, qui intègre plusieurs fonctionnalités afin de répondre à vos besoins. En effet, le recours à cette solution vous permettra non seulement de sécuriser votre réseau interne, mais aussi de minimiser les coûts car c'est une solution **gratuite et open source**.



PfSense est basé sur le système d'exploitation FreeBSD, basé sous Unix. Il utilise le pare-feu à états, qui garde en mémoire l'état de connexions réseau, comme les flux TCP, ou les communications UDP qui le traversent.

Aussi, cette solution intègre des fonctionnalités permettant de mettre en place la solution de redondance au niveau des pare-feux, et des liaisons WAN. Les principales fonctionnalités pour répondre à ces besoins sont :

- **CARP**, pour Common Address Redundancy Protocol, est un protocole réseau pour mettre en place de la tolérance aux pannes et la redondance au niveau des interfaces physiques des pare-feux. La redondance est réalisée par le fait que les équipements du segment réseau partageront un **IP virtuel**. Ainsi, si l'un des pare-feux tombe, le second pare-feu du cluster prendra le relais, et cela, avec la même IP virtuelle.
- **PfSync**, est le protocole qui permettra de **synchroniser** entre deux pare-feux pfSense, l'**état des connexions en cours**, notamment utile pour le partage des règles de pare-feu. De ce fait donc, à défaut du pare-feu primaire, l'état des liens de connexion sur le réseau restent opérationnel, et aucune coupure du réseau est apparente lors du basculement.
- **XML-RPC**, protocole qui permettra la réplication de données, notamment les configurations des pare-feux entre eux. Il est recommandé que ce protocole utilise la même interface que celle utilisée par le protocole pfSync.

Serveur d'annuaire redondés : Microsoft Active Directory

Tout d'abord, comme serveur d'annuaire, nous recommandons la solution Active Directory de Microsoft.

Windows Server dispose de tout ce qu'il faut pour créer un serveur d'annuaire d'authentification. Permettant de créer, modifier, supprimer et gérer en profondeur des ordinateurs comme des utilisateurs, il offre la possibilité d'administration la plus optimale. Son interface n'est pas en ligne de commande, tout se fait comme sur une interface de bureau Windows ce qui est un bon avantage. De plus, le serveur d'annuaire d'authentification peut être redondé avec un autre Active Directory distant pour permettre plus de sécurité et également plus de flexibilité s'il se trouve sur un autre site.



De ce fait il est donc optimisé pour permettre d'y ajouter d'autres fonctionnalités qui permettront la polyvalence du système pour les utilisateurs en y ajoutant d'autres fonctionnalités dans le futur par exemple si une évolution future, devait s'effectuer dans la poursuite des activités ou de l'agrandissement de l'infrastructure de KGambit.

Ainsi, nous avons déjà travaillé à plusieurs reprises sur cette fonctionnalité majeure. Nous maîtrisons déjà une bonne partie de l'installation et de la configuration jusqu'à la mise en place réalisé dans d'autres projets. De ce point de vue, nous évaluons Windows Server comme solution envisagée afin de réaliser ce projet.

Serveur IPBX : Asterisk

Asterisk est un **autocommutateur téléphonique privé** ou PABX (*Private Automatic Branch Exchange*) sous licence libre GPLv2 (*General Public License*) pour **les systèmes Unix** (Linux, macOS, ...).



Il permet, entre autres, **la messagerie vocale, les files d'attente, les agents d'appels, les musiques d'attente des appels**, la distribution des appels, il existe également d'autres modules pouvant être ajoutés pour les conférences par exemple.

Pour information, il utilise les protocoles **H.320/323** (*permettant la communication de la voix et image par IP*), le protocole **SIP** (*Session Initiation Protocol*), **MCGRP** (*Media Gateway Control Protocol*) et d'autres standards de communication (**IAX, IAX2, SCCP**).

Le choix de serveur IPBX s'est porté sur Asterisk du fait que cette solution :

- Offre un nombre très élevé de fonctions permettant l'intégration complète pour répondre à la majorité des besoins en téléphonie.
- Solution **gratuite et open-source**, donc ouvert au grand public et accessible aux entreprises de toutes tailles ou pour des besoins à domicile, générant ainsi le moins de coût possible en gestion de budget pour le déploiement.
- Solution logicielle qui peut être installé sur des distributions Linux sans l'accordement à un matériel spécifique.
- **Peu gourmand** en ressources : 512MB RAM, processeur de 700mhz, 10 Gb stockage
- Solution **flexible et personnalisable** par sa nature open-source et ses modules facilement modifiable sur GNU/Linux, et compatible avec plusieurs modèles de téléphonie IP.
- Supporte le chiffrement TLS des protocoles de téléphonie comme **SIPS** et **SRTP**.

Client sofphone : Linphone

Linphone est un logiciel de téléphonie par Internet ou par VoIP (Voice over IP) et de messagerie instantanée. Principalement conçu pour Linux, il s'agit d'un logiciel libre au téléchargement et à l'utilisation. Le code source est distribué sous double licence : avec une licence GNU GPL v3 pour une utilisation open source, ou sous licence propriétaire pour les entités désirant garder fermées les sources de leur produit dérivé de Linphone, pour la protection.



Nous vous recommandons Linphone car il possède dans son fonctionnement des algorithmes d'adaptation de qualité en fonction du réseau, et des mécanismes de correction de transmission lors des appels. Une authentification sécurisée des utilisateurs, établissement sécurisé des appels avec SIP/TLS et un Chiffrement de bout-en-bout des appels audio/vidéo et des conversations texte.

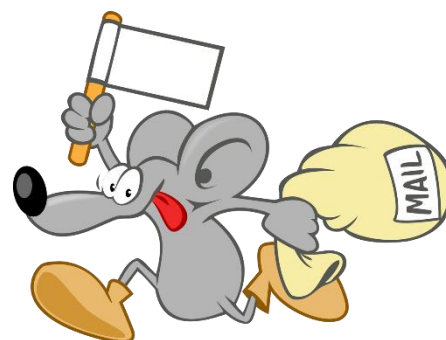
Cette solution nous semble donc la plus adaptée pour ce qu'il nous faut mettre en place dans ce projet. De plus, c'est un logiciel libre donc gratuit d'utilisation, compatible sur IOS ou Android ou même tablettes, elle peut aussi s'utiliser sur tous les systèmes d'exploitation d'un ordinateur. Un vrai plus si une évolution devait s'effectuer dans la poursuite des activités ou de l'agrandissement de l'infrastructure téléphonique de KGambit.

Serveur de messagerie : Postfix & Dovecot

Pour la solution de serveur de messagerie, nous avons choisi de mettre en place Postfix pour agent MTA (Mail Transfert Agent) et Dovecot comme MDA (Mail Delivery Agent), tous deux hébergés sur le même serveur. Ces solutions ont l'avantage d'être à la fois **open-source et gratuit**.

Postfix est un serveur de messagerie utilisé pour acheminer les courriels à partir d'un serveur vers leur destination finale (rôle MTA). Il est connu pour sa **fiabilité, sa performance et sa sécurité**, faisant donc une option populaire pour les entreprises et les organisations de toutes tailles.

La **sécurité** de Postfix se situe sur les fonctionnalités d'authentification SMTP, la détection et prévention de spams. La **flexibilité**, car il offre diverses options de personnalisation selon les besoins techniques en messagerie (messagerie Internet, messagerie internet, environnement groupes de travail...). Et enfin, sa **performance**, car il est connu pour être rapide et efficace, même en cas de charge importante.



Postfix s'installe sur les distributions Unix uniquement, et constitue donc l'un de ses inconvénients pour les administrateurs débutants. En effet, Postfix, étant une solution performante et appréciée, a une **configuration complexe**, et donc difficile à configurer notamment sur des environnements de messagerie complexes. En termes de **documentation**, elle peut parfois être limitée et difficile à assimiler pour les débutants.



Aussi, Postfix seul ne permet pas de mettre en place une solution de messagerie opérationnel au sein d'un parc informatique, et agit uniquement en tant que relais **SMTP**. Ainsi, pour pallier ce problème, il coexiste avec une autre solution **open source et gratuit** : Dovecot.

Dovecot est un serveur IMAP et POP3 qui permet de rendre le serveur hébergeant Postfix d'être un serveur de messagerie complète. Dovecot se chargera de délivrer les courriers sur les clients de messagerie des utilisateurs. De plus d'être gratuit, l'un des avantages de Dovecot est qu'il est **stable et fiable**, et compatible avec une couche de sécurité SSL/TLS afin d'effectuer les échanges de courriels avec les protocoles IMAPS ou POP3S.

En outre, Dovecot permet également d'effectuer la liaison du serveur de messagerie avec les comptes Active Directory des utilisateurs, et nous permettra donc de rentrer dans un principe de **Single Sign On** au niveau de l'authentification sur les comptes de messagerie des utilisateurs. Et comme les identifiants AD sont nominatifs et confidentielle par utilisateur, la solution de serveur de messagerie respectera donc la **conformité au RGPD**.

Serveur de supervision : ZABBIX

Comme l'infrastructure informatique à mettre en place dispose de plusieurs éléments : serveur web, serveur d'annuaire, messagerie, téléphonie, etc... Afin de s'assurer du bon fonctionnement de la **production de chaque service**, il nous est nécessaire de mettre en place une **solution de supervision**, et à la demande du client, une solution à coût minimale.

Sur le marché, nous disposons d'une large gamme de choix comme Nagios, Centreon, Zabbix, Eyes of Network, CheckMK, LibreNMS, etc ... mais notre recommandation, parmi toutes ces solutions, se porte sur **Zabbix**.

En effet, parmi les solutions gratuites et open-source, nous considérons que Zabbix fait partie des solutions les plus simples à mettre en place, ce qui conviendra donc à la réalisation du projet pour le **respect de la Qualité-Coût-Délai**.



Dans le cadre technique, Zabbix propose une solution de supervision technique et applicative, décomposée en 3 composants :

- Un serveur reposant sur un **moteur de base de données**
- Une interface d'administration écrite en PHP permettant la visualisation des informations stockées en base, et la configuration des objets de supervision
- Un serveur de **traitement avec plusieurs méthodes de supervision**.

Cette solution se démarque en particulier par son **interface**, qui est **plus interactif et user-friendly**, et s'ouvre donc à un large public. De ce fait, cela faciliterait le transfert de compétence à l'équipe technique, et l'administration de la supervision du parc.

Cependant, cette solution nécessite l'installation d'un agent Zabbix sur les machines à superviser pour le bon fonctionnement de la supervision. Cet agent est disponible sur toutes les plateformes (Windows, Mac, Linux, FreeBSD...)

Serveur VPN RoadWarrior : OpenVPN

Pour la connexion à distance sécurisé, il nous est demandé de mettre en place une connexion VPN RoadWarrior pour les accès des ressources internes de l'organisation depuis le réseau externe. Une connexion VPN RoadWarrior est une connexion VPN distant, c'est-à-dire client to site où les utilisateurs, depuis Internet, peuvent accéder aux ressources du réseau LAN de la Sécurité Civile de manière sécurisée et chiffrée.

De manière générale, une authentification est requise afin de pouvoir valider la connexion VPN sur le serveur VPN en place. Ce type de connexion est donc une connexion Client-Serveur, nécessitant des protocoles de transport chiffré comme le SSL/TLS pour Secure Socket Layer/Transport Layer Security. La solution recommandée pour cette connexion est **OpenVPN**, qui est une solution intégrée à notre pare-feu pfSense.

**OPENVPN®**

OpenVPN est une solution **open-source et gratuit** de **VPN client-to-site** qui peut nous offrir une sécurité renforcée grâce à des protocoles de chiffrement robustes et

authentification forte. Il est multiplateforme, et donc compatible aux divers systèmes d'exploitation comme Windows, Linux, Mac, Android, iOS. Aussi, il est à savoir qu'OpenVPN est un **protocole VPN de niveau 4**, qui intervient surtout

sur la couche Transport du modèle pour sécuriser les communications.

De plus, les méthodes de communications d'OpenVPN s'effectuent par certificats qui utilisent des algorithmes de chiffrement sécurisé comme l'**AES-256**, et donc parmi les raisons de ce choix est qu'une OpenVPN est difficile à compromettre.

Application e-brigade : Serveur LAMP

Nous avons choisi comme solution pour le serveur WEB, l'ensemble de la pile **LAMP** afin d'installer le logiciel **e-brigade**. En effet, avant d'expliquer le choix et pourquoi nous l'utiliserons, définissons et voyons ce qu'offre LAMP.

LAMP est l'acronyme de différents éléments :

- Le **L** de « **Linux** » pour le système d'exploitation
- Le **A** de « **Apache** » pour le serveur Web
- Le **M** pour « **MySQL** ou pour **MariaDB** » pour le serveur de base de données
- Le **P** pour « **PHP** » ou bien « Python » qui nous parle des scripts.



Mis à part les acronymes, Il s'agit en fin de compte d'un ensemble de logiciels libres de droits pouvant **permettre la création des serveurs de sites web**. De plus, LAMP est connu comme un « tout » qui n'est pas forcément coordonné étant des logiciels libres et créés par des individus dans le monde, mais plutôt comme **le faible coût de l'ensemble de la présence de tous ces composants dans la plupart des distributions GNU/Linux**.

Nous l'avons choisi car il s'agit d'une solution que nous connaissons. Nous avons déjà travaillé sur ce matériel et à la configuration de celui-ci. Dans l'optique de mettre en place un serveur web pour le besoin de ce projet, il est pour nous une **solution abordable, à moindre coût, simple d'utilisation, rapidement disponible** et nous permettant de pouvoir réaliser une autre étape ; la mise en place du E-Brigade. En résumé, nous allons pouvoir **créer et héberger efficacement un/des site(s) Web(s) dynamique(s) si une évolution** devait s'effectuer dans la poursuite des activités ou de l'agrandissement de l'infrastructure de KGambit.

Pour synthétiser les solutions retenues pour la réalisation du projet, ci-dessous un tableau de synthèse reprenant les solutions ainsi que leurs avantages et inconvénients :

Tableau de synthèse des solutions

SOLUTIONS RETENUES		
<p><u>Redondance WAN</u></p> 	<ul style="list-style-type: none"> ▪ Gratuit et open-source ▪ Intègre VPN RoadWarrior ▪ Intègre des fonctionnalités de redondance demandées ▪ Peu gourmand en ressources matérielles ▪ Solution maîtrisée par l'équipe 	<ul style="list-style-type: none"> ▪ Langue du clavier en ENG par défaut sur le CLI ▪ Pas de mise à jour régulier en comparaison de son concurrent
<p><u>Serveur d'annuaire</u></p>  <p>Active Directory</p>	<ul style="list-style-type: none"> ▪ Facilité d'administration ▪ Administration simplifiée et centralisée des actifs de l'infrastructure ▪ Administration en interface graphique 	<ul style="list-style-type: none"> ▪ Nécessite une licence Windows Server ▪ Fonctionne uniquement avec Windows ▪ Gourmand en ressources matérielles
<p><u>Serveur IPBX</u></p> 	<ul style="list-style-type: none"> ▪ Open source et gratuit ▪ Multiplateforme ▪ Gratuite ▪ Simple d'utilisation ▪ Peu gourmand en ressources matérielles ▪ Installation simple ▪ Flexible et personnalisable ▪ Supporte le chiffrement TLS de téléphonie comme SIPS et SRTP ▪ Interface graphique possible avec l'intégration de FreePBX 	<ul style="list-style-type: none"> ▪ Apprendre/connaitre le plan de numérotation ▪ Peut paraître difficile pour des initiés aux systèmes Unix ▪ Peut présenter des risques de sécurité ▪ Dispose d'un support limité
<p><u>Client softphone</u></p> 	<ul style="list-style-type: none"> ▪ Algorithmes d'adaptation de qualité en fonction du réseau ▪ Mécanismes de correction de transmission lors des appels. ▪ Une authentification sécurisée des utilisateurs 	<ul style="list-style-type: none"> ▪ Interface utilisateur complexe ▪ Dépend beaucoup de la qualité de la bande passante ▪ Difficulté à configurer pour un nouvel utilisateur

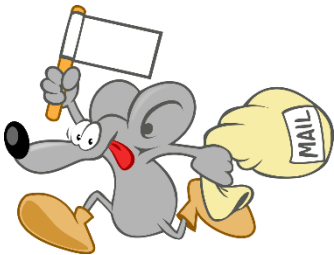




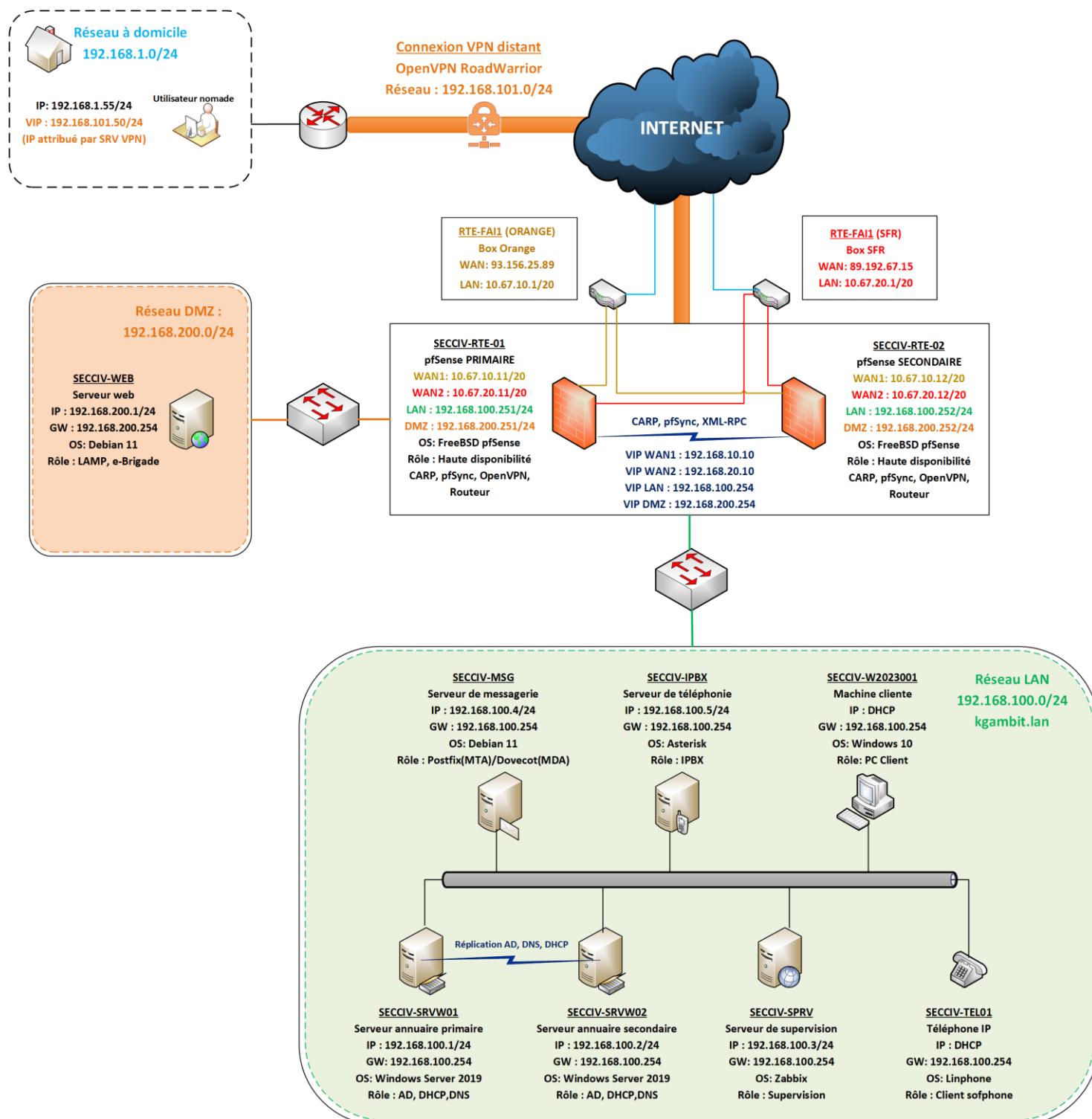
<p><u>Serveur de messagerie</u></p>  	<ul style="list-style-type: none"> ▪ Open-source et gratuit ▪ Flexible et personnalisable dans son mode de fonctionnement ▪ Compatible avec les protocoles de sécurité SSL/TLS ▪ Compatible avec tous les protocoles de messagerie ▪ Compatible avec l'utilisation des identifiants AD ▪ Très performant même sur un environnement de grande taille ; ▪ Faible consommation de ressources matérielles ; ▪ Possibilité d'appairer à un webmail type Squirrel ▪ Compte de messagerie créé automatiquement 	<ul style="list-style-type: none"> ▪ Uniquement disponible sous système Unix ▪ Configuration complexe à comprendre ▪ Administration majoritairement en CLI
<p><u>Serveur de supervision</u></p> 	<ul style="list-style-type: none"> ▪ Open source et gratuit ▪ Interface web ▪ Multiplateforme ▪ Evolutivité et flexibilité ▪ Plusieurs méthodes de supervision 	<ul style="list-style-type: none"> ▪ Moins de documentation en français ▪ Gourmand en ressources matérielles en cas d'un large parc informatique ▪ Configuration complexe au déploiement
<p><u>VPN RoadWarrior</u></p> 	<ul style="list-style-type: none"> ▪ Gratuit et open-source ▪ Chiffrement SSL/TLS ▪ Rapide et sécurisé ▪ Divers mécanismes de chiffrement de flux 	<ul style="list-style-type: none"> ▪ Nécessite une installation de client VPN (OpenVPN Connect)
<p><u>Application e-brigade</u></p> 	<ul style="list-style-type: none"> ▪ Open source et gratuit ▪ Simple d'utilisation ▪ Flexible et personnalisable ▪ Meilleure pour les performances et la sécurité 	<ul style="list-style-type: none"> ▪ Pas de prise en compte d'autres OS ▪ Problèmes de performances (si beaucoup de données)

Schéma réseau



Pour compléter le schéma réseau, ci-dessous le tableau d'adressage complet :

Tableau d'adressage complet

Plan d'adressage et définitions des rôles - Sécurité Civile						
Secteur	Nom	Rôle	Adresse IP	Masque	Passerelle	Adresse WAN
Pare-feu	SECCIV-RTE-01	Routeur et pare-feu pfsense PRIMAIRE (High sync. CARP, pfsync, OpenVPN, XML-RPC)	192.168.100.251	255.255.255.0		WAN1 10.67.10.11/20 WAN2 10.67.20.11/20
Pare-feu	SECCIV-RTE-02	Routeur et pare-feu pfsense SECONDAIRE (High sync. CARP, pfsync, OpenVPN, XML-RPC)	192.168.100.252	255.255.255.0		WAN1 10.67.10.12/20 WAN2 10.67.20.22/20
DMZ	SECCIV-WEB	Serveur Web dans la DMZ (LAMP, e-brigade)	192.168.200.1	255.255.255.0	192.168.200.254	x
LAN	SECCIV-SRVW01	Windows Server PRIMAIRE (AD DS, DNS, DHCP)	192.168.100.1	255.255.255.0	192.168.100.254	x
LAN	SECCIV-SRVW02	Windows Server SECONDAIRE (AD DS secondaire , DNS secondaire, DHCP de basculement)	192.168.100.2	255.255.255.0	192.168.100.254	x
LAN	SECCIV-SPRV	Serveur de Supervision	192.168.100.3	255.255.255.0	192.168.100.254	x
LAN	SECCIV-MSG	Serveur de messagerie (Postfix(MTA)/Dovecot(MDA)	192.168.100.4	255.255.255.0	192.168.100.254	x
LAN	SECCIV-IPBX	Serveur de téléphonie (Asterisk avec IPBX)	192.168.100.5	255.255.255.0	192.168.100.254	x
WAN	RTE-FAI1	Box orange	10.67.10.1	255.255.240.0		WAN1 93.156.25.89
WAN	RTE-FAI2	Box SFR	10.67.20.1	255.255.240.0		WAN1 89.192.67.15
LAN	SECCIV-W202300x	Ordinateur du client	192.168.100.50	255.255.255.0	192.168.100.254	
		Début du bail		Fin du bail		
Bail sur le réseau LAN		192.168.100.50		192.168.100.200		
Bail sur OpenVPN		192.168.101.50		192.168.101.52		
Adresse IP de la DMZ						
RTE-01		192.168.200.251/24				
RTE-02		192.168.200.252/24				
Adresse VIP						
VIP WAN1		192.168.10.10/28				
VIP WAN2		192.168.20.10/28				
VIP LAN		192.168.100.251/24				
VIP DMZ		192.168.200.254/24				

Afin de sécuriser l'infrastructure de KGambit, des règles de pare-feu sont à mettre en place. Ainsi pour faciliter la mise en place des règles de pare-feu, un schéma des flux a été réalisé.

Tableau des flux

Source	Destination	Protocole	Service	Action	Log	Description
Règles des flux d'administration du pare-feu						
Sous-réseau admin	Interface d'administration	TCP	https/443 ssh/22	Autoriser	Oui	Administrateur → Interface web et SSH
Serveur de supervision	Interface d'administration	UDP	get-snmp/161	Autoriser	Oui	Supervision → Pare-feu
Règle des flux émis par le pare-feu						
Interface d'administration	Serveur supervision	UDP	trap-snmp/162	Autoriser	Oui	Pare-feu → Supervision
Cluster pare-feu	Interface d'administration	TCP	https/443	Autoriser	Oui	Synchronisation XML-RPC
Cluster pare-feu	Cluster Active Directory	TCP/UDP	ldap/389 ldaps/636 dns/53 kerberos/88,464	Autoriser	Oui	Flux authentification AD depuis pare-feu
Cluster pare-feu	Interface d'administration	PFSYNC	--	Autoriser	Oui	Synchronisation pfSync
Toutes	Interface VIP WAN	TCP	OpenVPN/1194	Autoriser	Oui	Autoriser flux OpenVPN

Règle de protection du pare-feu						
Toutes	Interface d'administration	Tous	Tous	Interdire	Oui	Bloquer tous les autres accès à la passerelle
Règle de flux dans la DMZ						
Réseau LAN	Serveur web	TCP/UDP	https/443 dns/53 get-snmp/161	Autoriser	Oui	Accès et supervision du serveur web
Serveur web	Serveur supervision	UDP	trap-snmp/162	Autoriser	Oui	Serveur web → Supervision
Réseau WAN	Serveur web	TCP/UDP	https/443 dns/53	Autoriser	Oui	Accès au serveur web
Réseau DMZ	Réseau WAN	Tous	Tous	Autoriser	Oui	Autoriser flux DMZ → WAN
Réseau DMZ	Réseau LAN	Tous	Tous	Interdire	Oui	Règle protection du réseau LAN
Règle d'accès au service						
Réseau LAN	Toutes	TCP/UDP	https/443 dns/53	Autoriser	Oui	Accès Internet
Réseau LAN	Cluster Active Directory	TCP/UDP	ldap/389 ldaps/636 dns/53 dhcp/67,68 smb/445 rpc/135 kerberos/88,464 rdp/3389 catalog/3268,3269 netbios/137,138,139	Autoriser	Oui	Accès service Active Directory
Réseau LAN	Serveur de messagerie	TCP	smtp/25,587 smtps/465 imap/143 imaps/993	Autoriser	Oui	Accès messagerie
Sous-réseaux utilisateurs	Server IPBX	UDP	sip/5060 rtp/20000-22000	Autoriser	Oui	Flux VoIP
Serveur supervision	Réseau LAN	UDP	get-snmp/161 zabbix/10050	Autoriser	Oui	Supervision des éléments sur LAN
Réseau LAN	Serveur supervision	UDP	trap-snmp/162 zabbix/10051	Autoriser	Oui	Réponse vers supervision
Règle de flux d'accès distant						
Sous réseau VPN	Cluster Active Directory	TCP/UDP	ldap/389 ldaps/636 dns/53 smb/445 rpc/135 kerberos/88,464 rdp/3389 catalog/3268,3269 netbios/137,138,139	Autoriser	Oui	Accès ressources AD des utilisateurs nomades
Sous réseau VPN	Serveur de messagerie	TCP	smtp/25,587 smtps/465 pop3/143 pop3s/993	Autoriser	Oui	Accès messagerie des utilisateurs nomades
Sous réseau VPN	Serveur IPBX	UDP	sip/5060 rtp/20000-22000	Autoriser	Oui	Accès téléphonie IP des utilisateurs nomades

Règle de protection finale						
Réseau LAN	255.255.255.255	UDP	netbios/137-138	Interdire	Non	Règle « antiparasite »
Toutes	Toutes	Tous	Tous	Interdire	Oui	Règle d'interdiction finale

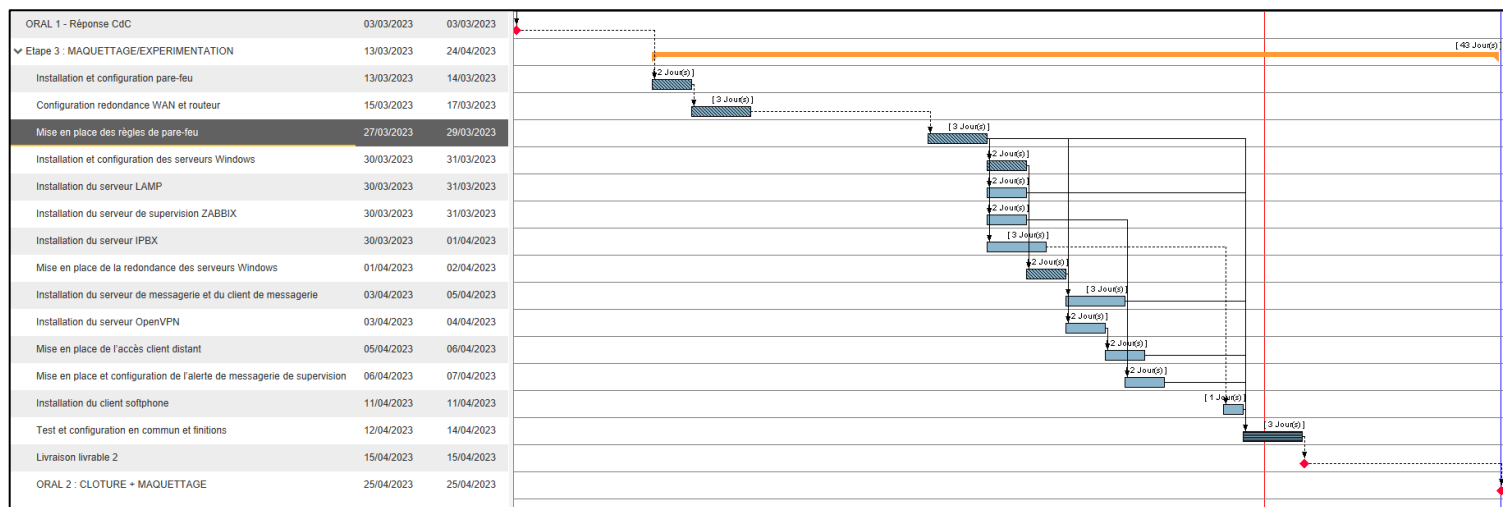
Coût du projet

Pour l'entreprise KGambit, l'utilisation de ces ressources impliquerait des frais. Afin de clarifier la situation, un tableau présentant le coût total des équipements à acheter et le coût des services nécessaires pour la réalisation du projet est fourni ci-dessous.

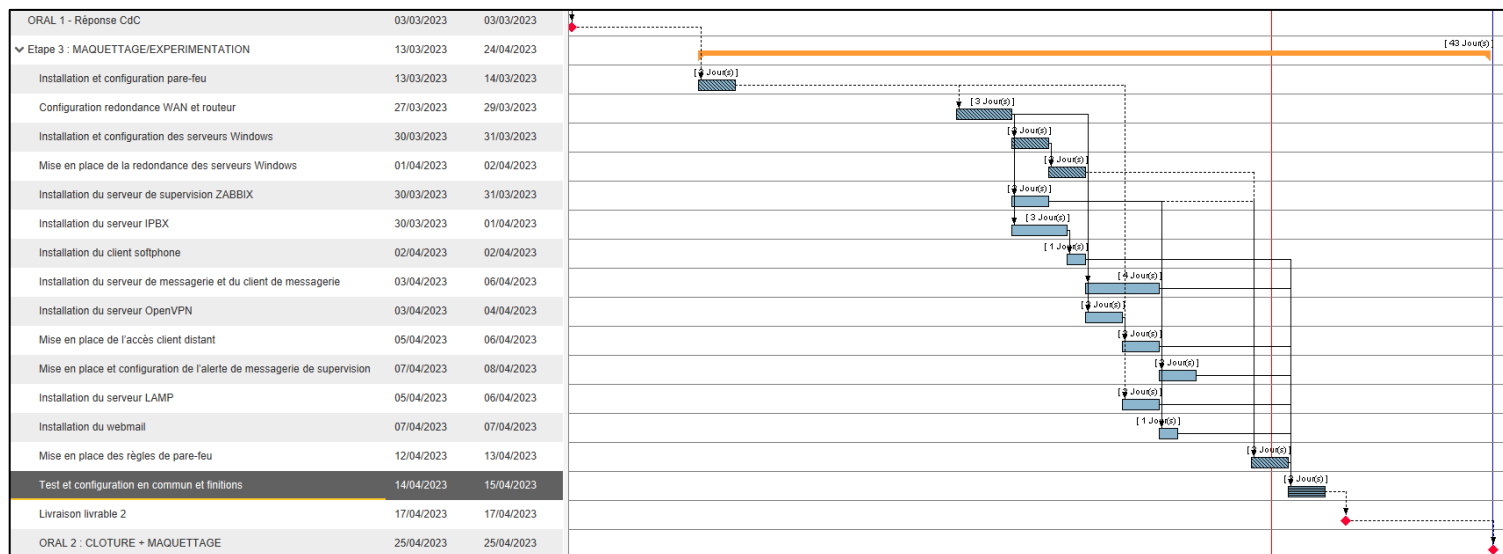
Description	Quantité/ Heures	Prix unitaire HT	Prix HT
Cisco Catalyst 1000 C1000-24T-4G-L	5	542,49 €	2 712,45 €
Routeur/Pare-feu NetGate 7100 1U BASE Pfsense+	2	959,20 €	1 918,40 €
Dell PowerEdge R340-903 Xeon Quad-Core 16Go RAM 1To	2	1 166,62 €	2 333,24 €
Dell PowerEdge T40-138 Xeon Quad-Core 8Go RAM 1To	4	724,96 €	2 899,84 €
PC bureau Lenovo M70s i3 10th Gen – 8Go RAM – 256 SSD	50	555,00 €	27 750,00 €
PC portable Lenovo Thinkpad L13	10	540,00 €	5 400,00 €
Moniteur LED Philips 22"	50	74,80 €	3 740,00 €
Clavier Lenovo 300	50	9,60 €	480,00 €
Souris Lenovo	50	7,68 €	384,00 €
Câble RJ45-Cat6a 10m	20	4,99 €	99,80 €
Câble RJ45-Cat6a 5m	100	2,77 €	277,00 €
Câble fibre optique multimode 20m	10	13,91 €	139,10 €
Licence Windows Server 2019 (16 cœurs + 10 CALs users Pack)	2	1 344,00 €	2 688,00 €
Licence Windows CALs Pack 5 Users	10	104,79 €	1 047,90 €
Licence Windows 10 Pro Retail	50	119,99 €	5 999,50 €
Lexar NM620 SSD 2To NVMe	2	129,99 €	259,98 €
Lexar NM620 SSD 512Go NVMe	4	49,99 €	199,96 €
Installation et configuration pare-feu	14	50,00 €	700,00 €
Configuration redondance WAN et routeur	14	50,00 €	700,00 €
Mise en place des règles de pare-feu	21	50,00 €	1 050,00 €
Installation et configuration des serveurs Windows	7	50,00 €	350,00 €
Mise en place de la redondance des serveurs Windows	7	50,00 €	350,00 €
Installation du serveur de messagerie et du client de messagerie	21	50,00 €	1 050,00 €
Installation du serveur IPBX et client softphone	14	50,00 €	700,00 €
Installation du serveur LAMP	7	50,00 €	350,00 €
Installation du serveur de supervision ZABBIX	7	50,00 €	350,00 €
Mise en place et configuration de l'alerte de messagerie de supervision	4	50,00 €	200,00 €
Installation du serveur OpenVPN	4	50,00 €	200,00 €
Mise en place de l'accès client distant	4	50,00 €	200,00 €
Prix Total HT			64 529,17 €
Total TVA (20%)		12 905,83 €	
Prix Total TTC			77 435,00 €

Planning prévisionnel

Pour ce projet, nous avons élaboré un Diagramme de Gantt. Il va nous permettre de mettre sous forme les échéances, et les éléments importantes à prêter attention avant d'entamer une autre tâche, et ainsi ne pas oublier d'étapes pouvant gêner l'organisation globale.



Planning réel



Planning prévisionnel vs réel

Comme indiqué dans les pages suivantes, nous avons dû changer quelques éléments de l'organisation dans la réalisation du projet. Il s'agit de la tâche de **réalisation du serveur e-brigade** du 31/03, qui n'a été repoussé le 05/04. Ce décalage est dû au fait que nous n'avions pas trouvé l'archive d'installation de la solution applicative, et qu'apparemment cette solution est actuellement limitée en tant que SaaS, software as a service. Cependant, la solution apportée à ce problème fut l'usage d'une ancienne version d'e-brigade, mais dont des mesures de sécurité devraient être appliquées pour pallier les vulnérabilités.

Aussi, nous avons rajouté la tâche de **mise en place d'un accès webmail**, service en plus pour le confort de l'utilisateur, afin d'avoir un accès mobile de la messagerie à travers le VPN.

Enfin, la tâche de **mise en place des règles a été déplacé** en tout dernier, pour ne pas entraver le bon déroulement du maquettage et expérimentation, cependant la date de fin de projet **n'a pas été décalée.**, dû la bonne communication et à l'organisation du groupe

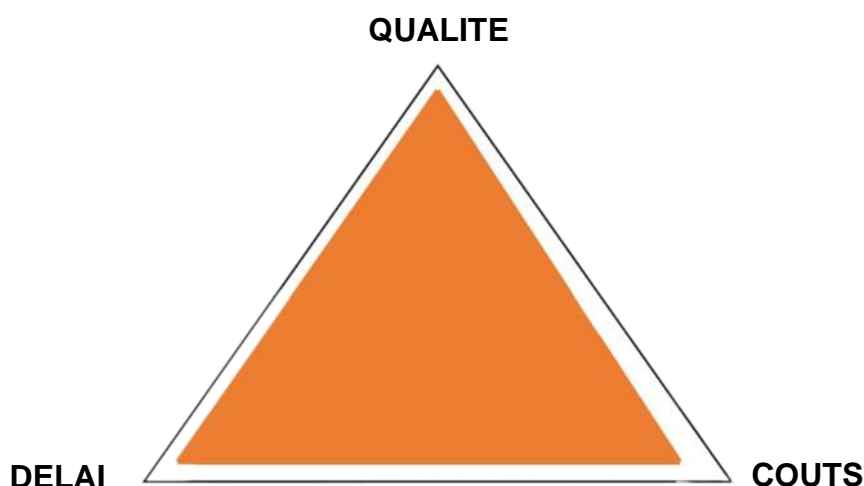
Conclusion

Nous avons pu voir une synthèse des différents éléments du projet afin de répondre aux besoins et aux objectifs fixés lors du cahier des charges.

- ✓ Réalisation à 100% de l'infrastructure et ses composantes (services et moyens d'interconnexion)
- ✓ Le schéma réseau et le plan d'adressage respectent la réalité actuelle des configurations.
- ✓ Le planning prévisionnel et le diagramme de gantt ont été respecté pour notre organisation dans la réalisation du projet
- ✓ Les dates initialement fixées du 13/03/2023 au 15/04/2023 de la documentation technique ont été respectées avec la livraison de ce présent livrable et de l'infrastructure en conséquence.
- ✓ Technique : Mention des éventuels problèmes pouvant réapparaître sur le domaine et comment les résoudre afin d'effectuer une maintenance curative.
- ✓ Énumération des pratiques à pérenniser qui nous ont permis de mener à bien une gestion de projet juste et efficiente dans le cadre de la réalisation du projet cité. S'en suit les pratiques observées pour chaque domaine Organisationnel, comme Technique
- ✓ Mention des ressources prévues et utilisées

Les éléments voulus étant réalisés et documentés avec succès, nous tenons à remercier les formateurs et professionnels ayant contribué à la réalisation du projet et la bienséance qui a été observée dans l'organisation.

En termes de **Qualité-Coût-Délai**, ci-dessous une synthèse globale de la réalisation du projet :



Comme on peut le voir, la qualité et les délais de réalisation de l'infrastructure a été réalisée dans les temps et opérationnelle à l'utilisation. Cependant une petite augmentation des coûts et à noter après l'ajout d'un service de Webmail comme cité auparavant, qui nous a pris 1 jour supplémentaire sans déranger l'organisation globale, mais opérationnel dans l'infrastructure et améliore grandement la qualité des services proposés aux utilisateurs.

Améliorations possibles

Dans cette section, nous allons vous proposer des améliorations possibles pour permettre d'améliorer l'infrastructure et l'architecture dans son ensemble. Les idées sont uniquement des suggestions mais peuvent s'avérer utiles dans le cadre de l'évolutivité des Systèmes d'Information de KGambit.

Chiffrements de communication sur tous les flux type SSL/TLS

Nous avons vu dans l'infrastructure interne et externe que plusieurs éléments cohabitent dans un même réseau ; Messagerie, Téléphonie, Windows Server, Zabbix, ou bien encore le serveur Web dans la DMZ. Cependant, nous pouvons améliorer les flux entre ces différents éléments pour sécuriser encore plus les communications et n'autoriser que les personnes autorisées à accéder aux données (Confidentialité), et assure que les données ne peuvent être modifiées pendant leur transfert, traitement et stockage (Intégrité). Pour permettre cela, nous pouvons mettre en place des flux de type SSL/TLS qui est un chiffrement crypté pour les communications. Les certificats peuvent aussi permettre cela, et l'ajout du chiffrement des communications peut s'avérer un vrai plus dans l'architecture de KGambit

Accès webmail à la messagerie

Comme amélioration possible pour la partie Haute Disponibilité et confort utilisateur, il est possible d'ajouter un accès webmail à la messagerie ; cela signifie d'avoir accès à sa messagerie depuis un mobile ou à distance. Cette solution a déjà été installée avec le webmail et est donc opérationnelle. Ainsi, l'accès à la messagerie depuis le mobile pourrait être réalisé.

Serveur de centralisation de logs

Comme cité dans le cahier des charges, il a été demandé d'installer, de configurer et de tester un serveur de supervision sur les éléments composants l'infrastructure, qui a été réalisé, mais il est aussi possible d'y ajouter, en complément, un autre élément permettant l'administration. Il s'agit de la mise en place d'un serveur de centralisation de logs pour centraliser tous les fichiers journaux des équipements en cas d'attaque ou de violation. Ce serveur récapitulerait et centraliserait tous les fichiers logs de tous les serveurs de la KGambit (Messagerie, Téléphonie, Windows Server, Zabbix...) afin de pouvoir, à la manière de Zabbix pour les postes et les utilisateurs, centraliser et superviser les mouvements et problèmes du domaine, de façon plus approfondie.

Nous pouvons vous proposer comme solution à cette possible amélioration de l'infrastructure, Graylog, ou ELK qui pourrait apporter un complément à Zabbix et à l'administration.

Solution de sauvegarde

L'ajout d'un ou plusieurs disques de sauvegarde peut s'avérer utile. En effet, actuellement, KGambit possède 2 serveurs Windows opérationnels et redondés. Cependant, si l'un des deux tombent hors service avec des données corrompues, nous allons devoir réaliser à nouveau les configurations malgré la redondance. Nous vous proposons donc d'ajouter un ou plusieurs disques couplés à Windows Server permettant la restauration des données pour maintenir durablement et continuellement les opérations de KGambit