

Projet Carmichael Industries

-

BTS SIO 2023 Option SISR



Epreuve E5

-

Situation professionnelle 2

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 : FEVRE Dan	N° candidat : 02243995903
Épreuve ponctuelle <input checked="" type="checkbox"/> Contrôle en cours de formation <input type="checkbox"/>	Date : 01 / 04 / 2023
Organisation support de la réalisation professionnelle L'entreprise de sécurité privée Carmichael Industries, sollicite une proposition et mise en place d'une infrastructure. La demande consiste à permettre aux employés d'accéder aux ressources de l'entreprise lors de leurs missions sur le terrain.	
Intitulé de la réalisation professionnelle Projet Carmichael Industries	
Période de réalisation : 02/01/2022 au 30/03/2022 Lieu : Strasbourg..... Modalité : <input checked="" type="checkbox"/> Seul(e) <input 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) <ul style="list-style-type: none"> • 2 serveurs Active directory en redondance • 1 serveur de messagerie + déploiement client messagerie • 1 serveur de supervision • 1 serveur de téléphonie IPBX +déploiement softphone • 1 serveur web contenant un logiciel privé • 2 routeurs-pares-feux • 1 VPN Road Warrior avec authentification RADIUS 	
Description des ressources documentaires, matérielles et logicielles utilisées² <ul style="list-style-type: none"> • 2 Windows Server 2019 • 1 serveur de supervision ZABBIX sur Debian 11 • 1 serveur Asterisk sur Debian 11 + déploiement Linphone • 2 routeurs / pares-feux Pfsense • Postes clients / Logiciels / applications clients en Windows 10 • 1 serveur de messagerie HmailServer/Thunderbird 	
Modalités d'accès aux productions³ et à leur documentation⁴ https://fevredan.wordpress.com/ -> Situations professionnelles -> Situation professionnelle 2	
BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	
SESSION 2023	

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.

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

ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (recto)	2
ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)	3
1. Contexte	5
1.1. Description de la demande.....	5
2. Besoins et contraintes	5
2.1. Besoins.....	5
2.2. Contraintes	6
3. Solutions retenues et argumentations	6
3.1. Choix de solutions	6
4. Schéma réseau	14
5. Coût du projet	15
5. Conclusion	18
6. Améliorations possibles	18

1. Contexte

1.1. Description de la demande

Carmichael Industries m'a contacté pour la mise en place d'une infrastructure complète avec une accessibilité des agents en intervention.

L'infrastructure devra comporter un routeur en Haute disponibilité, deux serveurs AD DS redondés, un serveur de messagerie ainsi que le déploiement d'un client de messagerie, un serveur de VOIP et le déploiement d'un client softphone et l'utilisation d'un serveur web eBrigade. La demande comporte également la mise en place d'un VPN ROAD WARRIOR pour accéder à la téléphonie, la messagerie ainsi que l'accès au serveur eBrigade en DMZ.

2. Besoins et contraintes

2.1. Besoins

L'infrastructure devra comporter :

- Haute disponibilité de Routeur/Pare-feu avec une DMZ
- Redondance de serveur AD
- Serveur VOIP avec une QoS (Qualité de service)
- Serveur Messagerie
- Serveur web eBrigade
- Un VPN ROAD WARRIOR
- Un outil de supervisions des équipements

2.2. Contraintes

De conception :

- La messagerie, la téléphonie doivent être accessible depuis les sites d'interventions avec une authentification AD.
- eBrigade accessible depuis la DMZ en mode dégradé.
- Règles de pare-feu strictes.
- Supervision/Monitoring avec envoi d'email aux admins en cas de panne.
- Qualité de service.

De coûts :

- Le projet devra être à moindre coûts, l'utilisation de logiciel libre est encouragée.

3. Solutions retenues et argumentations

3.1. Choix de solutions

Routeur :















Un pare-feu/routeur est un dispositif de sécurité qui permet de connecter plusieurs réseaux entre eux, tout en sécurisant le trafic réseau entrant et sortant grâce au pare-feu intégré. CARP (Common Address Redundancy Protocol) est un protocole de redondance qui permet de partager une adresse IP virtuelle entre plusieurs pare-feu/routeurs pour assurer une haute disponibilité. CARP émule une adresse IP unique partagée par plusieurs équipements, de sorte que si un équipement tombe en panne, un autre équipement prend automatiquement le relais en utilisant l'adresse IP partagée. Les équipements communiquent via le protocole multicast IGMP pour détecter les autres équipements qui participent au groupe et coordonner l'utilisation de l'adresse IP virtuelle partagée. J'ai choisi de me concentrer sur les systèmes d'exploitation open-source PFSense et OPNSense :

- PFSense

PFSense est un système d'exploitation open source pour les routeurs et les pare-feux basé sur FreeBSD. Il est conçu pour offrir une solution de sécurité pour les réseaux domestiques et les petites entreprises. Il inclut des fonctionnalités telles que le filtrage de paquets, la détection d'intrusion, la gestion de VPN et la gestion de la bande passante. Il permet également de configurer des règles de filtrage pour les protocoles de couche réseau comme TCP/IP, DHCP, DNS et SNMP.

- OPNSense

OPNSense est un fork (copie) open-source de PFSense qui a été créé en 2014. Il est également basé sur FreeBSD et offre des fonctionnalités similaires à PFSense, mais avec une interface utilisateur plus moderne et intuitive. Il inclut des fonctionnalités telles que la gestion des utilisateurs, la gestion des groupes, la gestion des rôles, la gestion des certificats, la gestion des mises à jour. Il intègre également des fonctionnalités de sécurité telles que le filtrage de paquets, la détection d'intrusion et la gestion de VPN. Il propose également une large gamme de plugins pour étendre les fonctionnalités de base de l'application.

	PFSense	OPNSense
Haute disponibilité (protocole CARP)		
Routage WAN en mode Dual WAN		
Fonctionnalités de pare-feu avancées		
Intégration dans un domaine/ Active Directory		
IP virtuelles / DMZ		
QoS (Quality of Service)		
Sauvegarde et de restauration de configuration intégrée		

Serveur AD :











Un serveur Active Directory (AD) est un système de gestion de répertoire qui est utilisé pour stocker les informations d'identification des utilisateurs, des ordinateurs et des groupes dans un réseau d'entreprise. Il permet également de gérer les stratégies de sécurité, les autorisations et les authentifications pour les utilisateurs d'un réseau. J'ai sélectionné deux solutions :

- Windows Server 2019

Windows Server 2019 est un système d'exploitation serveur développé par Microsoft, qui inclut des fonctionnalités pour la gestion de domaine Active Directory (AD) telles que la gestion des utilisateurs et des groupes, la gestion des stratégies de groupe, l'authentification et l'autorisation. Il permet de créer un domaine AD et d'y inclure des utilisateurs et des groupes. Il est facile à installer et à configurer, et bénéficie d'un support technique et d'une assistance étendue de la part de Microsoft. Cependant, il nécessite une licence pour être utilisé.

- Samba/OpenLDAP

Samba est un projet open-source qui permet à des systèmes d'exploitation non-Windows de participer à un domaine Active Directory existant mais aussi de créer un domaine Active Directory (AD) avec Samba4. Il permet également de partager des fichiers et des imprimantes avec des ordinateurs Windows. En utilisant Samba et OpenLDAP ensemble, on peut bénéficier de la flexibilité et des fonctionnalités de Samba pour créer un domaine AD et pour partager des fichiers et des imprimantes, tout en utilisant OpenLDAP pour gérer efficacement les utilisateurs et les groupes d'un domaine AD existant en utilisant des scripts et des configurations LDAP. Cependant, cela nécessite une configuration et une maintenance supplémentaires, et il peut y avoir des différences dans les fonctionnalités par rapport à Windows Server. Il bénéficie d'une communauté de développeurs et d'utilisateurs actifs qui fournissent de l'aide et des mises à jour.

	Windows Server 2019	Samba/OpenLDAP
Gestion Domaine/utilisateurs AD		
DNS		
Facilité d'intégration serveur de messagerie		
Facilité d'intégration serveur de téléphonie		
Intégration avec PFSense		

Serveur de téléphonie (IPBX) :

Un serveur IPBX (Internet Protocol Private Branch Exchange) est un système de téléphonie qui utilise des protocoles de communication sur IP pour gérer les appels téléphoniques dans un réseau d'entreprise. Il permet aux utilisateurs de passer des appels téléphoniques via leur réseau IP plutôt que via des lignes téléphoniques traditionnelles et offre des fonctionnalités avancées comme la gestion des appels, la messagerie vocale, la gestion des conférences téléphoniques, la gestion des files d'attente d'appels et la gestion des appels en attente. Il peut également être intégré à d'autres systèmes tels que les systèmes de gestion de la relation client (CRM) pour améliorer les communications d'entreprise. Il existe plusieurs logiciels de serveur de téléphonie IP, je vais en comparer deux qui font parties des logiciels open-source :













- Asterisk

Asterisk est un logiciel open-source de serveur de téléphonie IP qui permet de gérer les communications vocales et vidéo sur IP. Il est souvent utilisé pour construire des solutions de téléphonie sur IP, des plateformes de communication unifiée, des systèmes de centre d'appel et des réseaux privés virtuels (VPN). Il prend en charge un large éventail de protocoles de téléphonie, y compris SIP, H.323, IAX et WebRTC. Il peut également être intégré à d'autres systèmes pour améliorer les

communications d'entreprise.

- FREESWITCH

FreeSWITCH est une autre plateforme open source qui offre des fonctionnalités similaires à celles d'Asterisk. Il est également très abordable et facile à déployer et à gérer. FreeSWITCH offre des fonctionnalités supplémentaires par rapport à Asterisk, telles que la prise en charge multi-plateforme, l'accès modulaire à d'autres protocoles et un support pour des systèmes de numérotation avancés.

	Asterisk	FREESWITCH
Compatibilité avec la majorité des protocoles et codecs		
Compatibilité OS		
Logiciels multiplateformes		
Intégration simple et fiable		
Plateforme multi-tenant		
Communication avancée (ex : chat, vidéo-conférence, ...)		

Serveur de messagerie :

Un serveur de messagerie est un logiciel permettant de gérer les transferts de messages. Celui-ci comporte trois services principaux qui sont les suivants :

- Mail User Agent ou MUA décrypte et transfère les messages, c'est un client de messagerie tel que Mozilla Thunderbird ou encore Microsoft Outlook.
- Mail Transfert Agent ou MTA est un logiciel élaboré pour transférer les messages entre les serveurs.
- Mail Delivery Agent ou MDA représente la fin du processus d'envoi d'un message électronique et est associé aux protocoles IMAP et POP.

Grâce à ces services, les mails envoyés arriveront à destination.











- HmailServer

HmailServer est un serveur de messagerie open source confectionné tout particulièrement pour les systèmes d'exploitation sous Windows. Disposant de quelques fonctionnalités (anti-spams, antivirus, création d'alias, ...), il fonctionne avec les protocoles SMTP, POP3 et IMAP. Le dernier permet de supporter une majorité d'interface web de messagerie. HmailServer fonctionne principalement

avec la base de données MySQL mais aussi avec des bases de données externe tel que MS SQL. L'authentification des utilisateurs s'effectue aussi bien sur le système local HmailServer que sur l'Active Directory.

- Bluemind

Tout comme HmailServer, Bluemind est un serveur de messagerie open source mais qui est à l'inverse compatible sur les trois systèmes d'exploitation : Windows, Mac OS et Linux. Ce serveur propose des fonctionnalités tels qu'un calendrier partagé, un mode "hors connexion", la synchronisation des mails mais aussi des services plus larges comme les mises à jour automatique et des outils de gestion. De plus, Bluemind adopte Thunderbird comme client lourd faisant concurrence à Outlook qui a actuellement le monopole. Bluemind offre un support à la messagerie Thunderbird avec l'intégration d'un plugin doté de fonctionnalités diverses et variés.

	HmailServer	Bluemind
Compatibilité OS		
Fonctionnalités intégrées		
Facilité de prise en main		
Compatibilité clients messagerie (outlook, ...)		
Compatible avec l'AD		

Serveur de Supervision/Monitoring :

Définit comme étant un processus qui permet le suivi ou la surveillance de l'ensemble des activités d'une infrastructure informatique dont les éléments peuvent être virtuels ou physiques. Il vise à maintenir le bon fonctionnement des systèmes, de prévenir les pannes et de détecter les incidents en donnant l'alerte. Ainsi, cet outil contrôle les différents composants (processeurs, mémoire, disques, ...), périphériques des équipements présents sur le réseau (commutateur, routeurs, serveurs, ...) mais analyse également leurs performances et leur disponibilité. Cette supervision est possible grâce à la communication des applications et des périphériques avec l'outil de supervision via une variété de protocoles (SNMP, HTTP, WMI, ...).

Il existe une large palette de logiciels de supervision sur le marché, cependant j'en ai tiré 2 répondants aux attentes et aux besoins de ce projet :

- EyesofNetwork













EyesofNetwork est un outil Open Source de supervision pour les systèmes

informatiques. Il combine plusieurs solutions en une seule plateforme pour aider les administrateurs à surveiller les performances du réseau, gérer les incidents et optimiser l'infrastructure informatique. Il inclut des fonctionnalités telles que Nagios pour la supervision du réseau, EyesofApplication pour le suivi des applications, EyesofReport pour la gestion du catalogue de services, EyesofIndicator pour les informations système sur un tableau de bord, et EyesofLog pour la centralisation des logs, analyses et événements. La plateforme est basée sur Linux et offre une interface de configuration simple et facile à utiliser. EyesofNetwork est une solution complète pour les besoins de gestion d'un environnement informatique.

Ce logiciel se compose de plusieurs fonctionnalités octroyant une gestion optimisée et précise d'une infrastructure informatique qu'elle soit grande ou petite.

- Nagios

Nagios est un logiciel de supervision de réseau Open Source qui permet aux administrateurs informatiques de surveiller les performances des équipements réseau, tels que les serveurs, les ordinateurs, les équipements réseau, et d'être alertés en cas de problèmes. Il se compose d'un ordonnanceur pour contrôler l'ordre d'exécution des services, d'une interface web pour faciliter le suivi de l'infrastructure, et de plugins permettant d'intégrer d'autres fonctionnalités. L'ordonnanceur surveille les performances des équipements réseau et les plugins vérifient la disponibilité et la santé des services. L'interface web affiche les résultats de ces vérifications, permettant aux administrateurs de surveiller facilement leur réseau. Nagios est une solution fiable et puissante pour la supervision des systèmes informatiques.

	Eyes of networks	Nagios
Game ITIL		
Interface de configuration WEB		
Configuration et gestion simplifié		
Authentification LDAP		
Notifications d'alerte par mail ou sms		
Fonctionnalités intégrées		

VPN ROAD WARRIOR :

Un VPN (Virtual Private Network) est un réseau privé virtuel qui utilise des protocoles de tunneling pour connecter des ordinateurs distants en toute sécurité.

Les deux types de VPN les plus courants sont les VPN site à site et les VPN road warrior.

Les VPN site à site sont utilisés pour connecter des réseaux locaux (LAN) distants pour former un réseau privé étendu. Ce type de VPN est généralement utilisé par les entreprises pour connecter leurs filiales ou les différents sites de l'entreprise. Le VPN site à site crée une connexion permanente entre les deux réseaux et permet aux utilisateurs de partager des fichiers et d'accéder aux ressources comme s'ils étaient physiquement connectés au même réseau.

Les VPN road warrior, quant à eux, sont utilisés pour connecter des ordinateurs individuels à un réseau privé à distance. Ce type de VPN est utile pour les employés qui se déplacent et qui ont besoin d'accéder à des ressources sur leur réseau d'entreprise à partir de n'importe où dans le monde. Le VPN road warrior crée une connexion sécurisée entre l'ordinateur de l'utilisateur et le réseau d'entreprise lorsque l'utilisateur se connecte à Internet à partir d'un emplacement distant.

En résumé, les VPN site à site sont utilisés pour connecter des réseaux distants pour former un réseau privé étendu, tandis que les VPN road warrior sont utilisés pour connecter des ordinateurs individuels à un réseau privé à distance. Les deux types de VPN offrent une connexion sécurisée pour les communications et l'accès à des ressources à distance.

Les deux outils que j'ai sélectionné pour cette solution sont les suivants :

- OPENVPN :











OpenVPN, c'est deux choses à la fois : un protocole et un logiciel open source. Il a pour objectif d'élaborer un réseau virtuel privé pour une connexion distante entre un appareil et un réseau privé (LAN). De plus, sa compatibilité avec tous les systèmes d'exploitation sur le marché lui confère un avantage à ne pas négliger. A noter, que c'est grâce à l'installation d'un client OpenVPN que la compatibilité OS peut fonctionner. Par ailleurs, son port d'écoute peut être modifié et personnalisé facilitant son usage pour un réseau donné. Ce protocole confère un bon compromis entre le chiffrement de données et la vitesse de connexion.

D'ailleurs, j'avais le choix entre deux protocoles de transmission de données : UDP ou TCP. L'une privilégie la vitesse l'autre assure la sécurité et la transmission des données. D'autres protocoles sont tout aussi utilisés pour la manière d'encrypter les données (OpenSSL) ou de s'authentifier (SSL/TLS).

- Wireguard :

Déjà populaire dans le monde des VPN, Wireguard est un protocole moderne venant concurrencer les anciens présents sur le marché tel que OPENVPN en jouant la carte de la simplicité et de la sécurité. Sa création en 2017 est due par son créateur afin de pallier les problèmes de performances et de gestion des VPN existants. De plus, le choix du chiffrement ne dépendra plus de celui qui configure l'outil mais plutôt des algorithmes de chiffrement. Pour couronner le tout, le cryptage des données

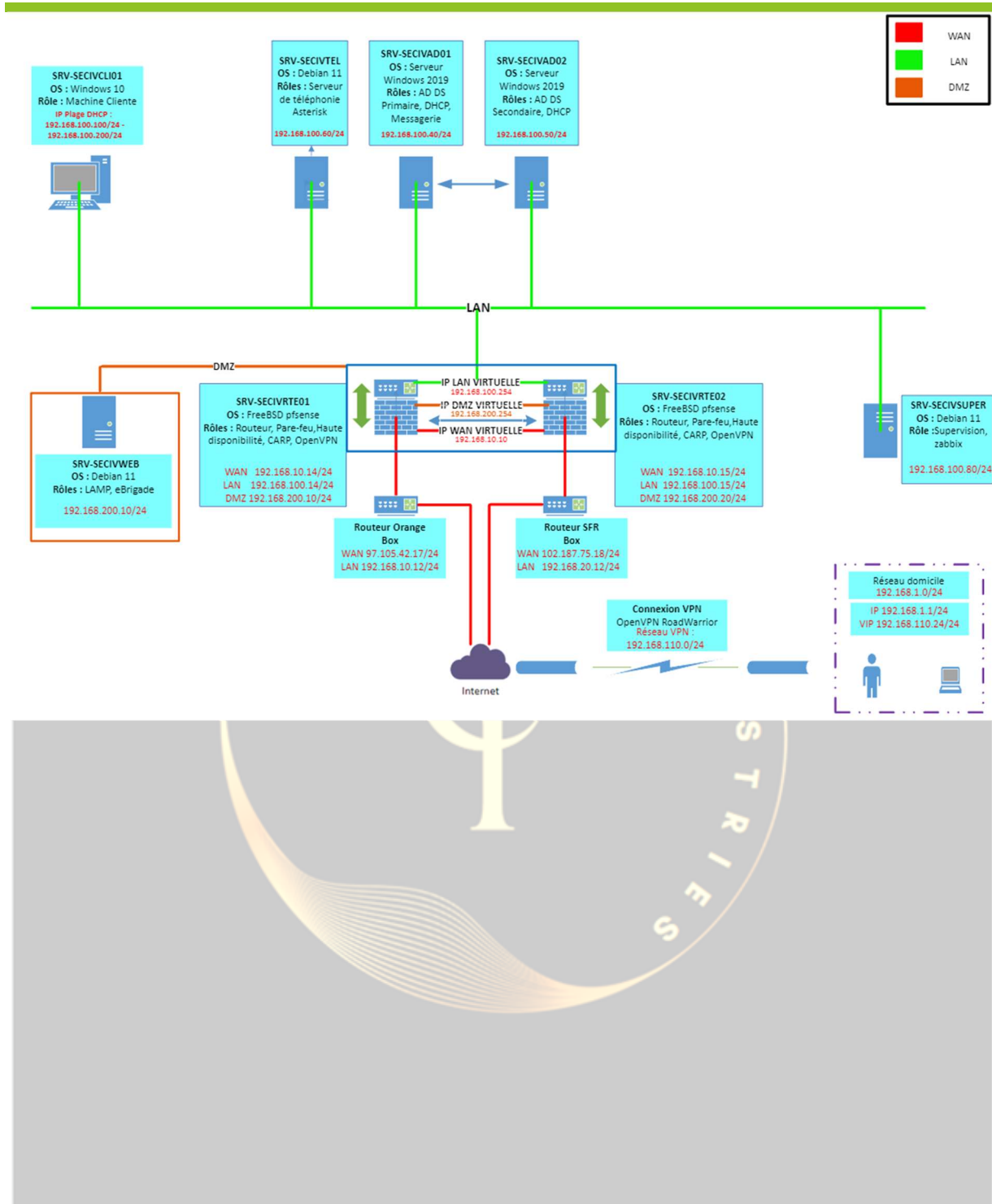
s'effectue non pas avec l'AES moins performante mais avec la combinaison du ChaCha 20 et de Poly1305 en ce qui concerne l'authentification. Par ailleurs, un de ses avantages est sa furtivité c'est-à-dire que tous les équipements dont Wireguard ne reconnait pas ne pourront pas le détecter. Cependant, ce VPN a été conçu principalement pour les machines sous Linux avec un module Kernel.

	Wireguard	OpenVPN
Intégré à PfSense		
Connexion sécurisée		
Configuration simple et rapide		
Compatibilité OS		
Rapidité de connexion		

3.2. Solutions choisies

Routeur	Pfsense
Serveur d'annuaire	Windows server 2019 (Active Directory)
Serveur de téléphonie (IPBX)	Asterisk
Serveur de messagerie	HmailServer
Serveur de Supervision/Monitoring	zabbix
VPN ROAD WARRIOR	OpenVPN
Serveur pour le logiciel eBrigade	Debian 11

4. Schéma réseau



5. Coût du projet

Le devis ci-dessous prend en compte les différents équipements et licences nécessaires à l'élaboration du projet. De plus, la prestation de nos services vous sera également chargée à 100 € de l'heure et par personne.

Objet : Devis des équipements nécessaires

Désignations des produits	Quantité	Prix Unitaire HT	Total HT
Smart Selection PowerEdge R650 Server Rack	3	3 985,64 €	11 956, 92 €
Smart Selection PowerEdge R250 Rack Server	2	1 393,94 €	2 787,88 €
Smart Selection PowerEdge R250 Server Rack Plus	3	2 317,78 €	6 953,34 €
Licence Windows server 2019	3	1 946 €	5 838 €
Samsung 27" Écran incurvé - C27F396FHR	1	159 €	159 €
DELL Precision 3660 Tower	1	1 932,34 €	1 932,34 €
Licences CAL	50	50 €	2 500 €

Désignation des prestations	Délais	Temps	Quantité	Prix Unitaire HT	Total HT
Service	2/3 mois	Heure	56h	50 €/personne	5 600 €

-

Montant Total HT **37 727,48 €**

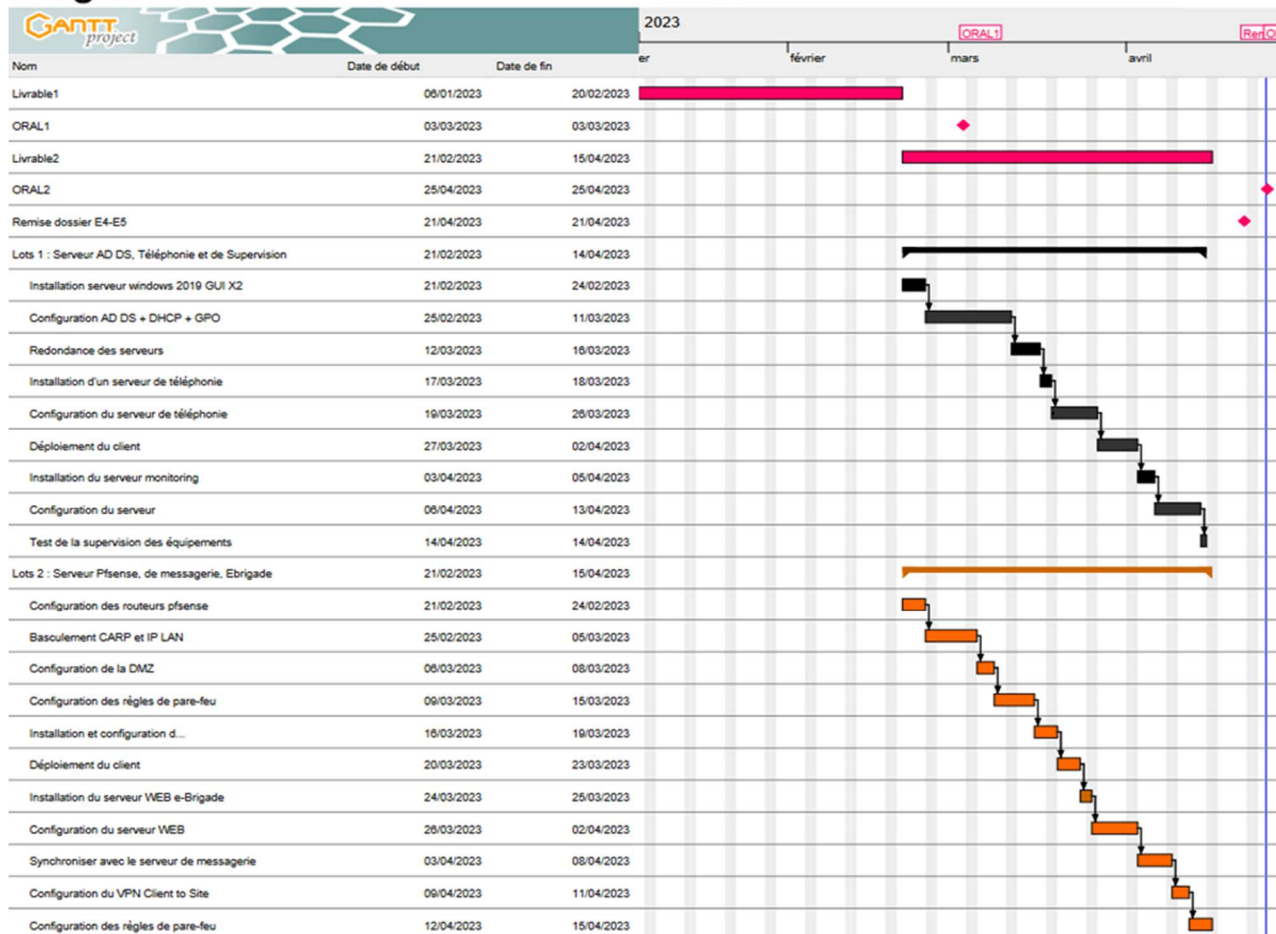
TVA (20 %) 7 545,50€

Montant Total TTC **45 272,98 €**

La loi n°92/1442 du 31 décembre 1992 nous fait l'obligation de vous indiquer que le non-respect des conditions de paiement entraîne des intérêts de retard suivant modalités et taux défini par la loi. Une indemnité forfaitaire de 40€ sera due pour frais de recouvrement en cas de retard de paiement.

Planning prévisionnel

Diagramme de Gantt



Heures totales lots 1 : 25h30

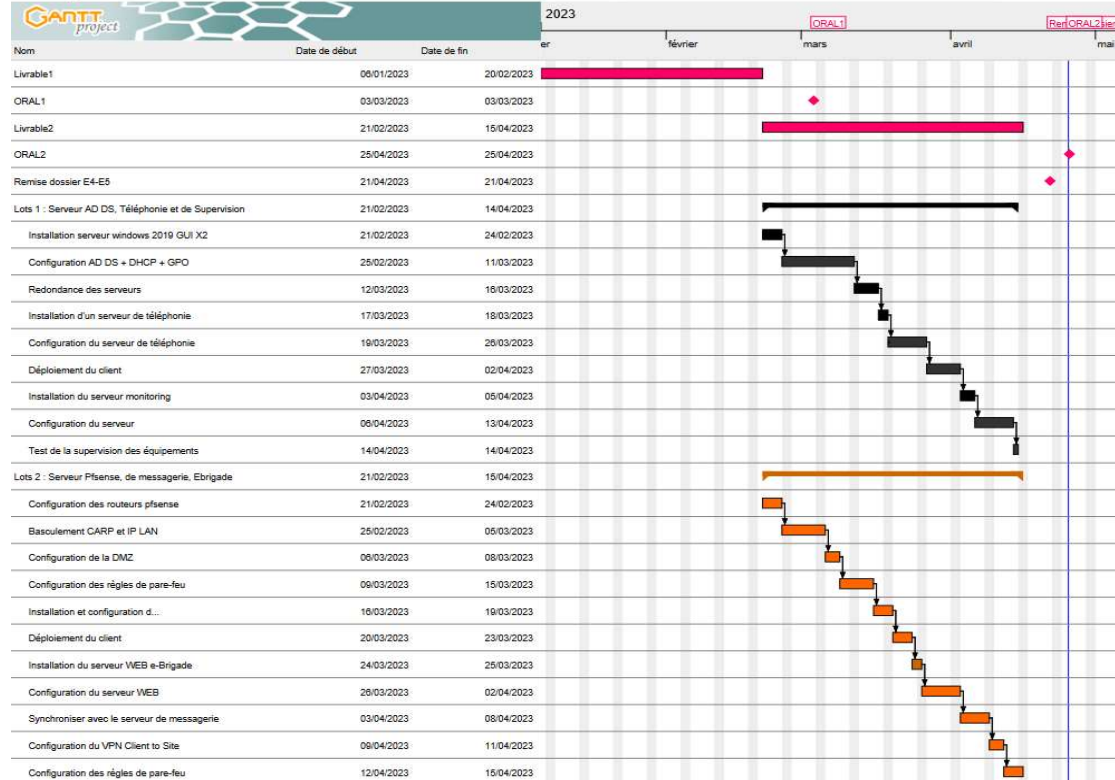
1h30
4h
1h
2h
8h
2h
1h
4h
2h

Heures totales lots 2 : 31h30

1h
4h
2h
8h
1h
1h30
1h
1h
4h
2h
2h
4h

Planning réel

Diagramme de Gantt



Heures totales lots 1 : 25h30

1h30

4h

1h

2h

8h

2h

1h

4h

2h

Heures totales lots 2 : 30h30

1h

4h

2h

8h

1h

1h30

1h

1h

4h

2h

2h

4h

5. Conclusion

Le projet a été incroyablement pédagogique et intéressant. Au cours de celui-ci, j'ai appris énormément de choses nouvelles et passionnantes, tout en développant mes compétences techniques. En conclusion, ce projet a été un succès malgré les problèmes rencontrés, et a permis de répondre aux besoins de l'entreprise Carmichael Industries en matière d'infrastructure réseau. Les solutions apportées ont permis de résoudre les problèmes techniques et ont permis de respecter les objectifs fixés. J'ai pu tirer parti de mes compétences techniques et de mes connaissances pour concevoir des solutions efficaces et efficaces, ce qui a été une expérience inestimable pour moi.

6. Améliorations possibles

Il est possible d'améliorer l'infrastructure de cette façon :

- Ajout d'une sauvegarde automatique des données importantes pour éviter toute perte de données en cas de panne ou d'incident.
- Mise en place de la redondance pour le serveur de messagerie : Bien que le rôle de serveur de messagerie ait été combiné avec le rôle AD du serveur principal, il pourrait être intéressant d'envisager une solution de redondance pour le serveur de messagerie. Cela permettrait d'assurer une disponibilité continue du service en cas de panne du serveur principal.
- Mise en place d'un système de gestion de configuration : Pour faciliter la gestion et la maintenance de l'infrastructure, il pourrait être utile de mettre en place un système de gestion de configuration tel que Puppet ou Ansible.
- Utilisation de la mise en cache pour le serveur web : Pour améliorer les performances du serveur web, il pourrait être utile d'utiliser un système de mise en cache tel que Varnish ou Squid.