AP4 - LIVRABLE 1

La mise en œuvre d'une connexion distante permettant l'accès aux ressources et outils métiers par les agents de terrain.

GROUPE 7

Victor WARTH / Nicolas TANT

PROPOSITION TECHNIQUE ET COMMERCIALE

Table des matières

1) PRÉSENTATION DU GROUPE

1.1) Composition et présentation

Notre groupe pour ce projet de BTS SIO SISR est composé de deux membres :

1. **Victor WARTH :** Administrateur systèmes et réseaux, Victor est passionné par l'informatique depuis qu'il est jeune. Méthodique, organisé et pointilleux, il pourra répondre au mieux aux besoins du projet ! En dehors du travail, Victor aime sortir avec ses amis, il joue aussi aux jeux vidéo et pratique souvent du sport.

2. **Nicolas TANT :** Administrateur systèmes et réseaux, Nicolas est lui aussi passionné par l'informatique ! Aventurier, curieux et organisé, il ira au bout du projet avec brio ! En dehors de son temps de travail, Nicolas aime jouer aux jeux vidéo et pratiquer divers sports.

Victor et Nicolas sont en 2ème année de **BTS SIO** (**S**ervices **I**nformatiques aux **O**rganisations) option **SISR** (**S**olutions d'**I**nfrastructure, **S**ystèmes et **R**éseaux) au CCI Campus de Mulhouse. Ce livrable rentre dans le cadre de l'atelier de professionnalisation numéro 4.

1.2) Définitions des rôles et responsabilités

Le projet vise à améliorer la résilience informatique des Centres Opérationnels Départementaux en mettant en place une solution technique robuste, incluant un accès distant sécurisé, une infrastructure informatique redondante et la gestion d'un logiciel de coordination des interventions.

Les administrateurs systèmes et réseaux **Victor WARTH** et **Nicolas TANT** se répartissent les tâches comme suit :

- **Victor** est responsable de la planification, de la conception du réseau, de la mise en place de la sécurité informatique (pare-feu, VPN, DMZ) et des tests de validation. Il supervise également la présentation finale et la documentation du projet.
- **Nicolas** prend en charge l'analyse des besoins, l'installation et la configuration des serveurs (AD, DHCP, messagerie, monitoring) ainsi que le déploiement du logiciel eBrigade. Il est également chargé de la rédaction de la documentation et du rapport final.

Les administrateurs systèmes et réseaux collaborent sur les tests, la validation et les simulations d'exercices pour garantir une solution fonctionnelle et sécurisée. Ils assurent ensemble la bonne gestion du projet, le respect des délais et des objectifs techniques.

2) ANALYSE DES BESOINS ET DES OBJECTIFS

2.1) Contexte et objectifs

Le projet vise à garantir la résilience informatique des Centres Opérationnels Départementaux (COD) et à assurer un accès distant sécurisé aux ressources pour les agents de terrain. L'objectif est de mettre en place une infrastructure fiable, redondante et sécurisée pour assurer la continuité des opérations en cas de crise.

2.2) Problématiques et besoins identifiés

D'après les retours d'expérience des services concernés, plusieurs problèmes critiques ont été identifiés :

1. **Fiabilité et résilience du réseau**
    - Les infrastructures actuelles manquent de redondance, ce qui entraîne des interruptions de service.
    - Besoin d'une solution Internet redondante avec deux accès distincts pour assurer une haute disponibilité.
2. **Sécurisation des accès et des données**
    - Accès distant aux ressources insuffisamment sécurisé.
    - Nécessité d'un VPN sécurisé (OpenVPN Road Warrior) pour les agents sur le terrain.
    - Besoin de contrôle d'accès et d'authentification via un Active Directory (AD).
3. **Mise en place d'une messagerie sécurisée**
    - Besoin d'un serveur de messagerie interne sécurisé.
    - Communication chiffrée avec intégration à l'Active Directory.
4. **Supervision et monitoring des infrastructures**
    - Actuellement, absence de supervision centralisée des équipements critiques.
    - Besoin d'un outil de monitoring pour surveiller l'état des routeurs, serveurs et connexions réseau.
    - Mise en place d'un système d'alerte par mail en cas de panne.
5. **Gestion des interventions et coordination des équipes**
    - Absence d'un outil centralisé pour gérer le personnel et les interventions.
    - Besoin d'un logiciel de gestion des opérations (eBrigade) permettant :
        - La gestion des effectifs et des missions.
        - Le suivi en temps réel des interventions.
        - L'enregistrement des rapports et historiques d'actions.
6. **Connexion Sécurisée pour l'Externe**
    - Accès aux outils et services depuis l'extérieur en toute sécurité.
    - Mise en place d'une DMZ pour héberger eBrigade et d'autres services accessibles depuis l'extérieur.

2.3) Besoins techniques

Besoins	Solutions Techniques à Mettre en Place
Accès Internet redondant	2 routeurs, 2 connexions Internet (simulation avec 1 accès)
Accès distant sécurisé	VPN OpenVPN Road Warrior avec authentification AD
Sécurisation du réseau	Pare-feu, filtrage réseau, DMZ
Gestion centralisée des utilisateurs	Active Directory (Serveur principal et secondaire)
Messagerie interne sécurisée	Serveur de messagerie local + AD
Supervision du système	Serveur de monitoring avec alertes par mail
Gestion des interventions	eBrigade installé en local et accessible en DMZ
Fiabilité des infrastructures	Onduleur, sécurisation électrique

2.4) Contraintes et exigences

- Contraintes de Temps :
  - Début du projet : 10 janvier 2025
  - Fin prévue : 14 avril 2025
  - Respect des livrables et du planning Gantt.
- Contraintes de Budget :
  - Solution à moindre coût, en privilégiant des outils open-source lorsque c'est possible.
  - Achat limité au matériel indispensable (serveurs, onduleurs, licences).
- Contraintes de Sécurité :
  - Conformité aux normes de cybersécurité.
  - Accès aux données uniquement via authentification AD.
  - Protection des flux réseau avec un pare-feu adapté.

2.5) Conclusion de l'analyse

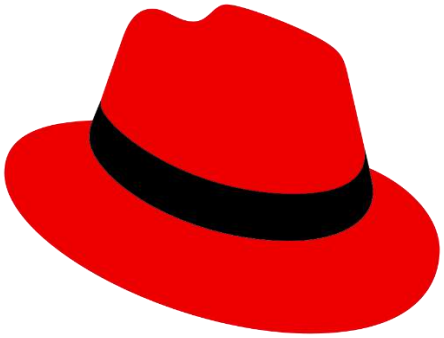
L'analyse des besoins met en évidence des problématiques critiques de sécurité, d'accessibilité et de continuité de service. La mise en place d'une infrastructure redondante et sécurisée, couplée à un VPN et un système de monitoring, assurera la fiabilité du système informatique des Centres Opérationnels Départementaux.

Ce projet nécessite une coordination étroite entre les responsables IT et la préfecture, ainsi qu'une rigueur dans la mise en œuvre technique pour garantir la réussite du déploiement.

3) SOLUTIONS

3.1) Solutions techniques et logicielles

3.1.1) OS des serveurs



Windows Server

Très adapté pour les environnements Active Directory, GPO, et autres services Microsoft. Il offre une compatibilité native avec de nombreuses solutions d'entreprise

Red Hat Enterprise Linux (RHEL)

Distribution Linux reconnue pour sa stabilité et son support en entreprise, idéale pour les serveurs web, bases de données et les environnements nécessitant une sécurité renforcée

Critère	Windows Server	Red Hat Enterprise Linux
Compatibilité	🟢 Élevée (Microsoft)	🟡 Moyenne avec Windows
Performance	🟢 Bonne	🟢 Excellente
Facilité d'utilisation	🟢 Environnement simple	🟡 Moins standard
Coût	🔴 Élevé	🔴 Élevé

Windows Server

Windows Server est imposé dans ce projet et nécessaire en vue des installations attendus. L'environnement Windows est maîtrisé par les techniciens missionnés pour l'installation et plus rependu.

3.1.2) Pare-feu

PfSense

PfSense est une solution de pare-feu open-source basée sur FreeBSD. Elle est largement utilisée pour sa flexibilité et son adaptabilité aux besoins des entreprises de toutes tailles. PfSense permet de configurer des règles de sécurité avancées, de gérer des VPN de site à site (IPsec, OpenVPN), et offre une large gamme de fonctionnalités pour la gestion du réseau

Stormshield

Stormshield est une solution propriétaire de pare-feu axée sur la sécurité avancée, adaptée aux environnements critiques. Elle propose des fonctionnalités telles que la prévention des intrusions (IPS), le filtrage d'URL, et la gestion centralisée des règles

Critère	PfSense	Stormshield
Type de licence	🟢 Open source	🔴 Payante
Interface	🟡 Classique	🟢 Professionnelle
Coût	🟢 Gratuit	🔴 Élevé
Complexité de déploiement	🟡 Moyenne	🔴 Configuration complexe

PfSense

PfSense est retenu pour sa flexibilité, son coût nul, et sa capacité à gérer un VPN inter-sites via IPsec, facilitant la connexion sécurisée entre le site A et le site B.

3.1.3) Annuaire et gestion d'identité

Microsoft Active Directory

Solution de gestion des identités et des accès (IAM) pour les environnements Windows, avec une intégration native aux services Microsoft (Exchange, SharePoint). Idéale pour centraliser la gestion des utilisateurs, des groupes et des politiques de sécurité

OpenLDAP

Solution open-source de gestion des répertoires pour centraliser l'authentification sur des environnements Linux et Unix. Sa flexibilité en fait une option personnalisable

Critère	Active Directory	OpenLDAP
Intégration	🟢 Native (Windows)	🟡 Moyenne
Facilité de gestion	🟢 Élevée	🟡 Moyenne
Coût	🔴 Élevé	🟢 Gratuit
Cloud	🟡 Moyenne (Azure AD)	🔴 Faible (Pas d'alternative native)

Microsoft Active Directory

L'AD est choisi pour sa robustesse, son intégration native avec l'infrastructure Windows Server et sa capacité à gérer les identités dans le cadre du projet ainsi qu'à l'intégration de différentes solutions nécessaires pour ce projet.

3.1.4) Supervision

CheckMk

CheckMk est une solution de supervision open-source basée sur Linux. Elle est connue pour sa légèreté, sa rapidité d'installation et sa gestion avancée des performances. CheckMk propose une interface moderne et intègre des fonctionnalités avancées comme la découverte automatique des hôtes, le monitoring cloud et conteneurs, ainsi qu'une API REST.

Centreon

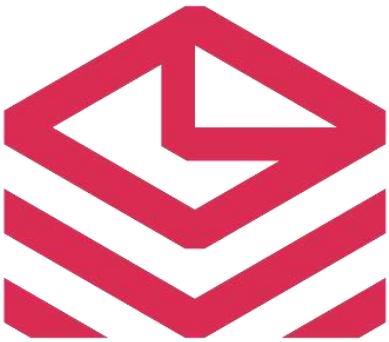
Centreon est une solution de supervision modulaire et extensible, particulièrement populaire en Europe. Elle offre une interface graphique détaillée et permet une supervision avancée des infrastructures IT, avec des tableaux de bord personnalisables, un moteur d'alertes performant et une API REST.

Critère	CheckMk	Centreon
Type de licence	🔴 Payante	🔴 Payante
Interface	🟢 Moderne et simple	🟡 Classique et détaillé
Installation	🟢 Rapide et simple	🔴 Complexe
Performance	🟢 Légé et optimisé	🟡 Gourmand mais optimisé

CheckMk

CheckMk est retenu pour sa simplicité de mise en place, son interface moderne et son efficacité en termes de supervision.

3.1.5) Serveur de messagerie



Stalwart

Stalwart est une solution de messagerie open-source qui regroupe un serveur SMTP, IMAP et JMAP dans un seul outil. Il se distingue par sa légèreté, sa sécurité avancée (MTA-STS, DANE) et sa simplicité de déploiement. C'est une alternative moderne aux solutions classiques, adaptée aux besoins actuels en matière de messagerie sécurisée.

Zimbra

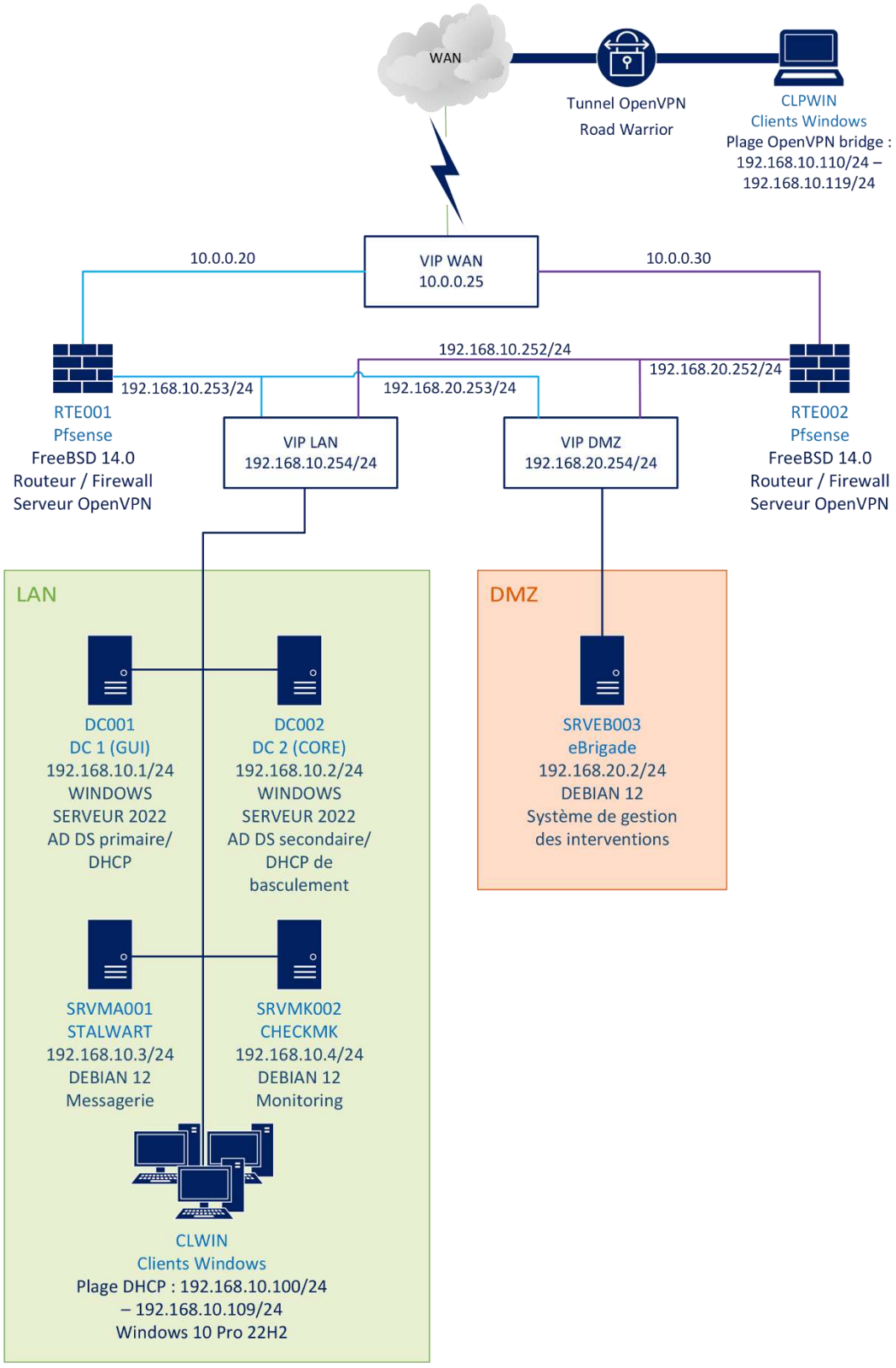
Zimbra est une solution de messagerie collaborative qui inclut e-mail, agenda, contacts et stockage de fichiers. Disponible en version open-source et commerciale, elle est largement utilisée pour ses fonctionnalités avancées et son interface web intuitive.

Critère	Stalwart	Zimbra
Type de licence	🟢 Open Source	🟢 Open Source & Propriétaire
Administration	🟢 Facilité d'utilisation	🟡 Complète mais plus lourde
Mise en place	🟡 Nécessite des connaissances de base en messagerie	🔴 Complexe, nécessite plusieurs composants
Performance	🟢 Légé et optimisé	🔴 Gourmand en ressource

Stalwart

Stalwart est retenu pour sa modernité, sa sécurité intégrée et sa simplicité de déploiement, offrant une alternative tout-en-un efficace.

3.2) Schéma réseau



4) BUDGET

Le 10-03-2025

Association - Sécurité civile
15 Rue de l'Ardèche
67100 Strasbourg
Siret: 390 060 259 00020
Code APE: 8899B

Association Securite Civile
15 Rue de l'Ardèche

67100 Strasbourg
France

Devis

D-2025-0002 Code Client : 1 TVA Client :

Réf	Désignation	Unité	Quantité	PU HT	PU TTC	Remise	Total HT	Total TTC	Taxe
P001	**Dell PowerEdge R350** - Processeur : Intel Xeon E-2334 (4 c œurs / 8 threads, 3.4 GHz) - Mémoire : 16 Go DDR4 ECC (extensible à 64 Go) - Stockage : 2x SSD 512 Go NVMe (RAID 1) - Réseau : 2x 1GbE	U	1,00	2 500,00	3 000,00		2 500,00	3 000,00	TVA 20%
P002	**HPE ProLiant DL160 Gen10** - Processeur : Intel Xeon Silver 4210 (10 c œurs / 20 threads, 2.2 GHz) - Mémoire : 32 Go DDR4 ECC (extensible à 128 Go) - Stockage : 4x SSD 1 To NVMe (RAID 10) - Contrôleur RAID : HPE Smart Array P408i-a - Réseau : 2x 1GbE + 1x 10GbE	U	1,00	3 000,00	3 600,00		3 000,00	3 600,00	TVA 20%
P003	**Onduleur - Eaton 9PX 1500VA, 1.5KW** - Modèle: 9PX - Puissance: 1.5KW - VA: 1500VA - Nombre de départs: 8 (IEC C13)	U	1,00	1 975,00	2 370,00		1 975,00	2 370,00	TVA 20%
P004	**Netgate 4200 pfSense+ Security Gateway** - Intel® Atom® C1110 with AVX2 4-core @ 2.1 GHz - 4 GB LPDDR5 - 16 GB eMMC Flash - 4x Intel 2.5 GbE i226 "direct" (unswitched)	U	2,00	609,00	730,80		1 218,00	1 461,60	TVA 20%
P005	**Licence WIndows Server 2022** - Licence de base pour un serveur de 16 coeurs	U	2,00	500,00	600,00		1 000,00	1 200,00	TVA 20%
P006	**Licence CAL User RDS Windows Server 2022**	U	2,00	25,00	30,00		50,00	60,00	TVA 20%
P007	**Licence CAL User Windows Server 2022**	U	10,00	33,33	40,00		333,30	399,96	TVA 20%
P008	**Abonnement FREEBOX Pro Fibre** - Abonnement mensuel FREEBOX Pro Fibre 8Gbits/s pour 49.99€HT par mois.	U	1,00	49,99	59,99		49,99	59,99	TVA 20%
P009	**Abonnement Livebox Pro Fibre** - Abonnement mensuel pour internet 8Gbits/s 50€HT par mois.	U	1,00	50,00	60,00		50,00	60,00	TVA 20%
P010	**Admin Sytèmes et réseaux Interne** - Salaire à 3500€ brut/mois - Coût brut pour 10 jours (1666€)	U	2,00	1 666,00	1 666,00		3 332,00	3 332,00	Exo.

Devis

D-2025-0002 Code Client : 1 TVA Client :

Réf	Désignation	Unité	Quantité	PU HT	PU TTC	Remise	Total HT	Total TTC	Taxe

Mode de règlement : Espèce

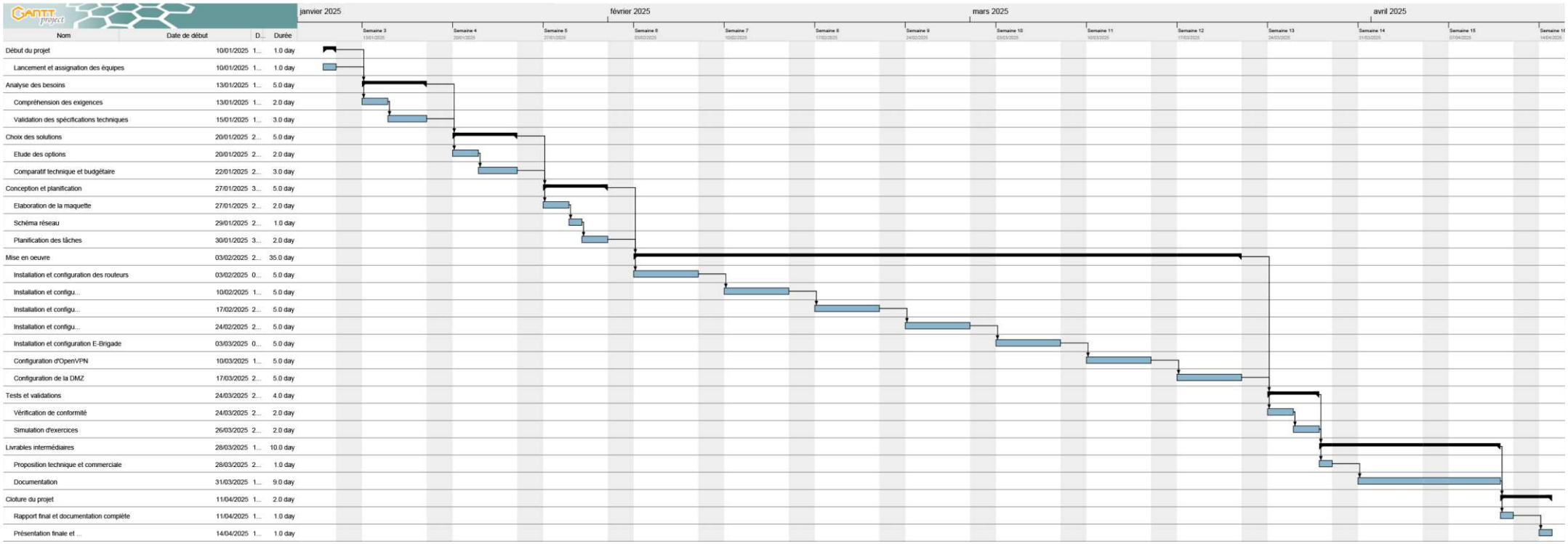
Devis valable jusqu'au: 10-03-2025

Total HT :		13 508,29€
TVA :	TVA 20% 10 176,29€	2 035,26€
	Exo. 3 332,00€	
Total TTC :		15 543,55€
Acomptes :		0,00€
Net à payer :		15 543,55€

Net à payer :quinze mille cinq cent quarante-trois euros et cinquante-cinq centimes

5) PLANNING

5.1) Planning prévisionnel



Nom	Date de début	D...	Durée
Début du projet	10/01/2025	1...	1.0 day
Lancement et assignation des équipes	10/01/2025	1...	1.0 day
Analyse des besoins	13/01/2025	1...	5.0 day
Compréhension des exigences	13/01/2025	1...	2.0 day
Validation des spécifications techniques	15/01/2025	1...	3.0 day
Choix des solutions	20/01/2025	2...	5.0 day
Etude des options	20/01/2025	2...	2.0 day
Comparatif technique et budgétaire	22/01/2025	2...	3.0 day
Conception et planification	27/01/2025	3...	5.0 day
Elaboration de la maquette	27/01/2025	2...	2.0 day
Schéma réseau	29/01/2025	2...	1.0 day
Planification des tâches	30/01/2025	3...	2.0 day
Mise en oeuvre	03/02/2025	2...	35.0 day
Installation et configuration des routeurs	03/02/2025	0...	5.0 day
Installation et configu...	10/02/2025	1...	5.0 day
Installation et configu...	17/02/2025	2...	5.0 day
Installation et configu...	24/02/2025	2...	5.0 day
Installation et configuration E-Brigade	03/03/2025	0...	5.0 day
Configuration d'OpenVPN	10/03/2025	1...	5.0 day
Configuration de la DMZ	17/03/2025	2...	5.0 day
Tests et validations	24/03/2025	2...	4.0 day
Vérification de conformité	24/03/2025	2...	2.0 day
Simulation d'exercices	26/03/2025	2...	2.0 day
Livrables intermédiaires	28/03/2025	1...	10.0 day
Proposition technique et commerciale	28/03/2025	2...	1.0 day
Documentation	31/03/2025	1...	9.0 day
Cloture du projet	11/04/2025	1...	2.0 day
Rapport final et documentation complète	11/04/2025	1...	1.0 day
Présentation finale et ...	14/04/2025	1...	1.0 day

5.2) Liste des taches prévisionnelles

Untitled Gantt Project 10 mars 2025

Tâches 2

Nom	Date de début	Date de fin	Durée
Début du projet	10/01/2025	10/01/2025	1
Lancement et assignation des équipes	10/01/2025	10/01/2025	1
Analyse des besoins	13/01/2025	17/01/2025	5
Compréhension des exigences	13/01/2025	14/01/2025	2
Validation des spécifications techniques	15/01/2025	17/01/2025	3
Choix des solutions	20/01/2025	24/01/2025	5
Etude des options	20/01/2025	21/01/2025	2
Comparatif technique et budgétaire	22/01/2025	24/01/2025	3
Conception et planification	27/01/2025	31/01/2025	5

Tâches

Nom	Date de début	Date de fin	Durée
Elaboration de la maquette	27/01/2025	28/01/2025	2
Schéma réseau	29/01/2025	29/01/2025	1
Planification des tâches	30/01/2025	31/01/2025	2
Mise en oeuvre	03/02/2025	21/03/2025	35
Installation et configuration des routeurs	03/02/2025	07/02/2025	5
Installation et configuration des serveurs AD et DHCP	10/02/2025	14/02/2025	5
Installation et configuration du service des mails	17/02/2025	21/02/2025	5
Installation et configuration de monitoring	24/02/2025	28/02/2025	5
Installation et configuration E-Brigade	03/03/2025	07/03/2025	5

Tâches

Nom	Date de début	Date de fin	Durée
Configuration d'OpenVPN	10/03/2025	14/03/2025	5
Configuration de la DMZ	17/03/2025	21/03/2025	5
Tests et validations	24/03/2025	27/03/2025	4
Vérification de conformité	24/03/2025	25/03/2025	2
Simulation d'exercices	26/03/2025	27/03/2025	2
Livrables intermédiaires	28/03/2025	10/04/2025	10
Proposition technique et commerciale	28/03/2025	28/03/2025	1
Documentation	31/03/2025	10/04/2025	9
Cloture du projet	11/04/2025	14/04/2025	2

Tâches

Nom	Date de début	Date de fin	Durée
Rapport final et documentation complète	11/04/2025	11/04/2025	1
Présentation finale et démonstration technique	14/04/2025	14/04/2025	1