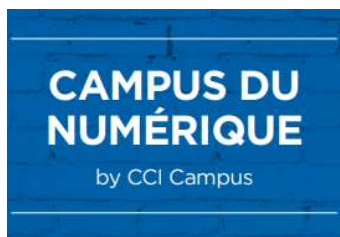


PROJET M2i



AP3

LIVRABLE 1

*Création d'un système d'information
hautement disponible et interconnecté*

PROPOSITION TECHNIQUE ET COMMERCIALE

Date limite de réponse : Dimanche 9 octobre 2022

Les résultats, opinions et recommandations exprimés dans ce rapport émanent de l'auteur ou des auteurs et n'engagent aucunement CCI Grand-Est ou CCI Campus

CONSIGNES

SOMMAIRE

1)	PRESENTATION DU GROUPE	3
	1.1) Composition et présentation	3
	1.2) Définitions des rôles et responsabilités	3
2)	RAPPEL DES BESOINS ET DES OBJECTIFS	3
	2.1) Rappel des besoins	3
	2.2) Objectifs	3
3)	SOLUTIONS	4
	3.1) Solutions techniques et logicielles	4
	3.2) Schéma réseau complet.....	5
	3.3) Tableau de synthèse.....	6
	3.4) Etude du choix de la solution VPN Site à Site.....	7
	3.5) Etude du choix de la solution de Portail Captif.....	9
5)	PLANNING	12
	5.1) Planning prévisionnel.....	12
	5.2) Liste des tâches prévisionnelles	13
	5.3) PERT prévisionnel	13

1) PRESENTATION DU GROUPE

1.1) Composition et présentation

Nom	Fonction / Rôles
FEVRE Dan	Chef de projet
HUBER Alexis	Technicien 1
YILMAZ Bünyamin	Technicien 2

1.2) Définitions des rôles et responsabilités

Le chef de projet s'occupe de la rédaction des livrables, schéma réseau et étude VPN et le GAANT.

Le technicien 1 s'occupe de l'étude du portail captif

Le technicien 2 s'occupe du budget, du tableau de synthèse

2) RAPPEL DES BESOINS ET DES OBJECTIFS

2.1) Rappel des besoins

- La CCI nous a sollicité pour la mise en place de 2 salles informatiques pour son nouveau cursus M2i à Strasbourg et Mulhouse.
- Chaque salle doit comporter 1 routeur/pare-feu, 2 serveurs redondés (AD, DHCP, DNS, DFS, DFS-R, RADIUS).
- La mise en place d'un VPN site à site (IPSEC avec protocole ESP) a également été demandé ainsi qu'un serveur de sauvegarde/NAS (ISCSI).

2.2) Objectifs

- Etude du projet et réponse au cahier des charges (planning, coûts...)
- La mise en œuvre d'une liaison WAN inter-sites chiffrée
- Harmoniser le plan d'adressage et de nommage sur l'ensemble des sites
- Création de serveurs et rôles/services suivants en haute disponibilité :
- Mise en œuvre d'un portail-captif avec authentification forte (Identification à l'AD via RADIUS)
- Accès aux données stockant les dossiers personnels des enseignants et des élèves à partir des 2 sites.

3) SOLUTIONS

3.1) Solutions techniques et logicielles

➤ LOT 1 : Routeurs/Pare-feu + VPN IPsec

Suite à l'étude du cahier des charges, nous avons décidé de mettre en place 2 Routeurs/Pare-feu l'un se situant à Strasbourg et l'autre à Mulhouse. Concernant les caractéristiques techniques, nous nous conformons à ce qui est demandé. Les deux routeurs/pare-feu seront des machines PfSense afin d'avoir l'ensemble des solutions sur les mêmes machines à savoir que le VPN IPsec peut aussi être mis sur une de ces machines ainsi que le portail captif du lot 4.

➤ LOT 2 : ADDS, DNS, DHCP, DFS, RADIUS + redondance (A+B)

Concernant les serveurs Windows nous avons choisis conformément au cahier des charges d'en mettre en place 2 par site. Ces serveurs seront donc redondés entre eux mais aussi intersites puisque dans l'éventualité où les 2 serveurs d'un site tombent il faut maintenir la disponibilité des ressources. Les rôles seront ADDS, DNS, DHCP, DFS, RADIUS sur l'ensemble des serveurs bien que l'on effectue une redondance via DFSR. Tous les serveurs seront évidemment des contrôleurs de domaine.

➤ LOT 3 : DFS et DFS Réplica + Serveurs de sauvegarde + SAN/iSCSI + Shadow Copy.

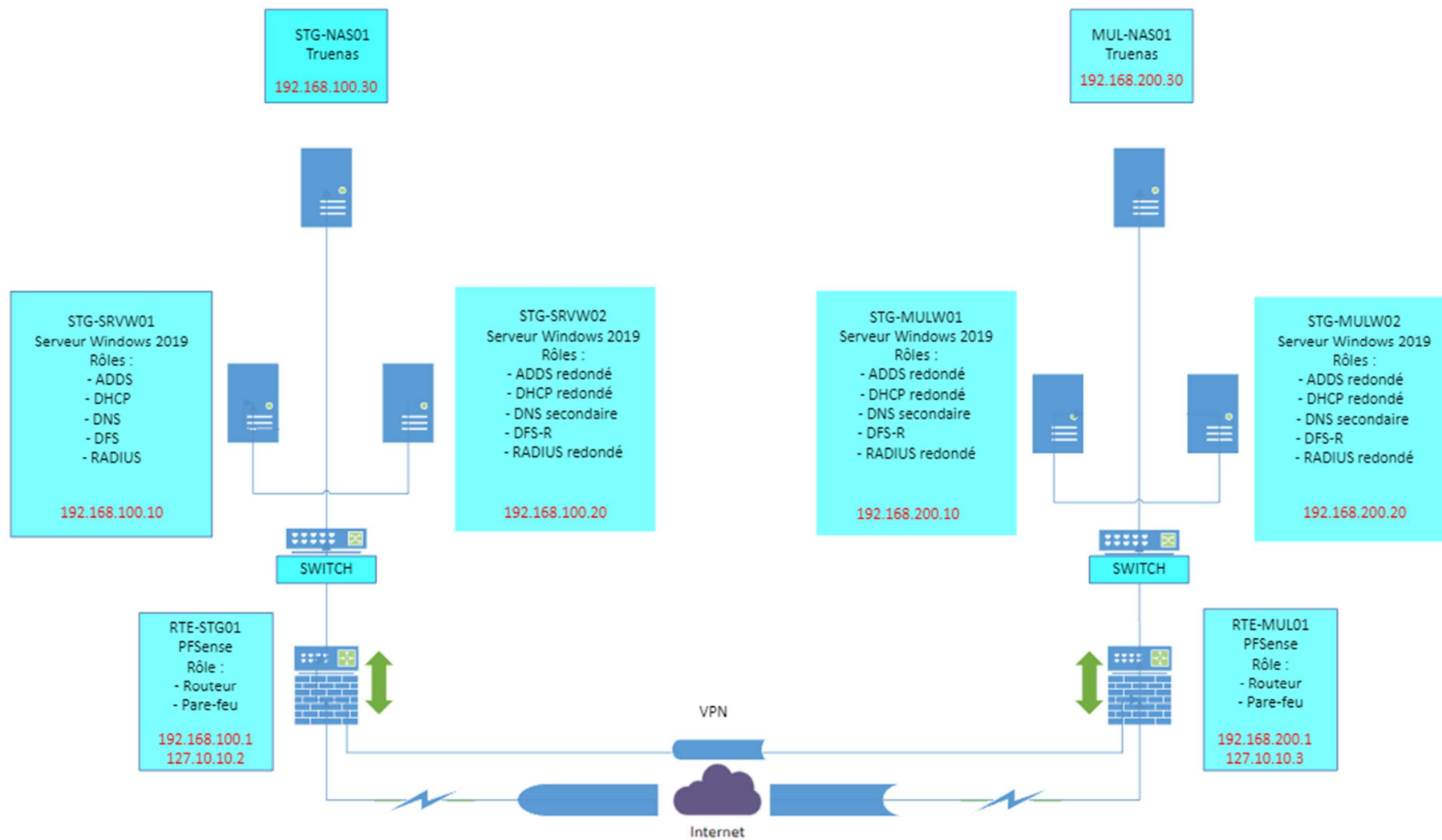
Le rôle DFS sera installé sur le serveur principal, avec mise en place d'un espace de noms et de réplication DFSR par la suite sur les autres serveurs Windows. Nous les promouvons aussi contrôleurs de domaine.

Pour ce qui se rapporte à la solution de sauvegarde, nous utiliserons TrueNAS

➤ LOT 4 : Portail Captif / Application des consignes de l'annexe 2

Nous avons choisi PfSense comme solution. C'est une solution complète qui intègre routeur, firewall et il est possible d'y intégrer une solution VPN. Malgré le fait que PfSense n'intègre pas de logs de connexion, nous avons choisi de le mettre en place avec une authentification forte via RADIUS et les identifiants utilisateur de l'AD.

3.2) Schéma réseau complet



3.3) Tableau de synthèse

Sites	Nom / Rôles	Adressage IP	Masque	Passerelle	DNS
A - Strasbourg	STG-SRVW01 : ADDS ; DHCP ; DNS ; DFS ; RADIUS	192.168.100.10	255.255.255.0	192.168.100.1	1:127.0.0.1 2:192.168.100.20
	STG-SRVW02 : ADDS redondé ; DHCP redondé ; DNS secondaire ; DFS-R ; RADIUS redondé	192.168.100.20	255.255.255.0	192.168.100.1	1:192.168.100.10 2:127.0.0.1
	STG-NAS01 : TrueNAS	192.168.100.30	255.255.255.0	192.168.100.1	1:192.168.100.10 2:192.168.100.20
	RTE-STG01 : Routeur ; Pare-feu	192.168.100.1 127.10.10.2	255.255.255.0	192.168.100.1	1:192.168.100.10 2:192.168.100.20
B - Mulhouse	STG-MULW01 : ADDS redondé ; DHCP redondé ; DNS secondaire ; DFS-R ; RADIUS redondé	192.168.200.10	255.255.255.0	192.168.200.1	1:127.0.0.1 2:192.168.200.20
	STG-MULW02 : ADDS redondé ; DHCP redondé ; DNS secondaire ; DFS-R ; RADIUS redondé	192.168.200.20	255.255.255.0	192.168.200.1	1:192.168.200.10 2:127.0.0.1
	MUL-NAS01 : TrueNAS	192.168.200.30	255.255.255.0	192.168.200.1	1:192.168.200.10 2:192.168.200.20
	RTE-MUL01 : Routeur ; Pare-feu	192.168.200.1 127.10.10.3	255.255.255.0	192.168.200.1	1:192.168.200.10 2:192.168.200.20

3.4) Etude du choix de la solution VPN Site à Site

Au moins 2 solutions techniques avec tableau comparatif (IPsec vs OpenVPN à minima)
Argumentation justifiée de la solution retenue

Synthèse des points forts et faibles des solutions proposées

IPsec

Probablement le protocole VPN le plus utilisé aujourd'hui, IPsec fit une première apparition dans les RFC numérotées de 1825 à 1829 parues lors de l'année 1995. Ce protocole prend directement en charge les trois composantes d'un VPN, à savoir : le transport, l'authentification et la sécurisation des données.

Tandis qu'il agit comme une couche supplémentaire dans IPv4, IPsec est partie intégrante de IPv6. Ceci ayant pour but de simplifier l'intégration de ce dernier au sein des futurs réseaux IP (pas de redirections de ports entre les routeurs d'une entreprise pour acheminer un tunnel correctement). IPsec est un protocole qui fonctionne sur l'espace noyau. Il s'exécute dans la couche IP du protocole internet et couvre tous les aspects de la sécurité. IPsec peut implémenter des VPN via deux modes :

- Le mode tunnel (mode par défaut).
- Le mode transport, qui sert à l'exécution d'une session avec un bureau à distance.

Il protège les données en chiffrant les paquets avant leur transmission sur un réseau et se soucie de l'intégrité des données : il vérifie que la transmission n'influence pas les paquets et ne les modifie pas.

IPsec est directement pris en charge par de nombreux systèmes d'exploitation modernes.

Les avantages d'IPsec :

- une protection solide pour un réseau.
- L'implémentation IPsec dans le pare-feu ne nécessite pas de modifier de logiciel sur les systèmes utilisateur ou serveur.
- IPsec est également préinstallé dans le système de l'utilisateur.

Inconvénients de IPsec

- Nécessite une configuration complexe.
- Dur à debugger en cas de dysfonctionnement ou indisponibilité.

OpenVPN

OpenVPN est un protocole rapide, sûr et stable utilisable avec un navigateur Web standard.

Il peut utiliser le port de son choix (qu'il soit UDP ou TCP)

Il s'exécute dans la mémoire réservée aux applications et non dans le noyau.

OpenVPN nécessite un logiciel supplémentaire que le système d'exploitation (OS) n'a généralement pas installé par défaut.

OpenVPN utilise un port UDP ou TCP choisi.













Les avantages d'OpenVPN

- Rend difficile la prise de contrôle des informations. (Clés de chiffrement 256 bits et chiffrements haut de gamme)
- Utilisation de n'importe quel port sur TCP ou UDP.
- S'il se déconnecte, il interrompra le réseau jusqu'à ce que la connexion puisse être réparée ou

reconfigurée ou ne maintenir que le trafic interne de l'entreprise.

Les inconvénients d'OpenVPN

- Nécessite une configuration complexe.
- Préinstallé sur aucun système d'exploitation, il nécessite donc la configuration de logiciels tiers.

	IPsec	OpenVPN
Authentification par mot de passe		
Autorisation par certificat		
Authentification par serveur (par exemple, LDAP, RADIUS, etc.)		
Facilité de l'installation		
Prise en charge de différents protocoles de transmission		
Préinstallé dans le système de l'utilisateur		

3.5) Etude du choix de la solution de Portail Captif

Concernant l'étude de choix de Portail Captif, nous allons retenir deux solutions :

PfSense :

PfSense qui est une solution open sources simple à mettre en place car tout se passe via une interface web.

Il est aussi possible de mettre en place le pare-feu ainsi que le routeur sur la même machine PfSense, de ce fait le coût de revient est moindre car une seule machine regroupe l'ensemble des rôles.

Nous pouvons tout à fait utiliser RADIUS afin de faire une authentification forte avec les identifiants de l'AD

Le VPN peut-être mise en place en point à point via PfSense

Cependant, cette solution n'est pas conforme au RGPD car nous n'avons pas de logs concernant les utilisateurs connectés au VPN

Alcasar :

Alcasar est l'autre solution que nous avons étudiée. C'est une solution bien plus complète et complexe à mettre en œuvre.















Il regroupe toutes les fonctionnalités sur une seule machine, routeur, pare-feu, VPN mais qui fonctionne sous linux.

Nous pouvons tout à fait mettre en place RADIUS et l'authentification forte via l'AD

Filtrage web avec accès aux données utilisateurs concernant les sites via des listes noires et blanches par utilisateurs ou groupe.

Conforme aux directives européennes sur la conservation et la communication des données permettant d'identifier toutes personnes ayant contribué à la communication d'un contenu mis en ligne.

En revanche, la difficulté de sa mise en œuvre et le fait que Alcasar fonctionne sous Linux nous ont fait pencher sur la solution PfSense qui sera plus simple à mettre en œuvre bien que non conforme dans un cadre professionnel en terme de RGPD.

	ALCASAR	PFSENSE
Authentification Forte		
Routeur, Pare-feu VPN, Portail captif sur la même machine		
Solution Gratuite		
Conforme RGPD		
Difficultés de mise en œuvre		
Filtrage des données WEB		
Conforme aux directives européennes sur la conservation et la communication des données permettant d'identifier toutes personnes ayant contribué à la communication d'un contenu mis en ligne		

4) BUDGET

(Devis et/ou un tableau complet reprenant les différentes ressources (humaines, financières, matérielles) nécessaires à la réalisation de votre projet et le coût global s'approchant du réel).

Dans un but pédagogique, il est demandé 2 versions :

- L'une en « Interne », coût du projet
- L'une en « externe » prix de vente (prévoir la TVA à 20% et une marge commerciale selon le budget fixé par le client)

DEVIS Interne – COUTS MATERIAUX + MAIN D'OEUVRE

Date d'émission : 12/09/2022

Quantité	Description	Réduction	Prix Unitaire HT	Prix HT
4	Serveur Dell PowerEdge T140 (5JV1T) Intel Xeon E-2224G, 16 Go, 1 To, Graveur DVD - <i>Serveur AD</i>	-	879,95€	3 519,80€
2	Serveur Dell PowerEdge T150 (M83C9) Intel Xeon E-2314, 8 Go, 1 To - <i>Serveur PfSense / VPN</i>	-	1 023,95€	2 047,90€
2	Serveur Dell PowerEdge T150 (M83C9) Intel Xeon E-2314, 8 Go, 1 To - <i>Serveur Sauvegarde TrueNas</i>	-	1 023,95€	2 047,90€
2	Onduleur APC Back-UPS Pro 1500VA – 6 Prises - Onduleur STR - Onduleur MLS	-	367,96€	735,92€
2	Switch Cisco CBS110-24T 22 ports 10/100/1000 Mbps + 2 ports combo Ethernet Gigabit/SFP	-	191,15€	382,30€
4	Licence Microsoft Windows Server Standard 2019 (16 Coeurs) 64 Bits	-	799,96€	3199,84€
8	Iiyama ProLite T2252MSC-B1 - Écran LED - 22" 1920 x 1080 Full HD - 60 Hz	-	247,99€	1 983,92€
8	Clavier HP K1500	-	21,58€	172,64€
8	Souris filaire HP X900	-	3,19€	25,52€
1	Contrat de maintenance Durée : 1an (24h24 7j/7)	-		
80	Main d'œuvre pour réalisation	-	119,99€	9 599,20€
TOTAL HT			23 714,94 €	
TVA 20%			4 742,99 €	
Total TTC				28 457,93 €
Net à payer				28 457,93 €

Livrables réalisés conformément au cahier des charges.

Signature du représentant de l'agence :
Lu et accepté

Signature de M. Beteta :
Lu et accepté

Signature de M. Klein :
Lu et accepté

DEVIS Interne – COUTS PC + LICENCES

Date d'émission : 15/09/2022

Quantité	Description	Réduction	Prix Unitaire HT	Prix HT
60	Ecran HP 22" LED - VH22 (X0N05AA) 1920x1080 px - 5 ms - VGA/DVI-D/DisplayPort	-	111,20€	6 672,00€
90	HP ProBook 450 G8 - Windows 10 Famille 64 bits, 15,6 HD, i3, 8 Go, 256 Go SSD	-	480,00€	43 200,00€
		-		
		-		
TOTAL HT			49 872,00 €	
TVA 20%			9 974,40 €	
Total TTC				59 846,40 €
Net à payer				59 846,40 €

Livrables réalisés conformément au cahier des charges.

Signature du représentant de l'agence :
Lu et accepté

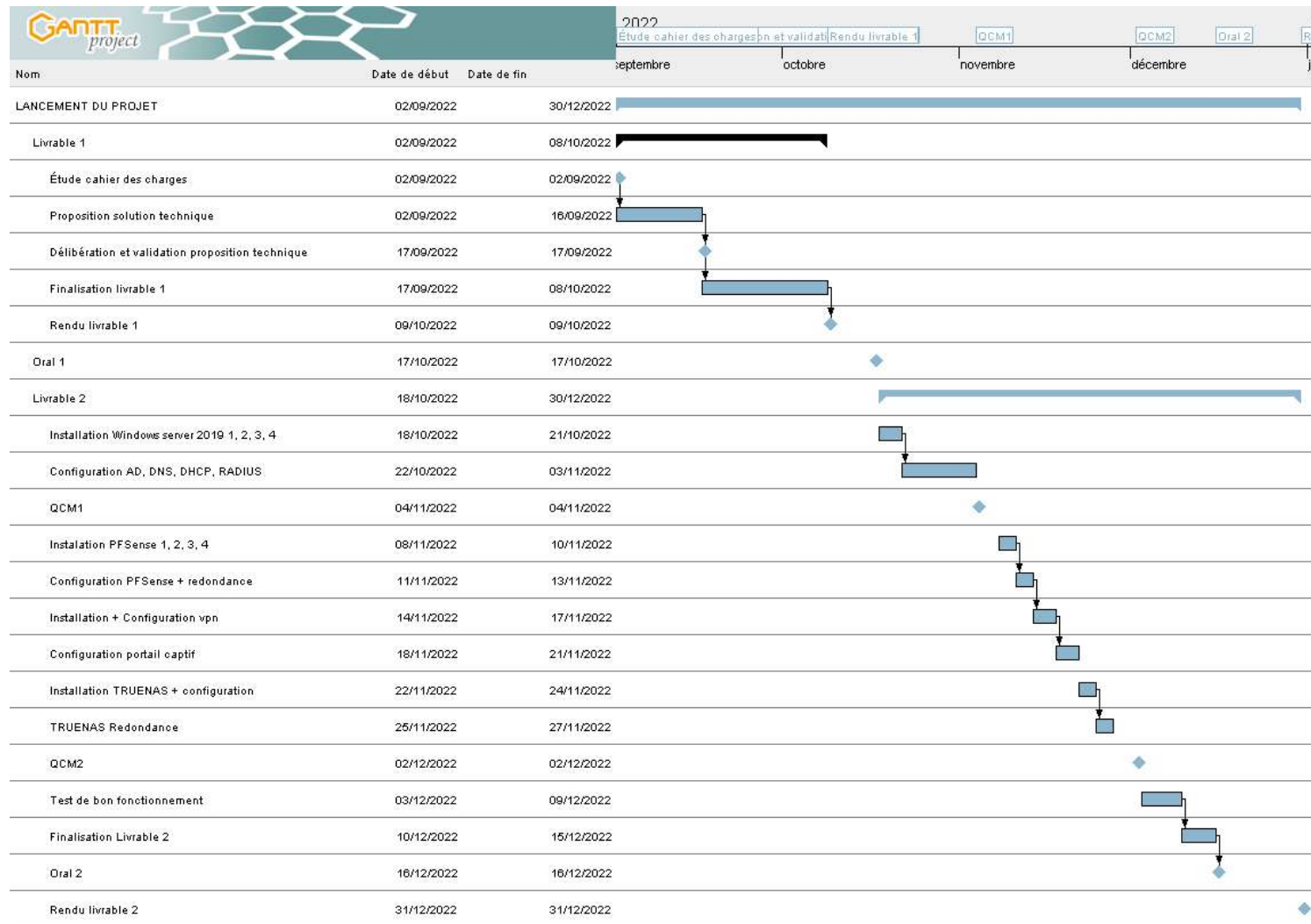
Signature de M. Beteta :
Lu et accepté

Signature de M. Klein :
Lu et accepté

Devis Interne – Cout des matériaux et main d'œuvre	28 457,93 €	
Devis Externe – Cout des PC et licences	59 846,40 €	
Total TTC		88 304,33 €
Net à payer		88 304,33 €

5) PLANNING

5.1) Planning prévisionnel



5.2) Liste des tâches prévisionnelles

Mettre en lumière les objectifs intermédiaires (jalons)

Jalons	Date
Étude cahier des charges	02/09/2022
Délibération et validation proposition technique	17/09/2022
Rendu livrable 1	09/10/2022
Oral 1	17/10/2022
QCM1	04/11/2022
QCM2	02/12/2022
Oral 2	16/12/2022
Rendu livrable 2	31/12/2022

Tâches

Nom	Date de début	Date de fin
LANCEMENT DU PROJET	02/09/2022	30/12/2022
Livrable 1	02/09/2022	08/10/2022
Étude cahier des charges	02/09/2022	02/09/2022
Proposition solution technique	02/09/2022	16/09/2022
Délibération et validation proposition technique	17/09/2022	17/09/2022
Finalisation livrable 1	17/09/2022	08/10/2022
Rendu livrable 1	09/10/2022	09/10/2022
Oral 1	17/10/2022	17/10/2022
Livrable 2	18/10/2022	30/12/2022
Installation Windows server 2019 1, 2, 3, 4	18/10/2022	21/10/2022
Configuration AD, DNS, DHCP, RADIUS	22/10/2022	03/11/2022
QCM1	04/11/2022	04/11/2022
Installation PFSense 1, 2, 3, 4	08/11/2022	10/11/2022
Configuration PFSense + redondance	11/11/2022	13/11/2022
Installation + Configuration vpn	14/11/2022	17/11/2022
Configuration portail captif	18/11/2022	21/11/2022
Installation TRUENAS + configuration	22/11/2022	24/11/2022
TRUENAS Redondance	25/11/2022	27/11/2022
QCM2	02/12/2022	02/12/2022
Test de bon fonctionnement	03/12/2022	09/12/2022
Finalisation Livrable 2	10/12/2022	15/12/2022
Oral 2	16/12/2022	16/12/2022
Rendu livrable 2	31/12/2022	31/12/2022

5.3) PERT prévisionnel

