

Projet NUMSCH
-
BTS SIO 2023 Option SISR



Epreuve E5
-
Situation professionnelle 1

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 : 1
Nom, prénom : FEVRE Dan		N° candidat : 02243995903
Épreuve ponctuelle <input type="checkbox"/>	Contrôle en cours de formation <input checked="" type="checkbox"/>	Date : 26/04/2023
Organisation support de la réalisation professionnelle L'entreprise NUMSCH nous a sollicité pour la mise en place de 2 salles informatiques pour son nouveau club d'échecs connecté. L'infrastructure devra intégrer un portail captif avec une authentification radius, un VPN et une redondance des serveurs, des fichiers.		
Intitulé de la réalisation professionnelle Projet NUMSCH		
Période de réalisation : 14/09/2021 au 31/12/2021 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) 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).		
Description des ressources documentaires, matérielles et logicielles utilisées² 2 Windows Server 2019 / 2 Windows Server CORE 2019 / 2 routeurs, Pare-feux Pfsense / 2 serveurs TrueNAS		
Modalités d'accès aux productions³ et à leur documentation⁴ Sur le site https://fevredan.wordpress.com , dans le menu, cliquez sur « Situations Professionnelles », une description et un lien git hub est disponible pour accéder à la documentation du projet.		
BTS SERVICES INFORMATIQUES AUX ORGANISATIONS		SESSION 2023
Épreuve E5 - Administration des systèmes et des réseaux (option SISR)		

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.

**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

Éléments voulus énumérés ci-dessous

PROJET MUNSCH

Table des matières

1) Introduction.....	5
2) Rappel des besoins	5
3) SOLUTIONS	5
3.1) Solutions techniques et logicielles.....	5
3.2) Schéma réseau complet.....	7
3.3) Tableau de synthèse	8
3.4) Etude du choix de la solution VPN Site à Site.....	9
3.5) Etude du choix de la solution de Portail Captif.....	11
5) PLANNING	15
5.1) Planning prévisionnel	15
5.2) Liste des tâches prévisionnelles	16
.....	16
5.3) PERT prévisionnel	17

PROJET MUNSCH

1) Introduction

L'entreprise NUMSCH a sollicité la mise en place de deux salles informatiques pour son nouveau club d'échecs connecté à Strasbourg et Mulhouse. Pour répondre aux besoins du club et de ses membres, il est nécessaire de fournir une infrastructure informatique hautement disponible, avec une connexion inter-sites et des services tels que l'authentification forte, le portail captif pour les accès visiteurs, un tunnel VPN, la redondance, et la mise en place d'un système de sauvegarde/NAS (ISCSI) entre les deux sites. Pour assurer la supervision technique de ce projet, Dan FEVRE, spécialiste de la mise en service et de la sécurité de l'infrastructure système et membre du club des passionnés d'échecs, aura la charge de la mise en place des salles informatiques.

2) Rappel des besoins

- 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

À la suite de 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 installer sur le serveur principal, avec mise en place d'un espace de noms et de réplication DFSR par la suite sur les autres serveur Windows. Nous les promouvons aussi contrôleurs de domaine.

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

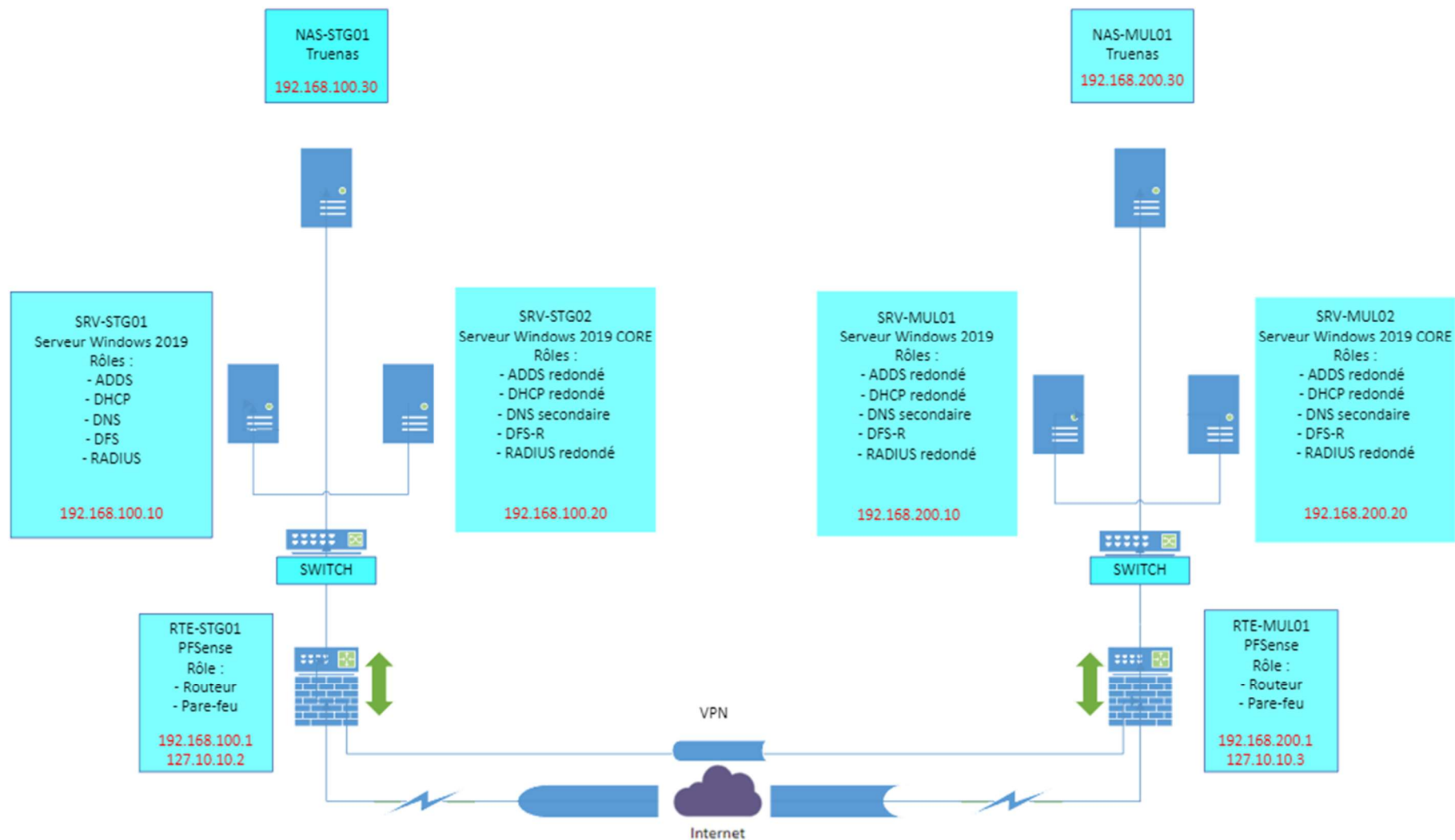
TrueNAS est un système d'exploitation basé sur FreeBSD. Nous l'utilisons en tant que serveur de stockage en réseaux NAS. Il supporte plusieurs protocole comme le FTP, NFS, rsync, iSCSI... Nous pouvons aussi faire du raid logiciel selon les variantes.

➤ 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 choisis de le mettre en place avec une authentification forte via RADIUS et les identifiants utilisateur de l'AD.

PROJET MUNSCHE

3.2) Schéma réseau complet



3.3) Tableau de synthèse

Sites	Nom / Rôles	Adressage IP	Masque	Passerelle	DNS
A - Strasbourg	SRV-STG01 : 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
	SRV-STG02 : 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
	NAS-STG01 : 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	SRV-MUL01 : 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
	SRV-MUL02 : 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
	NAS-MUL01 : 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		

PROJET MUNSCH

3.5) Etude du choix de la solution de Portail Captif

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

PfSense :

PfSense qui est une solution open source simple à mettre en place car tout se passe via une interface web, l'installation peut tout aussi bien se faire sous UNIX.

Il est aussi possible de mettre en place le pare-feu, ainsi que le routeur sur la même machine.

De ce fait le coût de revient est moindre car une seule machine regroupe l'ensemble des rôles.

Nous pouvons tout à fait utiliser le protocole RADIUS lié avec un annuaire LDAP afin de faire une authentification forte avec les identifiants de l'Active Directory.

Le VPN peut-être mise en place en point à point ou en distant via l'interface web.

Cependant, cette solution n'est pas conforme au RGPD car nous n'avons pas de logs concernant les tâches // recherches que les utilisateurs effectuent avec le VPN.

Pour la mise en conformité avec la RGPD il faudrait ajouter un module externe nommé Squid Guard qui lui permet d'identifier les logs utilisateurs avec les sites visités depuis le VPN.

L'authentification se ferait via le protocole RADIUS et un annuaire LDAP.

Nous avons cependant des logs concernant l'authentification au portail captif comme ci-dessous :

The screenshot shows the pfSense web interface. At the top, there's a navigation bar with 'System', 'Status', and 'Help' menus. Below it, the breadcrumb trail is 'Status / Captive Portal / PORTAIL'. A table titled 'Users Logged In (1)' shows one user with IP 192.168.2.103, username 'test', and session start time 06/04/2019 13:01:33. Below the table are buttons for 'Show Last Activity' and 'Disconnect All Users'. The main content area displays a 'Squid rapport d'accès utilisateur' for user 'bubu (?)' on 02 Oct 2018. It shows a total of 499 033 connections. A table lists the top accessed sites with columns for rank, site, connections, octets, and percentage.

#	Site(s) Accédé(s)	Connexion(s)	Octets	Somme	%
1	www.pc2s.fr:443	52 379 509	379 509	76.0%	
2	fonts.gstatic.com:443	1 33 675	413 184	6.7%	
3	safebrowsing.googleapis.com:443	1 15 922	429 106	3.1%	
4	tiles.services.mozilla.com:443	4 8 403	437 509	1.6%	
5	search.services.mozilla.com:443	2 6 341	443 850	1.2%	
6	snippets.cdn.mozilla.net:443	1 5 336	449 186	1.0%	
7	ocsp.pki.goog	6 4 974	454 160	0.9%	
8	id.google.fr:443	1 4 569	458 729	0.9%	
9	adservice.google.fr:443	1 4 405	463 134	0.8%	
10	activity-stream-icons.services.mozilla.com:443	1 4 345	467 479	0.8%	
11	www.gstatic.com:443	1 3 808	471 287	0.7%	
12	shavar.services.mozilla.com:443	1 3 687	474 974	0.7%	
13	ssl.gstatic.com:443	1 3 678	478 652	0.7%	
14	incoming.telemetry.mozilla.org:443	1 3 641	482 293	0.7%	
15	www.google-analytics.com:443	1 3 234	485 527	0.6%	
16	apis.google.com:443	1 3 063	488 590	0.6%	
17	ocsp.digicert.com	3 2 736	491 326	0.5%	
18	www.google.com:443	1 2 705	494 031	0.5%	
19	detectportal.firefox.com	5 2 420	496 451	0.4%	
20	192.168.0.1	2 1 569	498 020	0.3%	
21	ocsp.int-x3.letsencrypt.org	1 1 013	499 033	0.2%	
22	172.217.19.138:443	2 0	499 033	0.0%	

Alcasar :

Alcasar est l'autre solution que nous avons étudiée. C'est une solution bien plus complète et complexe à mettre en œuvre qui peut se configurer entièrement via une interface web. 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.

Alcasar dispose d'une traçabilité des données utilisateurs concernant les sites par utilisateurs ou groupe avec des flux Netflow, des journaux du pare-feu et du couple radius/mariaDB















Filtrage de domaine, d'URL, d'adresses IP, de malwares et de protocoles réseau réalisable avec un parefeu Netfilter et le coupe HAVP, (HTTP Anti Virus Proxy) Libclamav, 4 instances de DNSmasq et Dansguardian (Filtrage + contrôle parental)

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 on 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.

L'authentification se ferait via le protocole RADIUS relié à l'Active Directory.

Module supplémentaire : Ces modules ont pour objectif d'améliorer la sécurité globale du portail (anti-contournement, anti-usurpation MAC/IP, chiffrement des fichiers journaux, gestion des certificats, IDS, etc.) ou d'enrichir les possibilités du portail (installation, mise à jour, by-pass, Archivage, accélération de la consultation, cron, etc.).

	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
accepté

Signature de M. Beteta :
Lu et accepté

Signature de M. Klein :
Lu et

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€
90	Licence CAL 1/User	-	40,00€	4500,00€
90	Licence CAL 1/Device	-	32,00€	3600,00€
TOTAL HT			54 357,12 €	
TVA 20%			13 589,28 €	
Total TTC				67 946,40 €
Net à payer				67 946,40 €

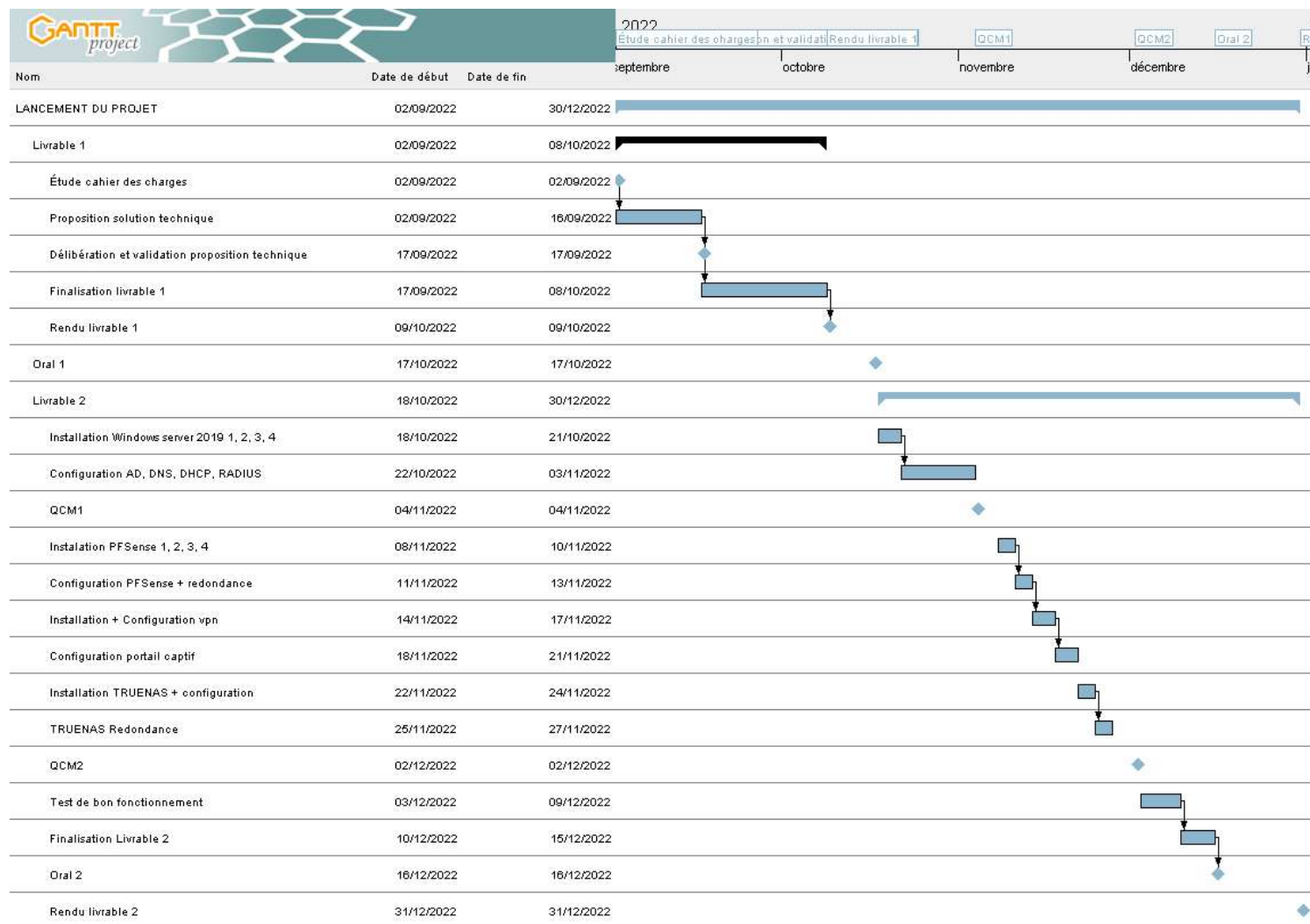
Livrables réalisés conformément au cahier des charges.

Signature du représentant de l'agence :
Lu et accepté
acceptéSignature de M. Beteta :
Lu et acceptéSignature de M. Klein :
Lu et

Devis Interne – Cout des matériaux et main d'œuvre	28 457,93 €	
Devis Externe – Cout des PC et licences	67 946,40 €	
Total TTC		96 404,33€
Net à payer		96 404,33€

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

