BTSSIO.

Atelier de Professionnalisation 4

AP4

LIVRABLE 1

PROPOSITION TECHNIQUE ET COMMERCIALE

Date limite de réponse : 8 AVRIL 2025

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

AP4 GROUPE 2

LIVRABLE 1 MEZZAROBBA Nathan

RICHTER Paul

Table des matières

PRESENTATION DU GROUPE

Composition et présentation

c

Bonjour je m'appelle RICHTER Paul, actuellement en BTS SIO SISR à la CCI et à l'UIMM, et en alternance dans le groupe Elypse-Autos. Je serai dans ce projet le 'Responsable Infrastructure et Réseaux' de l'entreprise plug&pray.

Bonjour je suis MEZZAROBBA Nathan. Je suis alternant dans la société Alsace Informatique situé à Illzach et étudiant chez CCI Campus à Mulhouse. Je suis 'Responsable Sécurité et Applications' de projet dans l'entreprise plug&pray.

Définitions des rôles et responsabilités

Dans le cadre du projet AP4 - Sécurité Civile, nous avons réparti les tâches de manière équitable afin d'assurer une gestion efficace et une bonne coordination de l'ensemble des étapes du projet. Chaque membre du groupe assume des responsabilités spécifiques tout en collaborant sur les parties transversales.

Responsable Infrastructure et Réseaux – RICHTER Paul

Missions :

- **Conception de l'architecture réseau** : Création du schéma réseau complet.
- **Mise en place des connexions distantes** : Configuration de la solution VPN pour garantir un accès sécurisé aux ressources.
- **Installation et configuration des serveurs** : Déploiement des serveurs Windows avec Active Directory et mise en place des services associés.
- **Supervision et monitoring** : Mise en place d'un outil de supervision permettant de surveiller l'état des infrastructures et d'envoyer des alertes en cas de dysfonctionnement.

Responsable Sécurité et Applications – MEZZAROBBA Nathan

Missions :

- **Sécurisation des accès** : Mise en œuvre des stratégies de sécurité, incluant les règles de pare-feu et les politiques d'accès utilisateurs.
- **Déploiement du logiciel métier** : Installation et configuration du logiciel eBrigade, permettant la gestion des interventions et des personnels.
- **Mise en place d'une messagerie électronique** : Déploiement et configuration d'un serveur de messagerie.
- **Tests et validation** : Vérification du bon fonctionnement des services mis en place et documentation des tests réalisés.

Tâches communes et collaboration

Certaines tâches nécessitent une collaboration étroite entre les deux membres de l'équipe :

- **Rédaction de la documentation technique** : Chaque membre est responsable de documenter ses propres tâches, avec une relecture croisée pour assurer la qualité.
- **Planification et gestion du projet** : Élaboration du **diagramme de Gantt**, suivi de l'avancement et ajustements si nécessaire.

RAPPEL DES BESOINS ET DES OBJECTIFS

Rappel du projet

Les Centres Opérationnels Départementaux jouent un rôle central dans la gestion des crises et des interventions d'urgence en assurant la coordination des acteurs et la continuité des services critiques. Dans ce cadre, l'infrastructure informatique doit être sécurisée, performante et accessible en toutes circonstances.

Le projet est mené pour le compte de la Sécurité Civile, un service interministériel en charge de la protection des populations et de la gestion des situations de crise. Son objectif est d'optimiser la résilience des infrastructures informatiques en garantissant la continuité des services des Centres Opérationnels Départementaux, la sécurisation des échanges et l'accessibilité des ressources aux agents sur le terrain.

Les besoins exprimés concernent plusieurs domaines essentiels de l'infrastructure informatique. Il s'agit de centraliser la gestion des accès, sécuriser les flux et les données, permettre un accès distant fiable, assurer une communication efficace et optimiser la gestion des interventions. La mise en œuvre de ces améliorations doit s'adapter aux contraintes opérationnelles et garantir une utilisation fluide et intuitive pour les agents.

Rappel des besoins

La gestion des accès doit être centralisée afin de sécuriser l'authentification des utilisateurs, attribuer des permissions adaptées selon les rôles et assurer une traçabilité complète des connexions. Une redondance des services d'authentification est nécessaire pour éviter toute interruption. Un contrôleur de domaine permettra d'assurer cette gestion.

La protection du réseau exige un filtrage rigoureux des accès, une surveillance en temps réel des menaces et une isolation des services critiques. La détection et la prévention des

cyberattaques doivent être assurées pour garantir la disponibilité et l'intégrité des systèmes. L'installation d'un pare-feu avec des règles de filtrage et un système de supervision permettra de répondre à ces exigences.

L'accès distant doit être sécurisé avec une authentification stricte et un chiffrement des communications pour les agents sur le terrain. Il est essentiel de contrôler les sessions actives et d'enregistrer les connexions pour assurer une utilisation conforme et sécurisée des ressources internes. Un système de VPN garantira une connexion sécurisée aux ressources internes depuis l'extérieur.

La communication interne et externe doit être protégée contre les cybermenaces, garantir une disponibilité continue et assurer la confidentialité des échanges. Une gestion efficace des courriers électroniques avec un filtrage anti-phishing et un archivage sécurisé est nécessaire. La mise en place d'un serveur de messagerie sécurisé assurera un échange fiable et protégé des informations.

La gestion des interventions doit permettre un suivi en temps réel des opérations, une coordination fluide des équipes et une optimisation des ressources disponibles. L'historisation des décisions et des comptes rendus doit faciliter l'amélioration continue des processus et la traçabilité des actions menées. Un logiciel de gestion des interventions centralisera ces informations et assurera leur accessibilité aux personnes autorisées.

Une zone démilitarisée (DMZ) est nécessaire pour isoler le logiciel de gestion des interventions qui est accessibles depuis l'extérieur. Cette séparation protège les ressources internes tout en permettant aux utilisateurs externes d'accéder au service. L'implémentation d'une DMZ avec des règles de pare-feu adaptées garantira la sécurisation des services exposés.

SOLUTIONS

Contrôleur de domaine

Un contrôleur de domaine est une solution utilisée pour centraliser la gestion des utilisateurs, des machines et des ressources. Il permet également de sécuriser et de contrôler les accès en appliquant des politiques réseaux uniformes. Deux solutions populaires sont Active Directory Domain Services (ADDS), développé par Microsoft, et OpenLDAP, une alternative open-source.

Active Directory Domain Services (ADDS)

ADDS est la solution propriétaire de Microsoft pour gérer les domaines dans un environnement Windows. Il fonctionne comme un annuaire hiérarchique qui permet de structurer les utilisateurs, les groupes et les ressources en différentes unités organisationnelles (OU). Il offre une administration simplifiée via une interface graphique intuitive, une gestion centralisée avec LDAP et Kerberos, et l'application des politiques réseau (GPO).

OpenLDAP

OpenLDAP est une implémentation open-source du protocole LDAP, conçue pour gérer des annuaires dans un réseau. Contrairement à ADDS, il n'est pas limité à Windows et peut être installé sur des systèmes Linux, UNIX, et même Windows avec des adaptations. Il se concentre principalement sur l'authentification et la gestion des ressources, avec une grande flexibilité pour s'intégrer à d'autres services. Cependant il demande des compétences avancées pour sa configuration et son administration.

Comparaison

Critères	ADDS	OpenLDAP
Coût	Payant, licences nécessaires	Gratuit
Installation	Simple, orientée Windows	Plus complexe
Administration	Interface graphique (GUI) intuitive	Complexe en ligne de commande (CLI) ou outils tiers
Compatibilité	Uniquement Windows	Multi-plateforme

Support	Support officiel de Microsoft.	Support communautaire, parfois limité.
Sécurité	Intégrée avec des protocoles comme Kerberos et GPO.	Dépend des configurations et modules tiers.
Fonctionnalités	Gestion centralisée avec GPO, intégration DNS, Kerberos.	Pur LDAP sans fonctionnalités étendues natives.

Notre choix

Nous avons choisi ADDS (Active Directory Domain Services) comme solution pour la gestion du contrôleur de domaine. Ce choix repose sur plusieurs arguments clés : sa facilité d'utilisation dans un environnement Windows, son intégration native avec des outils comme les GPO, et son support étendu. ADDS permet une gestion centralisée efficace et sécurisée, tout en offrant une documentation officielle et des mises à jour régulières par Microsoft.

Le pare-feu

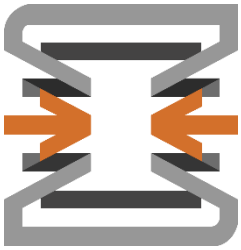
Un pare-feu (ou firewall) est un dispositif de sécurité réseau qui surveille et contrôle le trafic entrant et sortant d'un réseau informatique en fonction de règles prédéfinies. Il agit comme une barrière entre un réseau interne sécurisé et des réseaux externes non sécurisés, tels qu'Internet. Le pare-feu est essentiel pour protéger les données sensibles des attaques malveillantes, en bloquant les accès non autorisés tout en permettant des communications légitimes.

PFsense

PFsense est une solution open-source basée sur FreeBSD qui combine les fonctionnalités de pare-feu et de routeur. Elle est particulièrement appréciée pour sa fiabilité, sa robustesse et sa flexibilité. PFsense dispose d'une interface web intuitive permettant de configurer facilement des règles de sécurité, de routage, et des fonctionnalités avancées comme la gestion de VPN, la QoS (gestion de la bande passante), et la détection d'intrusion via IDS/IPS

C'est une solution polyvalente adaptée aux petites comme aux grandes infrastructures, offrant un large éventail de plugins et de fonctionnalités pour répondre à divers besoins de sécurité réseau.

OPNsense



OPNsense est également une solution open-source basée sur FreeBSD, qui reprend de nombreuses fonctionnalités de PFsense tout en améliorant l'interface utilisateur et en proposant des mises à jour plus régulières. OPNsense est apprécié pour son ergonomie moderne et ses outils de gestion simplifiés, rendant la configuration plus accessible.

Elle offre des fonctionnalités similaires : pare-feu, routage, VPN, QoS, et détection d'intrusion, mais se distingue par des options avancées pour le monitoring et un système de gestion des extensions intuitif.

Comparaison

Critères	PFsense	OPNsense
Prix	Gratuit (open-source)	Gratuit (open-source)
Plateformes supportées	Basé sur FreeBSD	Basé sur FreeBSD
Simplicité d'installation	Facile, installation intuitive	Facile, avec un assistant plus moderne
Administration	Interface web intuitive mais classique	Interface web moderne et plus ergonomique
Fonctionnalités de base	Pare-feu, routage, VPN	Pare-feu, routage, VPN
Fonctionnalités avancées	QoS, IDS/IPS, haute disponibilité	QoS, IDS/IPS, haute disponibilité
Extensions et plugins	Large choix (Snort, Squid, etc.)	Large choix, gestion simplifiée
Sécurité intégrée	Sécurisé avec IDS/IPS (Snort ou Suricata)	Sécurisé avec IDS/IPS intégré (Suricata)
Mises à jour	Moins fréquentes que OPNsense	Fréquentes et avec de meilleures corrections
Communauté et support	Communauté active et bien établie	Communauté active et réactive
Adapté pour	Petites à grandes infrastructures	Petites à grandes infrastructures

Notre choix

Nous avons choisi PFsense car c'est une solution fiable et simple à utiliser, avec une interface claire pour configurer le pare-feu et les VPN. Nous avons l'habitude de l'utiliser et il permet de répondre aux besoins du projet, comme sécuriser les connexions des agents à distance, tout en étant gratuit.

Le VPN

Le VPN (Virtual Private Network) est un outil essentiel pour sécuriser les connexions à distance, permettant aux utilisateurs d'accéder aux ressources du réseau local tout en garantissant la confidentialité des données échangées. Deux solutions principales ont été analysées : OpenVPN et IPsec VPN.

OpenVPN

OpenVPN est une solution open-source utilisant les protocoles SSL/TLS pour établir des tunnels sécurisés. Réputée pour sa simplicité de configuration et sa compatibilité avec de nombreux environnements, elle est idéale pour sécuriser les accès distants et les connexions site-à-site.

IPsec VPN

IPsec VPN est un protocole standard pour établir des connexions sécurisées. Intégré dans PfSense, il offre une solution robuste pour les communications réseau, notamment pour des connexions site-à-site.

Comparaison

Critères	OpenVPN	IPsec VPN
Coût	Gratuit, open-source	Gratuit, intégré à PfSense
Facilité de configuration	Très simple, avec une interface intuitive sur PfSense.	Plus complexe, nécessite une configuration minutieuse.
Gestion des certificats	Intégrée nativement via SSL/TLS (certificats, clés partagées).	Non intégrée, nécessite des outils externes pour la gestion des certificats.
Support accès distant	Idéal pour les connexions ponctuelles et multi-utilisateurs	Moins flexible pour un usage mixte (site-à-site et accès distant).

Flexibilité	Très adaptable aux besoins variés et aux réseaux hétérogènes.	Principalement adapté aux connexions fixes et homogènes
Chiffrement des données	Hautement configurable grâce à SSL/TLS.	Offre un chiffrement robuste avec AES/3DES.
Flexibilité d'accès	Convient parfaitement à des environnements mobiles et des utilisateurs nomades.	Principalement conçu pour des connexions fixes.

Notre choix

OpenVPN est clairement la solution la plus adaptée à nos besoins en raison de sa flexibilité, de sa compatibilité multi-plateforme et de sa simplicité de configuration. Sa capacité à gérer les accès VPN Road Warrior en fait un choix supérieur pour notre contexte. IPsec VPN, bien que robuste pour des connexions site-à-site, se montre moins flexible et plus complexe à configurer pour notre type d'infrastructure.

Superviseur

Un superviseur permet de surveiller les infrastructures informatiques en collectant, visualisant et analysant des données critiques. Ces outils sont essentiels pour anticiper les pannes, optimiser les performances et garantir la continuité des services.

Grafana

Grafana est une plateforme open-source de visualisation et d'analyse de données. Utilisée principalement pour afficher des tableaux de bord interactifs, elle s'intègre avec plusieurs bases de données pour offrir une supervision avancée.

Zabbix

Zabbix est une solution de supervision complète et open-source, conçue pour surveiller les infrastructures réseau, les serveurs et les applications. Elle combine la collecte, l'analyse et la visualisation des données dans un seul outil.

Comparaison

Critères	Grafana	Zabbix

Coût	Gratuit (open-source)	Gratuit (open-source). Type de supervision
Type de monitoring	Basé sur des visualisations de métriques	Surveillance active des systèmes et applications
Interface utilisateur	Moderne, intuitive, axée sur les tableaux de bord.	Fonctionnelle mais plus technique.
Collecte des données	Nécessite des intégrations externes comme Prometheus ou InfluxDB.	Intégrée nativement avec des agents ou SNMP.
Alertes et notifications	Possible via outils tiers	Alertes natives et configurables
Personnalisation	Hautement personnalisable grâce aux plugins et à la configuration des tableaux de bord.	Personnalisation via scripts et réglages avancés.
Courbe d'apprentissage	Facile pour la création de tableaux de bord simples.	Plus complexe pour les débutants.

Notre choix

Nous avons choisi Grafana pour ce projet en raison de sa simplicité, de son interface moderne et de ses capacités de visualisation avancées. Grafana est particulièrement adapté pour surveiller les métriques système et afficher des données en temps réel de manière intuitive.

Zabbix, bien qu'excellent pour des environnements complexes, demande une configuration plus technique et peut être surdimensionné pour des besoins centrés sur la visualisation.

Le serveur de mail

Un serveur mail est un logiciel ou un ensemble de logiciels qui permettent d'envoyer, de recevoir et de gérer des emails. Il fonctionne grâce à des protocoles standards comme SMTP pour l'envoi, POP3 et IMAP pour la réception. Ces serveurs sont essentiels dans une entreprise pour assurer une communication efficace entre les collaborateurs. En plus des fonctions de base, certains serveurs mail peuvent intégrer des outils de sécurité (anti-spam, anti-virus) ou des fonctionnalités collaboratives comme les calendriers partagés et les tâches. Ils sont souvent configurés pour fonctionner avec des services tels qu'Active Directory afin de simplifier la gestion des utilisateurs.

HMailServer

HMailServer est une solution de messagerie open-source simple et efficace, idéale pour des petites structures. Facile à installer et à configurer, il est compatible avec les protocoles standards SMTP, POP3 et IMAP, ce qui le rend pratique pour mettre en place une messagerie interne rapidement.

Il fonctionne très bien avec un Active Directory, ce qui permet de centraliser la gestion des utilisateurs. Cependant, il n'offre pas de fonctionnalités collaboratives comme les calendriers partagés ou les tâches. Mais pour répondre aux besoins de base du projet, il fait parfaitement l'affaire.

Zimbra

Zimbra est une solution de messagerie complète et surtout orientée vers les entreprises qui ont besoin de collaborer. En plus des mails, elle intègre des calendriers partagés, des tâches, et même un espace pour stocker des fichiers. Elle est disponible en version open-source et payante, mais même en open-source, elle offre déjà beaucoup de fonctionnalités.

Zimbra est compatible avec plusieurs systèmes comme Windows, Linux ou macOS, ce qui la rend p polyvalente. En revanche, elle demande plus de ressources pour fonctionner et l'installation est plus complexe, donc mieux adaptée pour des infrastructures moyennes à grandes.

Comparaison

Critères	HMailServer	Zimbra
Prix	Gratuit	Gratuit (open-source) ou payant pour version commerciale
Plateformes supportées	Windows uniquement	Windows, Linux, macOS
Simplicité d'installation	Très simple	Installation complexe
Administration	Facile via interface graphique	Plus complexe et technique
Fonctionnalités de base	SMTP, POP3, IMAP	SMTP, POP3, IMAP, calendriers, tâches
Fonctionnalités avancées	Pas de collaboration	Collaboration (calendrier, tâches, etc.)
Performance système	Léger, demande peu de ressources	Exigeant en termes de ressources système
Sécurité intégrée	Nécessite configuration supplémentaire	Sécurité avancée intégrée
Support	Communautaire uniquement	Communautaire et commercial (version payante)
Adapté pour	Petites structures	Moyennes et grandes structures

Notre choix

Nous avons opté pour HMailServer dans le cadre du projet car il répond parfaitement aux besoins identifiés, notamment une solution légère, rapide à mettre en œuvre. Il permet de configurer une messagerie fonctionnelle en LAN/VPN tout en intégrant Active Directory pour une gestion centralisée des utilisateurs. De plus, son coût nul s'aligne avec la contrainte budgétaire du projet.

Le logiciel de gestion des interventions

Un logiciel de gestion des interventions est un outil conçu pour aider les organisations, comme les services de sécurité civile ou les pompiers, à planifier, suivre et coordonner leurs missions. Il permet de centraliser les informations, de suivre la disponibilité des équipes, de gérer les ressources, et d'optimiser les réponses aux urgences. Ces logiciels sont essentiels pour améliorer l'efficacité et la réactivité des équipes sur le terrain.

eBrigade

eBrigade est un logiciel open-source conçu pour les organisations d'intervention comme les services de sécurité civile, les pompiers ou les associations. Il offre une gestion centralisée des équipes, des plannings et des interventions. Parmi ses fonctionnalités principales, on retrouve la gestion des disponibilités des intervenants, la planification des missions, une main courante informatisée pour le suivi des opérations, et des outils de génération de rapports. Sa gratuité et son ouverture permettent une grande flexibilité dans sa mise en place.

FireStation

FireStation est un logiciel de gestion dédié aux services d'incendie et de secours. Il permet une gestion avancée des ressources humaines et matérielles, tout en proposant des outils pour la planification et le suivi des interventions. FireStation est particulièrement adapté aux grandes organisations grâce à son interface moderne et ses fonctionnalités spécialisées, comme le suivi des formations et la gestion des équipements critiques. Cependant, il s'agit d'une solution payante et plus complexe à intégrer.

Comparaison

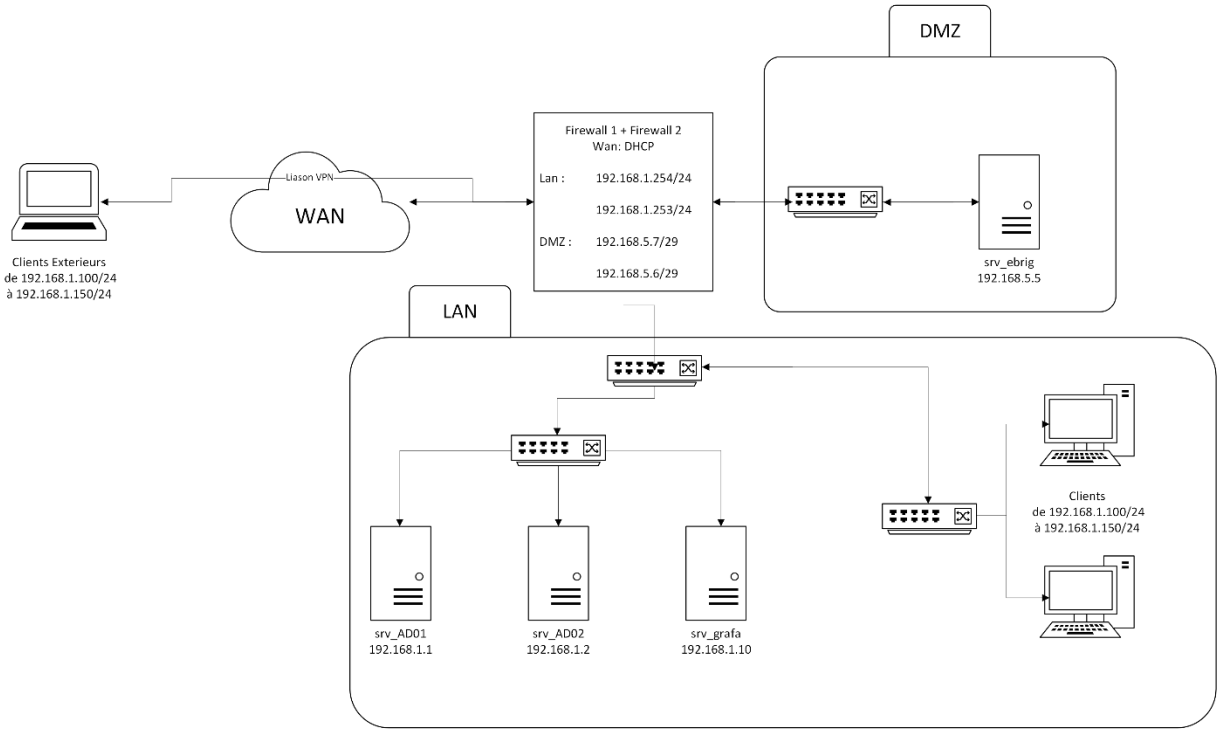
Critères	eBrigade	FireStation
Prix	Gratuit (open source)	Payant
Plates-formes supportées	Multi-plateforme	Multi-plateforme
Simplicité d'installation	Facile et rapide	Plus complexe à configurer
Administration	Interface simple et intuitive	Interface moderne et spécialisée
Gestion des équipes	Disponible	Disponible
Planification des interventions	Disponible	Disponible
Main courante informatisée	Incluse	Non incluse par défaut
Suivi des équipements	Non intégré	Gestion avancée des équipements
Rapports et statistiques	Rapports personnalisables	Rapports avancés
Communauté et support	Communauté active, open source	Support commercial
Public cible	Organisations variées, petite à moyenne taille	Services d'incendie, grandes organisations

Notre choix

Nous avons choisi eBrigade pour ce projet car il répond parfaitement aux besoins identifiés, tout en étant open-source. Sa simplicité d'utilisation et sa capacité à centraliser les informations sur les équipes et les interventions le rendent idéal pour une structure de taille moyenne. De plus, son caractère open-source permet une personnalisation en fonction des spécificités du projet, ce qui est un avantage majeur pour un usage flexible et adapté. Enfin Fire Station est beaucoup plus tourné vers les casernes de pompiers donc moins adaptés.

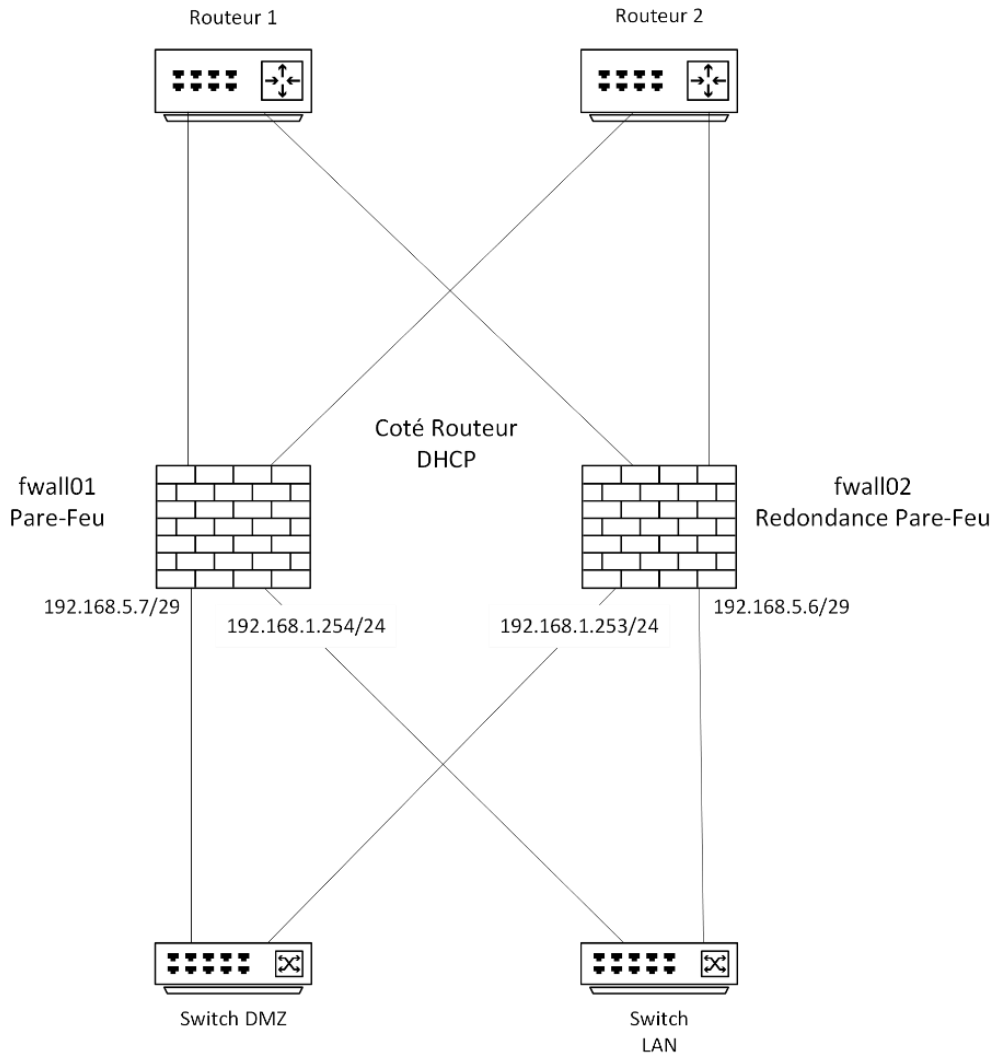
Schémas réseaux

Schéma global



- Srv_ebrig Serveur du logiciel de gestion d'interventions.
- Srv_AD01 Serveur du contrôleur du domaine avec DHCP.
- Srv_AD02 Redondance du serveur srv_AD01.
- Srv_grafa Serveur de supervision et de mail.

Schéma Pare-Feu



BUDGET

Date : 27 avril 2025
Numéro de devis 4869746C6572

Plug&Pray
13 rue du hache
94076 Villejuif
01 04 15 12 06
contact@plug&play.fr

Description	Unité	Quantité	Prix Unitaire HT	TVA	Total HT	Total TTC
Pare-feux (PFsense, Dell Optiplex 7010)	2	pcs	590 €	20%	236.00 €	1416.00 €
Serveur Mail & Graffana (HP ProLiant DL20 Gen 10)	1	pcs	1120 €	20%	224.00 €	1344.00 €
Contrôleur de domaine (Serveur tour Dell T40 Intel Xeon E-2224G 1 TB 8 GB DDR4)	2	pcs	883 €	20%	353.20€	2119.20 €
Routeurs (TP-Link Archer C20)	2	pcs	30 €	20%	12.00 €	72.00 €
Switchs (Netgear GS108)	3	pcs	50 €	20%	30.00 €	180.00 €
Serveur eBrigade (HP ProLiant ML110)	1	pcs	1,200 €	20%	240€	1440 €
Routeurs (TP-Link Archer C20)	1	pcs	30 €	20%	6.00€	36.00 €
PC Fixes (Acer Aspire XC-1760)	10	pcs	380 €	20%	760.00 €	4560.00 €
PC Portables (Lenovo V15 G2)	10	pcs	260 €	20%	520.00 €	3120.00 €

Description	Estimation (heures)	Coût Horaire (€)	Coût Total (€)
Choix des solutions	4h	50€	200€
Mise en place de la virtualisation	8h	60€	480€
Installation pare-feu et vpn	10h	60€	600€
Installation ADDS / Hmail / Grafana / eBrigade	23	55€	1265€
Mise en place de la documentation	5h	50€	250€
Test et ajustement	8h	55€	440€
Présentation	4h	50€	200€

Montant Total HT	14177,76€
Total TVA	20%
Montant Total TTC	17722,2€

PLANNING

5.1) Planning prévisionnel

Dates clés, Diagramme de Gantt, explications et argumentation