

Projet Pro. n°4



LIVRABLE 1



UIMM

LA FABRIQUE
DE L'AVENIR

Contexte Du Projet

Le projet consiste à mettre en place une infrastructure résiliente pour les Centres Opérationnels Départementaux (COD) afin de garantir une continuité de service en toutes circonstances. Il inclut la mise en œuvre d'une connectivité sécurisée, d'outils de gestion des interventions (eBrigade) et de solutions de supervision pour assurer la protection des données et l'efficacité des opérations.

Points clés :

- **Résilience informatique** : Redondance Internet et haute disponibilité des équipements.
- **Connexion sécurisée** : Déploiement d'OpenVPN pour les accès distants.
- **Outils métiers** : Installation du logiciel eBrigade pour la gestion des interventions.
- **Supervision et alertes** : Serveur de monitoring pour surveiller les équipements critiques.

Sommaire

Sommaire.....	2
1) Présentation des Groupes.....	3
1 b) Définitions des rôles et responsabilités.....	4
2) Rappel des Besoins et des Objectifs.....	4
3) Solutions.....	5
3.1) Solutions Technique et logiciels.....	5
Pare-feu / Router	5
VPN Virtual Private Network.....	10
Serveur De Messagerie.....	13
Contrôleur de domaine	17
Windows Server.....	20
Application WEB / DMZ	23
Superviseur	25
3.2) Tableau de Synthèse	28
3.3) Schéma Réseau.....	29
3.4) Tableau Adressage IP.....	30
4) Tarification	31
5) Planning	33
5.1) Liste des taches prévisionnelles.....	33
5.2) Diagramme Gantt prévisionnelles Fichier accessible ici :.....	34

1) Présentation des Groupes

Bonjour je m'appelle **SORG Benjamin**, âgé de 22 ans, en alternance chez Centre-Alsace Habitat dans le cadre de la formation à la préparation du BTS SIO SISR au sein de la CCI Campus. Pour ce projet Professionnel n°4, je serais Technicien Système et Réseau. Dans ce projet, la virtualisation, ainsi que la mise en place des solutions, se fera de manière équitable entre nous. Je suis chargé d'analyse et de comparaison de solutions.



Bonjour je suis **ALTUN Yanis**, âgé de 25 ans, actuellement en alternance chez A.R.S Telecom à Staffelfelden. Passionné par l'informatique dans tous ses rouages, je participerai donc à ce projet de création d'infrastructure numérique professionnelle en tant qu'Administrateur Système avec mon collègue Benjamin SORG. Je réaliserais principalement l'élaboration technique des solutions (avec coûts) et la partie virtuelle sera effectuée en binôme.

1 b) Définitions des rôles et responsabilités

SORG Benjamin	Technicien Système et réseau	Comparaison / Etude solution Virtualisation / mise en place. Planning Prévisionnel.
ALTUN Yanis	Administrateur Système et réseau	Comparaison / Etude solution Devis Virtualisation / mise en place

2) Rappel des Besoins et des Objectifs

L'objectif principal est de concevoir une infrastructure **fiable et performante**, comprenant la redondance des connexions Internet et la mise en place de serveurs critiques tels qu'Active Directory et un serveur de messagerie sécurisé. Le projet doit également inclure une **connectivité sécurisée** via une solution OpenVPN Road Warrior et une zone DMZ pour l'accès au logiciel eBrigade. En complément, une supervision proactive sera assurée grâce à un serveur de monitoring, capable d'envoyer des alertes en cas de panne ou d'anomalies. Enfin, la solution doit être validée par des tests, accompagnée d'une documentation technique complète pour garantir sa pérennité et faciliter son exploitation future. Le tout doit être réalisé en respectant les contraintes budgétaires et les délais impartis.

3) Solutions

3.1) Solutions Technique et logiciels

Pare-feu / Router

1) PfSense :



Est une **solution open-source** complète de pare-feu et routeur, largement utilisée pour sa **fiabilité** et sa **flexibilité** dans la gestion des réseaux. Basée sur FreeBSD, elle offre une interface web intuitive qui permet de configurer rapidement et efficacement des règles de sécurité, de routage et de gestion du trafic. Elle est idéale pour protéger les réseaux d'entreprises tout en garantissant une **sécurité renforcée** et des **performances optimales**. En plus de ses capacités de pare-feu, PfSense prend en charge une large gamme de services réseau, y compris la gestion des **VPN**, la **détection d'intrusion**, et la **haute disponibilité**.

- Support des VPN (IPsec, OpenVPN)
- Pare-feu et filtrage d'IP configurable et flexible
- Gestion de la bande passante et QoS (Qualité de Service)
- Détection et prévention d'intrusion (IDS/IPS)
- Prise en charge des VLANs et des configurations haute disponibilité

II) OpnSense :

OPNsense est une autre solution open-source basée sur FreeBSD, très similaire à PfSense, mais avec un accent particulier sur la **sécurité** et l'**interface utilisateur**. Elle propose des fonctionnalités de **pare-feu**, **VPN**, **IDS/IPS** et **QoS**, tout en offrant des mises à jour fréquentes et une interface web moderne. OPNsense est également apprécié pour sa **gestion simplifiée** et son **évolutivité**, ce qui en fait un excellent choix pour les entreprises et les environnements complexes.



- **Basé sur FreeBSD** : Comme PfSense, OPNsense utilise le système d'exploitation FreeBSD.
- **Sécurité** : Mise en avant de la sécurité avec des fonctionnalités avancées.
- **Interface utilisateur** : Interface web moderne et conviviale.
- **Fonctionnalités** :
 - o Pare-feu
 - o VPN
 - o IDS/IPS (Système de Détection/Prévention d'Intrusion)
 - o QoS (Qualité de Service)
- **Mises à jour fréquentes** : OPNsense propose des mises à jour régulières.
- **Gestion simplifiée** : Conçu pour une gestion facile et intuitive.
- **Évolutivité** : Adapté aux entreprises et aux environnements complexes.

III) Fortinet :



Propose des **pares-feux** et routeurs intégrant des fonctionnalités avancées telles que pare-feu, **VPN**, prévention des intrusions (**IPS**), **filtrage web et antivirus**. Les appareils **FortiGate** sont connus pour leur performance élevée et leur gestion centralisée via **FortiManager**. Ils offrent une grande flexibilité et sont adaptés aux environnements de réseau complexes, ce qui les rend populaires parmi les entreprises de toutes tailles.

Liste à points :

- **Fonctionnalités avancées** : Pare-feu, VPN, IPS, filtrage web, antivirus.
- **Performance élevée** : Capacités de traitement optimales.
- **Gestion centralisée** : Avec FortiManager.
- **Flexibilité et scalabilité** : Adapté aux environnements complexes.
- **Popularité** : Choisi par les entreprises de toutes tailles.

Critère	PfSense	OPNsense	Fortinet
Basé sur FreeBSD	☑	☑	✗
Support VPN (IPsec, OpenVPN)	☑	☑	☑

Pare-feu configurable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Gestion de la bande passante et QoS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Détection et prévention d'intrusion (IDS/IPS)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Prise en charge des VLANs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Haute disponibilité	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Interface web moderne	✗	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Mises à jour fréquentes	✗	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Gestion centralisée	✗	✗	<input checked="" type="checkbox"/>

Performance élevée	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Flexibilité et scalabilité	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Popularité auprès des entreprises	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Prix	Gratuit (open-source, support payant)	Gratuit (open-source, support payant)	Variable / Payant(département de vente)

Nous avons choisi d'opter pour la solution **pfSense** en tant que routeur/pare-feu pour ce projet. Cette décision repose sur notre expérience éprouvée avec cette solution open source, qui s'est montrée fiable, performante et flexible dans des contextes similaires. pfSense offre une intégration native de **OpenVPN**, ce qui simplifie la mise en place d'un accès distant sécurisé tout en garantissant une configuration robuste et cohérente avec les exigences de sécurité. De plus, pfSense propose une gestion intuitive des pare-feux, une redondance facile à configurer pour les connexions WAN, et une supervision avancée. Ces fonctionnalités en font un choix idéal pour répondre aux besoins spécifiques du projet tout en respectant les contraintes de coût et de complexité technique.

VPN | Virtual Private Network

I) IPsec VPN :

IPsec (Internet Protocol Security) est un protocole VPN largement utilisé pour sécuriser les communications sur un réseau IP, offrant des mécanismes de cryptage, d'authentification et d'intégrité des données. Gratuit et intégré dans PfSense, il permet de créer des connexions sécurisées entre sites distants ou pour des utilisateurs en accès distant. Bien que puissant, IPsec peut être un peu plus complexe à configurer.



- **Gratuit et intégré** dans PfSense.
- **Cryptage sécurisé** (AES, 3DES).
- **Authentification et intégrité des données** garanties.
- **Connexions site-à-site** sécurisées.
- **Administration via interface web** intuitive.
- **Compatible** avec IPv4, IPv6, et multi-plateformes.
- **Stabilité et fiabilité** pour des connexions robustes.
- **Facile à configurer** et à gérer.

II) OpenVPN :



OpenVPN est un protocole VPN open-source qui utilise les protocoles SSL/TLS pour établir des tunnels sécurisés sur Internet. Il est flexible, capable de contourner les pare-feu et facile à configurer, tout en fournissant un haut niveau de sécurité. OpenVPN est souvent préféré pour sa simplicité et sa compatibilité avec divers environnements.

- **Open-source et gratuit.**
- **Utilise SSL/TLS** pour sécuriser les connexions.
- **Facilité de configuration** via l'interface web de PfSense.
- **Compatible multi-plateforme** (Windows, Linux, macOS, etc.).
- **Capacité à contourner les pare-feu.**
- **Authentification flexible** (certificats, clés partagées).
- **Support des connexions site-à-site et accès distant.**
- **Haute flexibilité** pour divers scénarios réseau.


Critère	IPsec VPN (sur PfSense)	OpenVPN
Sécurité	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cryptage	<input checked="" type="checkbox"/> (AES, 3DES, etc.)	<input checked="" type="checkbox"/> (SSL/TLS)
Gratuit sur PfSense	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Compatibilité multi-plateforme	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Facilité de configuration	<input checked="" type="checkbox"/> (Plus complexe)	<input checked="" type="checkbox"/> (Facile à configurer)

Performances	☑	☑
Contourne les pare-feu	✗	☑
Gestion des certificats	✗ (non natif)	☑ (SSL/TLS avec certificats)
Utilisation pour les réseaux d'entreprise	☑	☑
Flexibilité	✗	☑

Nous avons décidé d'utiliser **OpenVPN Road Warrior** pour ce projet en raison de son adéquation avec nos besoins. Un **VPN Road Warrior** est une configuration qui permet à des utilisateurs mobiles—appelés "road warriors"—de se connecter de manière sécurisée au réseau interne depuis n'importe quel endroit, simplement via une connexion Internet. Cette solution est idéale pour les agents sur le terrain qui ont besoin d'un accès fiable aux ressources du Centre Opérationnel Départemental. De plus, OpenVPN est nativement intégré à **pfSense**, notre choix de routeur/pare-feu basé sur notre expérience positive avec cette plateforme. Cela facilite grandement la mise en place et la gestion de la connectivité sécurisée, tout en respectant les contraintes budgétaires du projet.

Serveur De Messagerie

I)HmailServer :

hMailServer est une  **hMailServer** solution de serveur de messagerie open source permettant de gérer des services de messagerie électronique de manière locale et sécurisée. Il supporte les principaux protocoles de messagerie tels que **SMTP, IMAP et POP3**, garantissant une compatibilité avec la plupart des clients de messagerie. Facile à configurer et à administrer, hMailServer offre des fonctionnalités avancées, notamment un système intégré de gestion des utilisateurs, une prise en charge des annuaires Active Directory pour une authentification centralisée, ainsi que des options de filtrage anti-spam et antivirus. Sa légèreté et son efficacité en font une solution idéale pour des environnements nécessitant un contrôle total des communications internes et externes, tout en assurant une sécurité et une résilience accrues.

- **Protocoles pris en charge** : SMTP, IMAP et POP3, compatibles avec la plupart des clients de messagerie.
- **Intégration Active Directory** : Gestion centralisée des utilisateurs et authentification simplifiée.
- **Sécurité avancée** : Filtres anti-spam et antivirus intégrés pour protéger les communications.
- **Administration simplifiée** : Interface utilisateur conviviale et configuration facile.
- **Solution locale** : Fonctionnement indépendant d'Internet, garantissant une messagerie résiliente en cas de coupure.
- **Open source** : Solution gratuite et adaptée aux contraintes budgétaires.

II) MailCOW :



MailCOW est une solution open source complète pour la gestion d'un serveur de messagerie électronique. Basée sur des technologies modernes telles que Docker, MailCOW intègre tous les composants nécessaires pour une messagerie performante et sécurisée, incluant un serveur de messagerie (Postfix), un serveur IMAP (Dovecot), un gestionnaire de calendrier et de contacts (SOGó), ainsi que des fonctionnalités anti-spam et antivirus avancées (Rspamd, ClamAV). Conçue pour être facile à déployer et à administrer, MailCOW offre une interface utilisateur intuitive pour la gestion des boîtes aux lettres, des domaines et des règles de sécurité. Sa modularité et sa capacité à gérer des environnements multi-domaines en font une solution idéale pour des organisations de toutes tailles.

- **Solution complète** : Comprend un serveur SMTP (Postfix), IMAP (Dovecot) et des outils de collaboration (SOGó).
- **Anti-spam et antivirus intégrés** : Protection avancée avec Rspamd et ClamAV.
- **Interface intuitive** : Administration simplifiée grâce à une interface web conviviale.
- **Support multi-domaines** : Gestion efficace de plusieurs domaines et boîtes aux lettres.
- **Basée sur Docker** : Déploiement rapide et portable, facile à maintenir.
- **Sécurité robuste** : Gestion des certificats SSL, des politiques DMARC, SPF et DKIM.
- **Open source et flexible** : Gratuit, personnalisable et adapté à des besoins variés.

Critères	hMailServer	MailCOW
Open source	☑	☑
Support multi-domaines	☑	☑
Anti-spam intégré	☑	☑
Antivirus intégré	☑	☑
Protocoles supportés (SMTP, IMAP, POP3)	☑	☑
Gestion via interface utilisateur	☑	☑
Intégration Active Directory	☑	✗
Facilité de déploiement	☑	☑
Basée sur Docker	✗	☑
Personnalisable	✗	☑

Moderne et modulaire		×	<input checked="" type="checkbox"/>
Compatibilité OS (Windows/Linux)		Windows uniquement	Linux uniquement

Nous avons choisi **hMailServer** pour sa compatibilité native avec les environnements Windows, déjà présents dans le projet, et son intégration fluide avec Active Directory pour une gestion centralisée des utilisateurs. Cette solution légère et locale répond parfaitement aux exigences de résilience et de sécurité, tout en offrant des fonctionnalités essentielles telles que les protocoles SMTP, IMAP et POP3, ainsi que des filtres anti-spam et antivirus. Facile à configurer et à administrer, hMailServer constitue un choix économique et efficace pour une messagerie fiable adaptée à nos besoins.

Contrôleur de domaine

I) Active Directory



Active Directory (AD) sur un serveur Windows est un service de gestion des identités et des accès essentiels pour les environnements d'entreprise, intégrant plusieurs composants clés : **LDAP** (Lightweight Directory Access Protocol) pour la gestion des informations d'annuaire, **DNS** (Domain Name System) pour la résolution des noms de domaine et la localisation des services réseau, et **Kerberos** pour l'authentification sécurisée des utilisateurs et des services. Grâce à ces composants, AD permet de centraliser la gestion des utilisateurs et des groupes, de contrôler les accès aux ressources, et d'appliquer des **politiques de sécurité** robustes tout en **automatisant les tâches administratives** et en **intégrant de manière fluide d'autres services Windows**.

Points importants :

- **Gestion des utilisateurs et des groupes** : Centralisation des informations sur les utilisateurs et les groupes.
- **Contrôle des accès** : Définition et gestion des permissions pour les ressources réseau.
- **Politiques de sécurité** : Application de règles de sécurité via les stratégies de groupe (GPO).
- **Automatisation des tâches** : Gestion automatisée des comptes et des ressources.
- **LDAP** : Protocole pour la gestion et l'accès aux informations d'annuaire.
- **DNS** : Résolution des noms de domaine et localisation des services réseau.
- **Kerberos** : Authentification sécurisée des utilisateurs et des services.
- **Intégration avec d'autres services Windows** : Compatibilité avec des services comme Exchange Server et SharePoint.

II) OpenLDAP



OpenLDAP est une solution open source qui implémente le protocole **LDAP (Lightweight Directory Access Protocol)**, permettant de centraliser la gestion des utilisateurs, groupes et autres ressources. Utilisé pour l'authentification et l'organisation des données d'annuaire, il garantit une gestion unifiée des identités au sein des systèmes. Robuste et flexible, OpenLDAP est compatible avec de nombreux environnements et constitue une solution économique et personnalisable pour les organisations de toutes tailles.

- **Open source** : Gratuit et personnalisable, adapté aux besoins variés.
- **Centralisation des identités** : Permet de gérer utilisateurs, groupes et autres ressources dans un annuaire unique.
- **Protocole LDAP** : Implémente le standard pour l'accès structuré aux données d'annuaire.
- **Authentification centralisée** : Simplifie la gestion des accès et des autorisations dans les systèmes.
- **Compatibilité étendue** : Fonctionne avec de nombreux systèmes et applications.
- **Flexibilité** : Hautement configurable pour s'adapter à des environnements divers.
- **Performance éprouvée** : Robuste et capable de gérer un grand volume de données.
- **Sécurité** : Supporte les politiques d'accès et le chiffrement des communications.

Critères	OpenLDAP	Active Directory
----------	----------	------------------

Open source	☑	✗
Compatibilité multiplateforme	☑	✗
Authentification centralisée	☑	☑
Gestion des utilisateurs et groupes	☑	☑
Support natif pour Windows	✗	☑
Support natif pour Linux	☑	✗
Protocoles pris en charge (LDAP, Kerberos, etc.)	☑	☑
Flexibilité et personnalisation	☑	✗
Intégration avec les services Microsoft	✗	☑
Coût d'utilisation	Gratuit	Payant

Nous avons choisi **Active Directory** non seulement parce qu'il est imposé dans le cadre du projet, mais aussi en raison de ses nombreux avantages qui répondent aux besoins de l'infrastructure. Active Directory est une solution éprouvée et largement utilisée pour la gestion centralisée des utilisateurs, des groupes, et des ressources dans les environnements Windows, qui constituent déjà une part essentielle de l'infrastructure du projet. Son intégration native avec les systèmes Microsoft, sa simplicité d'administration via des outils graphiques comme la console MMC, et ses fonctionnalités avancées telles que les politiques de groupe (GPO) en font un choix idéal pour assurer la cohérence, la sécurité, et l'efficacité de la gestion des identités. De plus, sa large adoption garantit un support étendu et une compatibilité avec d'autres logiciels et services, renforçant ainsi sa pertinence dans ce contexte.

Windows Server

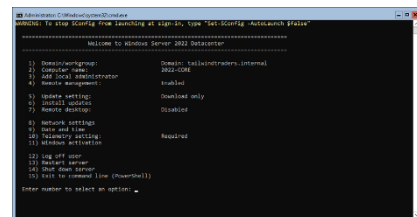
I) Expérience de bureau :

Windows Server avec interface graphique (GUI) offre une gestion intuitive via une interface visuelle, facilitant la configuration des services, la gestion des utilisateurs et la surveillance du serveur. Idéal pour une administration simplifiée. Il permet également d'installer et de gérer des services Active Directory (AD), offrant ainsi une solution complète pour la gestion des identités et des accès.



II) Version Invité de CMD :

Windows Server Core offre une gestion minimaliste via une interface en ligne de commande, réduisant l'empreinte système et les vulnérabilités potentielles. Bien que sans interface graphique, il permet d'installer et de gérer des services Active Directory (AD) ainsi que d'autres rôles serveur, offrant une solution efficace pour des environnements nécessitant une gestion plus légère et sécurisée.



Critère	Windows Server GUI	Windows Server Core
Interface graphique	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Gestion via ligne de commande	<input checked="" type="checkbox"/> / <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Installation des services AD	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Consommation des ressources	✗	☑
Surface d'attaque (sécurité)	☑	☑
Simplicité d'administration	☑	✗
Évolutivité	☑	☑
Maintenance et mises à jour	☑	☑
Performance	✗ (moins optimisée)	☑ (plus optimisée)

Le premier Windows Server sera installée en version GUI pour bénéficier de la simplicité et de l'intuitivité de l'interface graphique, facilitant ainsi la gestion et la configuration. En revanche, le deuxième Active Directory sera configurée en version Core afin de maximiser les performances et minimiser l'empreinte système, en exploitant une gestion via ligne de commande plus légère et sécurisée.

Application WEB / DMZ

I) eBrigade



eBrigade est un logiciel open source conçu pour la gestion des interventions et des ressources dans des contextes variés, notamment pour les services de secours et de sécurité civile. Il offre des fonctionnalités complètes permettant de gérer le personnel, planifier des interventions, suivre les missions en temps réel et générer des mains courantes et rapports d'activités. Grâce à son interface intuitive, eBrigade facilite la coordination des équipes sur le terrain et centralise les informations pour une meilleure visibilité et prise de décision. Sa flexibilité et son adaptabilité en font un outil précieux pour optimiser la gestion des crises et améliorer l'efficacité opérationnelle des services impliqués.

- La gestion des personnels et des compétences.
- La planification et le suivi des interventions.
- La génération de mains courantes et de rapports pour une documentation complète des opérations.

II) OTRS



OTRS (Open Ticket Request System) est un logiciel open source destiné à la gestion des demandes et interventions, largement utilisé pour le support technique et la gestion des services informatiques (ITSM). Il centralise les demandes, suit leur progression en temps réel et planifie les ressources nécessaires. Avec une interface intuitive et personnalisable, OTRS propose des fonctionnalités comme la gestion des tickets, l'automatisation des processus, et des outils d'analyse, ce qui en fait une solution efficace pour la coordination et le suivi des interventions.

- **Open source** et personnalisable.
- **Gestion des tickets** et suivi en temps réel.
- **Automatisation des processus** pour gagner en efficacité.
- **Interface intuitive** et multi-utilisateurs.
- **Outils d'analyse** pour optimiser les performances.

Critères	eBrigade	OTRS
Open source	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Gestion des personnels	<input checked="" type="checkbox"/>	✗
Planification des interventions	<input checked="" type="checkbox"/>	✗
Suivi en temps réel	<input checked="" type="checkbox"/>	✗
Génération de mains courantes	<input checked="" type="checkbox"/>	✗
Interface intuitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Accessible en ligne	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Gestion des compétences	<input checked="" type="checkbox"/>	✗
Multi-utilisateurs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Personnalisable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Critères	eBrigade	OTRS

Superviseur

I) Nagios

Nagios Nagios est une solution open source de supervision et de monitoring des systèmes, réseaux et applications. Il permet de surveiller en temps réel l'état des équipements et des services, tels que les serveurs, bases de données, routeurs, et applications critiques. Nagios alerte les administrateurs en cas de pannes ou d'anomalies, facilitant une intervention rapide pour minimiser les interruptions. Grâce à son architecture modulaire et à ses nombreux plugins, il est hautement personnalisable pour répondre à divers besoins. Idéal pour les environnements complexes, Nagios offre une visibilité complète et une gestion proactive des infrastructures IT.

- **Open source** : Gratuit avec de nombreuses options de personnalisation.
- **Supervision complète** : Surveille les systèmes, réseaux, applications, et services.
- **Alertes en temps réel** : Notifie immédiatement en cas de panne ou d'anomalie.
- **Personnalisable** : Supporte de nombreux plugins pour s'adapter aux besoins spécifiques.
- **Architecture modulaire** : Flexible pour les environnements complexes.
- **Rapports détaillés** : Fournit des données pour analyser les performances et les incidents.
- **Large support communautaire** : Documentation et ressources accessibles pour la configuration.

II) Zabbix

Zabbix est une solution open source de supervision et de surveillance des infrastructures IT, des systèmes, des



réseaux et des applications. Elle permet de collecter et d'analyser des métriques en temps réel, offrant ainsi une visibilité complète sur les performances et la disponibilité des ressources. Grâce à ses alertes configurables, Zabbix notifie les

administrateurs dès qu'un problème est détecté, facilitant une intervention rapide. Son interface intuitive, ses tableaux de bord personnalisables et ses capacités d'extensibilité via des scripts ou des intégrations en font un outil puissant pour la gestion proactive des infrastructures IT, adapté aux environnements de toutes tailles.

- **Open source** : Gratuit, puissant et flexible.
- **Supervision complète** : Surveille les infrastructures, systèmes, réseaux et applications.
- **Alertes en temps réel** : Notifications configurables pour réagir rapidement aux incidents.
- **Collecte de métriques** : Permet le suivi détaillé des performances et des ressources.
- **Interface intuitive** : Tableau de bord personnalisable pour une visualisation claire des données.
- **Extensibilité** : Prend en charge des scripts et des intégrations avec d'autres outils.
- **Rapports avancés** : Génération de graphiques et d'analyses détaillées.
- **Support multiplateforme** : Compatible avec Windows, Linux, et autres environnements.

Critères	Nagios	Zabbix
Open source	☑	☑
Supervision complète	☑	☑
Alertes en temps réel	☑	☑
Interface intuitive	✗	☑

Personnalisable	☑	☑
Support multiplateforme	☑	☑
Rapports détaillés	☑	☑
Extensibilité via plugins/scripts	☑	☑
Collecte de métriques avancée	✗	☑
Configuration initiale simplifiée	✗	☑

Nous avons choisi **Zabbix** pour sa combinaison de simplicité d'utilisation, de fonctionnalités avancées et de flexibilité. Sa **supervision complète** des infrastructures, incluant les systèmes, réseaux, et applications, répond parfaitement aux besoins du projet. Zabbix se distingue par son **interface intuitive** et ses tableaux de bord personnalisables, qui offrent une visibilité claire et en temps réel des performances. De plus, ses **alertes configurables** et sa capacité à collecter des métriques avancées permettent une gestion proactive des infrastructures. Enfin, sa facilité de configuration initiale et sa compatibilité multiplateforme en font une solution moderne et adaptée à des environnements complexes tout en restant accessible aux administrateurs.

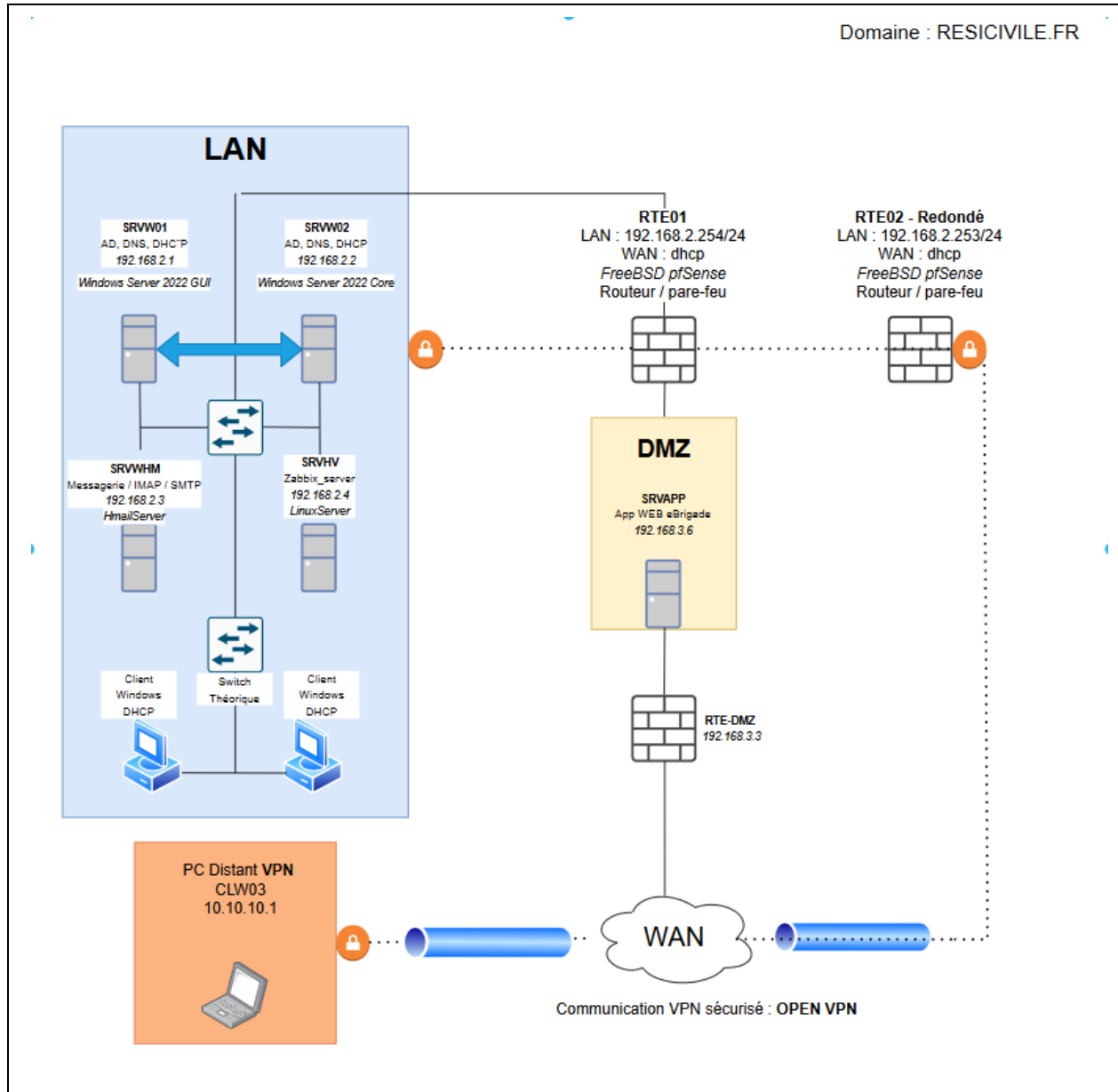
3) Solutions

3.2) Tableau de Synthèse

Solutions	Retenues
PfSense	<input checked="" type="checkbox"/>
Active Directory	<input checked="" type="checkbox"/>
Windows Server GUI + CORE	<input checked="" type="checkbox"/>
OpenVPN	<input checked="" type="checkbox"/>
HMail Server	<input checked="" type="checkbox"/>
eBrigade (imposé)	<input checked="" type="checkbox"/>
Zabbix	<input checked="" type="checkbox"/>

3) Solutions

3.3) Schéma Réseau




SchémaRéseau_AP4.d
rawio

Fichier accessible ici :

3.4) Tableau Adressage IP

Equipement Infrastructure	Adressage IP
SRVW01	192.168.2.1 /24
SRVW02	192.168.2.2 /24
SRVWHM	192.168.2.3 /24
SRVHV	192.168.2.4 /24
SRVAPP	192.168.3.6 /24
RTE01	LAN: 192.168.2.254 /24 WAN: DHCP; 192.168.1.158 /24 OPT1: 192.168.4.1 /24 DMZ: 192.168.3.1 /24
RTE02	LAN: 192.168.2.253 /24 WAN: DHCP; 192.168.1.100 /24 OPT1: 192.168.4.2 /24 DMZ: 192.168.3.2 /24
RTE VIRTUAL IP	Redondance WAN: 192.168.2.154 /24 DMZ: 192.168.3.3 /24
CLW01	DHCP : 192.168.2.10 /24
CLW02	DHCP : 192.168.2.11 /24
CLW03	OPENVPN : 10.10.10.1 /24

4) Tarification

	Quantité à l'unité	Prix HT à l'unité	Total
Serveur reconditionné (Dell R720 - 6000GB - 128 GB RAM Xeon E5-2660 v2)	1	926 €	926 €
Serveur reconditionné (Dell R720 - 3000GB - 64 GB RAM Xeon E5-2660 v2)	1	500 €	500 €
Ordinateur portable reconditionné (Lenovo ThinkPad T440 8Go DDR4, 500 Go Nvme)	10	150 €	1 500 €
Windows 10 x64 Professionnel	10	139,95 €	1 399,50 €
Windows Server 2022 Standard Edition (Licence par coeur) - 16 coeurs	2	1 069 €	2 138 €
Windows Server 2022 Standard Edition (Licence par coeur) – 8 coeurs	2	534.50 €	1069 €

Ekivalan Coffret CEPA 19" 16U profondeur 450 mm - charge utile 80 kg - coloris noir	1	450 €	450 €
Cisco CBS350-48T-4G	1	163 €	163 €
Netgear Nighthawk AX4	1	200 €	200 €
Onduleur APC 1500VA	1	250 €	250 €
Configuration et installation de l'infrastructure (messagerie, VPN, Active Directory, Zabbix)	1	1 200 €	1 200 €
Sous-total		8 265.50 €	
TVA 20%		1 653.10 €	
Total TTC		9 919,50 €	

5) Planning

5.1) Liste des taches prévisionnelles

Étape	Durée	Début	Fin
Début du Projet	5 jours	10 janv. 2025	14 janv. 2025
Mise en place des infrastructures	7 semaines	15 janv. 2025	2 mars 2025
Livrable 1	1 jour	3 mars 2025	3 mars 2025
Présentation orale 1	1 jour	12 mars 2025	12 mars 2025
Finalisation des livrables	4 semaines	13 mars 2025	7 avril 2025
Livrable 2	1 jour	8 avril 2025	8 avril 2025
Présentation finale	1 jour	14 avril 2025	14 avril 2025



PalnGANTTap4.gan

5.2) Diagramme Gantt prévisionnelles | | Fichier accessible ici :

