Projet NovaResQ

BTS SIO 2025 Option SISR

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

ANNEXE 9-1-A : Fiche descriptive de réaisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 2**
Nom, prénom : ERNST Nicolas	**N° candidat : 02442761572**
Épreuve ponctuelle ☐ **X Contrôle en cours de formation** ☒	**Date : 06** / 01 /2025

Organisation support de la réalisation professionnelle

Dans le cadre d'un appel d'offre visant à renforcer la résilience informatique des Centres Opérationnels Départementaux, le projet prévoit la mise en place d'une infrastructure assurant la continuité des services en situation de crise. Il comprend la sécurisation des accès, le déploiement d'une solution de connexion distante pour les agents de terrain, ainsi que l'intégration d'outils de communication et de supervision adaptés aux exigences de la sécurité civile.

Intitulé de la réalisation professionnelle

Projet « **NovaResQ** »

Période de réalisation : 06/01/2025 au 13/04/2025 **Lieu :** Strasbourg.....

Modalité : ☒**X Seul(e)** ☐ **En équipe**

Compétences travaillées

- ☒ Concevoir une solution d'infrastructure réseau
- ☒ Installer, tester et déployer une solution d'infrastructure réseau
- ☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)

Mise en place d'un pare-feu PfSense avec VPN IPsec pour la sécurité réseau et la connectivité distante.
Déploiement de Active Directory pour la gestion centralisée des utilisateurs et des ressources.
Installation de PRTG Network Monitor pour la supervision en temps réel du réseau et des services critiques.
Mise en place d'un serveur Asterisk pour une solution de téléphonie IP interne.
Configuration de Modoboa pour une messagerie d'entreprise sécurisée.
Intégration de eBrigade, logiciel métier de gestion d'interventions et de plannings.

Description des ressources documentaires, matérielles et logicielles utilisées[2]

- Ressources matérielles : 3 serveurs physiques, 2 commutateurs managés, 1 firewall dédié, Postes clients de test
- Ressources logicielles : P**fSense** (Firewall / VPN IPsec), **Windows Server 2022 ADDS, PRTG Network Monitor (version d'évaluation), Asterisk** (téléphonie VoIP), **Modoboa (messagerie open source), eBrigade (plateforme de gestion métier)**

Modalités d'accès aux productions[3] et à leur documentation[4]

Lien portfolio et éventuellement le mot de passe d'accès (page ou .zip à déchiffrer)

[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.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Durée du projet : 06/01/2025 - 13/04/2025

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

SOMMAIRE

1) Résumé du projet

A) Définitions des rôles et des responsabilités

Le projet **NovaResQ** a été réalisé en autonomie. J'ai endossé l'ensemble des responsabilités liées au projet, en tant que chef de projet, administrateur système, réseau et sécurité, ainsi que technicien d'exploitation. J'ai assuré la coordination générale, validé les solutions techniques, exécuté les différentes tâches, participé aux phases de test et effectué les ajustements nécessaires en fonction des résultats. Cette organisation m'a permis de mener une progression fluide et méthodique du projet, tout en maîtrisant chaque aspect de sa réalisation.

B) Rappel des objectifs fixés

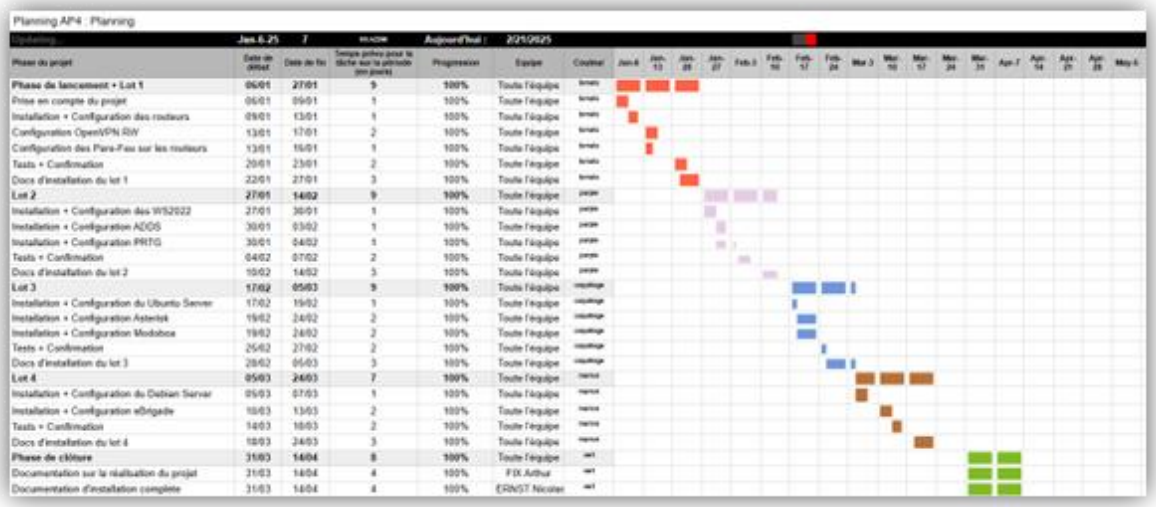
Les objectifs initiaux du projet étaient d'assurer une infrastructure informatique sécurisée, résiliente et capable de fonctionner en toute circonstance, notamment en période de crise. Il s'agissait de garantir la connectivité à distance pour les agents de terrain, de mettre en place une téléphonie IP efficace, une supervision en temps réel des équipements critiques ainsi qu'un serveur de messagerie fiable. Le tout devait être réalisé dans un cadre budgétaire fixé à environ 30 754 euros TTC, et sur une durée de quarante-cinq jours, représentant un total de 315 heures de travail. Aucun changement majeur n'est intervenu en cours de projet, que ce soit en matière de rôles, de responsabilités ou d'objectifs. Le cadre initial a été respecté du début à la fin, ce qui a grandement facilité la conduite du projet.

2) Conduite du projet

A) Planning prévisionnel VS planning réel

En comparant le planning initialement prévu avec le déroulement réel du projet, on observe une assez bonne concordance entre les deux. Quelques ajustements ont été nécessaires, notamment en ce qui concerne la configuration de la DMZ et du serveur eBrigade, ainsi que le paramétrage avancé des règles de filtrage réseau sous pfSense. De plus, la mise en place d'OpenVPN, pourtant prévue dès le départ pour assurer la connexion distante des agents, n'a finalement pas pu être réalisée, ce qui constitue un écart notable par rapport aux objectifs initiaux. De plus, le serveur prévu pour la DMZ, initialement sous Debian, a été remplacé par Ubuntu Server, dont l'environnement s'est révélé plus adapté à notre contexte. Ces étapes, plus complexes que prévu, ont légèrement décalé certaines échéances. Ces décalages n'étaient pas complètement imprévisibles mais ont été sous-estimés dans leur technicité. Afin d'éviter une telle situation à l'avenir, il serait pertinent d'approfondir l'étude des solutions techniques et de renforcer la phase de tests préparatoires en amont de leur implémentation. Malgré cela, les dates de livraison majeures ont été tenues, et aucun retard significatif n'a compromis l'intégralité du projet.

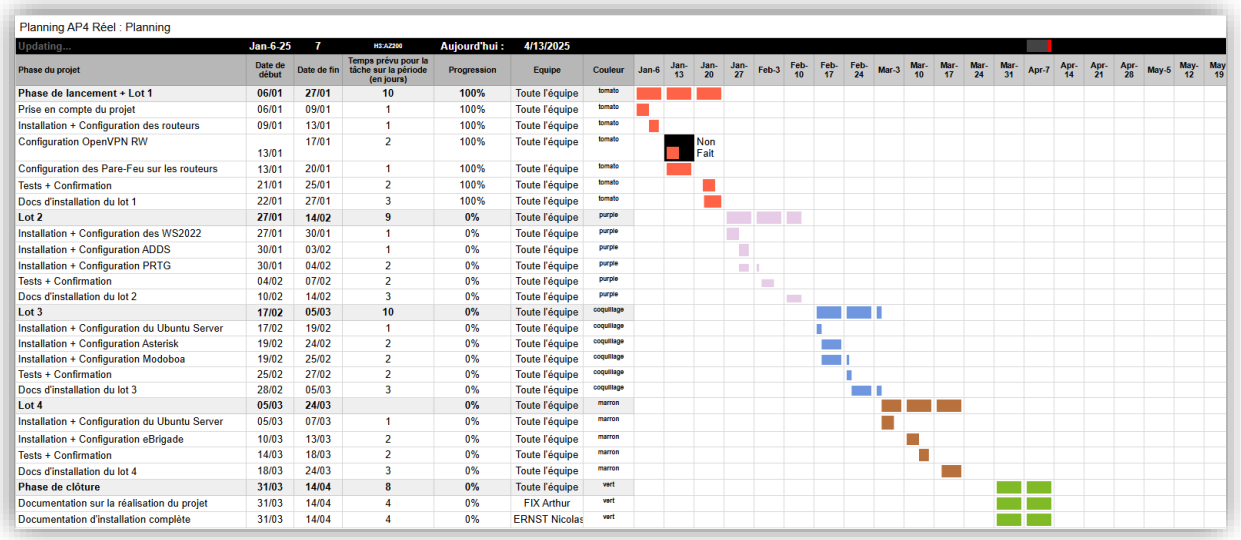
- Planning prévisionnel :



https://docs.google.com/spreadsheets/d/e/2PACX-1vSvchMNfA9vK_RgMTylhMwlXh2QeXEuVDbAVWxn2aid0vn4rjtXwhnectpVhB5EG38hNMBwV-WBGrcd/pubhtml

Le planning prévisionnel a été élaboré afin d'anticiper et structurer les différentes étapes du projet dans le temps. Il permet de visualiser la répartition des tâches, les ressources mobilisées et les échéances clés, tout en servant de base à l'organisation et au suivi.

- Planning réel :



Phase du projet	Date de début	Date de fin	Temps prévu pour la tâche sur la période (en jours)	Progression	Equipe	Couleur
Phase de lancement + Lot 1	**06/01**	**27/01**	**10**	**100%**	Toute l'équipe	tomato
Prise en compte du projet	06/01	09/01	1	100%	Toute l'équipe	tomato
Installation + Configuration des routeurs	09/01	13/01	1	100%	Toute l'équipe	tomato
Configuration OpenVPN RW	13/01	17/01	2	100%	Toute l'équipe	tomato
Configuration des Pare-Feu sur les routeurs	13/01	20/01	1	100%	Toute l'équipe	tomato
Tests + Confirmation	21/01	25/01	2	100%	Toute l'équipe	tomato
Docs d'installation du lot 1	22/01	27/01	3	100%	Toute l'équipe	tomato
Lot 2	**27/01**	**14/02**	**9**	**0%**	Toute l'équipe	purple
Installation + Configuration des WS2022	27/01	30/01	1	0%	Toute l'équipe	purple
Installation + Configuration ADDS	30/01	03/02	1	0%	Toute l'équipe	purple
Installation + Configuration PRTG	30/01	04/02	2	0%	Toute l'équipe	purple
Tests + Confirmation	04/02	07/02	2	0%	Toute l'équipe	purple
Docs d'installation du lot 2	10/02	14/02	3	0%	Toute l'équipe	purple
Lot 3	**17/02**	**05/03**	**10**	**0%**	Toute l'équipe	coquillage
Installation + Configuration du Ubuntu Server	17/02	19/02	1	0%	Toute l'équipe	coquillage
Installation + Configuration Asterisk	19/02	24/02	2	0%	Toute l'équipe	coquillage
Installation + Configuration Modoboa	19/02	25/02	2	0%	Toute l'équipe	coquillage
Tests + Confirmation	25/02	27/02	2	0%	Toute l'équipe	coquillage
Docs d'installation du lot 3	28/02	05/03	3	0%	Toute l'équipe	coquillage
Lot 4	**05/03**	**24/03**		**0%**	Toute l'équipe	marron
Installation + Configuration du Ubuntu Server	05/03	07/03	1	0%	Toute l'équipe	marron
Installation + Configuration eBrigade	10/03	13/03	2	0%	Toute l'équipe	marron
Tests + Confirmation	14/03	18/03	2	0%	Toute l'équipe	marron
Docs d'installation du lot 4	18/03	24/03	3	0%	Toute l'équipe	marron
Phase de clôture	**31/03**	**14/04**	**8**	**0%**	Toute l'équipe	vert
Documentation sur la réalisation du projet	31/03	14/04	4	0%	FIX Arthur	vert
Documentation d'installation complète	31/03	14/04	4	0%	ERNST Nicolas	vert

https://docs.google.com/spreadsheets/d/e/2PACX-1vSgdCAX9Y3Hh7H1E9mTTIEmPpiMAi6B6D_JGZxicm9RvOHK_FbKU-vLlgIYM7pqnsc-Fo4917n5Uya7/pubhtml

Le planning réel a été construit pour documenter le déroulement effectif du projet, en mettant en évidence les écarts éventuels entre la théorie et la pratique (retards, ajustements, imprévus…). Cette double approche permet ainsi une analyse complète de la gestion du temps, et offre des enseignements utiles pour l'optimisation des futurs projets.

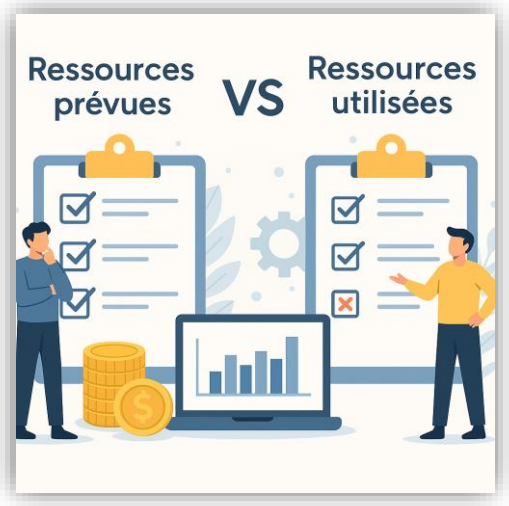
B) Ressources prévues VS ressources utilisées

Concernant les ressources humaines, la répartition du travail entre les deux membres de l'équipe s'est déroulée comme prévu. Chacun a respecté ses engagements, et les 315 heures estimées ont été tenues. Le budget global a également été maîtrisé, avec des dépenses conformes aux prévisions. Cependant, une erreur a été commise dans le choix initial du matériel réseau. Un routeur Cisco avait été sélectionné pour gérer les connexions VPN, mais il

s’est avéré incompatible avec pfSense, notamment en ce qui concerne la redondance et les règles de pare-feu. Ce contretemps a entraîné une perte de temps et a nécessité le remplacement du matériel.

Un modèle de routeur plus adapté à pfSense a donc été acquis, ce qui a permis de poursuivre la configuration du réseau sans compromettre le reste du projet. Cette situation met en évidence l’importance d’une veille technique plus rigoureuse en amont. D’un point de vue technique, tous les serveurs, systèmes et logiciels prévus ont été correctement installés, notamment les environnements Windows Server, Ubuntu, et les outils comme Asterisk, Modoboa, PRTG et eBrigade. Certaines configurations, notamment au niveau de la supervision et de la sécurité, doivent encore être améliorées. Par ailleurs, un changement a également été effectué concernant le serveur destiné à héberger eBrigade en DMZ. Initialement prévu sous Debian, il a finalement été remplacé par Ubuntu Server, jugé plus accessible pour ce type d’hébergement web et mieux documenté, facilitant ainsi le déploiement.

Dans l’ensemble, les ressources ont été bien utilisées, mais cette erreur de matériel rappelle l’importance de bien vérifier la compatibilité entre équipements et logiciels en amont d’un projet.



C) Problèmes rencontrés et solutions apportées ou envisagées

Le projet n’a pas échappé à quelques difficultés techniques. L'intégration avancée de certains capteurs dans PRTG a exigé un temps d’adaptation plus long que prévu, en raison de la spécificité de certains équipements. Cette difficulté a été surmontée grâce à la consultation approfondie de la documentation

officielle et des forums spécialisés. Le déploiement sécurisé de la plateforme eBrigade en DMZ a également représenté un défi important. Il a fallu adopter une stratégie stricte d'isolation réseau à travers pfSense et ajuster les règles de pare-feu pour concilier sécurité et accessibilité. Ces situations ont été traitées avec rigueur et ont permis à l'équipe de monter en compétence sur des solutions techniques de haut niveau.

3) Solutions

Nous avons réalisé une analyse approfondie des différentes solutions techniques disponibles afin de répondre aux exigences du projet d'optimisation de la résilience informatique des Centres Opérationnels Départementaux. Cette évaluation a pris en compte les performances des solutions, leur coût, ainsi que leur adéquation aux besoins spécifiques identifiés dans l'expression des besoins.

Cette démarche nous a permis d'identifier les solutions les plus adaptées, garantissant ainsi que chaque aspect du projet soit couvert de manière optimale, tout en respectant les exigences de sécurité, de disponibilité et d'accessibilité définies.

Dans le cadre de la mise en place d'un accès distant sécurisé, les solutions retenues devront permettre l'implémentation d'un VPN Road Warrior assurant la connexion entre les agents de terrain et le système d'information des Centres Opérationnels Départementaux. Concernant la gestion des services internes, les infrastructures déployées seront compatibles avec des serveurs Windows Server assurant les fonctions essentielles telles que l'authentification centralisée via Active Directory, la gestion des ressources réseau et la redondance des services critiques.

En ce qui concerne la supervision et le monitoring des équipements critiques, les solutions choisies devront permettre un suivi en temps réel de l'état des serveurs et de l'infrastructure réseau, avec des alertes automatiques envoyées aux administrateurs en cas d'incident. Enfin, les règles de sécurité, incluant les configurations de pare-feu, la segmentation des réseaux et la gestion des accès VPN, seront définies et appliquées conformément aux standards en vigueur pour assurer une protection optimale des systèmes.

Lot 1:
2 Routeurs/Pare-Feu avec 1 VPN RoadWarrior

Lot 2:
1 Serveur Windows Serveur 2022 Standard avec les rôles: AD DS (principal), PRTG.
1 Serveur Windows Core avec AD DS (secondaire)

Lot 3:
1 Serveur Debian/Ubuntu avec Asterisk et Modoboa

Lot 4:
1 Serveur Ubuntu en tant que Serveur web en DMZ hébergeant eBrigade

A) Solutions techniques et logicielles

a) PfSense

Figure 1: Pfsense

Pour assurer la mise en œuvre d'une solution de routeurs haute disponibilité avec VPN, nous avons choisi pfSense. Cette solution open-source et robuste offre toutes les fonctionnalités nécessaires pour sécuriser et optimiser le réseau tout en restant économique.

Grâce à CARP et PFSYNC, pfSense permet une redondance des routeurs, garantissant la haute disponibilité des connexions Internet et des services. Son module VPN (OpenVPN/IPSec) assure un accès sécurisé aux ressources internes pour les utilisateurs distants tout en utilisant les comptes Active Directory pour l'authentification.

En plus de ses performances, pfSense dispose d'une interface web intuitive, simplifiant la gestion et l'administration du réseau. Son caractère open-source permet une réduction significative des coûts tout en bénéficiant d'une large communauté et d'une documentation complète.

Cette solution répond donc parfaitement aux exigences de sécurité, haute disponibilité et accessibilité des services dans un cadre budgétaire maîtrisé.

b) Active Directory

Figure 2: Active Directory

Pour la gestion des utilisateurs et des permissions, nous avons opté pour Active Directory Domain Services (AD DS) sous Windows Server. Ce choix permet une gestion centralisée et sécurisée des comptes utilisateurs, facilitant ainsi l'accès aux ressources réseau et aux applications tout en garantissant un haut niveau de contrôle.

L'implémentation de deux serveurs AD (principal et secondaire) assure la continuité de service en cas de panne d'un des contrôleurs de domaine. De plus, AD DS est intégré aux autres services comme la messagerie, la téléphonie IP et le VPN, garantissant une authentification unique et simplifiée pour les utilisateurs.

En choisissant AD DS, nous répondons aux exigences de sécurité, scalabilité et administration centralisée, tout en s'appuyant sur une technologie éprouvée et compatible avec l'ensemble des outils utilisés.

c) PRTG Network Monitor

Figure 3: PRTG

Pour assurer la supervision et le monitoring de l'ensemble de l'infrastructure, nous avons retenu PRTG Network Monitor. Cet outil performant permet une surveillance en temps réel des routeurs, serveurs et services critiques, garantissant ainsi une meilleure réactivité en cas de problème.

PRTG offre une interface graphique intuitive permettant de visualiser l'état du réseau et de détecter rapidement toute anomalie.

Il permet également de configurer des alertes par email pour prévenir les administrateurs en cas d'incident, contribuant ainsi à une maintenance proactive et efficace.

En intégrant PRTG à notre architecture, nous garantissons une disponibilité maximale des services et une réduction des temps d'interruption grâce à une gestion optimisée des alertes et des historiques de pannes.

d) Asterisk

Figure 4: Asterisk

Pour la mise en place d'un serveur de téléphonie IP, nous avons choisi Asterisk, une solution open-source robuste et largement utilisée pour la gestion des communications VoIP.

Asterisk permet de gérer les appels internes et externes, les files d'attente, la messagerie vocale et les conférences téléphoniques. Il est compatible avec les softphones, les téléphones SIP et les trunk SIP pour l'interconnexion avec des opérateurs téléphoniques.

L'un des avantages d'Asterisk est sa flexibilité et sa personnalisation avancée, permettant d'adapter la solution aux besoins spécifiques de l'organisation. Il peut être configuré pour s'intégrer à Active Directory, facilitant ainsi la gestion des comptes utilisateurs et l'authentification.

En choisissant Asterisk, nous garantissons une solution de téléphonie économique, modulaire et évolutive, capable de s'adapter aux besoins futurs de l'infrastructure.

e) Modoboa

Figure 5: Modoboa

Pour la mise en place d'un serveur de messagerie performant et sécurisé, nous avons opté pour Modoboa, une solution open-source et complète permettant d'héberger un service de messagerie professionnel.

Modoboa supporte les protocoles IMAP, SMTP et POP3, offrant une expérience fluide pour les utilisateurs avec un webmail intégré. Il permet également une authentification centralisée via Active Directory, simplifiant ainsi la gestion des comptes.

En plus de sa flexibilité, Modoboa intègre des outils de sécurité avancés comme SPF, DKIM et DMARC, garantissant la protection contre le spam et le phishing. Ce choix nous permet de proposer une solution fiable, sécurisée et économique pour les communications internes et externes.

e) eBrigade

Figure 6: eBrigade

Pour la gestion des interventions et des équipes, nous avons retenu eBrigade, une application web open-source répondant parfaitement aux besoins de gestion de plannings, de missions et de ressources humaines.

Déployé sur un serveur Ubuntu, eBrigade est accessible via une interface web sécurisée, permettant aux utilisateurs de consulter leurs tâches et leurs plannings depuis n'importe quel appareil.

Afin de garantir une protection optimale, le serveur eBrigade est hébergé en DMZ, avec des règles de pare-feu strictes assurant un accès sécurisé sans compromettre le réseau interne.

Cette solution offre une gestion efficace et centralisée des opérations, tout en garantissant un accès sécurisé et fluide aux utilisateurs.

1. Windows server 2022

Pour mettre en place un annuaire d'authentification ainsi que les autres services, il faudra disposer d'une licence Windows server 2022.

Deux types de licences sont proposées :

- Standard
- Datacenter

Voici un tableau récapitulatif des deux types de licences :

Windows Server 2022 Standard 16 cœurs

Nombre de VM montable	Prix (HT)
2	844,99 €

Tableau 1: WS STD 2022

Windows Server 2022 Datacenter 16 cœurs	
Nombre de VM montable	Prix (HT)
Illimitées	4460,99 €

Tableau 2: WS DC 2022

Nous avons opté pour la version datacenter qui permet plus de liberté (VM illimitées). Cette licence convient au projet.

2. Serveur Physique

Pour mettre en place Windows Server 2022 ainsi qu'Ubuntu Server et un Debian Server, nous aurons besoin d'un serveur physique.

Avant tout voici la configuration requise pour mettre en place Windows Server 2022 :

Composant	Caractéristiques
Processeur	3.1 Ghz Multicore
RAM	16Go ou plus
Espace Disque	40Go

Tableau 3: Configuration requise WS2022

Voici la configuration requise pour mettre en place un Ubuntu Server :

Composant	Caractéristiques
Processeur	1 Ghz Multicore
RAM	512Mo ou plus
Espace Disque	2.5Go (Installation minimale)

Tableau 4: Configuration requise Ubuntu Server

Voici la configuration requise pour mettre en place un Debian Server :

Composant	Caractéristiques
Processeur	1 Ghz Multicore
RAM	256Mo ou plus
Espace Disque	10Go

Tableau 5: Configuration requise Debian Server

Ici nous nous sommes intéressés à deux serveurs qui sont le DELL PowerEdge R450 et le Lenovo ThinkSystem SR630 V2 4314 32Go.

Dell met à disposition un outil de configuration sur son site web pour personnaliser les spécifications des serveurs. Leur matériel est d'origine française, ce qui évite les frais de douane. De plus, Dell assure la configuration du RAID et du système d'exploitation.

Nous avons choisi de le comparer à Lenovo, un acteur majeur du marché, ainsi qu'à leur serveur le moins cher.

Composant	DELL PowerEdge R450	Lenovo ThinkSystem SR630 V2 4314 32Go
Processeur	Xeon Gold 5315Y 3.2 GHz 8C/16T	Xeon Silver 4314 2.4Ghz 16C/32T
RAM	16Go RDIMM 3200MT/s	32Go DDR4 3200MT/s ECC
Espace Disque	3x 2.4To HDD	8x2.5To
Prix HT	4940,16 €	13 102,00 €

Tableau 6: Comparatif Serveurs

On peut constater une différence de prix allant du simple au double entre les deux serveurs. Le serveur de Dell est suffisant pour notre utilisation et ce tarif.

3. Routeur

Pour mettre en place le VPN qui permet une connexion intersite, nous aurons besoin d'un routeur.

Ici nous nous sommes intéressés à deux routeurs qui sont le MikroTik RB4011iGS+RM et le Cisco C927-4P.

Cisco est un leader mondial sur le marché des routeurs, réputé pour ses solutions réseau fiables et performantes, adaptées aux besoins des entreprises de toutes tailles. Il nous a semblé essentiel de faire le comparatif avec un de leur routeur.

Le routeur MikroTik se distingue par son excellent rapport qualité-prix, offrant de nombreuses fonctionnalités avancées à un coût très compétitif. Malgré son prix abordable, il propose des spécificités telles que plusieurs ports Gigabit Ethernet, un port SFP+ 10 Gbps, et un large support de protocoles VPN, en faisant un choix idéal pour les entreprises cherchant des performances élevées sans sacrifier leur budget.

Composant	Cisco C927-4P	MikroTik RB4011iGS+RM
Processeur	ARM-based CPU	Quad-core Cortex A15 (1.4 GHz)
RAM	2Go	1Go DDR3
Ports Ethernet	4xRJ45 + 1 WAN port	10xGigabit Ethernet + 1xSFP
VPN	Oui (IPsec, SSL VPN)	Oui (IPsec, SSTP, L2TP, OpenVPN, WireGuard)
Prix HT	533,86 €	245,65 €

Tableau 7: Comparatif Routeurs

Même s'il vaut plus du double de l'autre, nous allons opter pour le routeur Cisco, car il reste tout de même plus performant et il prend en compte le VPN que nous utilisons (IPsec).

B) Schéma Réseau Complet

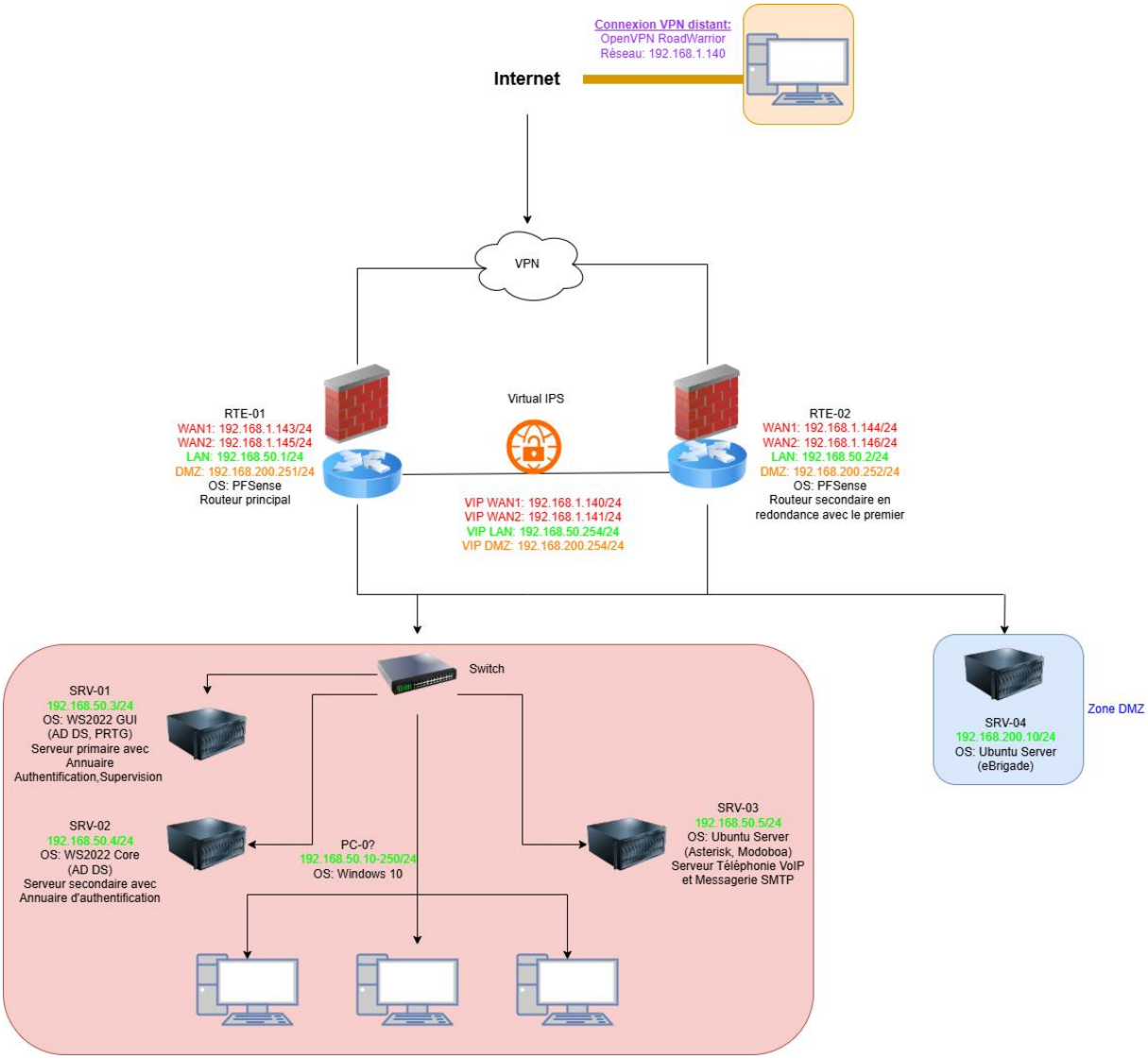


Figure 7:Schéma réseau

Le schéma réseau représente de manière visuelle l'architecture technique de l'infrastructure mise en place dans le cadre du projet. Il permet de comprendre la structure globale du système, les liaisons entre les différents équipements (serveurs, pare-feu, routeurs, postes clients, etc.), ainsi que leur rôle au sein du réseau.

C) Tableau de synthèse

Nom de la solution	Avantages	Désavantages	Coût	Bilan	Choix

PFSense	Open-source, fiable, complet en fonctionnalités (pare-feu, VPN, NAT, proxy). Large communauté et support commercial disponible.	Certaines fonctionnalités avancées nécessitent du matériel performant (ex : Netgate).	X	Solution mature et évolutive, idéale pour gérer le réseau et la sécurité.	V
CARP - PFsync	Permet la haute disponibilité et la redondance des pare-feu avec bascule automatique en cas de panne.	Configuration avancée requise, nécessite des machines identiques.	X	Assure une continuité de service critique.	V
XML RPC	Permet la synchronisation de configuration entre plusieurs instances PFSense, sans nécessiter un second pare-feu actif.	Moins performant que CARP-PFSync pour la haute disponibilité, pas de bascule automatique en cas de panne.	X	Moins adapté aux besoins de redondance et de haute disponibilité.	
OpenVPN RW	Configuration simplifiée, compatible avec plusieurs OS, sécurisé avec chiffrement fort.	Gestion fine des certificats et des règles de pare-feu nécessaire.	X	Solution flexible et sécurisée pour les connexions distantes des utilisateurs.	V
Centreon	Open-source, très puissant et flexible, adapté aux grandes infrastructures.	Interface plus complexe que PRTG, nécessite des compétences en administration Linux.	X	Meilleur contrôle sur la supervision, mais demande plus d'expertise.	
PRTG	Interface intuitive, déploiement rapide, alertes et supervision en temps réel.	Version complète payante, plus limité en open-source.	1 600€ / an pour la version complète.	Plus simple que Centreon mais avec un coût pour la version complète.	V
CheckMK	Supervision avancée avec auto-découverte des équipements.	Moins d'intégration native avec Windows que PRTG ou Centreon.	X	Centreon et PRTG sont plus adaptés au projet.	
Windows Server 2022	Intégration complète avec les outils Microsoft, gestion centralisée des utilisateurs et ressources.	Licence payante, nécessite une expertise pour l'administration.	Environ 1 000€ par serveur.	Solution éprouvée et standard pour la gestion d'annuaire et des services réseaux.	V
Asterisk	Open-source, très flexible, compatible avec de nombreux équipements VoIP.	Nécessite une configuration avancée et des connaissances télécom.	X	Meilleur choix pour une solution VoIP complète et évolutive.	V
3CX	Interface intuitive, support commercial et configuration rapide.	Version complète payante, dépendant d'un environnement Windows.	**295€/an minimum.**	Asterisk est plus ouvert et sans coût de licence.	
Ubuntu Server	Facile à installer et configurer, large communauté, mises à jour fréquentes et support commercial disponible.	Légèrement plus lourd que Debian, mises à jour parfois plus fréquentes	X	Meilleur choix pour un environnement nécessitant des mises à jour fréquentes et un	V

				support étendu.	
Debian	Très stable, idéal pour les serveurs nécessitant peu de maintenance, léger.	Moins de mises à jour, logiciels parfois moins récents, configuration légèrement plus complexe.	X	Debian est plus stable, mais Ubuntu est plus accessible et mieux documenté pour l'hébergement d'applications.	
Modoboa	Open-source, auto-hébergé, intégration avec Postfix et Dovecot.	Plus complexe à configurer qu'Exchange, nécessite du monitoring.	X	Meilleur choix pour une messagerie auto-hébergée économique.	V
Microsoft Exchange + Outlook	Fonctionnalités complètes, intégration parfaite avec Active Directory et Outlook.	Coût élevé des licences et de la maintenance.	Environ 700€ par utilisateur.	Trop coûteux pour le projet.	

Tableau 8: Tableau de synthèse solutions

Le tableau de synthèse a pour objectif de comparer les différentes solutions techniques envisagées dans le cadre du projet. Il centralise les informations clés pour chaque option : les avantages, les inconvénients, les coûts associés ainsi qu'un bilan global permettant d'évaluer leur pertinence.

4) Résultats

A) Résultats attendus VS résultats obtenus

Les résultats attendus pour ce projet comprenaient notamment la mise en place d'un VPN sécurisé de type Road Warrior, la supervision complète de l'infrastructure réseau via PRTG, la mise en œuvre d'une solution de téléphonie IP fonctionnelle, un serveur de messagerie interne sécurisé et l'intégration d'une plateforme web dédiée à la gestion des interventions. À l'issue du projet, la majorité de ces objectifs ont été atteints, mais certains résultats restent partiellement réalisés ou à améliorer.

La solution de téléphonie IP avec Asterisk a été correctement installée et permet d'assurer les communications internes. Le serveur Modoboa a également été mis en place avec succès, fournissant un service de messagerie fiable et conforme aux standards de sécurité. La plateforme eBrigade est déployée sur un serveur Ubuntu en DMZ et accessible via une interface web, bien que certaines configurations spécifiques soient encore en cours d'ajustement.

En revanche, la mise en œuvre du VPN Road Warrior avec OpenVPN n'a pas pu être finalisée dans les délais impartis. Des difficultés techniques liées à la configuration et à l'intégration dans l'infrastructure existante ont empêché sa mise en service opérationnelle. Le paramétrage des règles de pare-feu sous pfSense a été réalisé dans les grandes lignes, mais reste trop général et devrait être approfondi pour garantir une segmentation plus fine et une meilleure sécurité du réseau. De même, bien que l'outil PRTG soit installé et fonctionnel, la configuration des capteurs est jugée incomplète. Il manque notamment certains éléments de supervision avancée et des alertes spécifiques qui doivent encore être paramétrés pour atteindre un niveau de surveillance optimal.

En résumé, si la structure du projet est bien en place et que plusieurs briques fondamentales fonctionnent, certains points clés nécessitent encore des ajustements techniques. Ces écarts ne remettent pas en cause la viabilité de l'architecture proposée, mais appellent à une phase de finalisation post-projet afin d'atteindre pleinement les résultats initialement visés.

5) Analyse finale

A) Analyse et état final du projet

À la clôture de ce projet, un constat globalement positif peut être dressé, malgré certains écarts techniques. La grande majorité des objectifs fixés ont été atteints, notamment la mise en place des services critiques comme la messagerie, la téléphonie IP et la plateforme de gestion eBrigade. L'infrastructure réseau a été correctement installée, documentée et testée dans ses fonctions principales. Le client peut se satisfaire de la robustesse générale du système et de la qualité des solutions proposées, qui sont conformes à ses attentes stratégiques en matière de continuité d'activité.

B) Améliorations possibles

Néanmoins, plusieurs points nécessitent une attention particulière dans le cadre d'une potentielle phase de finalisation ou de maintenance. Le VPN Road Warrior, bien qu'anticipé dans l'architecture, n'a pas pu être mis en place correctement, ce qui impacte l'un des objectifs majeurs du projet : la connexion distante sécurisée. De plus, le paramétrage des règles de pare-feu et la configuration de PRTG restent trop généraux, ne permettant pas encore une supervision suffisamment fine ni une segmentation réseau pleinement sécurisée. Enfin, une erreur de choix matériel concernant le routeur initial (modèle Cisco incompatible avec pfSense) a généré une perte de temps non négligeable, compensée par l'achat d'un routeur plus adapté en cours de projet.

Ces difficultés témoignent de la complexité d'un déploiement complet dans un contexte aussi technique et de la nécessité d'approfondir certains points en amont. Elles ont cependant été gérées avec réactivité, et des solutions viables ont été apportées, ce qui a limité l'impact global sur le projet.

6) Conclusion

Le projet **NovaResQ** a été mené avec rigueur et implication, et son déroulement témoigne d'une capacité d'adaptation et de résolution de problèmes réelle de la part de l'équipe. Malgré des obstacles techniques ponctuels, l'essentiel de l'architecture réseau et des services critiques a été livré conformément aux attentes. L'échec de la mise en œuvre du VPN et les paramétrages encore

partiels ne remettent pas en cause la valeur globale de ce projet, mais montrent que certaines briques techniques doivent être approfondies dans le cadre d'un perfectionnement post-livraison.

Les choix technologiques, dans leur ensemble, ont été pertinents. La gestion du projet a su rester professionnelle, tant dans l'organisation des tâches que dans le respect du budget. Cette expérience a également été riche en enseignements, notamment sur la compatibilité entre matériels et logiciels, l'importance de la documentation technique, et la nécessité d'une planification réaliste des phases complexes.

Ce projet peut désormais constituer une base fiable pour une infrastructure opérationnelle en contexte de sécurité civile, tout en mettant en évidence les marges de progression nécessaires pour atteindre un niveau de maturité optimale.