Université Sorbonne Paris Nord
Section IUT Villetaneuse
2ère année BUT Réseau et Télécom

RAPPORT DE STAGE

Entreprise: DG ROBOTICS

ANNEE 2024-2025
UNIVERSITE SORBONNE PARIS NORD
99 Avenue Jean Baptiste Clément, 93430 Villetaneuse

JOURDAIN ELODIE

Durée: 14/04 - 15-06

Remerciement

Je tiens à remercier DG Robotics et en particulier Monsieur Gonçalves David pour m'avoir accordé sa confiance et offert l'opportunité de réaliser ce projet.

Grâce à son encadrement, ses conseils et ses retours d'expérience, j'ai pu approfondir mes compétences dans le domaine de l'administration réseau et de la sécurisation des systèmes d'information.

Enfin, je remercie Madame Louadj pour son suivi tout au long de ce projet.

Sommaire:

Abstract:

This report present the project carried out at DG Robotics, a company specializing in industrial programming. DG Robotics primarily operates in the fields of robotics, industrial computing, electronnics, and automation. In addition to offering services in these areas, the company also acts as a reseller of technical equipment.

The main objective of the project was to design and implemented a secure network infrastructure tailored to the needs of a small business. This included the installation of a NAS server, the creation of a local network segmented between administrator and guest users, and the integration of secure remote access via VPN.

The project have enhanced the availability, confidentiality, integrity, and traceability of the company's data, while also ensuring regular backups and controlled access to internal resources.

This document outlines the different stages of the project, the technical decisions made, the challenges encountered, and the technical and professional skills acquired throughout its completion.

Introduction

Dans un contexte où la sécurité des données et la fiabilité des accès réseau deviennent des enjeux majeurs, même pour les petites structures, le projet confié par DG Robotics consistait à moderniser et sécuriser son infrastructure informatique interne.

Ce projet, qui m'a été confié durant mon stage, a été l'occasion de mener une refonte complète du réseau local.Travailler auprès d'un auto-entrepreneur m'a permis d'intervenir sur l'ensemble du processus, depuis la définition des besoins jusqu'à l'installation final, en passant par la recherche de matériel adapté et la configuration réseau.

L'étude a porté principalement sur :

- Le choix et l'installation d'un serveur NAS pour le stockage sécurisé des données sensibles et l'enregistrement de flux vidéo.
- La mise en place d'un accès distant sécurisé par VPN.
- La segmentation du réseau pour séparer les utilisateurs administrateurs et invités.
- L'organisation d'un système de sauvegardes régulières pour assurer la disponibilité et la pérennité des données.

Ce rapport présente l'ensemble des étapes réalisées, les choix techniques retenus, et les enseignements tirés de cette expérience. Il témoigne également de l'autonomie, de la rigueur et de l'adaptabilité nécessaires pour piloter un projet informatique dans une structure à taille humaine.

I / Présentation de l'entreprise DG ROBOTICS:

DG ROBOTICS est une entreprise fondée par David Gonçalves, auto-entrepreneur spécialisé dans la programmation industrielle. Elle exerce principalement son activité dans les domaines de la robotique, de l'informatique industrielle, de l'électronique et de l'automatisme. En plus des prestations de service dans ces secteurs, l'entreprise propose également la re-vente de matériel technique.

DG ROBOTICS intervient dans le champ plus large de la programmation, du conseil et d'autres activités informatiques liées à l'ingénierie industrielle.

L'entreprise adopte une forme d'exercice commerciale à travers un statut d'auto-entrepreneur. Elle met en œuvre son expertise pour offrir des solutions techniques sur mesure à ses clients, dans le cadre de projets d'automatisation, de développement de systèmes programmés et de mise en service de dispositif robotisé.

II / Description du projet

A - Contexte du projet

Lors de mon stage chez DG Robotics, il m'a été confié un projet de refonte du réseau informatique de l'entreprise. Ce projet s'inscrit dans une volonté de renouvellement technologique, face à un environnement devenu inadapté aux besoins actuels. L'ancien matériel montrait des signes de lenteur, de manque de fiabilité et une interface de gestion peu ergonomique, ce qui compliquait les opérations techniques et ralentissait la productivité.

Mais au-delà de ces limites techniques, une autre raison a motivé ce projet : un incident de sécurité survenu auparavant. En effet, M. Gonçalves, le responsable de l'entreprise, a été victime d'une attaque par malware, plus précisément un ransomware. Ce type de logiciel malveillant chiffre les données de la victime et réclame ensuite une rançon pour les restituer. Cet épisode a mis en évidence la vulnérabilité de l'ancien système et l'importance cruciale de renforcer la sécurité informatique.

Face à ces contraintes, la direction a souhaité investir dans une solution plus moderne, facilitant à la fois l'administration du réseau et la protection des informations. Mon rôle est donc d'accompagner cette transition en concevant un réseau qui répond aux attentes techniques de l'entreprise tout en intégrant une dimension forte de sécurisation.Ce souci de sécurité se retrouve tout au long du projet, notamment dans la mise en place de sauvegardes régulières et sécurisées, aussi bien pour le poste principal que pour le NAS.

B - Missions

Mon intervention démarre en amont du projet technique : je dois d'abord analyser les besoins spécifiques de l'entreprise en matière de connectivités, d'accès distant, de gestion des données et de sécurité (donc pour chacun des objectifs du projet). Ce qui me permettra par la suite de faire une étude comparative du matériel réseau afin de proposer une architecture adaptée aux usages et au volume de données à traiter.
Une fois le choix du matériel validé, je m'occuperai de son déploiement physique, de la mise en réseau des différents composants, ainsi que de la configuration des accès, des droits, et des services. L'ensemble de ces tâches devra être exécuté avec une réflexion spécifique à l'entreprise pour permettre un fonctionnement fluide, évolutif et sécurisé du nouveau réseau.

C - Matériel / logiciels utilisés

- **NAS Synology DS224+ :**
  Utilisé pour centraliser les fichiers sensibles de l'entreprise et permettre les sauvegardes automatiques. Il servira également de support pour l'enregistrement vidéo des caméras de sécurité.

- **Routeur Netgear Nighthawk RS300 :**
  Ce routeur performant permet de créer un réseau stable avec de bonnes performances, tout en intégrant des fonctions de sécurité avancées comme le contrôle d'accès, la segmentation réseau, et la gestion VPN.

- **Caméras IP :**
  Des caméras de surveillance connectées au réseau pour assurer la traçabilité visuelle. Elles enregistrent en continu ou par détection de mouvement, avec stockage des images sur le NAS.

- **Disque dur externe dédié aux sauvegardes :**
  Branché au NAS, il permet de créer des copies de sécurité mensuel des données critiques.

- **Logiciel Synology DSM (DiskStation Manager) :**
  L'interface de gestion du NAS. Elle permet de configurer les accès, les sauvegardes, la sécurité (toute la configuration qui peut ce faire sur le NAS) et est nativement installée.

- **OpenVPN :**
  Utilisé pour établir une connexion sécurisée entre les utilisateurs distants et le réseau local, en chiffrant les échanges.

D - Objectif

Dans le cadre de ce projet, l'objectif principal est de mettre en place une infrastructure réseau sécurisée permettant l'accès à des données sensibles depuis n'importe quel endroit, tout en garantissant leur confidentialité et leur intégrité. Pour cela, un serveur physique sera choisi en fonction de critères techniques définis à l'avance. Ce serveur aura pour rôle central le stockage des données sensibles ainsi que l'enregistrement des flux provenant des caméras de sécurité.

Le réseau sera divisé en deux segments distincts. Le premier sera destiné aux administrateurs, qui disposeront de tous les droits d'accès et de gestion sur le système. Le second sera réservé aux invités, dont les droits seront limités et définis ultérieurement en fonction des besoins. Cette séparation permettra de limiter les risques liés à une mauvaise manipulation ou à une intrusion.

L'accès à distance aux données devra être sécurisé, notamment par la mise en place de mots de passe robustes et, potentiellement, d'autres mesures d'authentification si elles sont requises par la suite. De plus, afin de garantir la disponibilité des données, une sauvegarde hebdomadaire sera effectuée sur le NAS Synology.

Nous pouvons constater que ce projet respecte les principes fondamentaux du modèle DCI, à savoir la Disponibilité, la Confidentialité, l'Intégrité et la Traçabilité.

La confidentialité est assurée par la mise en place de deux réseaux distincts : invité et administrateur, chacun avec des droits adaptés. L'intégrité est garantie grâce aux sauvegardes hebdomadaires, permettant de restaurer les données en cas de modification ou de perte. La disponibilité est assurée par l'accès distant sécurisé au serveur, permettant de consulter les données sensibles à tout moment. Enfin, la traçabilité est prise en compte via l'enregistrement de journaux d'accès.

III / Organisation de l'étude

Comme pour tout projet, j'ai commencé par la réalisation d'un planning sous la forme d'un diagramme de Gantt. En effet cette étape est cruciale pour organiser le travail à venir et suivre l'avancement du projet de manière structurée.

Cependant, comme c'est souvent le cas avec les plannings prévisionnels, celui-ci n'est pas resté fidèle à 100 % tout au long du projet. Des imprévus sont venus perturber certaines tâches, entraînant des retards, mais à l'inverse, certaines étapes ont été réalisées plus rapidement que prévu ce qui a permis de gagner du temps.

C'est pourquoi il existe un écart visible entre le Gantt initial et celui réalisé en fin de projet, reflétant la réalité du déroulement de la mission.

Planning initial

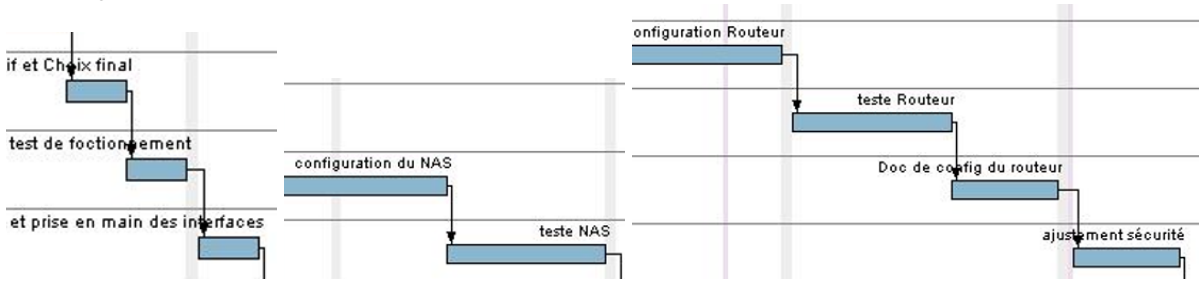


figure 1

Planning réalisé

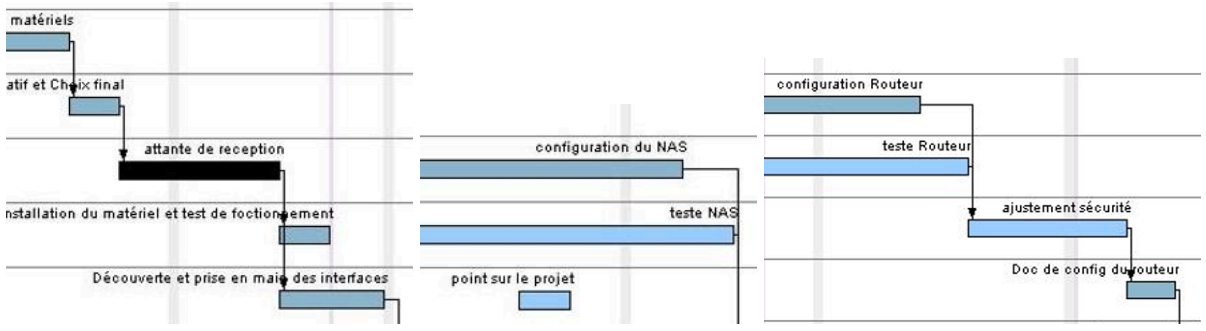


figure 2

Les parties en bleu clair servent ici à mettre en évidence les ajustements apportés au planning initial, tandis que la section noir correspond à une tâche à laquelle je n'avais pas pensé lors de la planification : l'attente du matériel.
Cela illustre bien la différence entre un projet scolaire et un projet en conditions réelles.

Dans le cadre professionnel, chaque détail logistique compte, y compris les délais de livraison ou les imprévus techniques.

Au départ, je pensais réaliser tous les tests à la fin des configurations. Mais je me suis rapidement rendue compte que valider chaque étape au fur et à mesure était plus logique. Par exemple, après avoir configuré une sauvegarde ou mis en place un pare-feu, je testais directement son bon fonctionnement afin de ne pas passer à une autre tâche sans être certaine que celle-ci était finalisée.

Enfin, j'ai également ajusté l'ordre de certaines tâches. Par exemple, les ajustements de sécurité ont été réalisés avant la rédaction du document de configuration du routeur. Cela m'a permis d'inclure les derniers réglages (comme retirer l'autorisation de connexion de mon ordinateur) directement dans la documentation finale ainsi que dans la configuration.

IV / Analyse des problèmes et solutions

A - Analyse des besoins et choix/installation du matériel

J'ai débuté ce projet en identifiant les besoins spécifiques de l'entreprise, ainsi que les contraintes techniques et organisationnelles qui y étaient associées. Cette phase préliminaire a été déterminante pour orienter les choix à venir et assurer la cohérence de l'ensemble de la mise en œuvre. Une fois ce cadre posé, j'ai pu procéder à une première sélection du matériel en m'appuyant sur plusieurs critères, parmi lesquels :

- la capacité à gérer des données sensibles,
- la possibilité d'accéder à distance de manière sécurisée,
- la compatibilité avec un usage multi-utilisateur et évolutif.

J'ai ensuite éffectué toutes les recherches nécessaires et consulté diverses documentations techniques sur les équipements envisagés. Afin d'avoir un aperçu plus visuel pour faciliter le choix, j'ai fait un tableau comparatif recensant fonction par fonction, ce que chaque matériel (que ce soit le routeur ou le serveur NAS) est capable ou non de faire. Cela m'a permis de comparer efficacement les capacités de chaque appareil et d'identifier rapidement ceux qui répondaient le mieux aux attentes. À l'issue de cette analyse, deux équipements

sont sortis du lot, le NAS *Synology DS224+* et le routeur *Netgear RS300* se sont révélés être les équipements les plus pertinents, puisqu' ils répondent à un maximum de critères tout en offrant un bon rapport qualité-prix.

Suite à cela et une fois le matériel reçu, j'ai pu passer à la phase d'installation. Cette étape a été une expérience intéressante et différente de mes précédentes pratiques. En effet, dans le cadre de mes cours, j'ai principalement l'habitude de manipuler des routeurs et de réaliser des simulations de réseau (avec des topologies incluant des routeurs, des serveurs et des machines), le tout en utilisant uniquement un terminal Linux en ligne de commande. Ici, la situation était différente : le routeur comme le NAS disposent d'interfaces graphiques (IHM) assez complètes qui facilitent la configuration du matériel (adresses IP, pare-feu, gestion du stockage, etc.).

Ce changement d'environnement m'a également confronté à l'utilisation d'un ordinateur sous Windows pour la configuration du réseau, ce qui m'a permis de découvrir de nouvelles méthodes de travail. Notamment, j'ai appris à créer des ponts réseau directement via les paramètres réseau de Windows, alors que je n'avais jusqu'à présent vu ces opérations uniquement en ligne de commande sur Linux. Cela m'a permis d'enrichir ma compréhension des outils réseau et d'adapter mes compétences à différents types d'environnements techniques.

B - Première prise en main du NAS

Dès la première connexion au NAS Synology, la création d'un volume s'est imposée comme une étape préalable indispensable. Elle permet de définir l'espace de stockage sur lequel les fichiers seront enregistrés et les services s'appuieront. Une fois cette configuration réalisée, j'ai pris le temps d'explorer l'interface web afin de me familiariser avec les différentes fonctionnalités proposées.

Cette exploration m'a permis d'identifier plusieurs options intéressantes, notamment en matière de sécurité, que j'ai pu activer immédiatement. Par exemple, j'ai mis en place un système de blocage automatique des adresses IP après plusieurs tentatives de connexion échouées dans un court laps de temps, afin de prévenir les attaques par force brute. J'ai également activé le chiffrement des communications via le protocole TLS/SSL pour garantir la sécurité des échanges avec le NAS.

En parcourant l'interface, j'ai aussi découvert des fonctionnalités proches de celles d'un Active Directory, comme la gestion des utilisateurs et des groupes avec différents niveaux de

droits. J'ai ainsi créé un compte "invité" avec des permissions restreintes, et un compte "admin" doté de l'ensemble des privilèges, afin de mieux contrôler les accès par la suite.

Enfin, j'ai remarqué que le NAS intégrait une fonctionnalité de pare-feu, cela a constitué la première grande étape de la configuration réseau que je détaillerai dans le paragraphe suivant.

C - Mise en place des pares feux :

Au début du projet, j'avais provisoirement configuré le même mot de passe pour l'ensemble des équipements. Bien que celui-ci soit robuste, le fait qu'il soit identique sur tous les matériels représentait un risque critique. C'est pourquoi, dès la prise en main du NAS Synology, j'ai commencé par configurer un pare-feu afin de restreindre les accès.

Au début du projet, j'étais connecté directement au Synology avec un câble Ethernet. Mon ordinateur et le NAS n'étaient donc pas sur le même réseau. En effet le Synology était déjà branché au routeur et recevait une adresse IP locale de ce réseau ("Reseau routeur")via le serveur DHCP du routeur. De son côté, mon PC était encore connecté à la Livebox, et recevait une adresse IP différente, issue d'un autre réseau ("Reseau box") attribuée par le serveur DHCP de la Livebox.

Cette séparation empêchait mon ordinateur d'accéder au NAS. Pour contourner ce problème, j'ai créé une règle de pare-feu temporaire. Elle autorisait uniquement l'adresse IP de mon PC à accéder au Synology, ce qui m'a permis de poursuivre la configuration en toute sécurité.

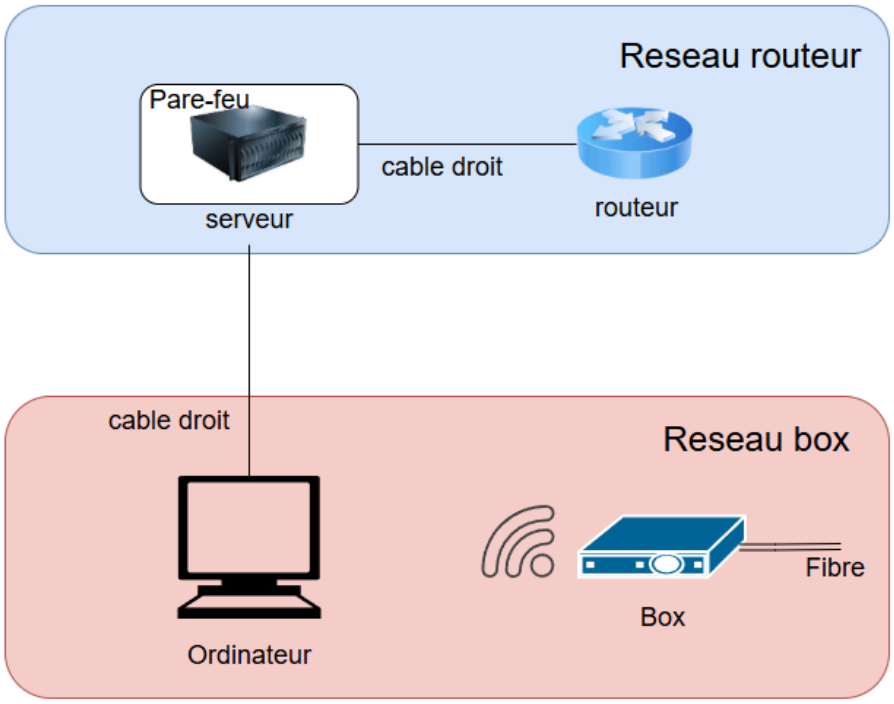


figure 3

Une fois le réseau correctement câblé et structuré, cette règle temporaire a été supprimée. D'autres, en revanche, ont été maintenues tout au long du projet, notamment celles qui restreignent l'accès à l'interface d'administration du NAS uniquement aux adresses IP du réseau interne.

Certaines règles ont aussi évolué en fonction de l'avancement du projet. Par exemple, les règles bloquant les connexions distantes (comme celles nécessaires au fonctionnement de QuickConnect ou OpenVPN) ont été désactivées temporairement pour permettre la mise en place des accès à distance, puis réactivées ou ajustées une fois les tests terminés et les configurations stabilisées.

Cela m'a permis de travailler efficacement, tout en gardant une structure de sécurité évolutive : des règles temporaires pour les phases de test, et des règles définitives qui seront actives.

Cette configuration fine du pare-feu a donc constitué la première grande étape de sécurisation du réseau. Mais pour que cette sécurité soit pleinement efficace, il était également nécessaire de stabiliser l'infrastructure réseau. En particulier, la situation

provisoire avec deux réseaux distincts (l'un relié à la box, l'autre au routeur) devait être résolue par la mise en place d'une connectivité Internet unifiée et maîtrisée. C'est donc cette étape qui a ensuite mobilisé mon attention.

D - Mise en place de la connectivité Internet

Dans le cadre de ce projet, l'un des objectifs techniques fixés était de remplacer la box Internet fournie par le fournisseur d'accès (FAI) par un routeur professionnel, en l'occurrence un Netgear Nighthawk RS300. L'idée derrière ce choix était d'avoir un meilleur contrôle sur le réseau, d'optimiser la sécurité et d'exploiter les fonctions avancées que ce type de matériel permet (gestion fine des VLANs, pare-feu, VPN, etc…). Cependant, dès cette première étape, nous avons rencontré une contrainte matérielle importante.

En effet, la fibre fournie par le FAI arrivait directement via un câble optique qui se connectait à la box, et le routeur ne disposait pas de port SFP (fibre) compatible avec ce type de raccordement. Il nous était donc impossible de brancher directement la fibre optique sur le routeur.

Nous avons envisagé dans un premier temps d'activer le mode bridge (pont) sur la box afin qu'elle transmette simplement la connexion Internet sans faire de routage, laissant cette fonction au routeur. Cela aurait permis de respecter notre architecture initiale. Malheureusement, après plusieurs vérifications, nous avons constaté que le modèle de box utilisé (une LiveBox), ne proposait pas cette option, ce qui ma a obligé à revoir notre stratégie.

Plusieurs alternatives ont été envisagées. L'une d'elles consistait à utiliser un module SFP externe compatible avec le port WAN du routeur, ce qui aurait permis de connecter directement la fibre optique au routeur via un adaptateur. Une autre option consistait à insérer un boîtier ONT (Optical Network Terminal) entre la fibre et le routeur, jouant le rôle d'interface entre la fibre optique et une prise Ethernet standard. L'ONT est un équipement essentiel dans les installations FTTH (Fiber To The Home), car il permet de convertir le signal lumineux transmis par le câble de fibre optique en un signal électrique exploitable par les équipements Ethernet, comme un routeur classique. Il agit ainsi comme un traducteur entre la technologie fibre optique et le monde IP, garantissant une transition fluide et stable des données. Ce type de boîtier est parfois intégré à la box fournie par le FAI, mais peut aussi être séparé dans une architecture plus modulaire.

Cependant, ces deux solutions présentaient des inconvénients majeurs : elles impliquaient du matériel supplémentaire, donc des délais d'attente liés à la commande et à la livraison, mais aussi une phase de configuration et d'incertitudes techniques (compatibilité, stabilité, etc.).

Face à ces contraintes, nous avons finalement opté pour une solution plus pragmatique : : désactiver le Wi-Fi de la Livebox et connecter un câble Ethernet entre le port LAN 2.5G de la Livebox et le port WAN du routeur pour n'avoir que le routeur connecté à la Livebox, et ainsi traiter la Livebox comme un modem classique. Cette méthode consiste à rediriger l'ensemble du trafic réseau vers une adresse IP spécifique, ici celle du routeur. Cela permet de faire passer tout le flux réseau vers le routeur sans filtrage ni gestion particulière de la box, tout en gardant celle-ci comme passerelle d'accès Internet. Autrement dit, la box est utilisée ici principalement comme un modem; une fonction qui consiste à convertir les signaux optiques du FAI en un signal Ethernet que le routeur peut ensuite exploiter. Même si cela ne correspondait pas exactement à notre plan initial, cette solution s'est révélée stable et efficace dans notre contexte.

Cette situation m'a permis de mieux comprendre les rôles respectifs d'un modem, d'un routeur et d'une box dans un réseau domestique ou professionnel. J'ai compris que, dans ce cas précis, la box se limitait à assurer la connexion avec le fournisseur d'accès (rôle de modem), tandis que notre propre équipement prenait en charge l'ensemble des fonctions réseau : routage, gestion des VLANs et sécurité. Ce compromis entre la solution idéale sur le papier et les exigences du terrain illustre bien les réalités du travail en environnement réel, où les contraintes matérielles et logistiques imposent parfois des ajustements aux choix techniques initiaux

Une fois cette connectivité stabilisée, l'étape suivante a naturellement consisté à prendre en main le routeur, afin d'affiner les réglages réseau et de poser les bases d'une architecture cohérente. C'est dans cette continuité que j'ai entamé les premiers réglages sur le routeur, en commençant par l'exploration des fonctionnalités offertes.

E - Premiers réglages sur le routeur

Dès ma première prise en main du routeur, j'ai commencé par explorer l'ensemble des options disponibles via son interface. Comme pour le NAS, cette phase d'observation m'a permis d'avoir une vision claire des fonctionnalités offertes, et ainsi anticiper celles qui me seraient utiles par la suite dans le cadre du projet. J'ai notamment repéré les paramètres liés à l'accès à distance, ce qui m'a permis d'éviter de mettre en place trop tôt certaines règles

de sécurité, comme un filtrage strict par pare-feu, qui aurait pu me bloquer pendant la configuration. Le NAS étant déjà protégé, il était plus stratégique de laisser un accès temporairement plus souple au niveau du routeur. J'ai tout de même mis en place un pare-feu basique, suffisant pour garantir un minimum de sécurité sans gêner mon travail. J'ai aussi activé une option permettant de forcer l'utilisation du protocole HTTPS pour tout accès aux services web, afin de garantir une navigation sécurisée dès le départ. Enfin, j'ai configuré des réservations d'adresses IP, notamment pour la box, le routeur et le NAS, afin de mieux m'y retrouver dans mon adressage. Cela m'a permis d'identifier rapidement l'origine d'un problème en cas de conflit réseau ou d'erreur de configuration.

Ces premiers réglages ont permis d'assurer une base stable et sécurisée pour la suite des configurations. Une fois l'environnement maîtrisé, j'ai pu aborder une étape clé dans la structuration du réseau : sa segmentation.

F - Segmentation réseau

Dans le cadre de ce projet, j'ai décidé de mettre en place deux réseaux distincts afin de bien séparer les usages professionnels des usages personnels. J'ai donc configuré un réseau privé, dédié aux équipements sensibles comme le NAS et les postes administrateurs, et un réseau invité, qui permet uniquement un accès à Internet, sans pouvoir atteindre les ressources critiques du réseau principal. Ce réseau invité est notamment utilisé par le PC loisir, prévu pour un usage plus personnel ou non professionnel. Pour gérer cette séparation, je suis simplement passée par le routeur en créant deux réseaux Wi-Fi différents (deux SSID), ce qui m'a permis d'éviter l'ajout de matériel supplémentaire comme un switch. Grâce à cette configuration, j'ai pu renforcer la sécurité du réseau tout en gardant une architecture simple et adaptée à la taille du projet.

Topologie du réseau:

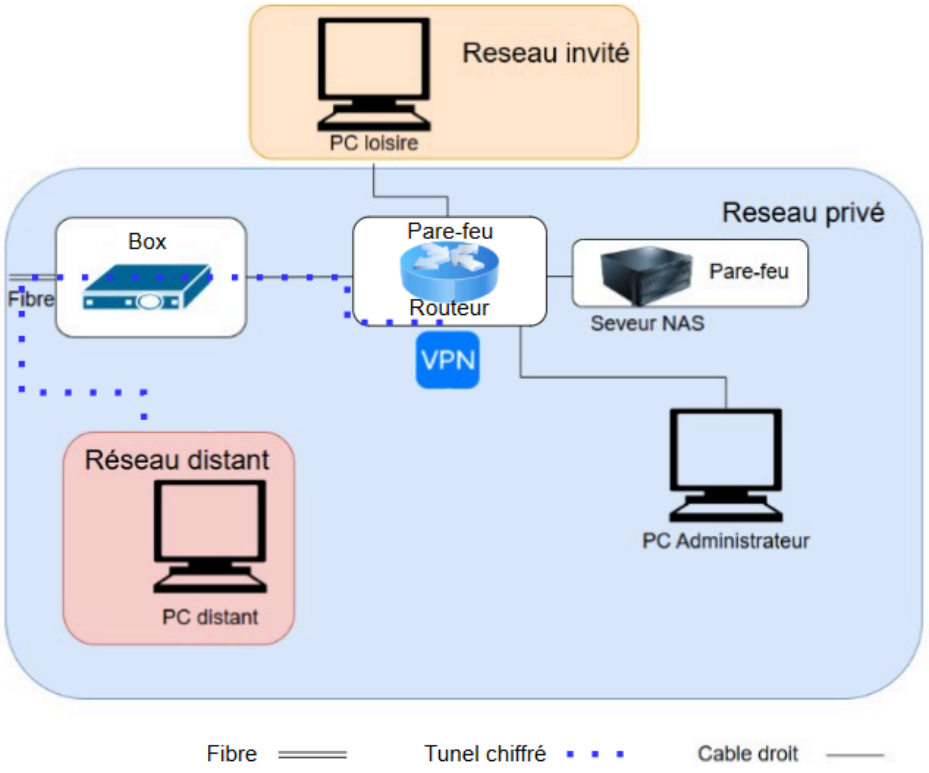


figure 4

G - Accès distant sécurisé

Dans le cadre de ce projet, il était prévu de mettre en place un accès distant sécurisé, à la fois pour assurer l'administration du réseau en situation de télétravail, et pour répondre à un besoin exprimé par M. Gonçalves : pouvoir accéder à son poste de travail et à ses fichiers lors de ses déplacements. L'objectif était donc d'assurer à la fois la supervision technique du réseau à distance et l'accès aux ressources professionnelles, peu importe le lieu.

Dans un premier temps, j'ai envisagé d'utiliser l'interface d'administration à distance du routeur. Cette solution, intégrée à certains modèles de routeurs professionnels, permet de se connecter directement à l'interface web de gestion du routeur depuis l'extérieur, via une adresse IP publique ou un nom de domaine. Cela permet une configuration fine des paramètres réseau sans passer par une machine intermédiaire. Cependant, dans notre cas, cette fonctionnalité n'était pas disponible sur le routeur Netgear Nighthawk RS300. Nous avons donc dû nous tourner vers une autre méthode.

L'alternative retenue a été la mise en place d'une connexion via le protocole Remote Desktop Protocol (RDP) vers un ordinateur déjà présent sur le réseau local. Contrairement à l'administration directe du routeur, cette méthode implique d'accéder à une machine du

réseau pour ensuite, à partir de celle-ci, gérer les autres équipements (comme le routeur ou le NAS). C'est donc une approche indirecte, mais qui permet malgré tout de reprendre la main sur l'ensemble du réseau à distance.

Bien que je n'ai mis en place aucun filtrage strict sur le routeur au départ, certaines sécurités sont initialement activées par l'équipement. Il m'a donc fallu ouvrir manuellement le port utilisé par le protocole RDP afin de garantir une connexion fluide et sans blocage.

Pour sécuriser cette connexion, deux mesures principales ont été mises en œuvre. Tout d'abord, un VPN déjà actif sur la machine distante assurait un tunnel chiffré entre le réseau local et le poste de travail distant, empêchant toute interception des données. Ensuite, une redirection de port spécifique a été configurée sur le routeur, permettant de limiter les ouvertures réseau aux seuls services nécessaires.

Une fois cette première solution en place et opérationnelle, une alternative plus stable et autonome m'a été proposée : héberger une machine virtuelle directement sur le NAS Synology. Cette approche s'est révélée particulièrement avantageuse, car elle permet de libérer le poste physique utilisé jusque-là pour le RDP; ce qui réduit la consommation électrique, tout en garantissant une session distante stable et constante, indépendamment de l'activité locale. Étant donné que le NAS reste allumé en permanence pour assurer le stockage et les sauvegardes, il s'agissait d'une solution optimisée.

Grâce au service QuickConnect de Synology, j'ai pu accéder au NAS à distance et y installer une machine virtuelle dédiée à l'administration. Cette VM m'a permis de poursuivre la configuration du routeur et du NAS comme si j'étais sur place. Cette approche, bien qu'un peu plus technique à mettre en œuvre, s'est montrée fiable, sécurisée, et particulièrement adaptée aux besoins du projet.

Avant cette expérience, j'avais encore du mal à concevoir les machines virtuelles comme des systèmes à part entière, capables d'assurer les mêmes rôles qu'un ordinateur physique. Je les considérais comme de simples environnements d'entraînement, utiles surtout pour faire des tests sans risques. Ce projet m'a permis de réaliser qu'elles peuvent être de véritables outils professionnels, capables d'assurer des fonctions critiques dans une infrastructure, au même titre qu'un poste physique.

H - Mise en œuvre de la sauvegarde hebdomadaire

Une fois le projet suffisamment avancé, un point d'étape qu'on appellera "bilan de mi parcours", a été effectué afin de dresser un état des lieux clair des actions réalisées et des tâches restantes. Cette revue avait pour objectif de s'assurer de la cohérence de mes choix, avec les besoins définis en amont et d'éviter tout écart par rapport aux orientations initiales. Elle a permis de clarifier les priorités et de mieux structurer la suite du travail. À l'issue de cette réévaluation, la configuration du système de sauvegarde automatique et des mécanismes de restauration des fichiers a pu être engagée.

Je savais, grâce à mes recherches initiales sur le matériel, que le NAS Synology permettait la mise en place de ces fonctionnalités. Ce qui me manquait, en revanche, c'était la méthode pour les configurer correctement. Je me suis alors documentée en m'appuyant sur des ressources techniques et des tutoriels afin de comprendre comment créer une tâche de sauvegarde hebdomadaire, et savoir comment procéder à la restauration de fichiers en cas de besoin.

Dans un premier temps, j'ai décidé de configurer une sauvegarde complète de l'image du PC.

Au début de la configuration, j'ai opté pour une sauvegarde complète du système, car je pensais que cela me permettrait de restaurer un fichier spécifique si nécessaire notamment celui que l'entreprise avait identifié comme critique. Cette décision reposait sur l'hypothèse que la solution ne permettait pas de cibler un fichier unique dès la configuration initiale.

Ce n'est qu'après avoir terminé l'opération que j'ai constaté que cette fonctionnalité existait bel et bien. Heureusement, le type de sauvegarde choisi permettait une modification a posteriori des paramètres. J'ai donc pu recentrer la sauvegarde sur le fichier réellement concerné, ce qui s'est avéré bien plus pertinent au regard des besoins exprimés au lancement du projet.

Cette expérience, bien qu'elle soit issue d'un malentendu technique, m'a apporté une meilleure compréhension des différentes approches de sauvegarde. J'ai pu mesurer concrètement la différence entre une image système complète (très lourde en termes de volumétrie et de temps de traitement) et une sauvegarde ciblée (bien plus légère, rapide et adaptée à une exécution hebdomadaire). Elle m'a aussi appris à tirer parti de mes erreurs, à réévaluer une situation en cours de route et à ajuster ma stratégie en gardant à l'esprit les objectifs fixés.

Plutôt que d'écarter totalement l'idée de sauvegarde complète, j'ai pris l'initiative de la soumettre à mon maître de stage comme solution complémentaire. Ayant trouvé cette proposition pertinente, notamment dans une logique de sécurité renforcée ou de reconstitution rapide en cas de défaillance grave. Il m'a même suggéré d'aller plus loin, en mettant en place une tâche de sauvegarde du contenu du NAS sur un périphérique de stockage externe dédié.

I - Mise en place de l'accès VPN

Afin de permettre un accès sécurisé au réseau distant, j'ai poursuivi mon projet avec la mise en place d'un VPN via le routeur Netgear, qui propose nativement la prise en charge d'OpenVPN.

Côté serveur, la configuration était plutôt simple : il suffisait d'activer OpenVPN et de choisir un port d'écoute. En revanche, lors de l'activation, le routeur me demandait de sélectionner une adresse IP publique statique ou alors de configurer un DDNS (DNS dynamique) c'est après réflection que j'ai compris pourquoi. Pour que la connexion puisse s'établir depuis l'extérieur, il fallait s'assurer que le serveur VPN soit joignable depuis Internet. Pour cela, deux solutions sont possibles : soit utiliser une adresse IP publique statique, soit configurer un service DDNS . Dans notre cas, nous avons opté pour une IP publique statique.

Cette adresse IP fixe est essentielle, car le client VPN a besoin de savoir où se connecter pour atteindre le serveur. Si l'adresse change régulièrement (comme c'est souvent le cas avec une IP dynamique fournie par un FAI), la connexion devient impossible sans reconfigurer à chaque fois le client. À l'inverse, une IP fixe garantit que le serveur soit toujours joignable à la même adresse.

Un service DDNS pourrait également remplir ce rôle, en associant un nom de domaine à l'IP publique du serveur, même si celle-ci vient à changer. Le client se connecte alors au nom de domaine, et c'est le service DDNS qui met à jour l'IP automatiquement. Mais dans notre projet, cela n'était pas nécessaire puisque nous disposions d'une IP statique fournie par le fournisseur d'accès.

En revanche, la partie client a demandé davantage d'attention. J'ai dû :

- Installer l'application OpenVPN sur le poste client
- Ajouter les certificats et fichiers de configuration fournis par le routeur dans le bon répertoire

- Modifier le fichier .ovpn pour m'assurer que tous les chemins et paramètres étaient corrects

Malgré cela, la connexion échouait systématiquement. Après plusieurs essais, j'ai sollicité l'aide de mon maître de stage. Ensemble, nous avons analysé la situation en testant la configuration sur un autre poste. C'est à ce moment-là que nous avons identifié la cause du problème : l'adresse IP locale de ma carte réseau n'était pas adaptée.

En effet, pour établir une connexion VPN fonctionnelle, il est essentiel que la configuration réseau du client soit compatible avec le sous-réseau distant. Une fois l'ajout d'une nouvelle adresse IP sur ma carte réseau afin de correspondre au plan d'adressage du réseau cible, la connexion a pu s'établir correctement et de manière sécurisée.

Cette expérience m'a permis de mieux comprendre les enjeux liés aux configurations VPN, notamment :

- l'importance des paramètres IP
- la gestion des certificats (autorisation)
- et la nécessité de bien analyser chaque étape lors d'un échec de connexion

Elle m'a également donné l'opportunité d'appliquer concrètement les connaissances en configuration réseau Windows que j'avais récemment acquises, dans un contexte réel et opérationnel. Cela m'a permis de consolider mes compétences et de mieux saisir leur utilité dans une situation professionnelle.

Le choix de mettre en place deux méthodes d'accès distant n'est pas anodin. La première, via QuickConnect et la machine virtuelle hébergée sur le NAS, répond avant tout à un besoin technique : celui de pouvoir intervenir à distance sur l'infrastructure, même lorsque je ne suis pas physiquement sur site. La seconde, basée sur OpenVPN via le routeur, a été pensée pour répondre à une demande utilisateur, en l'occurrence permettre à M. Gonçalves d'accéder à ses fichiers et à son environnement de travail lors de ses déplacements. En combinant ces deux approches, le réseau gagne en souplesse et en résilience : si l'une des méthodes venait à rencontrer un problème (comme une coupure de service sur le VPN) l'autre peut prendre le relais, assurant ainsi une continuité d'accès et une meilleure sécurité globale.

J - Dossier partagé avec gestion des droits

Après avoir exploré l'interface DSM du NAS, j'ai identifié plusieurs options permettant de créer un espace de stockage partagé. Parmi elles, les protocoles NFS et SMB ont rapidement retenu mon attention, car ils répondaient à mon besoin principal : rendre un dossier partagé accessible à plusieurs machines virtuelles ou non.

En lisant leurs descriptions, je me suis interrogée sur leurs différences et sur leur fonctionnement respectif. Mes recherches m'ont permis de comprendre que le protocole SMB (Server Message Block) était plus adapté à ma situation. Celui-ci est conçu pour fonctionner principalement avec les systèmes d'exploitation Windows. À l'inverse, NFS (Network File System) est plutôt utilisé dans des environnements basés sur Linux.

Un autre objectif que je m'étais fixé était de définir des droits d'accès différents à ce dossier partagé en fonction des utilisateurs. Cette réflexion m'a ramenée à un sujet abordé en cours : Active Directory. J'ai alors revu la différence entre SMB et AD, notamment sur la manière dont chacun gère les autorisations. J'ai compris que SMB permet de définir directement des droits sur les fichiers et dossiers partagés, tandis qu'Active Directory va plus loin, en centralisant la gestion des comptes utilisateurs et en permettant d'attribuer des autorisations de manière plus souple, à travers des groupes ou des stratégies globales.

SMB est un protocole de partage simple et rapide à mettre en place, adapté aux environnements de petite taille; contrairement à Active Directory, qui nécessite une infrastructure plus lourde. SMB permet un accès direct aux ressources sans passer par une authentification centralisée.

Dans mon cas, la gestion des comptes utilisateurs était déjà en place, et les fonctionnalités avancées d'Active Directory ne m'étaient pas indispensables. J'ai donc choisi de me concentrer uniquement sur la configuration du partage via SMB. Ce choix m'a permis d'approfondir mes connaissances sur ce protocole, de mieux comprendre son fonctionnement dans un environnement Windows, et surtout d'apprendre à le configurer efficacement sur un NAS Synology.

K - Gestion des accès utilisateurs et filtrage web

Pour rendre mon réseau réellement fonctionnel et sécurisé en conditions réelles, j'ai aussi mis en place une gestion fine des utilisateurs dès le début du projet. Grâce à l'interface du NAS, j'ai créé plusieurs comptes répartis en groupes, chacun avec des droits adaptés à son usage. Cela m'a permis de limiter les actions possibles selon le profil, un peu comme on le

ferait dans une logique d'Active Directory. Ensuite, j'ai prolongé cette logique au niveau du routeur, en définissant des règles de filtrage basées sur les adresses IP des postes associés à ces utilisateurs. J'ai ainsi pu autoriser ou restreindre l'accès à certains sites web en fonction de la personne qui utilise l'équipement. Par exemple, un site a été bloqué sur l'ensemble du réseau, sauf pour un ordinateur précis dont l'utilisateur avait besoin pour y accéder. Inversement, certains postes plus sensibles ont été davantage limités, afin de réduire les risques de fuite de données ou de comportements à risque. Cette granularité dans les règles m'a permis d'adapter la sécurité tout en gardant une certaine souplesse selon les profils.

V / Mise en évidence des résultats obtenus

A - Ce qui a été mis en place

Au terme du projet, les fonctionnalités suivantes ont été intégralement mises en œuvre et validées :

- **Sauvegarde automatique hebdomadaire**

  Une sauvegarde automatique complète de l'image du PC est effectuée chaque lundi à deux heures du matin. Cet horaire a été choisi pour éviter toute interférence avec l'utilisation normale du poste ou une surcharge du réseau.

  Cette sauvegarde vient en complément de la sauvegarde ciblée initialement prévue, qui concernait uniquement un fichier sensible. L'ajout de la sauvegarde de l'image complète n'était pas prévu à l'origine, mais il a permis de renforcer la stratégie de sauvegarde en assurant une restauration intégrale possible du système en cas d'incident.

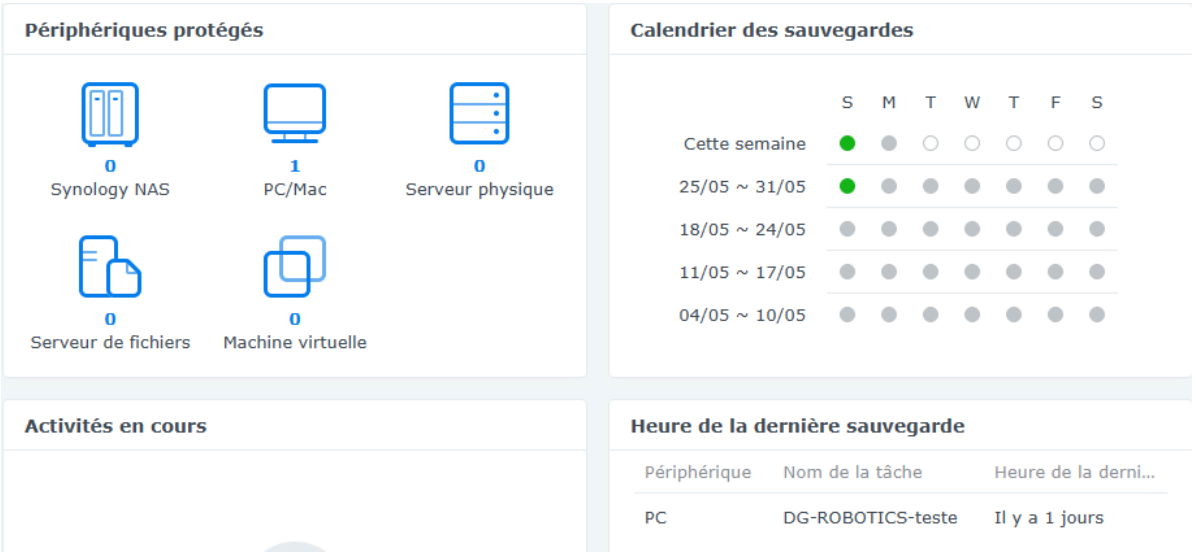


figure 5

- **Réseaux isolés : admin et invité**

  Une séparation nette a été mise en place entre le réseau principal (admin) et le réseau invité. L'objectif était d'empêcher toute communication entre les deux, afin de protéger les équipements critiques comme le NAS et le routeur. Cette configuration garantit que les utilisateurs du réseau invité ne peuvent pas accéder à l'interface d'administration ni aux fichiers sensibles. Concrètement, deux réseaux Wi-Fi distincts ont été créés via le routeur, chacun avec son propre SSID et ses propres règles d'accès.

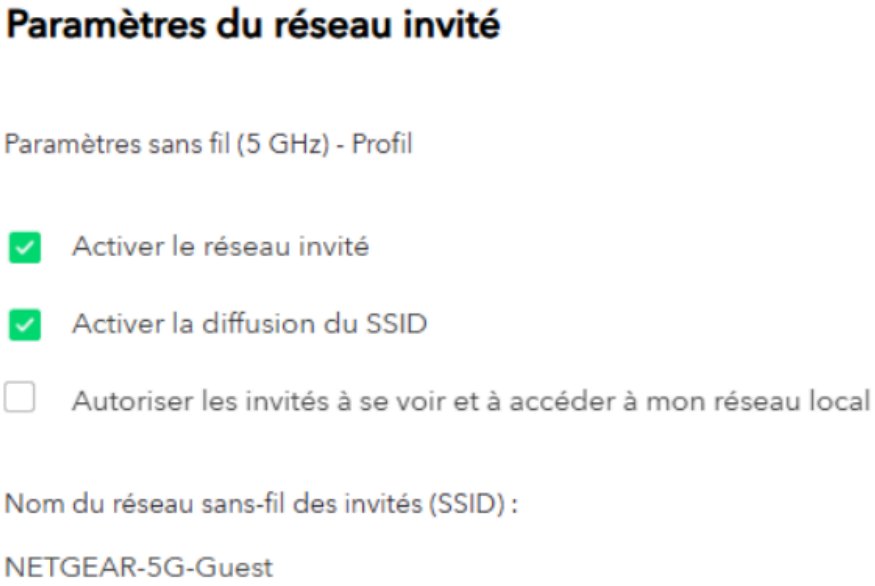


figure 6

- **Accès à distance via Synology**

Un premier accès à distance a été mis en place à travers la solution QuickConnect, proposée par Synology. Cette solution permet de prendre la main sur le NAS à distance, de façon simple et sécurisée sans avoir besoin de modifier les paramètres complexes de redirection de port sur la box. Elle a surtout été utilisée pour les phases de configuration, mais elle reste active en cas de besoin ponctuel. De plus, une VM a été installée sur le NAS; ce qui permet également de se connecter au réseau local depuis l'extérieur, soit via QuickConnect, soit par le protocole RDP. Cela offre un accès complet aux ressources internes comme si l'on était physiquement sur place.

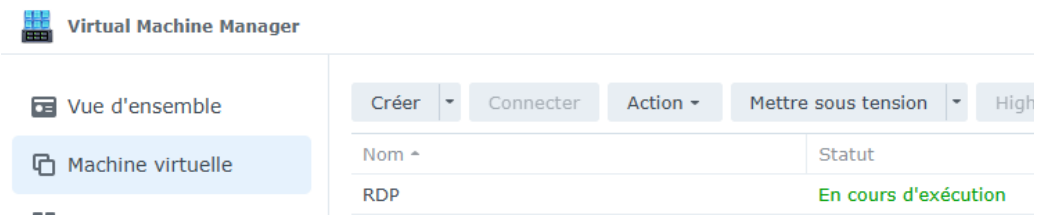
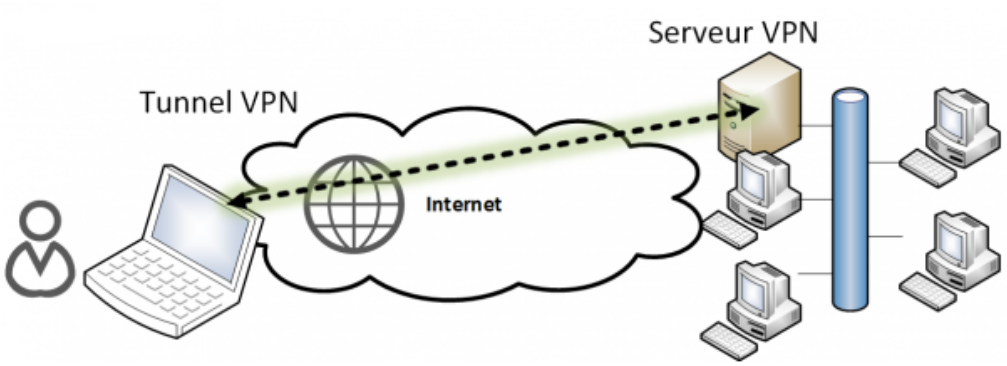


figure 7

- **Accès à distance via OpenVPN**



En complément de l'accès QuickConnect, une seconde solution a été mise en place avec OpenVPN, directement sur le routeur Netgear. Cet accès est plus sécurisé et permet de se connecter au réseau interne comme si l'on était physiquement sur place, tout en offrant une meilleure stabilité et une latence réduite par rapport à la VM sur QuickConnect. L'idée était d'avoir une solution principale robuste, mais aussi

de conserver un accès de secours si OpenVPN venait à rencontrer un problème. Les deux accès coexistent donc, chacun ayant son rôle et ses conditions d'utilisation.

B - Comparaison avec les objectifs initiaux

Objectif initial	**État actuel de réalisation**	**Commentaire**
Sauvegardes automatiques hebdomadaires	Réalisé	Fonction stable et supervisée
Isolation réseau admin / invité	Réalisé	Communication interdite entre les réseaux
Accès distant sécurisé	Réalisé	Accès distant et répertoriés dans les log
Enregistrement vidéo sur le NAS	NON Réalisé	Non compatible avec les caméras
Interface claire et centralisée pour l'admin	Réalisé	Administration intuitive via DSM
Simplicité de déploiement pour l'utilisateur	Réalisé	L'utilisateur final accède via une URL personnalisée
Suppression complète de la Livebox	NON Réalisé	La box n'a plus ses propriétés initiale mais est toujours physiquement présente

C - Bénéfices pour l'entreprise

La mise en place de cette solution a apporté plusieurs avantages concrets :

- **Sécurité accrue des données** : Grâce à la séparation entre le réseau invité et le réseau administrateur, les équipements sensibles sont isolés des usages non maîtrisés. Les sauvegardes automatiques, chiffrées et régulières, assurent une protection continue contre les pertes de données, les erreurs humaines ou les attaques de type ransomware. Le pare-feu du routeur et la configuration des accès renforcent encore la sécurité globale.

- **Accessibilité à distance contrôlée** : Deux solutions distinctes ont été mises en place pour accéder à distance aux ressources du réseau : QuickConnect via le NAS Synology et OpenVPN via le routeur Netgear. Elles permettent de travailler à distance comme si l'on était sur place, tout en garantissant un accès sécurisé et contrôlé selon le profil de l'utilisateur.
- **Autonomie de gestion** : L'interface DSM du NAS et celle du routeur Netgear ont été configurées pour offrir à l'entreprise une gestion simple et centralisée des utilisateurs, des sauvegardes, et des paramètres réseau. Cela permet au personnel autorisé de prendre la main sur l'infrastructure sans recourir à une aide technique extérieure pour chaque ajustement.
- **Evolutivité** : Le système en place a été pensé pour pouvoir évoluer facilement. Il est possible d'ajouter de nouveaux postes, de connecter des caméras compatibles, ou encore d'étendre l'espace de stockage en ajoutant un disque. Le tout, sans devoir réorganiser toute l'architecture déjà en place.

D - Limites rencontrées

Même si la majorité des objectifs ont été atteints, tout n'a pas pu être mis en place comme prévu. Certaines limites sont apparues au fil de la configuration, souvent en lien avec des contraintes techniques ou matérielles qui ont empêché d'aller au bout de certaines intentions initiales.

La première difficulté rencontrée a concerné la suppression complète de la Livebox. L'objectif initial était de faire du routeur Netgear le cœur du réseau, en remplaçant entièrement la box de l'opérateur. En pratique, cela n'a pas été possible, car certains services réseau nécessitent le maintien de la Livebox. Pour contourner cette contrainte sans compromettre la cohérence du réseau, le Wi-Fi de la Livebox a été désactivé et un câble Ethernet relie le port LAN 2.5G de la Livebox au port WAN du routeur Netgear, de façon à ce que la Livebox ne serve que d'accès Internet, sans intervenir dans la gestion du réseau local, désormais entièrement piloté par le routeur.

Une autre limite est apparue concernant l'installation des caméras de surveillance. Le NAS Synology était prêt à recevoir des flux vidéo grâce à l'application Surveillance Station, qui avait été installée et configurée en amont. Cependant, il s'est avéré que les caméras disponibles n'étaient pas compatibles avec cette solution. Les protocoles utilisés par ces caméras, ou les formats de flux qu'elles proposaient, n'étaient pas reconnus par l'outil, ce

qui empêchait tout enregistrement ou affichage dans l'interface du NAS. Une solution technique aurait pu être d'utiliser des caméras certifiées ONVIF, un standard permettant une meilleure compatibilité entre matériels de marques différentes, notamment dans les systèmes de vidéosurveillance IP. Malheureusement, ce type de matériel n'était pas à disposition, ce qui nous a contraint à mettre cette partie du projet en pause.

Conclusion technique

Résultats obtenus

Le projet a permis de mettre en place une architecture réseau fonctionnelle, sécurisée et adaptée aux besoins identifiés dès la phase de conception. Un NAS Synology DS224+ a été installé avec succès et configuré pour assurer des sauvegardes automatiques hebdomadaires vers un disque dur externe, réduisant considérablement le risque de perte de données. L'interface d'administration DSM a été restreinte aux seuls administrateurs, garantissant un contrôle total sur l'infrastructure.

Le réseau local a été segmenté grâce au routeur Netgear Nighthawk RS300, avec la création de deux réseaux distincts (admin et invités) via des SSID. Cette séparation permet d'éviter tout accès non autorisé aux équipements sensibles par les utilisateurs du réseau invité. Par ailleurs, un VPN a été mis en place, permettant aux administrateurs d'accéder à distance de façon sécurisée aux ressources internes. Des règles de sécurité, une politique de mot de passe rigoureuse et un système de journalisation ont renforcé la protection du système.

Limites rencontrées

Malgré ces résultats positifs, certaines difficultés techniques ont limité la portée du projet. L'intégration des caméras de vidéosurveillance prévue initialement n'a pas pu être réalisée. Les modèles choisis se sont révélés incompatibles avec le protocole ONVIF (Open Network Video Interface Forum), un standard qui permet normalement aux caméras IP de communiquer avec les systèmes de gestion vidéo comme Surveillance Station de Synology. Il sera donc nécessaire d'acquérir des caméras ONVIF pour finaliser cette fonctionnalité.

D'autre part, bien que le routeur Netgear ait pris le relais sur la gestion du réseau, la Livebox de l'opérateur n'a pas pu être totalement écartée. Elle reste indispensable pour l'accès à

Internet et a été configurée avec le Wi-Fi désactivé, en connectant un câble Ethernet entre son port LAN 2.5G et le port WAN du routeur, afin de limiter son emprise sur le reste du système. Une solution plus pérenne consisterait à basculer vers un mode bridge, voire à envisager une box opérateur plus flexible ou une infrastructure fibre dédiée.

Pistes d'amélioration

Plusieurs pistes pourraient être envisagées pour approfondir la sécurisation du système. L'ajout d'un pare-feu plus avancé, voire d'un système de détection d'intrusion (IDS) open source comme Snort, permettrait une surveillance plus fine du trafic réseau. De même, l'automatisation de tests de sauvegardes, la centralisation des journaux avec un serveur Syslog, ou encore le chiffrement des disques pourraient renforcer la robustesse globale de l'installation.

Vision à long terme

Le projet a été pensé pour être évolutif et maintenable. Le NAS dispose de plusieurs possibilités d'extension, tant en stockage qu'en fonctionnalités, notamment via les nombreux paquets proposés par Synology. Le réseau peut également s'adapter à de futurs besoins : ajout de VLANs, mise en place de services collaboratifs ou hébergement d'applications internes.

En garantissant une structure solide et des accès sécurisés, ce système peut accompagner l'entreprise durablement, en s'adaptant à la croissance de ses besoins tout en assurant un haut niveau de sécurité et de résilience.

Conclusion générale retour d'expérience humaine et professionnelle

Une montée en compétences concrète

Ce projet m'a permis d'approfondir de manière significative mes compétences techniques dans des domaines clés comme la gestion d'un NAS, la sécurisation réseau, la mise en place d'un VPN, et l'administration d'une architecture de type PME. J'ai appris à manipuler des outils professionnels comme l'interface DSM de Synology, le protocole openVPN ou encore la configuration réseau avancée d'un routeur. Ce fut également l'occasion d'aborder la problématique de la compatibilité des équipements (comme les caméras IP), et de comprendre à quel point un projet peut être impacté par des contraintes matérielles.

Une évolution personnelle forte

Au-delà de l'aspect technique, cette expérience m'a fait évoluer humainement. J'ai gagné en autonomie, notamment dans la recherche de solutions lorsque je me suis retrouvée face à des blocages imprévus. J'ai aussi beaucoup travaillé ma rigueur, en veillant à documenter chaque étape, à tester les configurations dans un ordre logique, et à anticiper les risques. Enfin, j'ai pu améliorer ma communication, que ce soit pour rendre compte de l'avancement du projet, pour expliquer mes choix techniques, ou pour demander de l'aide de manière claire et ciblée.

Une relation constructive avec le tuteur

Les interactions avec mon tuteur ont été trés enrichissantes. Il m'a laissé une réelle liberté d'action tout en me guidant lorsque cela était nécessaire. Nos échanges ont souvent dépassé le cadre strictement technique pour aborder des questions de méthodologie, de gestion de projet ou encore de bonnes pratiques professionnelles. Cette collaboration m'a permis de me sentir pleinement impliquée, tout en bénéficiant d'un cadre rassurant et bienveillant.

Une confirmation de mes choix

Ce projet a confirmé mon intérêt pour les métiers de l'administration système et de la cybersécurité. J'ai particulièrement apprécié le fait de devoir penser l'infrastructure dans son ensemble, tout en allant dans le détail des paramètrages. Ce genre de défi, à la fois concret et stratégique, correspond parfaitement à ce que je recherche professionnellement. Cela me motive d'autant plus à poursuivre dans cette voie et à me spécialiser davantage dans la sécurisation des architectures réseau.

Annexes :

Table des figures / illustrations

Bibliographie (organisée et commentée)

Sources techniques

- **Documentation Synology DSM**
  https://kb.synology.com/fr-fr
  -> Guide officiel très utile pour la configuration des services réseau, des sauvegardes et des utilisateurs sur le NAS.

- **Documentation Technique Synology**
  https://global.download.synology.com/download/Document/Software/UserGuide/Firmware/DSM/6.2/fre/Syno_UsersGuide_NAServer_fre.pdfhttps://global.download.synology.com/download/Document/Software/UserGuide/Firmware/DSM/6.2/fre/Syno_UsersGuide_NAServer_fre.pdf
  -> Document technique

- **Documentation Synology sauvegarde**
  https://kb.synology.com/fr-fr/DSM/tutorial/How_back_up_PC_physical_server_with_ABB
  -> Guide pour sauvegarder l'intégralité d'un ordinateur

- **Support Netgear Nighthawk RS300**
  https://www.netgear.com/fr/support/product/rs300/
  -> Manuel PDF du constructeur, utilisé pour accéder aux paramètres et personnaliser le routeur.

- **Guide d'achat netgear**
  https://www.netgear.com/fr/hub/wifi/routers/guide-dachat-nighthawk-wifi-7/
  -> Une fois la décision prise de prendre un routeur netgear il me fallait déterminer lequel était le plus optimale dans notre cas.

Ressources complémentaires

- **Plages d'adresses privées**
  https://www.ibm.com/docs/fr/networkmanager/4.2.0?topic=translation-private-address-ranges
  -> Référence utilisée pour justifier les plages d'adresses IP employées sur le réseau.

- **Tuto de sauvegarde hebdomadaire**
  https://www.youtube.com/watch?v=hnEQS9I-Ks4
  -> Explication de la mise en place des sauvegardes automatiques.

- **Protocole ONVIF (Open Network Video Interface Forum)**
  https://camera-videosurveillance.fr/blog/143_Qu-est-ce-que-le-protocole-onvif.html
  -> Compréhension des normes de compatibilité des caméras IP avec les enregistreurs type NAS.

- **Information forum ONT**
  https://www.reddit.com/r/NETGEAR/comments/1f15cs8/setting_up_fiber_bridge_between_netgear_aps/?show=original
  -> Ma permis de trouver des solution pour écarter la Box

- **SMB**
  https://www.it-connect.fr/le-protocole-smb-pour-les-debutants/
  -> Site expliquant la mise en place ainsi que le fonctionnement du protocole

Glossaire / lexique

Terme	Définition
NAS	Network Attached Storage -> Unité de stockage connectée au réseau local, accessible aux utilisateurs.
VLAN	Virtual Local Area Network -> Permet de segmenter un réseau physique en réseaux logiques indépendants.
Pare-feu	Dispositif qui protège un système informatique connecté à Internet des tentatives d'intrusion qui pourraient en provenir.
VPN	Virtual Private Network -> Tunnel sécurisé pour accéder à un réseau distant via Internet.

ONVIF	Open Network Video Interface Forum – Standard garantissant la compatibilité entre caméras IP et logiciels tiers.
DSM	DiskStation Manager – Système d'exploitation des NAS Synology.
SSID	Service Set Identifier – Nom d'un réseau Wi-Fi.
Port Forwarding	Redirection de port – Permet d'accéder à un service local via Internet.
HTTPS	HyperText Transfer Protocol Secure – Protocole de communication sécurisé pour le transfert de données sur le web, utilisant le chiffrement SSL/TLS.
SLL	Secure Sockets Layer – Protocole de chiffrement assurant la sécurité des communications sur Internet (remplacé par TLS mais souvent encore utilisé comme terme générique).
DNS	Domain Name System – Système de résolution des noms de domaine en adresses IP.
DDNS	Dynamic Domain Name System – Service permettant d'associer un nom de domaine à une adresse IP dynamique
Nom de domaine	Adresse textuelle d'un site web (ex. : exemple.com), liée à une adresse IP.
FAI	Fournisseur d'accès à Internet. Entreprise qui permet de se connecter à Internet (ex. : Orange, SFR).
PME	Petite ou Moyenne Entreprise

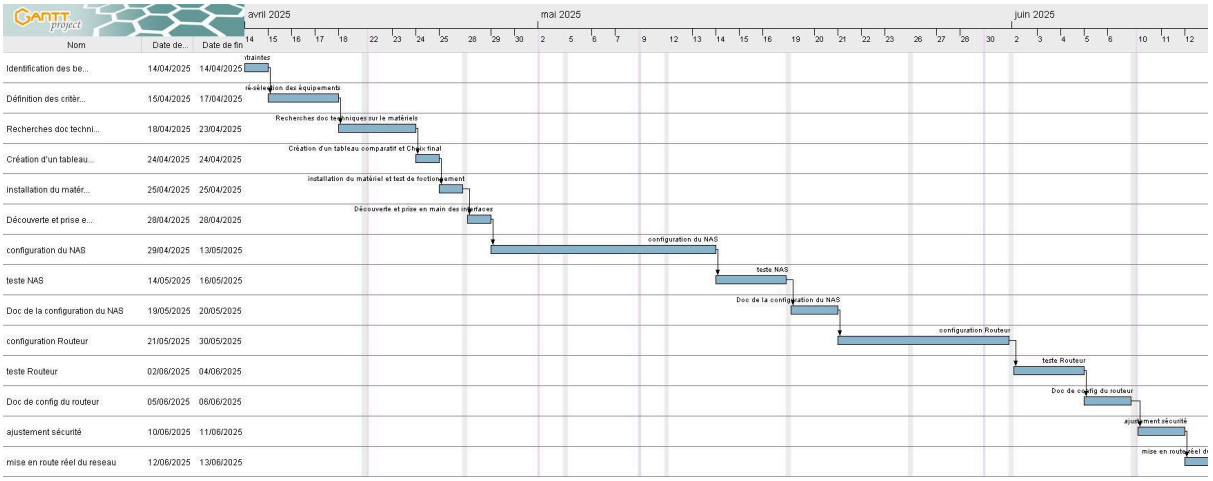
Index

		28;29; 31
Ethernet	Technologie de connexion réseau filair	14, 16
FAI	Fournisseur d'accès à Internet (ex. Orange, SFR)	15, 16,22
Pare-feu	Dispositif de sécurité filtrant les connexions réseau	14;15; 17
Adresse IP	Identifiant unique d'un appareil sur un réseau	14; 16; 19; 21, 22
IDS	Système de détection d'intrusion	30
Livebox	Routeur fourni par un FA	14; 16; 28
NAS	Serveur de stockage en réseau	10.13
ONVIF	Protocole standard pour caméras IP compatibles	29. 30
OpenVPN	Solution de VPN open source sécurisée	10; 21- 23
QuickConnect	Service Synology pour accès distant simplifié	15; 20
Réseau invité	Réseau isolé pour les visiteur, sans accès aux ressources internes	18
Router	Matériel qui relie un réseau local à Internet	9; 12-19, 21-23
Sauvegarde	Copie de sécurité des données	10; 20-21
Segmentation réseau	Séparation logique des sous-réseaux pour renforcer la sécurite	18
Serveur Syslog	Serveur centralisant les journaux systèm	30
Snort	Logiciel open source de détection d'intrusion (IDS)	30
SSID	Nom d'un réseau Wi-Fi	18
Synology	Marque du NAS utilisé dans ce projet	13-15, 19-21
VPN	Reseau privé virtuel sécurisé pour accéder à distance	19, 21-23

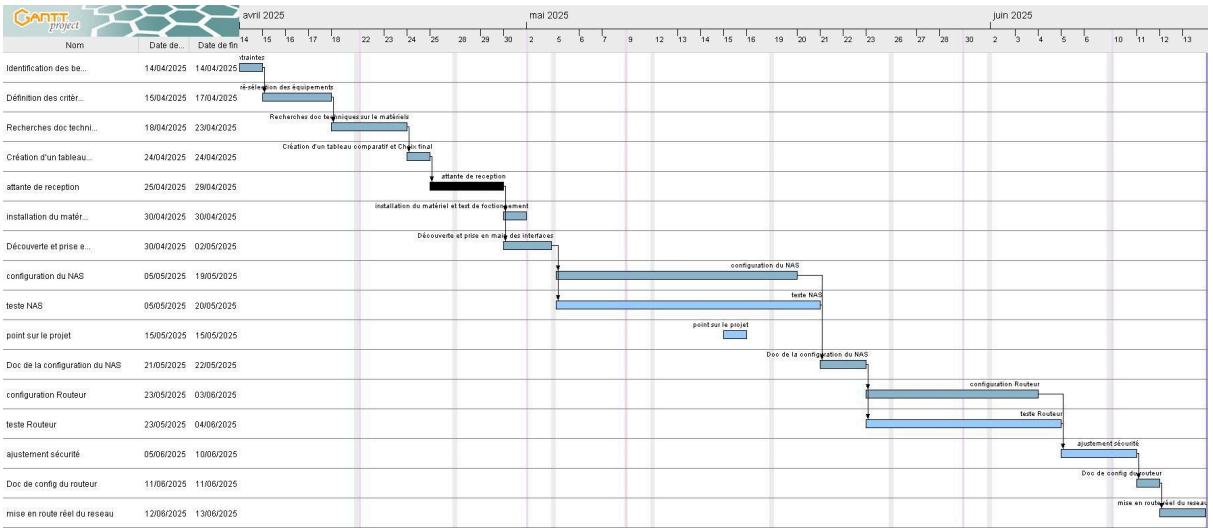
Documents utiles

Image du rapport:

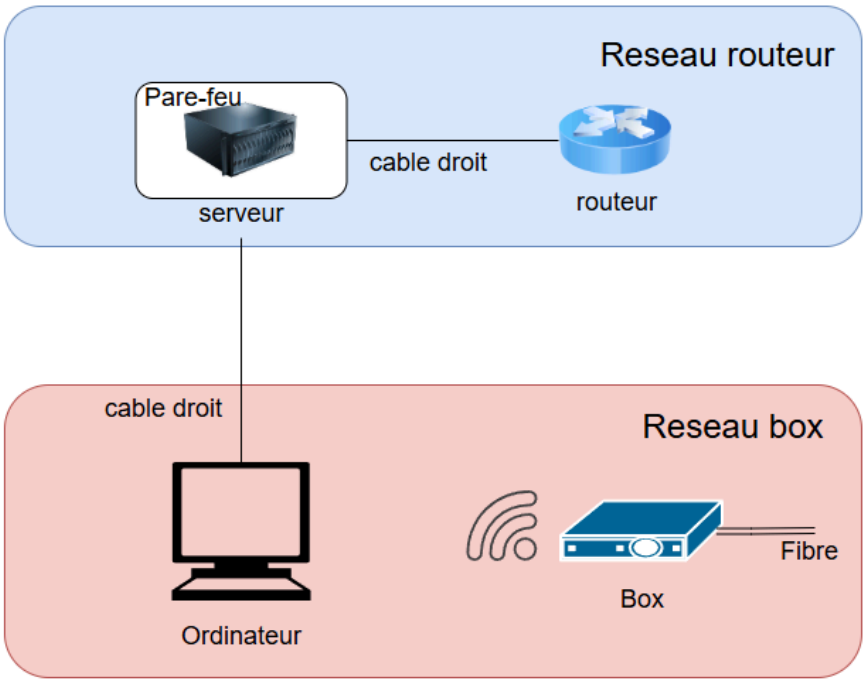
Planning initial:



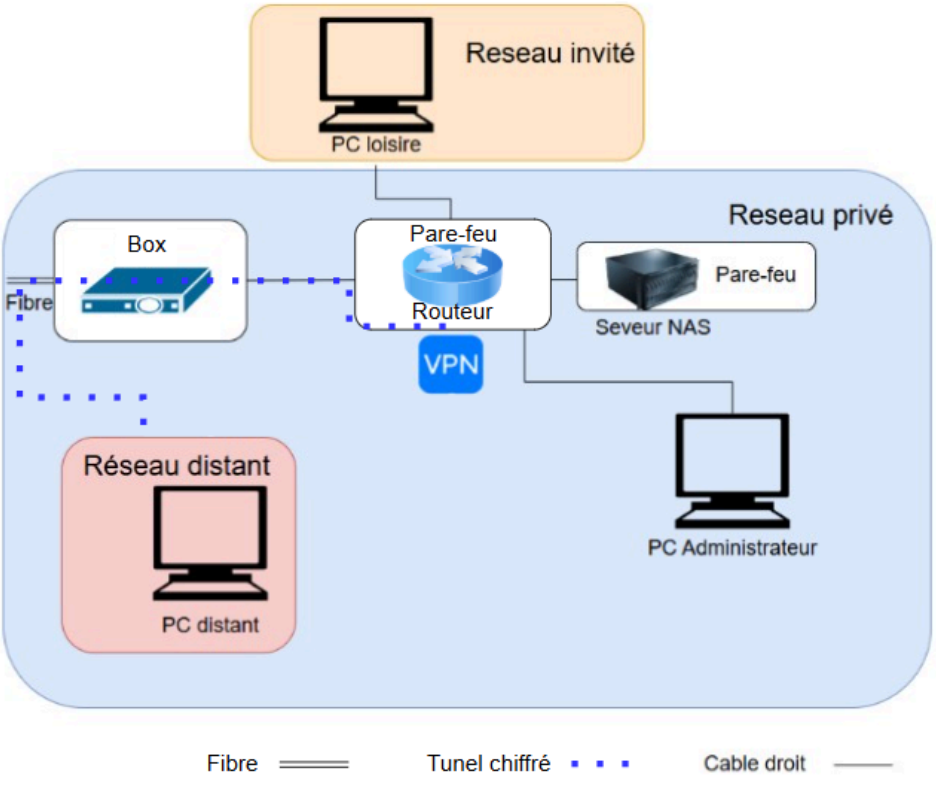
Planning réalisé:



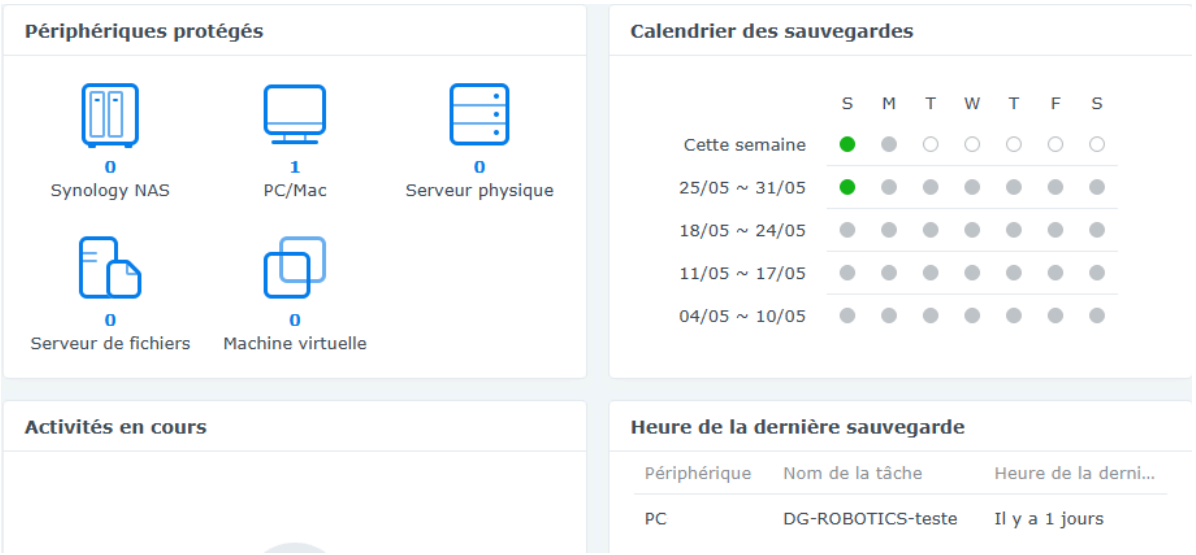
Topologie initial:



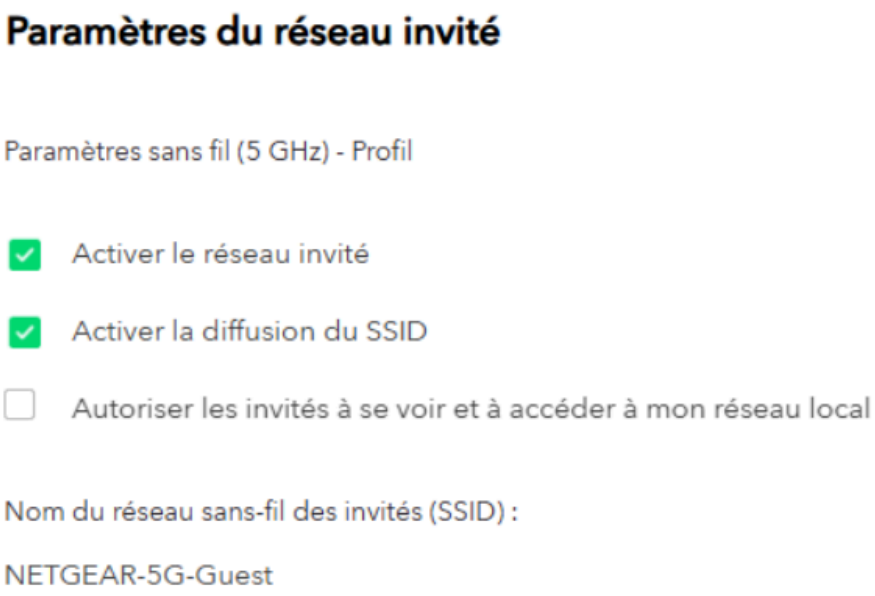
Topologie du final:



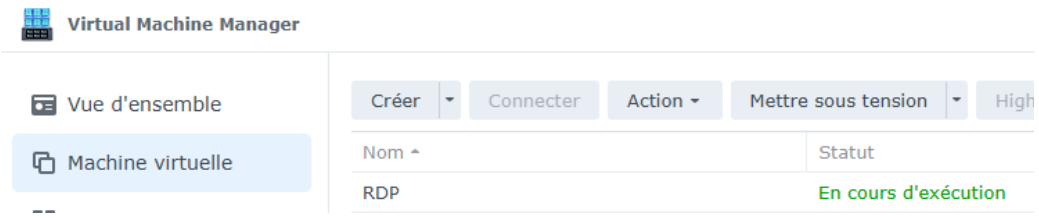
Interface des sauvegard:



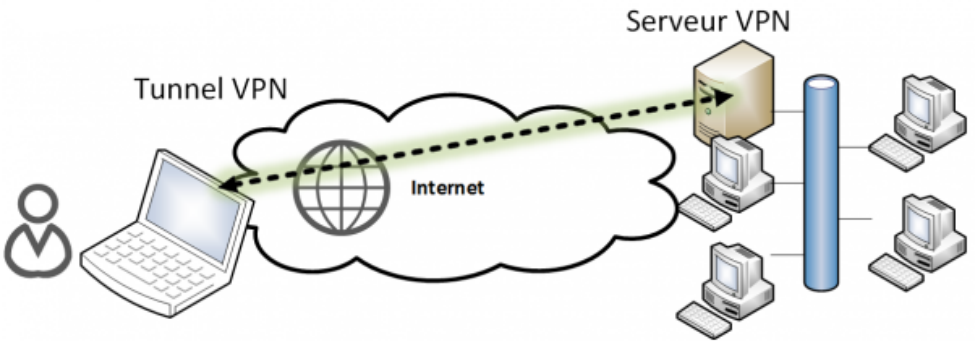
Réseau isolé:



Accès via la VM du NAS:



Open VPN:



Document réalisé:

Tableau permettant de comparer efficacement les capacités de chaque appareil :

recherche du materielle :

Les disques durs étaient déjà achetés par l'entreprise.
Référence des disque durs:

"-" signifie que ceci n'est pas essentiel (pas ce que l'on attend) pour le matériel

Fonction requise pour le projet	**Ce que fait le Synology DS224+ (Serveur)**	**Ce que fait le Netgear RS300 (Routeur)**
Accéder aux données à distance	Serveur FTP, stockage centralisé avec accès à distance via cloud, QuickConnect	Connexion rapide et stable pour appareils connectés, compatible Wi-Fi 7« jusqu'à 175 m² de couverture Wi-Fi à 360 degrés »
Sécuriser les données sensibles	Fonctions de sécurité intégrées, sauvegarde multicouche, chiffrement	pare-feu, WPA3 "une confidentialité accrue avec le VPN"
Créer deux réseaux (admin et invité)	-	possible
Réseau sécurisé	–" chiffrement de bout en bout protège contre les accès non autorisés "	sécurité réseau, pare feu intégré

Sauvegardes hebdomadaires automatiques	Active Backup : planification de sauvegardes	-
Stockage et enregistrement des caméras de sécurité	Surveillance Station + sauvegarde cloud (C2) + chiffrement	-
Bonne capacité de stockage évolutive	oui -> peut ajouter des disque	-
Accès multi-utilisateurs avec droits définis	Non précisé	Non précisé
Performances rapides pour transferts de fichiers lourds	Indexation rapide (Synology Drive, Photos, web apps)	Wi-Fi 7 (jusqu'à 9,3 Gbit/s), ports LAN jusqu'à 2.5 Gbit/s
Administration à distance	quickconnect	Non précisé