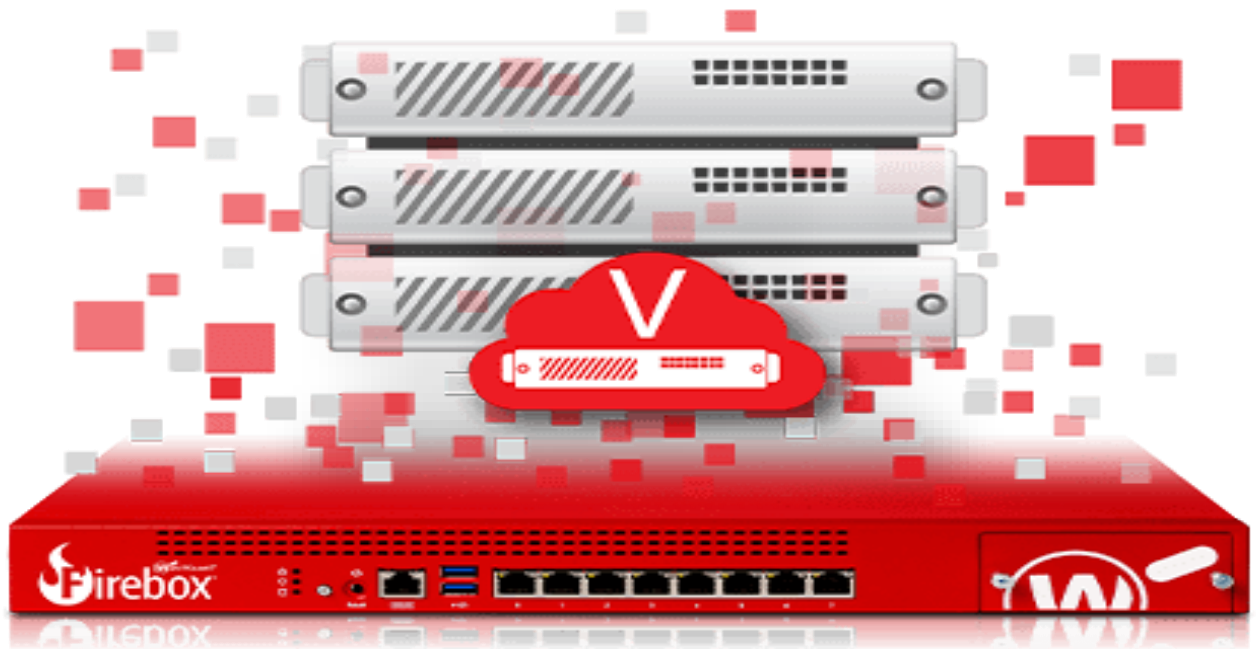


Mise en place d'un pare-feu virtuel



SECK Pape Abdoulaye

Tuteur de stage : M. Sébastien TOUCHET

Tuteur iut : M. Sébastien HERNANDEZ



3S2i

AU-DELÀ DES TECHNOLOGIES,
DES HOMMES !



Remerciements

Je tiens tout d'abord à exprimer ma gratitude envers l'entreprise 3S2I de m'avoir offert l'opportunité d'effectuer mon stage au sein de leur équipe.

C'était une expérience professionnelle enrichissante qui m'a permis de développer mes compétences et d'acquérir de nouvelles connaissances.

Je souhaite également remercier chaleureusement M. Sébastien TOUCHET, mon tuteur de stage et référent informatique, pour son accompagnement constant, sa disponibilité et ses conseils avisés tout au long de cette période.

J'adresse aussi mes remerciements à M. Karim AGREBI, directeur de l'entreprise, pour m'avoir accueilli au sein de 3S2I et pour la confiance qu'il m'a accordée.

Un grand merci également à Mme Sandes CHARIET, directrice opérationnelle, pour sa gestion rigoureuse de tous les aspects administratifs et pour sa disponibilité ainsi que toute l'équipe de 3S2I pour leur accueil chaleureux et leur bienveillance. Leur esprit de collaboration a rendu mon stage à la fois agréable et très formateur.

Enfin, j'adresse mes remerciements les plus sincères à M. Sébastien HERNANDEZ, pour son suivi attentif, sa pédagogie et ses conseils constants tout au long de cette période.

Sommaire

Remerciements	2
Introduction	7
I. Présentation de l'entreprise et son besoin	8
1. Présentation de la société 3S2I	8
1.1. Historique et organisation de la société 3S2I	8
1.2. Secteurs d'activités et partenaires	10
2. Le client : BIOBULLE	12
3. Le sujet	13
3.1. Besoin de l'entreprise	13
3.2. Existant technique	14
3.3. Objectifs	15
4. La procédure	17
4.1. Outils	17
4.2. Diagramme de Gantt	19
II. Réalisation du travail	19
1. Phase préparatoire	19
1.1. Mise en place du rôle Hyper-V	19
1.2. Installation du disque dur virtuel	21
2. Déploiement des équipements et services	22
2.1. Configuration de la FireboxV	22
2.2. Déploiement d'une machine virtuelle de test	27
2.3. Configuration d'un BOVPN en environnement de test	29
3. Virtualisation du serveur ERP	33
3.1. Mise en place d'un laboratoire de test	33
3.2. Virtualisation du serveur ERP et la mise en place du BOVPN	37
III. Bilan	38
1. Résultats	38

2. Difficultés	39
3. Perspectives	40
Conclusion	41
Bilan humain	42
English Summary	43
Glossaire	44
Bibliographie.....	46
Table des annexes.....	47
Annexes	48

Table des figures

Figure 1: Logo de la société 3S2I	8
Figure 2 : Zone de chalandise	8
Figure 3 : Situation géographique de la société 3S2I	9
Figure 4 : Organigramme de la société 3S2I	9
Figure 5 : Secteurs d'activités de la société 3S2I.....	11
Figure 6 / 7 : Logo du fournisseur BNP Paribas / GRENKE	12
Figure 8 / 9 : Logo du fournisseur TD SYNnex / Leasecom.....	12
Figure 10: Logo du fournisseur Locam.....	12
Figure 11 : Logo du client Biobulle.....	12
Figure 12 : Pare-feu T80 de l'existant technique	13
Figure 13 : Schéma de l'existant technique	15
Figure 14 : Schéma des objectifs	15
Figure 15 : Infrastructure de l'installation	16
Figure 16 : Logo du serveur Active Directory(AD).....	17
Figure 17 : Logo du serveur Hyper-V	17
Figure 18 : Logo de la FireboxV.....	17
Figure 19 : Disque dur externe	18
Figure 20 : Capture d'écran du logiciel Disk2VHD	18
Figure 21 : Diagramme de Gantt.....	19
Figure 22 : Capture d'écran du rôle Hyper-V	20
Figure 23 : Capture d'écran des commutateurs virtuels.....	21
Figure 24 : Capture d'écran du fichier "vhd" à télécharger	21
Figure 25 : Disque dur virtuel extrait	22
Figure 26 : Caractéristique de la FireboxV	23
Figure 27 : Capture d'écran des ressources recommandées.....	23
Figure 28 : Capture d'écran de l'emplacement du disque à sélectionner	24
Figure 29 : Ecran de démarrage de la FireboxV	25
Figure 30 : Capture d'écran de l'interface graphique de la FireboxV.....	26
Figure 31 : Capture d'écran de l'importation de la configuration.....	26
Figure 32 : Capture d'écran de l'activation de la licence	27
Figure 33 : Fichier ISO de la VM de test.....	28
Figure 34 : Capture d'écran de la configuration de la VM de test	28
Figure 35 : Capture d'écran de la configuration du BOVPN.....	29
Figure 36 : Configuration du tunnel BOVPN	30

Figure 37 : Configuration de la passerelle BOVPN.....	31
Figure 38 : Configuration de la passerelle BOVPN(suite)	32
Figure 39 : Capture d'écran du bon fonctionnement du BOVPN	33
Figure 40 : Caractéristique de la VM.....	34
Figure 41 : Logiciel Disk2vhd.....	34
Figure 42 : Conversion du disque	35
Figure 43 : Transfert de fichier via TeamViewer	36
Figure 44 : Configuration de la nouvelle VM de test	36
Figure 45 : Les VMs à virtualiser du serveur ERP.....	37
Figure 46 : Environnement final après le basculement	38
Figure 47 : Capture d'écran du BOVPN final.....	38
Figure 48 : Schéma des objectifs atteints	39

Introduction

Dans le cadre de ma deuxième année de BUT Réseaux et Télécommunications, j'ai eu l'opportunité d'effectuer un stage au sein de l'entreprise 3S2i.

Cette expérience m'a permis de mettre en pratique les compétences acquises durant ma formation et de découvrir concrètement le fonctionnement du milieu professionnel.

Dans ce cadre, j'ai eu l'opportunité de travailler sur un projet : la mise en place d'un pare-feu virtuel.

Un pare-feu est un dispositif de sécurité réseau chargé de contrôler le trafic entrant et sortant entre plusieurs réseaux, en appliquant des règles prédéfinies. Il permet ainsi de protéger les systèmes contre les accès non autorisés et les cyberattaques.

Un pare-feu virtuel est une version logicielle de ce dispositif, déployée dans le cloud. Il offre les mêmes fonctionnalités qu'un pare-feu matériel, tout en étant plus flexible et mieux adapté aux infrastructures modernes.

Dès lors, pourquoi mettre en place un pare-feu virtuel et comment procéder à son installation ainsi qu'à sa configuration pour garantir la sécurité du réseau ?

Pour répondre à cette problématique, je ferai tout d'abord une présentation de l'entreprise et son besoin, puis j'examinerai en détail les différentes étapes de ce processus, de son installation à sa configuration, et enfin, un bilan sera dressé afin d'aborder les difficultés rencontrées, les solutions apportées pour surmonter les obstacles et les enseignements tirés de cette expérience.

NB : tous les termes suivis du symbole « * » seront expliqués dans le glossaire.

I. Présentation de l'entreprise et son besoin

1. Présentation de la société 3S2i

1.1. Historique et organisation de la société 3S2i



Figure 1: Logo de la société 3S2i

3S2i est une société de services informatiques fondée en 2006, implantée à Nice et Monaco, et comptant environ 27 employés. M. Karim AGREBI est le fondateur et gérant de l'entreprise.

3S2i propose une gamme complète de services informatiques, incluant l'installation et la gestion de parcs informatiques, l'infogérance, la supervision des systèmes et réseaux, la sauvegarde externalisée, ainsi que l'impression.

Zone de chalandise



Figure 2 : Zone de chalandise

3S2i répond aux besoins de clients principalement situés dans les Alpes-Maritimes (Nice, Cannes, Antibes...) et à Monaco, mais intervient également sur l'ensemble de la région Provence-Alpes-Côte d'Azur.

Les locaux de 3S2i se trouvent à Nice, au 34 avenue Henri Matisse (Immeuble Le Minotaure), 06200, et à Monaco, 17 avenue Albert II, « L'ALBU », 8ème étage, 98000.

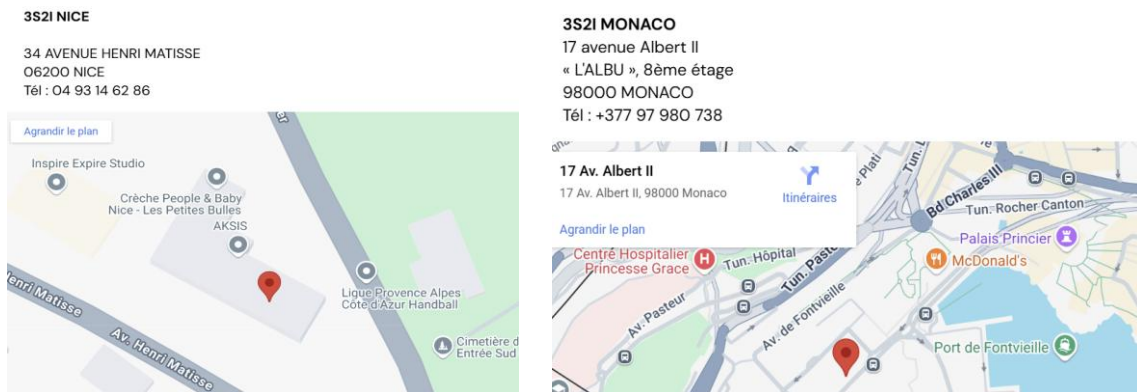


Figure 3 : Situation géographique de la société 3S2I

Organigramme

Dans le cadre de mon rapport de stage, j'ai réalisé un organigramme simplifié de l'entreprise 3S2I. J'ai choisi d'y représenter uniquement les postes de direction ainsi que le service informatique.

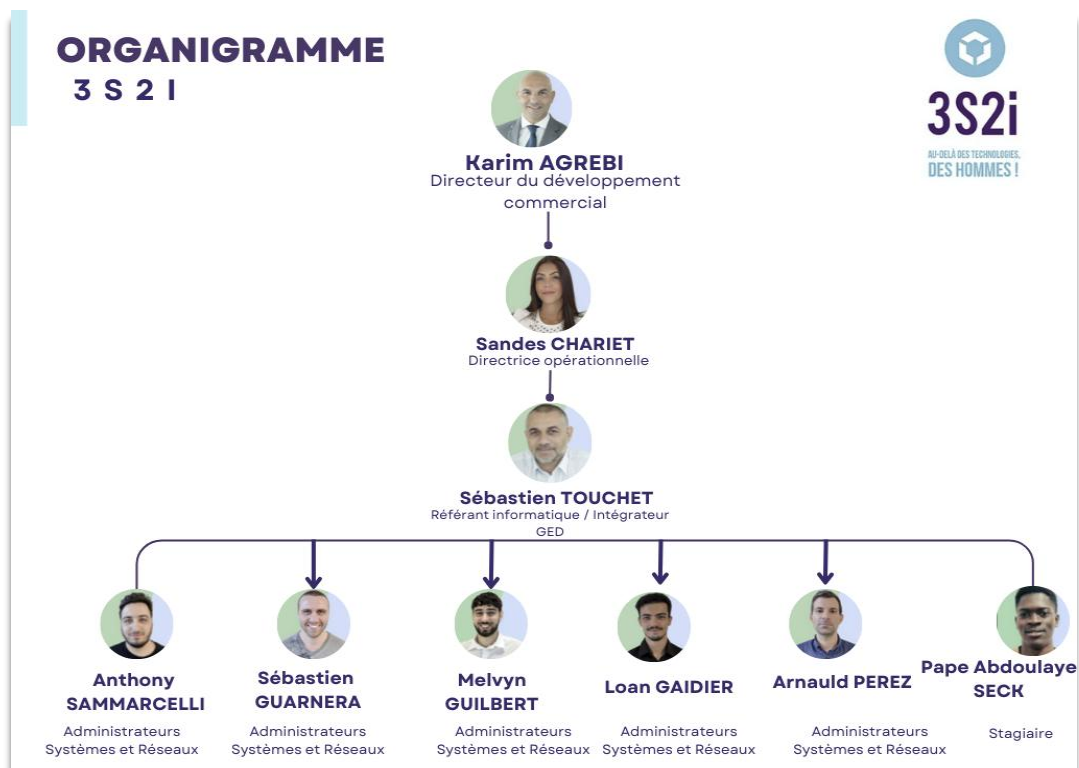


Figure 4 : Organigramme de la société 3S2I

1.2. Secteurs d'activités et partenaires

3S2I propose une gamme complète de services informatiques à destination des entreprises, collectivités et professionnels de la région Provence-Alpes-Côte d'Azur et Monaco. Les principaux métiers de 3S2I sont :

- **Infogérance :**
Gestion globale ou partielle du système d'information des clients : supervision, maintenance, assistance et support technique pour garantir la performance et la sécurité de l'infrastructure informatique.
- **Infrastructure et réseau :**
Conception, déploiement et gestion des réseaux informatiques (câblage, serveurs, équipements réseau), pour assurer la connectivité, la fiabilité et la sécurité des échanges de données.
- **Sécurité informatique :**
Mise en place de solutions de protection contre les cybermenaces (antivirus, pare-feu, sauvegarde, conformité RGPD), pour sécuriser les données et les systèmes d'information des entreprises.
- **GED (Gestion Électronique de Documents) :**
Solutions de dématérialisation, classement, archivage et partage sécurisé des documents, pour optimiser la gestion documentaire et faciliter le travail collaboratif.
- **Système d'impression :**
Gestion et maintenance des équipements d'impression professionnels : imprimantes, copieurs, optimisation des flux d'impression et gestion des consommables.
- **Affichage dynamique :**
Installation et gestion de supports d'affichage numérique pour la communication visuelle en entreprise ou en point de vente (écrans, bornes interactives, etc.).

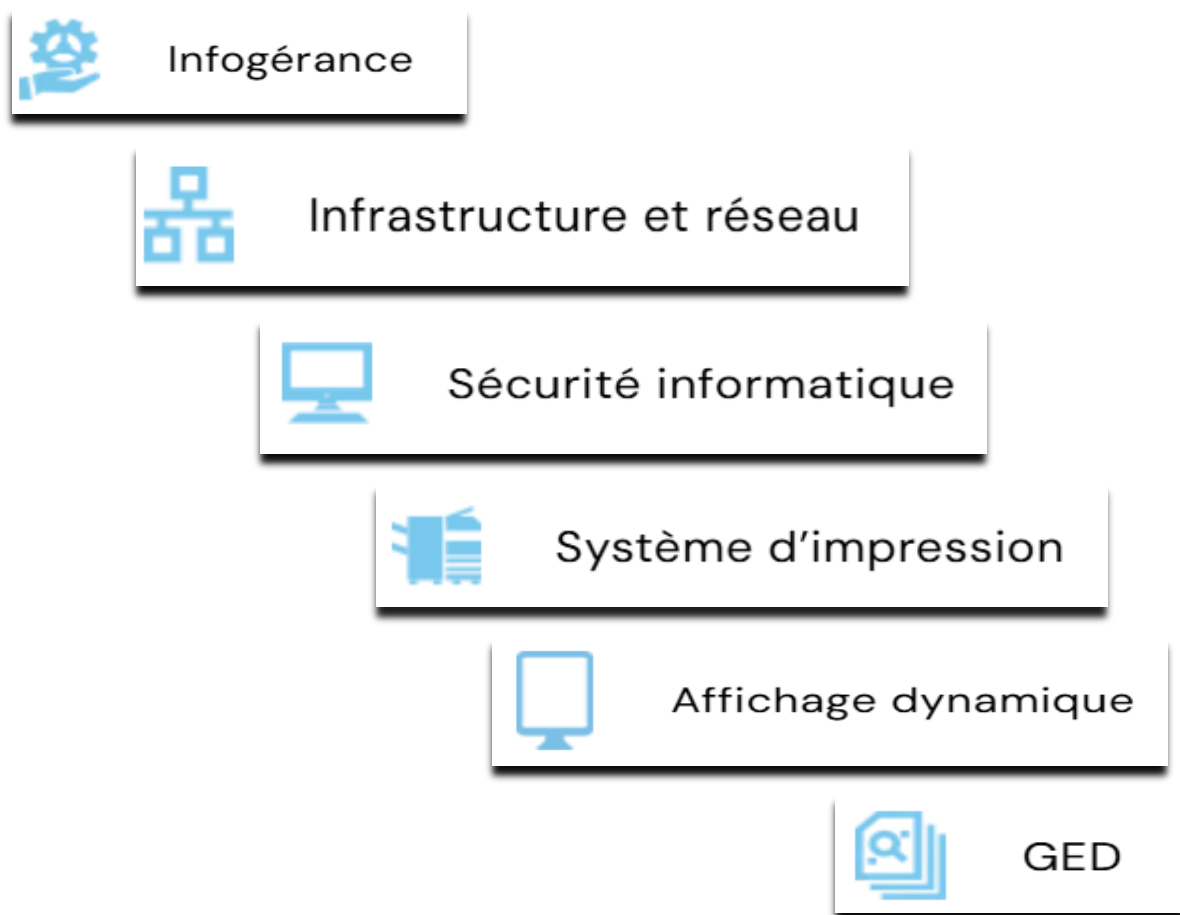


Figure 5 : Secteurs d'activités de la société 3S2I

Partenaires & Fournisseurs

3S2I s'appuie sur des partenariats solides avec plusieurs acteurs majeurs du secteur. Parmi leurs partenaires financiers et fournisseurs de confiance figurent BNP Paribas, Grenke, Leasecom et Locam, qui les accompagnent dans les solutions de financement pour leurs clients. Nous collaborons également avec TD SYNEX, l'un des principaux distributeurs mondiaux de technologies, pour l'approvisionnement en matériel informatique et solutions technologiques. Ces partenariats stratégiques nous permettent de garantir fiabilité, flexibilité et performance dans nos offres.

*Figure 6 : Logo du fournisseur BNP Paribas**Figure 7 : Logo du fournisseur GRENKE**Figure 8 : Logo du fournisseur TD SYNEX**Figure 9 : Logo du fournisseur Leasecom**Figure 10: Logo du fournisseur Locam*

2. Le client : BIOBULLE

*Figure 11 : Logo du client Biobulle*

Biobulle est une entreprise engagée dans la distribution de produits biologiques et naturels. Elle s'est développée autour de deux points de vente physiques : l'un situé à Nice et l'autre à Saint-Laurent-du-Var (SLV). Ces deux magasins ont longtemps fonctionné en synergie, avec un système informatique centralisé basé à SLV. Le magasin de SLV jouait un rôle stratégique, hébergeant notamment le serveur ERP* principal, chargé de la gestion des achats, des ventes, des stocks et des caisses pour l'ensemble de l'activité des deux boutiques.

Pour garantir une connexion fluide entre les deux sites, un VPN* site-à-site sécurisé (BOVPN*) avait été mis en place, permettant au magasin de Nice d'accéder en temps réel aux données et services du serveur centralisé à SLV.

À la suite d'une liquidation judiciaire du magasin SLV, Biobulle a dû procéder en urgence au déplacement de son infrastructure informatique. Ne disposant pas d'espace suffisant dans le magasin de Nice, 3S2I, en tant que prestataire informatique, a obtenu les droits légaux nécessaires pour héberger temporairement les équipements dans ses propres locaux.

Cette solution temporaire permet à Biobulle de continuer son activité à Nice tout en réfléchissant, avec l'aide de 3S2I, à une nouvelle solution d'hébergement adaptée.

3. Le sujet

3.1. Besoin de l'entreprise

Dans le cadre de la fermeture du magasin Biobulle de Saint-Laurent-du-Var, l'ensemble de l'infrastructure informatique a été déplacé temporairement dans les locaux de l'entreprise 3S2I. Cette solution visait à garantir la continuité de l'activité du magasin de Nice, encore actif.

Sur le plan technique, le matériel transféré comprenait notamment un pare-feu physique de type WatchGuard T80, ainsi que plusieurs équipements serveurs essentiels au fonctionnement du système ERP de Biobulle.



Figure 12 : Pare-feu T80 de l'existant technique

Une fois les équipements installés dans la salle serveur de 3S2I, plusieurs contraintes majeures sont rapidement apparues. Le matériel de Biobulle, devenu encombrant, ne correspondait plus aux standards actuels et utilisait une version obsolète du système d'exploitation, peu maintenue. En raison de la liquidation judiciaire de SLV, l'entreprise ne disposait pas des ressources financières nécessaires pour investir dans un nouveau serveur, plus compact et adapté. De plus, l'infrastructure physique hébergée chez 3S2I dépendait fortement de leur propre connexion fibre : en cas de panne, cela aurait également impacté les activités de Biobulle. Enfin, bien que le risque soit faible, un éventuel vol du matériel sur le site de 3S2I compromettrait sérieusement la continuité de leur activité.

Face à ces limites, 3S2I a pris la décision stratégique de virtualiser l'ensemble des équipements de Biobulle. Ce contexte a directement conduit au développement de mon sujet de stage : la mise en place d'un pare-feu virtuel destiné à sécuriser l'environnement virtualisé de Biobulle et garantir la continuité de son système d'information.

3.2. Existant technique

L'architecture technique actuelle s'appuie sur deux sites reliés entre eux : le site principal chez 3S2I et le site utilisateur situé dans le magasin Biobulle à Nice. Chacun de ces sites est protégé par un pare-feu WatchGuard, assurant une sécurité réseau renforcée. La communication entre les deux emplacements est assurée par un tunnel BOVPN, permettant un accès sécurisé et continu aux ressources à distance. Du côté de 3S2I, l'infrastructure comprend un serveur ERP centralisant les opérations de gestion (achats, ventes, stocks, caisses), un serveur de redondance garantissant la continuité de service en cas de panne, ainsi qu'un serveur NAS* dédié au stockage des données critiques. L'ensemble de ces équipements est connecté à un switch Netgear, assurant la circulation fluide des données entre les différents éléments. Grâce à cette configuration, les postes de travail de Biobulle peuvent accéder en toute sécurité aux ressources hébergées à distance. Cependant, l'ensemble des contraintes mentionnées précédemment a conduit à envisager une nouvelle solution, qui constitue

le cœur de mon stage.

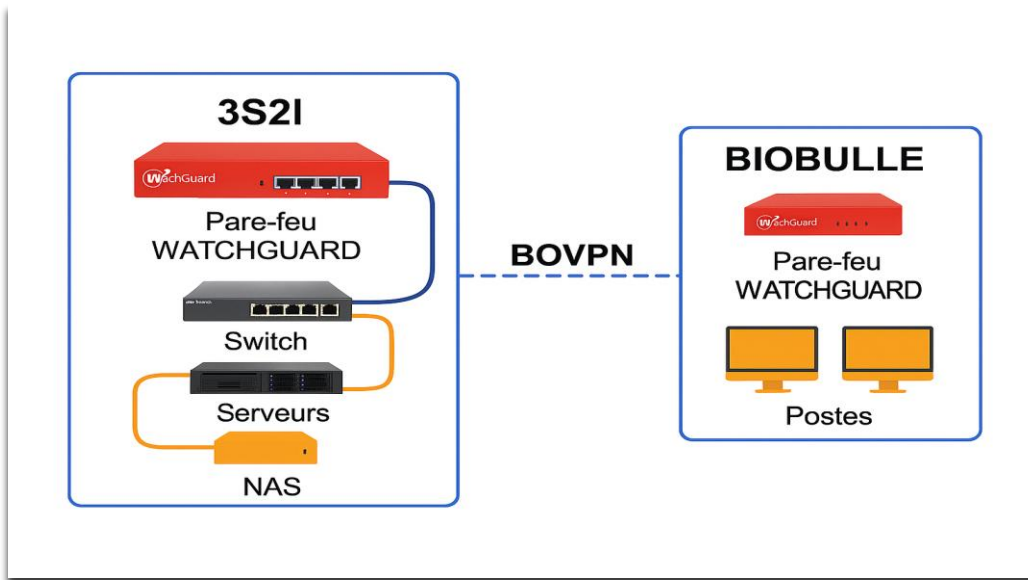


Figure 13 : Schéma de l'existant technique

3.3. Objectifs

Afin de mener à bien ce projet, il faudra atteindre les objectifs qui sont représentés dans le schéma ci-dessous :

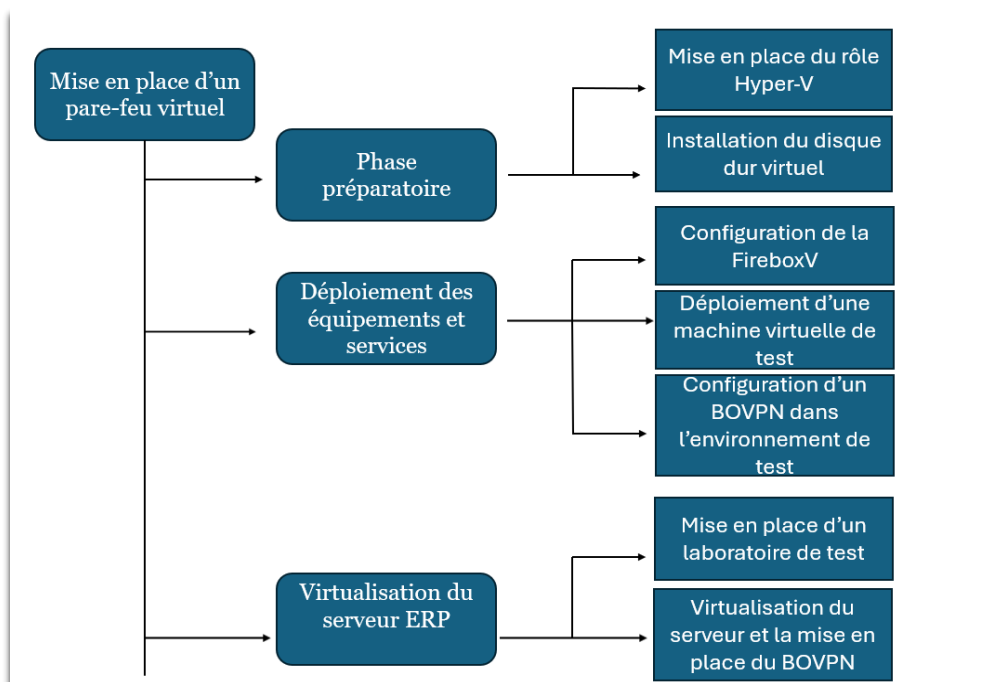


Figure 14 : Schéma des objectifs

Les objectifs sont divisés en trois grandes phases : la phase préparatoire, le déploiement des équipements et services, puis la virtualisation du serveur ERP. La phase préparatoire comprend l'activation du rôle Hyper-V et l'installation du disque dur virtuel, essentiels pour l'hébergement de la FireboxV. Ensuite, les équipements sont déployés avec la configuration de la FireboxV, le déploiement d'une machine virtuelle de test, et la mise en place d'un tunnel BOVPN dans un environnement de test. Enfin, la dernière étape concerne la virtualisation du serveur ERP ainsi que son intégration sécurisée via le BOVPN, dans un laboratoire de test. Ce processus global permet d'assurer un environnement sécurisé, stable et fonctionnel pour les besoins du projet.

Ci-après vous est présenté le schéma d'installation à mettre en place :

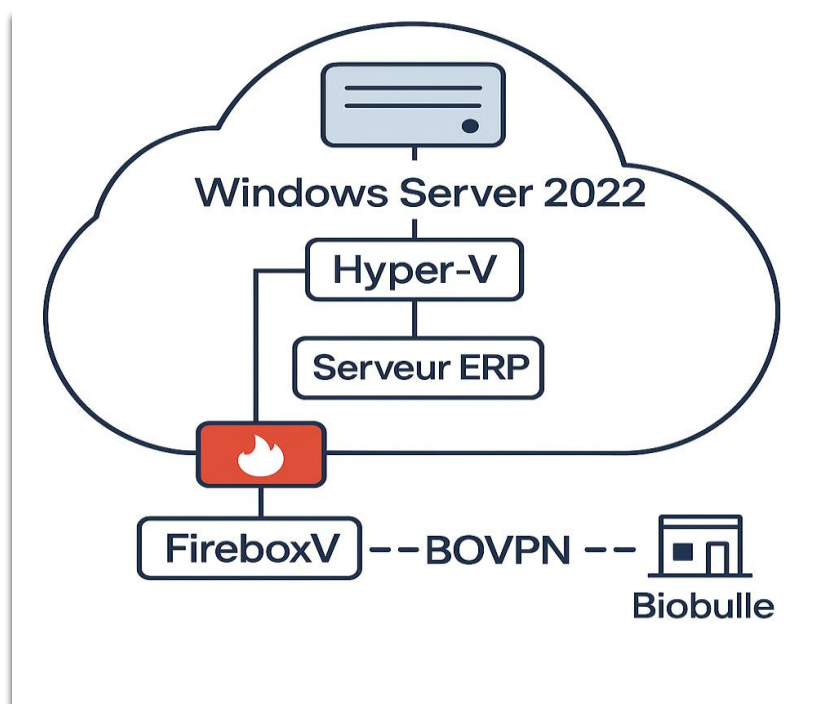


Figure 15 : Infrastructure de l'installation

4. La procédure

4.1. Outils

Pour la mise en place du pare-feu virtuel dans le cadre de mon projet, j'ai utilisé une série d'outils et de technologies essentiels afin de répondre aux besoins.



Figure 16 : Logo du serveur Active Directory(AD)

Le serveur Active Directory a été déployé pour centraliser la gestion des utilisateurs et des ressources réseau. Il a également permis l'installation du rôle Hyper-V, facilitant ainsi la virtualisation des services nécessaires au projet.



Figure 17 : Logo du serveur Hyper-V

Hyper-V a été utilisé comme hyperviseur pour créer et gérer les machines virtuelles, notamment celles hébergeant le pare-feu virtuel (FireboxV*) et le serveur. Cette solution a permis une gestion flexible et efficace des ressources virtualisées.



Figure 18 : Logo de la FireboxV

FireboxV, le pare-feu virtuel de WatchGuard, a été déployé pour sécuriser l'environnement virtualisé. Il offre des fonctionnalités avancées de sécurité réseau, assurant une protection robuste des données et des communications au sein de l'infrastructure.



Figure 19 : Disque dur externe

Ce disque, connecté au serveur, a servi à stocker le fichier VHD* généré via l'outil Disk2VHD. Ce processus a permis d'extraire l'image des VMs* à partir du serveur physique.



Figure 20 : Capture d'écran du logiciel Disk2VHD

Disk2VHD est un utilitaire développé par Microsoft permettant de convertir une machine physique en machine virtuelle en générant un fichier au format VHD (Virtual Hard Disk). Léger et simple d'utilisation, ce logiciel permet de capturer à chaud les

volumes d'un système en fonctionnement, sans avoir besoin de l'arrêter. Disk2VHD a été essentiel pour virtualiser le serveur ERP existant, en facilitant sa migration vers l'environnement Hyper-V après l'échec des tentatives de transfert via d'autres solutions.

4.2. Diagramme de Gantt

La planification des différentes étapes de ce projet est présentée dans le diagramme de Gantt ci-dessous :

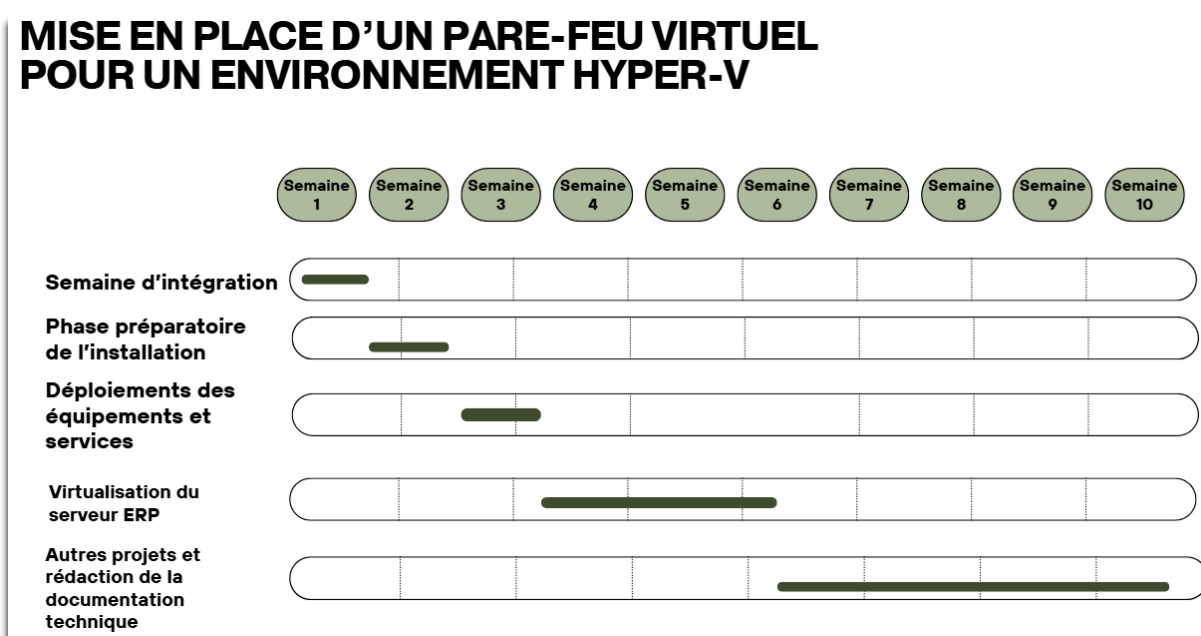


Figure 21 : Diagramme de Gantt

II. Réalisation du travail

1. Phase préparatoire

1.1. Mise en place du rôle Hyper-V

Le rôle de serveur Hyper-V permet de créer et de gérer des machines virtuelles dans un environnement isolé, offrant ainsi une solution de virtualisation performante, idéale pour le déploiement d'infrastructures réseau.

L'installation du rôle Hyper-V a été la première étape pour transformer l'ordinateur hôte en un environnement de virtualisation. Cette opération a été effectuée via le Gestionnaire de serveur de Windows. En accédant au menu "Ajouter des rôles et fonctionnalités", le rôle Hyper-V a été sélectionné, puis installé après validation des paramètres réseau et redémarrage de la machine. Une fois le système relancé, le Gestionnaire Hyper-V est devenu accessible, permettant de créer et gérer les machines virtuelles nécessaires au projet.

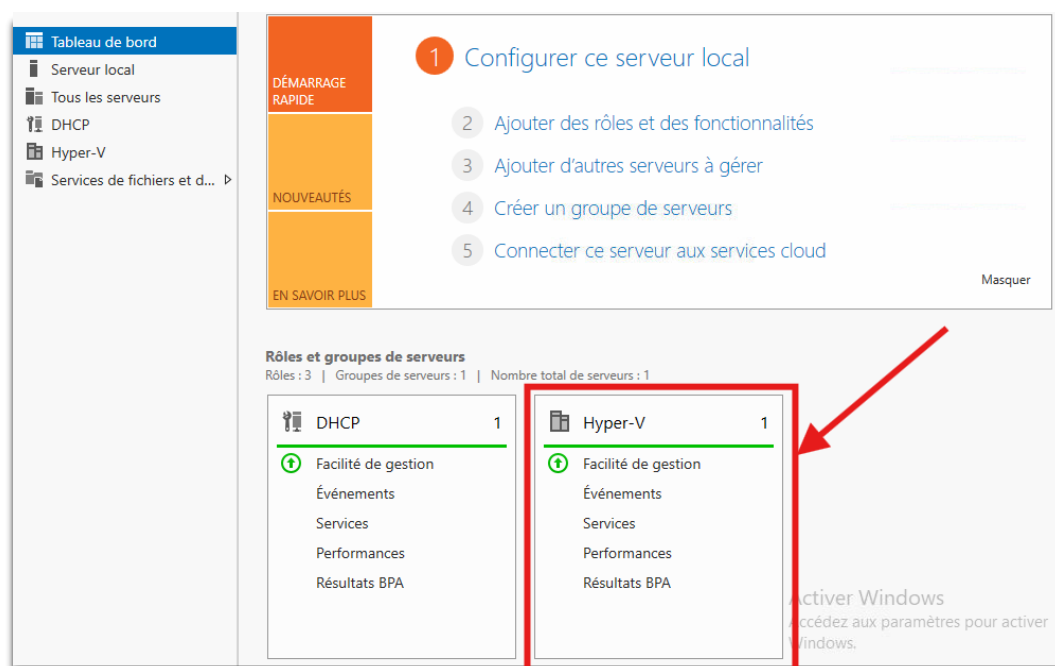


Figure 22 : Capture d'écran du rôle Hyper-V

La première étape de la configuration a consisté à créer des commutateurs virtuels*, indispensables pour connecter les machines virtuelles entre elles et à Internet.

Pour cela, il a fallu ouvrir le Gestionnaire Hyper-V (via le menu Démarrer) et accéder au Gestionnaire de commutateurs virtuels. Deux types de commutateurs ont été créés : un commutateur externe, nommé par "Commutateur du réseau externe", relié à la carte réseau physique de l'hôte, permettant aux machines virtuelles d'accéder au réseau réel ; et un commutateur interne, nommé "Commutateur du réseau interne", utilisé pour permettre la communication entre les machines virtuelles et l'ordinateur hôte, sans passer par le réseau externe. Ces deux commutateurs sont essentiels pour

segmenter logiquement les flux réseau entre la FireboxV et les autres composants de l'infrastructure.

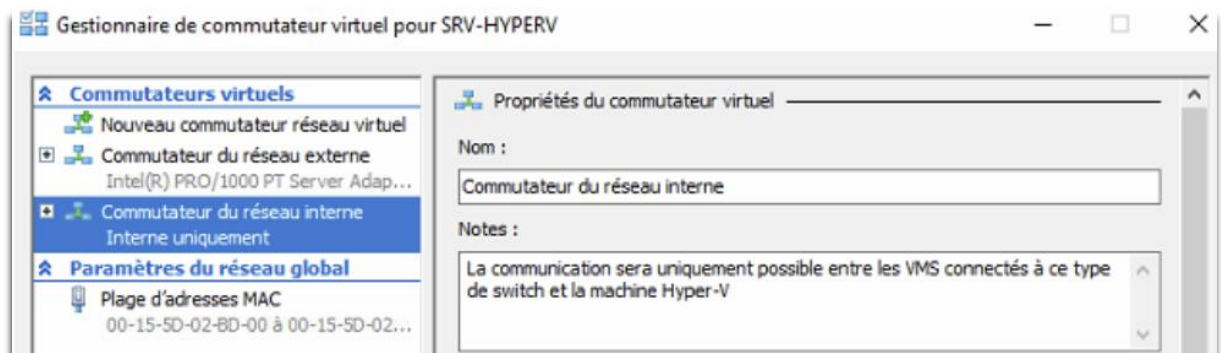


Figure 23 : Capture d'écran des commutateurs virtuels

1.2. Installation du disque dur virtuel

Dans le cadre de la mise en place de la FireboxV sur l'hyperviseur Hyper-V, l'installation du disque dur virtuel constitue une étape essentielle. WatchGuard fournit une image disque préconfigurée au format “.vhd “, spécialement conçue pour une intégration directe dans un environnement Hyper-V.

Le fichier “.vhd “ de la FireboxV a été téléchargé depuis le site officiel de WatchGuard, accessible aux utilisateurs enregistrés.

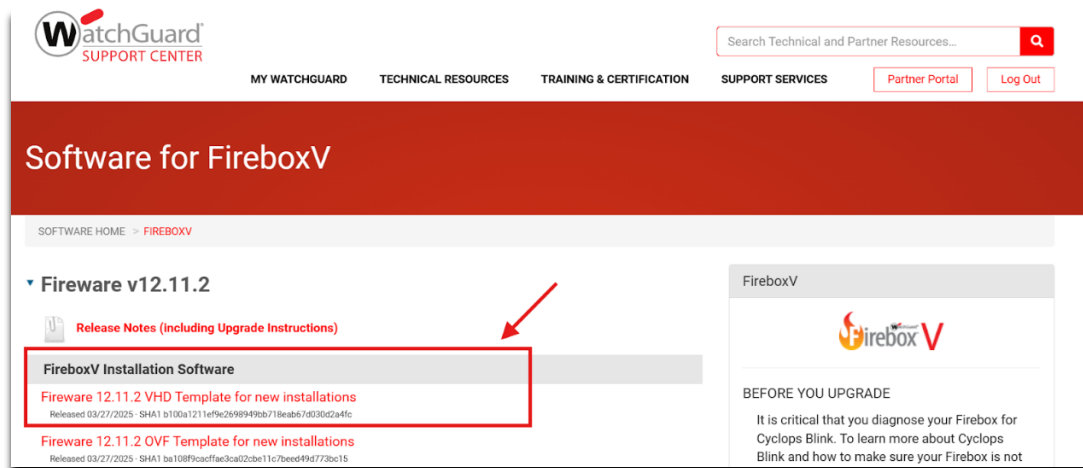


Figure 24 : Capture d'écran du fichier “.vhd“ à télécharger

Le fichier FireboxV_12_11_2.vhd est visible ici après extraction de l'archive téléchargée depuis le site officiel de WatchGuard. Ce fichier sera utilisé comme disque dur virtuel lors de la création de la machine virtuelle dans Hyper-V.


Nom	Type	Taille compressée
 FireboxV_12_11_2	Virtual Hard Disk	200430

Figure 25 : Disque dur virtuel extrait

L'installation du disque dur virtuel au format « .vhd », téléchargé depuis le site officiel de WatchGuard, marque la fin de la phase de préparation du support système de la FireboxV. Ce fichier est désormais prêt à être intégré à une machine virtuelle sous Hyper-V.

La prochaine étape consiste donc à créer et configurer une machine virtuelle capable d'exécuter ce pare-feu virtualisé, en lui associant le disque dur précédemment préparé, tout en définissant les ressources matérielles nécessaires et les interfaces réseau pour le routage.

2. Déploiement des équipements et services


2.1. Configuration de la FireboxV

Avant de procéder à la configuration proprement dite de la FireboxV, il a été essentiel de consulter la documentation officielle fournie par WatchGuard. Cette étape préparatoire m'a permis de mieux comprendre les prérequis, les options disponibles et les bonnes pratiques de déploiement pour l'environnement Hyper-V.

La documentation décrit de manière détaillée les différentes éditions disponibles (Small, Medium, Large) ainsi que de leurs ressources système recommandées.

Après analyse des besoins de notre projet (nombre d'utilisateurs limités, trafic modéré, infrastructure légère), la version Small de la FireboxV a été retenue.

FireboxV Small



WatchGuard FireboxV Small brings network security to virtual environments.

FireboxV Small is suitable for small offices and branch locations with up to 50 users.

- **2Gbps** Firewall Throughput
- **400Mbps** VPN throughput
- 8 to 10 Virtual Interfaces

Figure 26 : Caractéristique de la FireboxV

Cette version FireboxV Small est conçue pour les petits environnements, elle prend en charge jusqu'à 50 utilisateurs. Elle offre un débit pare-feu de 2 Gbps, un débit VPN de 400 Mbps et gère 8 à 10 interfaces virtuelles. Ces performances assurent une sécurité réseau efficace tout en restant légère pour Hyper-V.

Concernant les ressources système, la version FireboxV Small reste peu exigeante, ce qui facilite son déploiement dans un environnement virtualisé comme Hyper-V. Selon la documentation officielle, elle nécessite au minimum 2 048 Mo de mémoire, avec une mémoire recommandée de 4 096 Mo, et peut utiliser jusqu'à 2 vCPUs. Ces spécifications permettent un bon équilibre entre performance et consommation de ressources, rendant ce modèle parfaitement adapté à une infrastructure légère ou de test.

Ressources recommandées pour FireboxV par modèle : ^

Modèle de FireboxV	Mémoire Totale Minimum	Mémoire Recommandée	Nombre maximal de vCPU
Petite	2 048 Mo*	4 096 Mo	2
Moyenne	4 096 Mo	4 096 Mo	4
Large	4 096 Mo	8 192 Mo	8
Extra Large	4 096 Mo	16 383 Mo	16

Figure 27 : Capture d'écran des ressources recommandées

Après avoir validé le modèle FireboxV Small, la machine virtuelle a été créée sur Hyper-V avec les paramètres adaptés. L'élément central de l'installation réside dans l'intégration du disque virtuel fourni par WatchGuard. Celui-ci, au format « .vhd », a été téléchargé depuis l'espace officiel du site. Lors de la création de la VM, ce disque a été sélectionné comme support principal, ce qui permet d'éviter une installation manuelle du système.

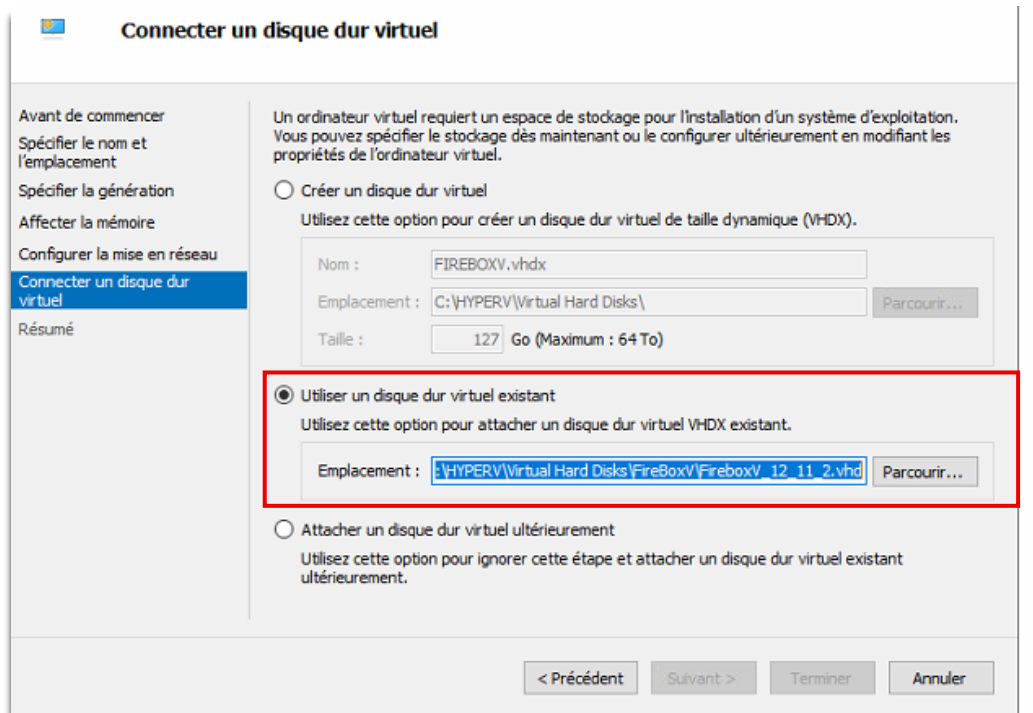


Figure 28 : Capture d'écran de l'emplacement du disque à sélectionner

Les ressources ont ensuite été allouées selon les recommandations : 4096 Mo de RAM et 2 vCPUs, et une carte réseau virtuelle a été associée à l'interface externe pour assurer la connectivité. Avant de démarrer la FireboxV, une seconde carte réseau a été ajoutée afin de permettre la gestion du trafic interne via le commutateur virtuel interne configuré précédemment dans Hyper-V. Cette interface est essentielle pour permettre la communication entre la FireboxV et les autres machines du réseau local virtuel. Notre FireboxV est prête à être démarrée.


```

WatchGuard-Firebox login: status
Password:
--
-- WatchGuard Firewall OS Version 12.11.2.B713726
-- Support: https://www.watchguard.com/support/supportLogin.asp
-- Copyright (C) 1996-2025 WatchGuard Technologies Inc.
--
WG>sh int
--
-- Interface Properties
-- Type: TR = trusted, EX = external, OP = optional, CS = custom, UL = vlan, BR
= bridge, CL = cluster, LA = <link aggregation, NA = not apply
--
physical interface count : 2
licensed interface count : 2
--
-- Interface Address & Status
--
Enabled If-# Name Address Type/MTU Status IP-Assignment
IP-Node-Type
yes 0 External 213.246. /24 EX/1500 Up Static
IPv4 Only
yes 1 Trusted 192.168.50.1/24 TR/1500 Up Static
IPv4 Only
WG>_

```

Figure 29 : Ecran de démarrage de la FireboxV

En se connectant avec l'identifiant "status" et le mot de passe par défaut "readonly", la commande "#sh int" a permis d'afficher l'état des interfaces et de confirmer que les deux cartes réseau étaient bien actives et correctement configurées.

La configuration a été modifiée pour attribuer une adresse IP publique statique à l'interface External* (interface 0), afin de permettre un accès à distance. De même, une adresse IP privée a été maintenue sur l'interface Trusted* (interface 1) pour le réseau interne.

Grâce à cette configuration, l'interface graphique de gestion de la FireboxV est désormais accessible via un navigateur web. Il suffit de saisir l'URL* suivante dans la barre d'adresse : "https://ip_public:8080"

Cela permet d'accéder à l'interface Web de la FireboxV pour effectuer la configuration avancée du pare-feu.

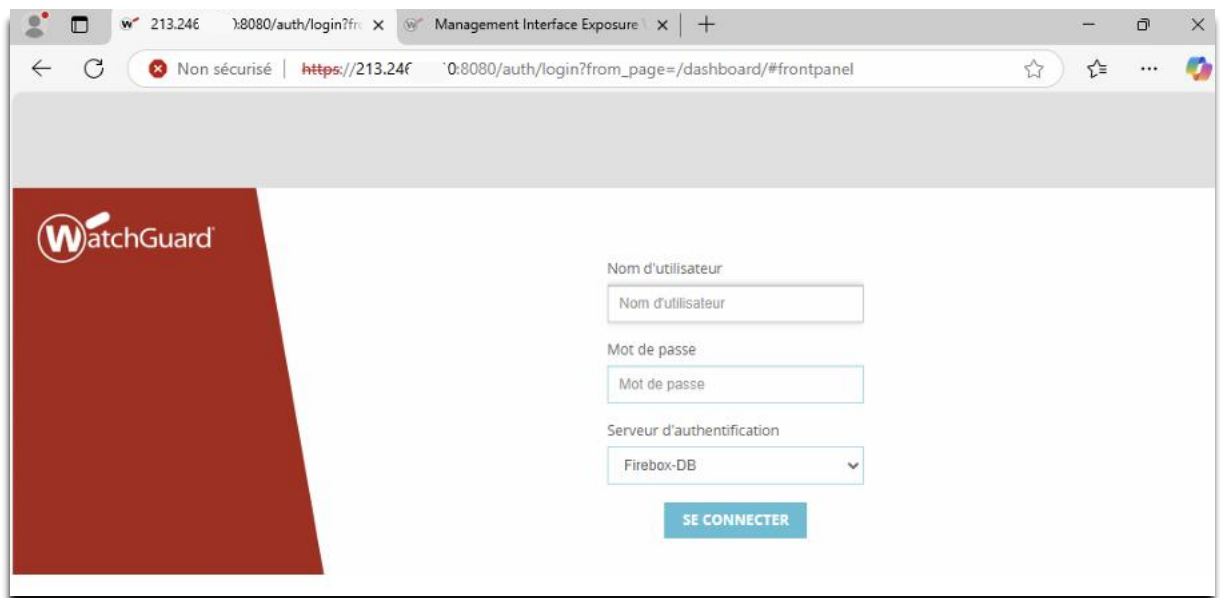


Figure 30 : Capture d'écran de l'interface graphique de la FireboxV

Une fois l'accès à l'interface graphique, on se connecte avec l'identifiant "admin" et le mot de passe par défaut "readwrite", qui offre un accès complet aux paramètres de configuration du pare-feu.

À ce stade, pour gagner du temps et garantir la continuité des règles de sécurité déjà en place, j'ai intégré la configuration existante du pare-feu utilisée dans l'environnement technique actuel, tout en assurant une transition fluide vers l'environnement virtualisé.

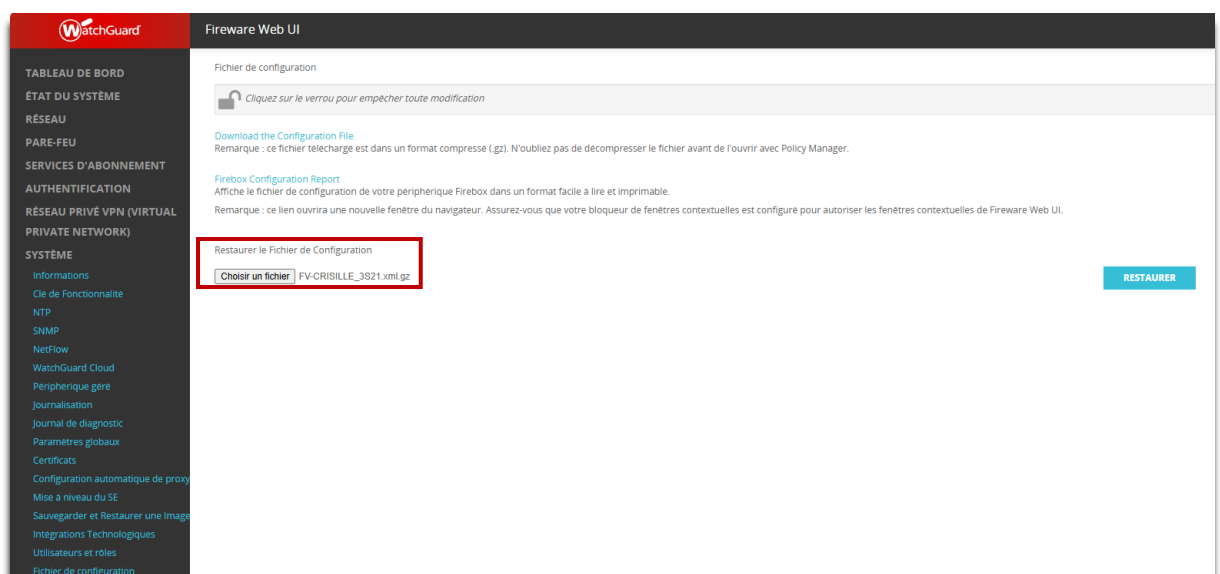


Figure 31 : Capture d'écran de l'importation de la configuration

Enfin, la dernière étape de la configuration de la FireboxV consiste à activer la licence du produit. Cette opération est essentielle pour débloquent l'ensemble des fonctionnalités de sécurité avancées proposées par WatchGuard. Une fois connecté à l'interface d'administration, on se rend dans le menu Système > Clé de fonctionnalité puis on colle la clé de fonctionnalité fournie lors de l'enregistrement de l'équipement sur le portail WatchGuard.

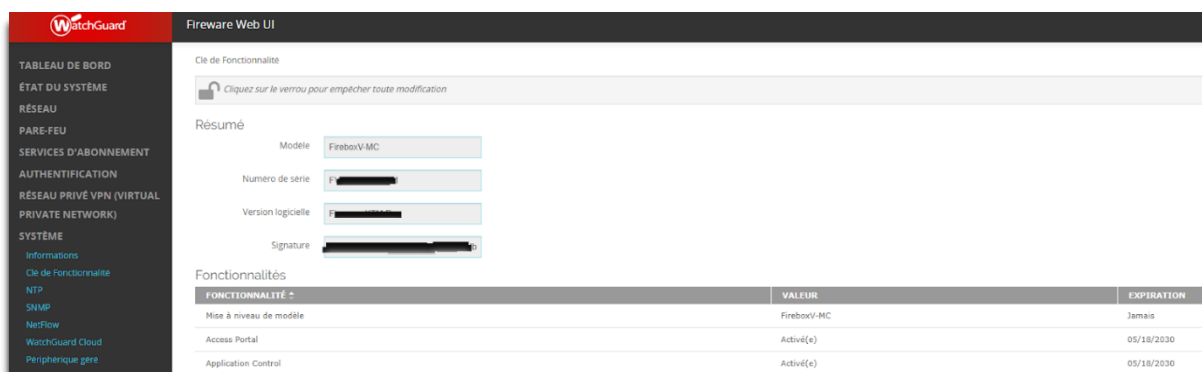


Figure 32 : Capture d'écran de l'activation de la licence

Cette section nous affiche les informations essentielles du périphérique, notamment le modèle (FireboxV-MC), le numéro de série, la version logicielle ainsi que la signature de l'appareil. En dessous, on retrouve la liste des fonctionnalités activées grâce à la clé de licence, accompagnées de leur statut et date d'expiration.

2.2. Déploiement d'une machine virtuelle de test

Pour valider le bon fonctionnement de la FireboxV avant de virtualiser le serveur principal, j'ai mis en place une machine virtuelle de test sous Windows 10, que j'ai nommée VM_TEMPORAIRE. Cette VM, intégrée au commutateur virtuel interne, m'a permis de simuler un poste client et de m'assurer que tout le trafic passait bien par le pare-feu. J'ai opté pour une génération 1, avec 4096 Mo de mémoire et un disque virtuel de 64 Go. J'ai ensuite sélectionné l'ISO de Windows 10 comme source d'installation.

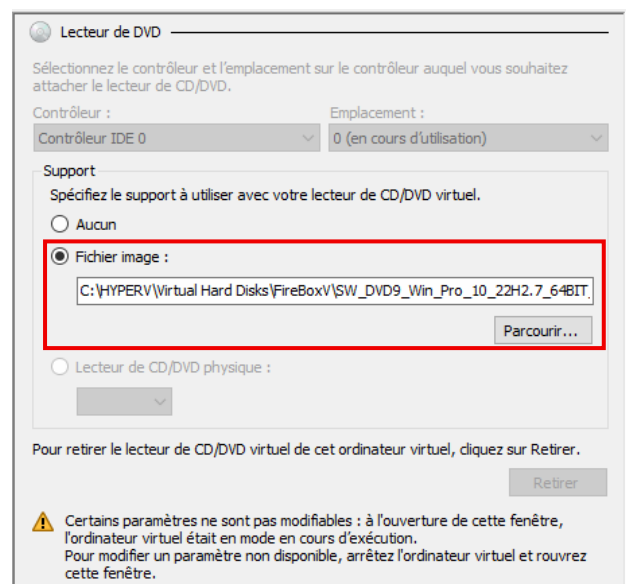


Figure 33 : Fichier ISO de la VM de test

Une fois la configuration terminée, la machine virtuelle a été créée et ajoutée à l'environnement de test.

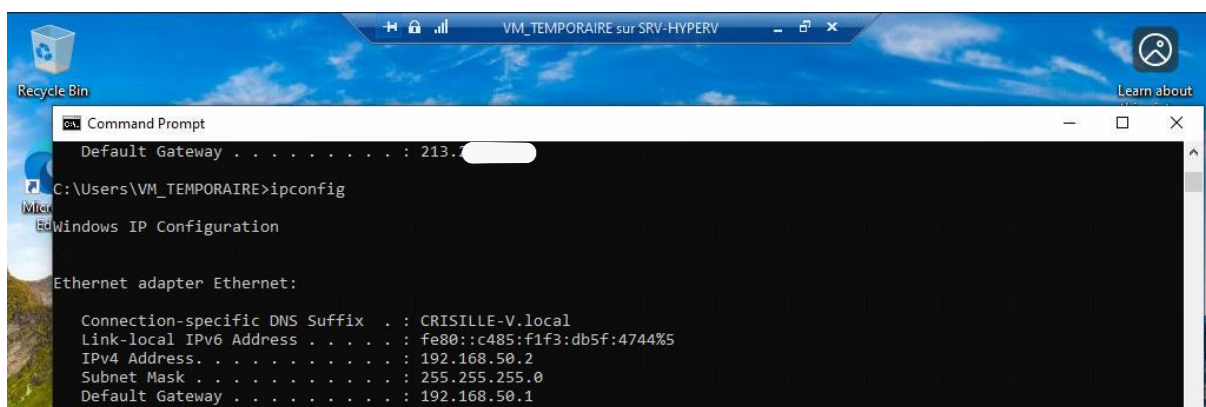


Figure 34 : Capture d'écran de la configuration de la VM de test

Une fois la machine de test démarrée, je lui ai attribué l'adresse IP 192.168.50.2, une adresse que j'avais préalablement réservée dans la FireboxV en fonction de son adresse MAC. Cela permet d'assurer une attribution cohérente et contrôlée au sein du réseau interne. La capture ci-dessus confirme que la machine utilise bien cette IP, avec comme passerelle par défaut 192.168.50.1, correspondant à l'interface interne (Trusted) du pare-feu. Cette étape m'a permis de valider la communication réseau et de m'assurer que la VM transite correctement par la FireboxV.

Une fois la machine de test correctement intégrée au réseau via la FireboxV, je poursuis avec l'étape suivante : la mise en place du BOVPN pour assurer une connexion sécurisée entre les deux sites.

2.3. Configuration d'un BOVPN en environnement de test

Pour connecter de manière sécurisée les deux sites distants à savoir la FireboxV et le pare-feu physique au siège de 3S2I, j'ai mis en place un BOVPN . Ce type de tunnel VPN site-à-site permet de relier directement les deux réseaux internes via un canal chiffré, comme s'ils étaient sur le même réseau local.

Pour établir un BOVPN fonctionnel entre les deux sites, deux éléments doivent impérativement être configurés : la passerelle VPN et le tunnel.

- La passerelle correspond à la configuration du point de connexion distant, c'est-à-dire l'adresse IP publique de l'autre site ainsi que les paramètres de chiffrement et d'authentification . C'est elle qui initie ou accepte la connexion.
- Le tunnel, quant à lui, permet de spécifier les sous-réseaux internes qui seront échangés entre les deux sites. C'est ce tunnel qui transporte réellement les paquets entre les réseaux locaux, en s'appuyant sur la passerelle configurée.

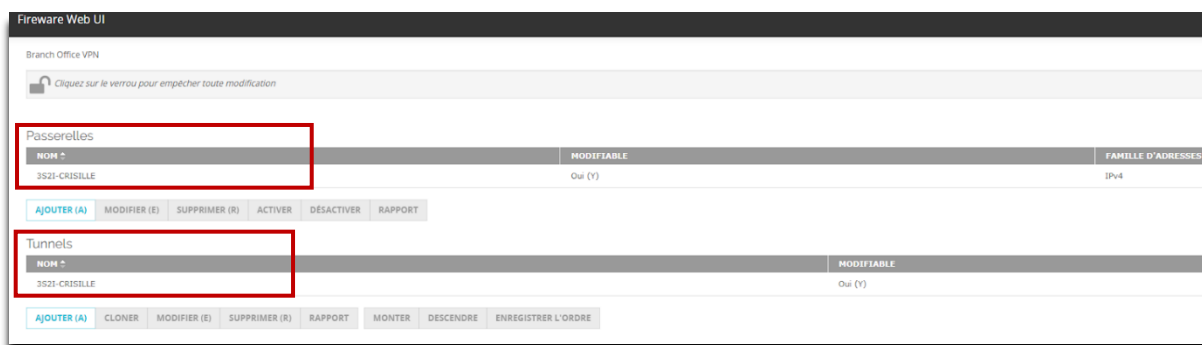


Figure 35 : Capture d'écran de la configuration du BOVPN

Dans la configuration ci-dessous, j'ai défini les deux sous-réseaux internes à connecter via le tunnel sécurisé. Le tunnel est configuré en Configuration du tunnel, ce qui signifie que le trafic est autorisé à circuler dans les deux sens entre les deux réseaux. Cette configuration permet ainsi à la machine de test présente dans le réseau interne de la

FireboxV d'accéder aux ressources du réseau du siège, et réciproquement, tout cela à travers une liaison sécurisée.

Figure 36 : Configuration du tunnel BOVPN

Puis on configure la passerelle VPN qui sert de point d'entrée au tunnel BOVPN entre les deux sites. Dans mon cas, j'ai défini l'adresse IP publique de la FireboxV comme extrémité locale, et celle du pare-feu physique de 3S2i comme extrémité distante. Une clé pré-partagée a été utilisée pour l'authentification mutuelle entre les deux équipements, ce qui garantit un échange sécurisé. Cette phase permet d'établir une base de confiance entre les deux pare-feux.

Fireware Web UI Utilisateur : admin

Nom de la passerelle: 3S2I-CRISILLE

Famille d'Adresses: Adresses IPv4

Paramètres généraux | Paramètres de phase 1

Méthode d'informations d'identification

☒ Utiliser une clé pré-partagée Chaîne

☐ Utiliser Firebox Certificate d'IPSec

☐ Afficher Tous les Certificats

ID	NOM DU CERTIFICAT	ALGORITHME	TYPE

Extrémité de la passerelle

	INTERFACE LOCALE	TYPE LOCAL	ID LOCALE	IP DISTANTE	TYPE DISTANT	ID DISTANTE
1	External	Adresse IP (I)	213.24.0	141.3	Adresse IP (I)	141.3

Figure 37 : Configuration de la passerelle BOVPN

Toujours dans la suite de la configuration de la passerelle, j'ai sélectionné le protocole IKEv2*, reconnu pour sa fiabilité et ses performances, et j'ai appliqué un chiffrement de type SHA2-256-AES* associé au groupe Diffie-Hellman* 14 pour l'échange de clés. Afin d'assurer la persistance du tunnel même en présence de NAT*, l'option NAT Traversal a été activée avec un intervalle d'activité de 20 secondes. La fonction DPD (Dead Peer Détection) est également en place pour détecter toute perte de connectivité et tenter de rétablir automatiquement la liaison, ce qui garantit une connexion VPN toujours disponible entre les deux sites.

Branch Office VPN / Modifier (E)

Cliquez sur le verrou pour effectuer des changements

Nom de la passerelle

Famille d'Adresses

Paramètres généraux Paramètres de phase 1

Version

☒ Parcours NAT

Intervalle d'activité secondes

☒ Detection DPD (Dead Peer Detection) (RFC3706)

Type

Délai d'inactivité du trafic secondes

Nombre maximal de tentatives

Paramètres de transformation

TRANSFORMATION DE PHASE 1	GROUPE CLÉ
SHA2-256-AES(256-bit)	Diffie-Hellman Groupe 14

Figure 38 : Configuration de la passerelle BOVPN(suite)

Ainsi, pour que le tunnel fonctionne correctement, il est indispensable de reproduire une configuration équivalente sur le pare-feu du site de 3S2I. Cela inclut la définition des mêmes paramètres : IP publiques et privées, clé pré-partagée, version du protocole (IKEv2), algorithmes de chiffrement et routes réseau. Cette symétrie garantit l'établissement du tunnel VPN de manière sécurisée et bidirectionnelle. La capture ci-dessus confirme que le tunnel est bien actif et opérationnel des deux côtés, ce qui permet désormais un accès fluide et sécurisé à la machine virtuelle de test hébergée derrière la FireboxV.

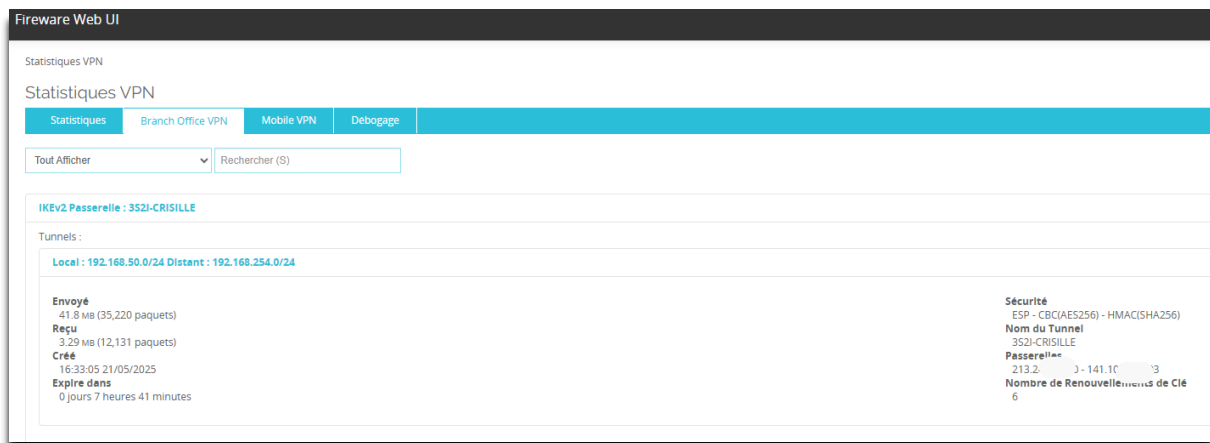


Figure 39 : Capture d'écran du bon fonctionnement du BOVPN

3.Virtualisation du serveur ERP

Avant de procéder à la virtualisation du serveur ERP, plusieurs contraintes ont dû être prises en compte, notamment celles liées au client. En effet, ce serveur est en production et héberge des services utilisés au quotidien. Toute opération de basculement devait donc être planifiée afin de ne pas perturber l'activité, ce qui constitue une contrainte organisationnelle importante. Pour garantir la réussite de cette transition, j'ai donc mis en place un laboratoire de test afin de valider l'intégration du serveur dans l'environnement virtualisé avant de lancer la migration finale.

3.1. Mise en place d'un laboratoire de test

3.1.1. Mise en place d'une machine de test sur le serveur

Une machine virtuelle Windows 10 a été créée sur le serveur physique exécutant VMware ESXi 6.5, hébergeant également la VM ERP en production. Cette VM de test visait à simuler un environnement proche de celui de l'ERP, afin de valider la migration vers Hyper-V sans impacter le système en service. Elle a été configurée avec 2 vCPUs, 4 Go de RAM, 32 Go de disque et une carte réseau active.

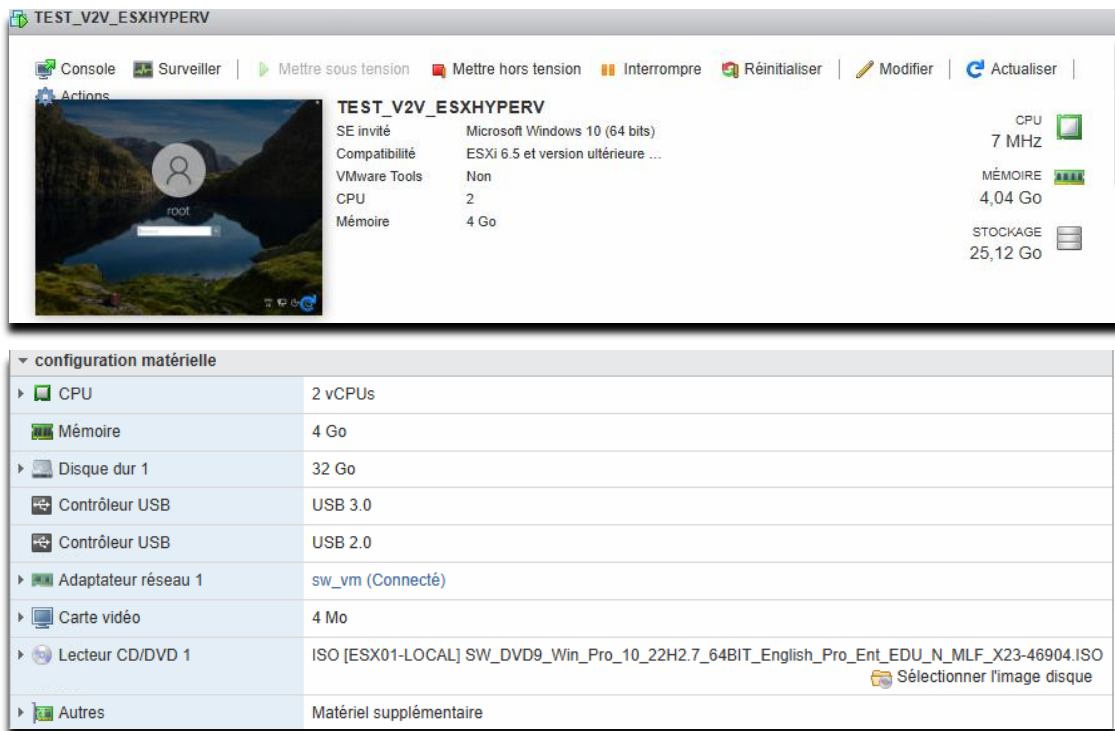


Figure 40 : Caractéristique de la VM

3.1.2. Conversion de disque

L'outil Disk2Vhd de Sysinternals a été installé sur la machine de test afin de générer une image du système au format VHDX*, compatible avec Hyper-V.



Figure 41 : Logiciel Disk2vhd

Les volumes système "C:\ " et partitions associées ont été sélectionnés, avec les options "Use VHDX" et "Volume Shadow Copy" activées pour assurer une image cohérente. Le fichier généré a été enregistré sur un disque dur externe branché au serveur.

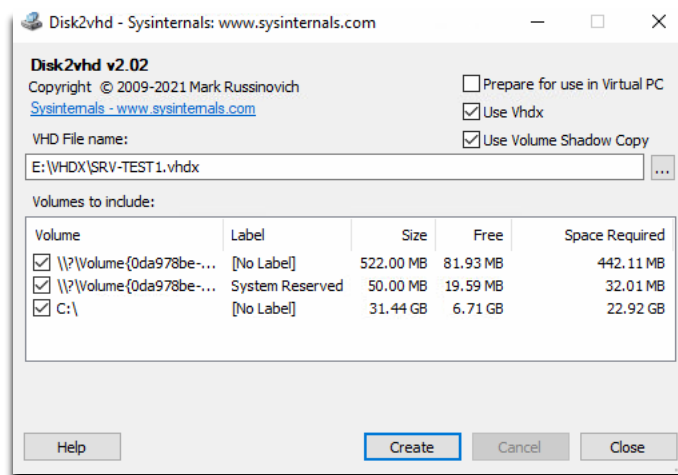


Figure 42 : Conversion du disque

- "Use VHDX" : cette option permet de sauvegarder l'image du disque au format VHDX, plus récent que le format VHD. Ce format est optimisé pour Hyper-V.
- "Volume Shadow Copy" : en activant cette option, Disk2Vhd crée une copie instantanée du disque pendant qu'il est utilisé.

3.1.3. Exportation et création de VM avec le disque VHD

Après la conversion, le fichier ".vhdx" a été stocké sur un disque dur externe, puis transféré très simplement vers le serveur Hyper-V via TeamViewer(logiciel de contrôle à distance) en le glissant depuis mon poste local.

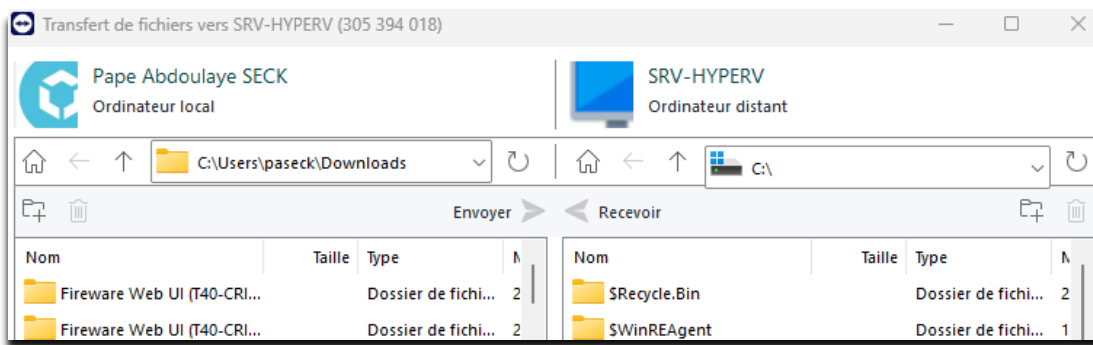


Figure 43 : Transfert de fichier via TeamViewer

Une fois le fichier copié dans le répertoire de stockage du serveur, une nouvelle VM nommée SRV_ESXITEST a été créée sur Hyper-V avec les paramètres suivants : génération 1, 4 Go de RAM, carte réseau connectée à un commutateur interne, et en utilisant le disque VHDX converti comme disque principal.



Figure 44 : Configuration de la nouvelle VM de test

Après cette configuration, la VM est prête à être utilisée et constitue une image instantanée fidèle de celle hébergée sur le serveur physique.

3.2. Virtualisation du serveur ERP et la mise en place du BOVPN

3.2.1. Virtualisation du serveur ERP

Pour clôturer ce projet, la dernière étape consistait à virtualiser le serveur ERP physique de Biobulle, qui hébergeait deux machines virtuelles importantes : BIOBULLE-V2V et SRV-VEEAM.



Figure 45 : Les VMs à virtualiser du serveur ERP

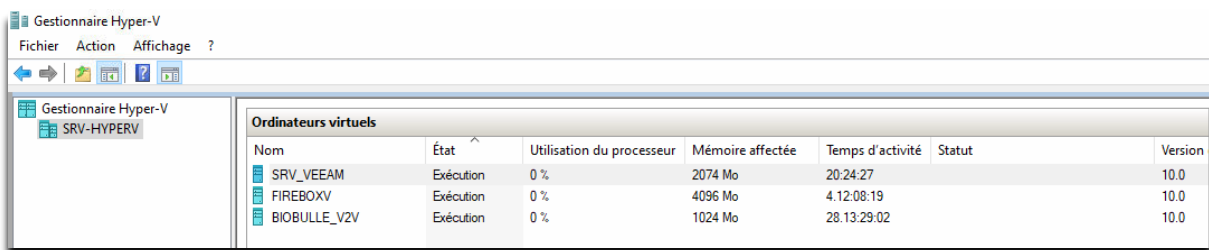
La première, BIOBULLE-V2V, contient le logiciel métier utilisé par le magasin pour sa gestion quotidienne. La seconde, SRV-VEEAM, est dédiée aux sauvegardes automatiques, assurant ainsi la sécurité et la restauration des données en cas d'incident.

Dans la phase finale, nous avons suivi la même procédure que celle utilisée lors du test. J'ai installé Disk2VHD sur les deux VMs afin de générer des images système au format VHDX, compatibles avec Hyper-V.

Ensuite, les fichiers ont été transférés via TeamViewer, simplement en les glissant depuis le serveur physique vers l'environnement Hyper-V.

Enfin, j'ai recréé manuellement les deux machines virtuelles dans Hyper-V en important les disques VHDX.

Après configuration, elles ont pu redémarrer et fonctionner normalement, il ne reste plus qu'à reconfigurer le BOVPN afin de permettre au magasin de Nice d'accéder à ses ressources virtualisées et assurer ainsi la continuité de son activité.



Gestionnaire Hyper-V						
Fichier Action Affichage ?						
Gestionnaire Hyper-V						
SRV-HYPERV						
Ordinateurs virtuels						
Nom	État	Utilisation du processeur	Mémoire affectée	Temps d'activité	Statut	Version
SRV_VEEAM	Exécution	0 %	2074 Mo	20:24:27		10.0
FIREBOXV	Exécution	0 %	4096 Mo	4:12:08:19		10.0
BIOBULLE_V2V	Exécution	0 %	1024 Mo	28:13:29:02		10.0

Figure 46 : Environnement final après le basculement

3.2.2. La mise en place du BOVPN

Pour la configuration finale du BOVPN, nous avons repris exactement la même procédure que celle utilisée durant les tests. Cela consistait à configurer la passerelle BOVPN et le tunnel associé sur la FireboxV, puis à réaliser la même configuration sur le pare-feu physique situé dans le magasin de Nice. Cette configuration a permis d'établir une connexion sécurisée entre les deux sites.



IKEv2 Passerelle : 3S2I-CRISILLE	
Tunnels :	
Local : 192.168.50.0/24 Distant : 192.168.1.0/24	
Envoyé 175 MB (1,165,232 paquets) Reçu 90.64 MB (1,210,949 paquets) Créé 09:53:13 12/06/2025 Expire dans 0 jours 3 heures 37 minutes	Sécurité ESP - CBC(AES256) - HMAC(SHA256) Nom du Tunnel 3S2I-CRISILLE Passerelles 192.168.1.0/24 - 192.168.50.0/24 Nombre de Renouvellements de Clé 13

Figure 47 : Capture d'écran du BOVPN final

III. Bilan

1. Résultats

Le schéma des objectifs atteints est le suivant :

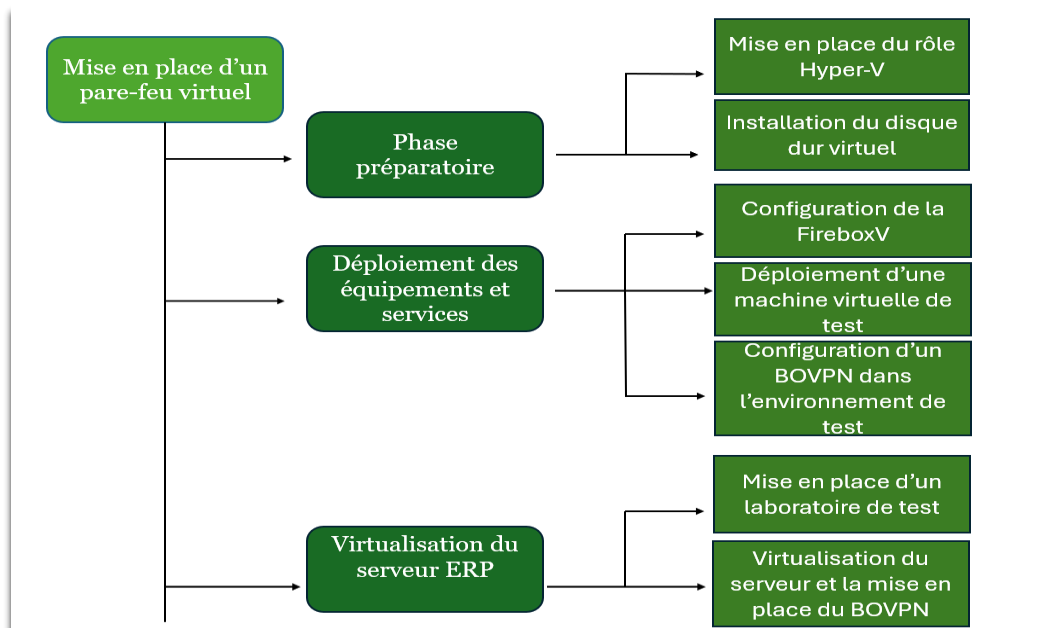


Figure 48 : Schéma des objectifs atteints

On constate que les objectifs définis au départ ont bien été atteints. En effet, j'ai pu mettre en place l'environnement virtuel avec Hyper-V, configurer le pare-feu FireboxV, déployer les machines de test et établir le tunnel BOVPN. La virtualisation du serveur ERP a également été finalisée avec succès, ce qui a permis d'assurer une communication sécurisée entre les deux sites.

2. Difficultés

Pour atteindre les résultats attendus dans ce projet, la principale difficulté rencontrée a été la virtualisation du serveur ERP. En effet, notre serveur physique hébergeait déjà plusieurs machines virtuelles via VMware, et notre objectif était de migrer ces VMs vers Hyper-V, en utilisant l'outil StarWind V2V Converter.

Cependant, malgré plusieurs tentatives, cette solution s'est révélée inefficace.

StarWind repose sur un échange via le protocole SSH, et bien que nous ayons configuré les ports nécessaires pour autoriser le trafic entre les deux environnements, aucun flux n'arrivait jusqu'au pare-feu. Pourtant, le ping vers l'adresse IP publique du pare-feu fonctionnait correctement, ce qui rendait le problème difficile à cerner. Face à cette

impasse, nous avons décidé de changer d'approche et opté pour Disk2VHD, une solution plus directe, qui nous a finalement permis de convertir et transférer l'image de la VM avec succès, et ainsi poursuivre le déploiement dans l'environnement Hyper-V. Une autre difficulté notable est apparue lors du basculement final de la solution. Il était nécessaire de programmer une intervention avec le client pour effectuer la mise en production, ce qui s'est avéré compliqué. Le magasin étant ouvert du lundi au samedi, de 8h à 21h, trouver une disponibilité compatible avec les contraintes techniques et commerciales a exigé une bonne coordination et beaucoup de patience.

3. Perspectives

Pour le moment, peu de prolongements sont envisagés, mais cette solution reste prometteuse et pourrait être proposée à d'autres clients de l'entreprise si le besoin se présente. Elle représente une alternative intéressante, notamment sur le plan économique : en effet, une licence Microsoft pour Hyper-V est nettement moins coûteuse qu'une licence VMware, souvent présente sur les serveurs physiques. De plus, depuis le rachat de VMware, le coût de ses licences a considérablement augmenté, rendant cette solution dix fois plus onéreuse.

Conclusion

Mon projet avait pour objectif la mise en place d'un pare-feu virtuel à travers un serveur Hyper-V hébergé chez Ikoula, afin de sécuriser les échanges réseau d'un environnement distant.

J'ai commencé par préparer l'infrastructure nécessaire à son installation, notamment en configurant les interfaces réseau, en accédant à l'interface graphique et en important la configuration existante.

J'ai ensuite intégré une VM de test au réseau interne virtuel pour valider le bon fonctionnement de la FireboxV. Cette VM a permis de tester l'accès sécurisé via le tunnel BOVPN que j'ai établi entre le site distant et le siège de 3S2i à Nice.

Enfin, la dernière phase du projet a concerné la virtualisation du serveur ERP. Après plusieurs tentatives infructueuses via l'outil StarWind, j'ai finalement utilisé Disk2VHD pour générer l'image du serveur et la transférer via un disque externe.

Ce projet, bien que complexe à certains moments, a été mené à terme avec succès, et pourra être réutilisé comme solution commercialisable pour d'autres clients.

Bilan humain

Mon stage chez 3S2I a été une expérience humaine très enrichissante. Il m'a permis de découvrir le fonctionnement concret d'une entreprise. Dès le début, j'ai été bien encadré et rapidement intégré à l'équipe, ce qui a facilité ma prise d'autonomie et ma compréhension des enjeux professionnels.

Ce stage m'a appris à mieux communiquer dans un cadre professionnel. Les échanges avec mon tuteur et mes collègues ont été très constructifs, ce qui m'a permis de poser des questions, de progresser techniquement, mais aussi d'exprimer mes idées et de les défendre avec assurance. J'ai également appris à m'adapter à un environnement de travail exigeant, où les priorités peuvent évoluer rapidement.

Ce développement de mes compétences humaines, en plus des compétences techniques acquises, a renforcé ma motivation à poursuivre dans le domaine des systèmes, réseaux et sécurité, en cherchant une alternance dès l'année prochaine.

Ce stage a marqué une étape importante dans mon parcours. Il m'a permis de confirmer mon projet professionnel tout en m'apportant des outils concrets pour réussir dans le monde du travail. Je remercie l'entreprise 3S2I pour leur confiance et accompagnement tout au long de cette période.

English Summary

I had the opportunity to complete a 10-week internship at 3S2I under the supervision of Mr. Sébastien TOUCHET. My main mission was to implement a virtual firewall in a Hyper-V environment hosted by Ikoula. The objective was to secure access between different sites through the creation of a BOVPN tunnel.

Firstly, I installed the Hyper-V role and created a virtual hard disk. Then, I configured the FireboxV virtual firewall to prepare the secure network environment.

Next, I deployed a test virtual machine and set up a BOVPN between the physical and virtual firewalls. I also built a test lab to simulate the ERP server environment.

Finally, I virtualized the ERP server and connected it to the BOVPN tunnel. This ensured secure communication while testing, without impacting the production server.

Throughout this internship, I gained valuable experience in both technical tasks and professional communication. I learned how to organize my work effectively, solve problems independently, and adapt to a fast-changing environment. These skills are essential for a future career in systems, networks, and security.

This internship was a valuable opportunity to apply the knowledge I gained at university in a real work environment. It helped me grow both technically and personally. I am grateful to all the team members at 3S2I, especially my tutor Mr. Sébastien Touchet, for their support and guidance throughout the experience. This internship gave me more confidence and motivation to continue my studies in a work-study program next year.

Glossaire

BOVPN (Branch Office VPN)

BOVPN est un tunnel VPN utilisé pour relier de manière sécurisée deux réseaux situés à distance (par exemple : deux sites d'une entreprise).

Commutateurs virtuels (Virtual Switches)

Les commutateurs virtuels permettent de connecter des machines virtuelles entre elles ou avec des réseaux physiques, à l'intérieur d'un environnement de virtualisation (comme Hyper-V).

Diffie-Hellman

C'est un protocole de cryptographie asymétrique permettant à deux parties d'échanger une clé secrète sur un canal non sécurisé. Il est souvent utilisé lors de l'établissement des connexions VPN.

ERP (Enterprise Resource Planning)

Un ERP est un logiciel qui centralise la gestion des processus d'une entreprise (ventes, stocks, comptabilité, etc.).


FireboxV

FireboxV est une appliance virtuelle de sécurité développée par WatchGuard, permettant de protéger les réseaux virtuels dans un environnement cloud ou virtualisé.

IKEv2 (Internet Key Exchange version 2)

IKEv2 est un protocole utilisé pour établir une connexion VPN sécurisée entre deux points. Il assure l'échange des clés et l'authentification entre les équipements.

NAT (Network Address Translation)

Mise en place d'un pare-feu virtuel 

Le NAT permet de faire correspondre plusieurs adresses IP privées à une adresse IP publique pour accéder à Internet.

NAS (Network Attached Storage)

Un NAS est un périphérique de stockage connecté au réseau, permettant à plusieurs utilisateurs d'accéder à des fichiers partagés.

SHA2-256-AES

SHA2-256 est un algorithme de hachage cryptographique assurant l'intégrité des données. Couplé avec AES (Advanced Encryption Standard), il est utilisé pour sécuriser les communications dans les tunnels VPN.

Trusted / External (interfaces réseau)

Dans une appliance WatchGuard, l'interface **Trusted** correspond au réseau interne sécurisé (LAN), tandis que **External** représente l'accès à Internet (WAN). Ces rôles sont essentiels pour définir les règles de sécurité dans un pare-feu.

VHD (Virtual Hard Disk)

VHD est un format de disque virtuel utilisé pour stocker le contenu d'un disque dur entier dans un seul fichier. Il est utilisé par Hyper-V ou VirtualBox pour créer des machines virtuelles.

VHDX

VHDX est la version améliorée du format VHD, introduite avec Hyper-V 2012. Il prend en charge de plus grandes tailles de disque, une meilleure protection contre la corruption, et de meilleures performances.

VM (Machine Virtuelle)

Abréviation de Virtual Machine. Une VM est un environnement logiciel qui émule un ordinateur physique. Elle permet d'exécuter un système d'exploitation et des applications comme si elles fonctionnaient sur un ordinateur indépendant.

Bibliographie

Recherches internet

Documentation interne

[Fiche technique - WatchGuard FireboxV | WatchGuard Technologies](#)

[Déployer FireboxV ou XTMv sur Hyper-V](#)

[Manual BOVPN Configuration Examples](#)

[Exporter et importer des machines virtuelles VMware ESXi 7.0 et 6.7 en OVF \(OVA\) - VMware - Tutoriels - InformatiWeb Pro](#)

[Installer Debian sur ESXI - Linux - Spiceworks Community](#)

[fonctionnalités Téléphonie Teams - Microsoft Teams | Microsoft Learn](#)

[Gérer et configurer des numéros Microsoft RTC - Training | Microsoft Learn](#)

Table des annexes

Annexe 1 : Autres projets : intégration de la téléphonie dans Microsoft Teams	50
Annexe 2 : Consignes de rapport de stage BUT2	54

Annexes

Autres projets : Intégration de la téléphonie dans Microsoft Teams

1. Contexte et objectif

Ce projet portera sur l'intégration de la téléphonie dans Microsoft Teams, en remplacement de la solution actuelle Rainbow d'Alcatel, utilisée en combinaison avec PimPhony. Cette nouvelle solution s'appuiera sur les services de Microsoft Teams Phone et l'environnement Microsoft 365, déjà en place au sein de 3S2I. Cette démarche s'inscrit dans une volonté de rationalisation des outils, d'amélioration de la qualité de service et de meilleure intégration avec notre écosystème Microsoft 365. La solution proposée par Adista permettra de moderniser notre téléphonie d'entreprise en la centralisant dans l'environnement Microsoft Teams, déjà largement adopté par nos équipes pour la collaboration et les réunions.

L'objectif sera de :

- Lever les contraintes de l'ancienne solution et définir clairement les nouveaux objectifs afin de les exposer aux prestataires.

2. Problématiques rencontrées avec la solution actuelle (rainbow + PimPhony)

La solution Rainbow, bien qu'opérationnelle, a montré de nombreuses limites techniques qui nuisent à l'efficacité des utilisateurs :

- Qualité sonore insatisfaisante, notamment avec des coupures et distorsions.
- Décalage vocal constaté lors de certaines communications.

- Fonctionnement instable sur mobile, rendant les appels peu fiables pour les collaborateurs en mobilité.
- Gestion complexe des licences et lignes internes via l'IPBX.
- Interruptions de service répétées, causant des indisponibilités critiques.
- Manque d'unification avec Microsoft Teams, obligeant à jongler entre plusieurs outils.
- Utilisation de PimPhony pour la gestion du standard : logiciel lourd, difficile à maintenir, se connectant à Rainbow.
- Fonctionnement de la CTI(couplage téléphonie-informatique : consiste à connecter le système de téléphonie au système informatique de l'entreprise) aléatoire. La CTI permettant d'ouvrir la fiche client de notre ARTIS(logiciel métier) lors d'un appel entrant.

3. besoins fonctionnels pour la future solution teams téléphonie

La future solution devra répondre à un ensemble de besoins fonctionnels clés, pour garantir un fonctionnement fluide, fiable et parfaitement intégré à l'environnement de travail Microsoft :

- Conservation des numéros de lignes existants.
- Intégration native avec Microsoft Teams, pour centraliser tous les canaux de communication.
- Choix du numéro affiché par utilisateur :

Exemple : les techniciens utilisent le numéro vert 0806 140 141
La direction utilise leur mobile professionnel personnalisé.

- Affectation de lignes SDA individuelles, telles que la ligne directe 04 93 14 29 02 pour le service comptabilité.

- Gestion centralisée du standard téléphonique :

 - Diffusion de musiques d'attente

 - Paramétrage des plages horaires d'ouverture/fermeture

 - Possibilité de déporter le standard sur un PC portable

- Fiabilisation de la CTI avec ARTIS : affichage automatique de la fiche client lors des appels entrants.

Annexe 1 : Autres projets : intégration de la téléphonie dans Microsoft Teams

Consignes de rapport de stage BUT2

Le rapport d'environ une trentaine de pages (hors annexes) fait état d'une mission ou d'un sujet réalisé durant votre période de stage/alternance. Si vous avez plusieurs sujets et que vous avez du mal à choisir, demandez conseil à votre tuteur IUT. Ce rapport doit être accompagné d'illustrations et de schémas explicatifs (toujours numérotés, intitulés et référencés en bas de page), il doit être aussi écrit dans un français correct et sans faute d'orthographe car il sera le plus souvent votre carte de visite dans vos recherches d'emploi à venir surtout si vous l'insérez à votre portfolio. Veillez donc à soigner ce travail, à bien lier vos idées en faisant des transitions et à suivre les consignes suivantes.

Le rapport comporte une couverture, des remerciements, un sommaire, une table des figures, une introduction, un développement, une conclusion, un bilan humain, un résumé anglais, un glossaire, une bibliographie, des annexes éventuellement et une quatrième de couverture.

La couverture : elle doit être agréable et illustrée. Vous devez y faire figurer votre appartenance universitaire, l'année, le nom de votre maître de stage, l'entreprise, le titre de votre rapport. (Pour les sujets longs, il faut les synthétiser).

Les remerciements : vous devez remercier par ordre hiérarchique : votre maître de stage et l'entreprise ou le service qui vous a accueilli. Si d'autres personnes vous ont aidé durant votre stage (un collègue d'un autre service, votre tuteur), elles doivent y figurer.

Le sommaire : il doit être clair, facilement lisible et paginé de façon exacte. Vous devez y faire figurer tous les éléments de votre rapport y compris les annexes quand il y en a. Vous devez utiliser la fonction du sommaire automatique.

La table des figures : nommez, numérotez la figure puis indiquez la page où se trouve cette dernière.

L'introduction : il faut tout d'abord justifier votre stage/alternance et votre sujet. Puis vous devez définir de façon rapide et vulgarisée les termes du sujet, poser une problématique (pourquoi, comment) et annoncer le plan. Pour que votre introduction soit efficace et donne envie à un lecteur de poursuivre, il faut qu'elle soit claire et concise.

Le développement : le plus souvent il est composé de la manière suivante :

1° partie : vous exposez l'environnement de travail puis le service dans lequel vous avez travaillé, **les besoins qui ont amené une entreprise à vous recruter** et votre sujet. Il est impératif d'exposer **les besoins** de l'entreprise car ce sont eux qui donnent un sens à votre travail et qui aident le lecteur à comprendre l'intérêt de votre sujet. Pour y parvenir, partez de l'existant de l'entreprise, faites-en un audit ou une présentation rapide et donnez ensuite **les objectifs à atteindre**. **Un schéma est alors nécessaire**. Expliquez ensuite votre cahier des charges, les outils à votre disposition et terminez par la procédure de travail, le planning (diagramme de GANTT) c'est-à-dire les étapes de ce dernier ce qui vous servira de structure pour votre seconde partie.

2° partie : vous développez votre procédure de travail, énoncée dans la partie précédente. Evitez les développements trop théoriques qui sont copiés collés ou plaqués, sauf si votre maître de stage/d'alternance vous a demandé d'étudier tel langage ou tel type de matériel par exemple. En revanche **aucun copié collé n'est toléré**. Vous pouvez toutefois citer un document en mettant l'extrait entre guillemets et en en donnant la source dans une note de bas de page. Il est demandé de noter dans cette partie ou ces parties ce que vous avez personnellement fait durant votre travail comme par exemple l'analyse de l'existant, les améliorations apportées, la démarche, le matériel installé... Toutefois il faut que vous justifiiez ce que vous faites, ce que vous avez choisi, que vous vulgarisiez vos explications.

Votre travail sera lu certes par quelqu'un de la spécialité mais aussi par un lecteur non averti.

Pensez à faire des schémas. Attention il faut toujours les intituler et les commenter. Un schéma non commenté reste incompréhensible. De plus il faut l'intégrer à votre texte en faisant des renvois de termes extraits de ce même schéma. Pensez à justifier sa présence. Pourquoi à ce moment de votre démonstration faites-vous ce schéma ? Une succession de captures écran non commentées reste indigeste et signe d'un remplissage qui sera peu apprécié du jury. Si vous avez fait des annexes, pensez à faire des renvois au sein de votre texte afin d'informer le lecteur de leur présence en fin de rapport. Un schéma récapitulatif est aussi toujours le bienvenu. Vous pouvez le mettre pour résumer par exemple des solutions que vous avez initialement comparées.

3° partie : au terme de votre travail, vous devez donner les résultats de votre stage/alternance. Où en êtes-vous techniquement ? Pour cela utilisez le schéma des objectifs de la première partie et comparez-le à un schéma final. Avez-vous rempli la tâche à 100%, oui, non ? Pourquoi ? Avez-vous rencontré des difficultés ? Avez-vous tout finalisé ou y a-t-il des prolongements ? Qu'avez-vous techniquement appris ?

Si vous devez faire des tests, expliquez ce que vous attendez comme résultats et pourquoi ? S'il y a des différences, expliquez pourquoi ?

La conclusion : elle est le résumé rapide de ce qui figure dans votre rapport. Elle doit permettre à un lecteur pressé de savoir ce que contient votre texte. Surtout elle doit répondre à la problématique de départ placée dans l'introduction. Comme il y a trois parties dans votre rapport, la conclusion se compose de trois paragraphes.

Le bilan humain : vous présentez ce que le stage /l'alternance vous a humainement apporté, sur le plan de l'insertion, de la communication, de la différence avec le monde universitaire par exemple...

Le résumé anglais : suivre les consignes données par le professeur de la spécialité.

Le glossaire : présentez-le par ordre alphabétique et définissez les termes techniques.

La bibliographie : elle est la liste des documents qui vous ont servi à composer votre rapport. Faites-les tous figurer y compris ceux qui sont internes à l'entreprise. Votre rapport doit être le plus honnête possible.

Annexes : elles ne sont pas obligatoires. Pensez à faire une table des annexes. Elles sont là pour illustrer un élément de votre travail ou une partie de votre stage. Elles peuvent être des plans, des devis, des bons de commandes, des pages de programmation..., autant d'éléments qui doivent être référencés dans votre développement.

4° de couverture : pensez à rédiger un court texte avec 5 mots clés (à mettre en gras) afin que votre lecteur connaisse immédiatement l'intérêt technique de votre travail.

Annexe 2 : Consignes de rapport de stage BUT2

AU COURS DE MON STAGE AU SEIN DE L'ENTREPRISE 3S2i, J'AI EU COMME MISSION PRINCIPALE LA MISE EN PLACE D'UN **PARE-FEU VIRTUEL**. CE PROJET VISAIT À **SÉCURISER UN ENVIRONNEMENT VIRTUALISÉ HÉBERGÉ CHEZ UN FOURNISSEUR CLOUD**, EN REMPLAÇANT L'ANCIENNE ARCHITECTURE PHYSIQUE PAR UNE SOLUTION MODERNE, PLUS FLEXIBLE ET MIEUX ADAPTÉE AUX BESOINS DE CONNECTIVITÉ ET DE SÉCURITÉ ACTUELS.

